Nearrings and a Construction of Triply Factorized Groups

Dissertation
zur Erlangung des Grades
„Doktor
der Naturwissenschaften“
am Fachbereich Physik, Mathematik und Informatik
der Johannes Gutenberg-Universität
in Mainz

vorgelegt von

Peter Hubert
geboren am 27. Oktober 1972 in Wiesbaden

univer
sität
mainz

Mainz, im Juli 2005

Tag der mündlichen Prüfung: 25. Oktober 2005

Summary

In this thesis a connection between nearrings and triply factorized groups is investigated. 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 in the theory of factorized groups can be reduced to triply factorized groups (c.f. [2]).

Triply factorized groups are 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, $b \in R$. In a 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 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. If, on the other hand, $G = AM = BM = AB$ is a triply factorized group with abelian subgroups A, B, and M and $A \cap B = 1$, there exists always a radical ring, from which G can be obtained as above (Sysak [20], see also [2]).

To construct triply factorized groups $G = AM = BM = AB$ with non-abelian normal subgroup M, a method using nearrings is described. Nearrings are a generalisation of rings in the sense that the additive group of a nearring is not necessarily abelian and only one distributive law holds. If R is a nearring with identity element 1 and U is a subgroup of the additive group R^+ such that $U + 1$ is a subgroup of the group of units of R, then U is called a *construction subgroup* of R. For instance the Jacobson radical $\mathcal{J}(R)$ of any ring R is a construction subgroup of R. It is shown that $U + 1$ operates on a construction subgroup U, such that the semidirect product $(U + 1) \ltimes U$ is a group triply factorized by two subgroups A and B isomorphic to $U + 1$ and a normal subgroup isomorphic to U. Conversely, it is proved that *every* triply factorized group $G = AM = BM = AB$ with $A \cap B = 1$ can be obtained by a suitable nearring with this method. This generalises the above mentioned theorem of Sysak.

To know more about construction subgroups, the structure of nearrings is investigated in detail. Here local nearrings, i.e. nearrings in which the set of all elements which are not right invertible forms an additive group, play a special rôle. In these nearrings the group of non-invertible elements forms a construction subgroup. Given an arbitrary p-group N of finite exponent (p a prime), a technique to construct local nearrings with a construction subgroup that contains a subgroup isomorphic to N is developed.

Moreover, all triply factorized groups that can be constructed using a local nearring R of order p^3 (p a prime) are described depending on the structure of the additive group of R. These triply factorized groups have order p^4. There exist two different triply factorized groups of order p^4 for every prime p. But it turns out that for $p \geq 5$ there is only one triply factorized group that can be constructed by a local nearring R of order p^3, if the exponent of R^+ is p^2 and R^+ is not abelian.

Finally, all local nearrings R with dihedral group of units are classified. It turns out that these nearrings are finite and their order does not exceed 16. It is shown that if R is such a local nearring, then its additive group is a p-group for $p = 2$ or $p = 3$. This is done by showing that no group of order 32 can occur as the additive group of a local nearring with dihedral group of units. Some of the calculations in this classification were made with the computer algebra system GAP. The programs used here are described in detail in Appendix B.

Contents

Introduction **6**

Notation **10**

1. Triply factorized groups **15**

1.1. Factorized groups . . . 15

1.2. A connection between triply factorized groups and radical rings . . . 16

2. Nearrings **18**

2.1. Basics about nearrings . . . 18

2.2. Homomorphisms and modules . . . 22

2.2.1. Nearring homomorphisms . . . 22

2.2.2. Nearring modules . . . 23

2.3. Ideals and special subgroups . . . 24

2.3.1. Nearring and module ideals . . . 24

2.3.2. R-subgroups . . . 26

2.3.3. Generalised annihilators . . . 26

2.3.4. Properties of ideals and R-subgroups . . . 28

3. Constructing triply factorized groups **29**

3.1. Construction of triply factorized groups . . . 29

3.2. Triply factorized groups constructible by nearrings . . . 31

4. More on nearrings **36**

4.1. Radical theory . . . 36

4.1.1. Monogenic R-modules and modules of type ν . . . 36

4.1.2. Quasiregularity . . . 37

4.2. Nearfields . . . 40

4.3. Prime rings . . . 40

4.4. More on construction subgroups . . . 44

4.5. Subdirect sums and products . . . 47

5. Local nearrings 49

5.1. Definition and basic properties . . . 49

5.1.1. Definition of local nearrings . . . 49

5.1.2. Basic properties of local nearrings . . . 50

5.1.3. Properties of the additive group R^+ . . . 52

5.1.4. The structure of L_R . . . 54

5.1.5. Simple local nearrings . . . 59

5.2. The structure of local nearrings . . . 62

5.2.1. Prime rings of local nearrings . . . 62

5.2.2. The multiplicative group $R^\times$ . . . 64

5.2.3. The nearfield R/L_R . . . 66

5.3. Local nearrings with nilpotent L_R . . . 69

5.4. Subdirect products of local nearrings . . . 70

6. An example for a local nearring 75

6.1. Construction of a local nearring R . . . 75

6.2. The examination of the structure of R . . . 78

6.2.1. The additive group R^+ . . . 78

6.2.2. The multiplicative group $R^\times$ . . . 81

6.2.3. The operation of $L_R + 1$ on L_R . . . 82

7. Triply factorized groups constructed by local nearrings of order p^3 84

7.1. Preliminary results . . . 84

7.2. The case R^+ cyclic . . . 85

7.3. The case R^+ elementary abelian . . . 86

7.4. The case R^+ abelian of exponent p^2 . . . 89

7.5. The case R^+ non-abelian of exponent p . . . 92

7.6. The case R^+ non-abelian of exponent p^2 . . . 98

8. Local nearrings with dihedral multiplicative group 106

8.1. General results . . . 106

8.2. Nearrings of odd order . . . 107

8.3. Nearrings of even order . . . 108

A. C++-Program used in Example 5.2.12 124

B. GAP-programs used in the proof of Theorem 8.3.11 139

Bibliography 145

Introduction

A group G is called *triply factorized* if $G = AM = BM = AB$ for two subgroups A and B and a normal subgroup M of G where $A \cap M = B \cap M = 1$, i.e. G is a semidirect product $A \ltimes M = B \ltimes M$ of A with M and of B with M. Many problems in the theory of factorized groups can be reduced to questions about triply factorized groups (c.f. Amberg, Franciosi, de Giovanni [2]). Therefore it is desirable to obtain examples of such groups.

A ring R is called radical, if R is a group R° under the "circle operation" $a \circ b = ab + a + b$ for all a, $b \in R$, or equivalently, if R coincides with its Jacobson radical $\mathcal{J}(R)$. If R is a radical ring, the group R° operates on the additive group R^+, such that the semidirect product $R^\circ \ltimes R^+$ is triply factorized. This observation was first described by Sysak [20] (c.f. [2, Section 6.1]). If $G = A \ltimes M = B \ltimes M = AB$ is a triply factorized group constructed with this method, the normal subgroup M is isomorphic to the additive group of R and hence always is abelian (c.f. Construction 1.2.2).

Conversely, Sysak proved that if $G = A \ltimes M = B \ltimes M = AB$ is a triply factorized group with abelian subgroups A, B, and M and $A \cap B = 1$, there is always a commutative radical ring R such that G can be obtained via the above construction using R (c.f. Theorem 1.2.3 below).

For further investigations it is desirable to have also triply factorized groups G in which the normal subgroup M is not necessarily abelian. In the following, nearrings will be used to find such groups.

Nearrings are a generalisation of rings in the sense that addition in nearrings need not be commutative and only one distributive law holds (c.f. Definition 2.1.1). In Chapter 2 some relevant facts about nearrings are collected, most of which are well-known and can be found for example in Meldrum [17], Pilz [18], or Clay [7].

In Chapter 3 a construction of triply factorized groups using nearrings is developed. For this, the notion of a *construction subgroup* is needed (c.f. Definition 3.1.1). This is a subgroup of the additive group of a nearring, which is connected in a natural way with some subgroup of the group of units of the given nearring. The following is proved.

Theorem (c.f. Construction 3.1.4)
If R is a nearring and U is a construction subgroup of R, then the set $U + 1 = \{u + 1 \mid u \in U\}$ is a subgroup of the group $R^\times$ of units of R, which operates on U. Then the semidirect product $G = G(R, U) = (U + 1) \ltimes U$ is a triply factorized group

$G = A \ltimes M = B \ltimes M = AB$, where $M = U$, $A = U + 1$, and $B = \{(u + 1, u) \mid u \in U\}$ is the "diagonal subgroup" of $G(R, U)$.

Note that here the normal subgroup M need not be abelian. If R is a ring with identity element, then $\mathcal{J}(R)$ is a construction subgroup of R and this construction is identical to that described in Construction 1.2.2.

In Section 3.2 it is shown that the above mentioned Theorem 1.2.3 holds for triply factorized groups in general. If M is a not necessarily abelian group, the set $M(M)$ of all mappings of M in M forms a nearring under pointwise addition and multiplication by composition. The following generalises Sysak's theorem.

Theorem 3.2.5.
If $G = A \ltimes M = B \ltimes M = AB$ is any triply factorized group with $A \cap B = 1$, then the nearring $M(M)$ contains a construction subgroup U with $G \cong G(R, U) = (U + 1) \ltimes U$. Thus every such triply factorized group can be obtained from a nearring.

For further investigations of construction subgroups, in Chapter 4 the structure of nearrings is studied in more detail. It is well-known that the Jacobson radical for rings can be described in several different ways, which lead to different radicals for nearrings. It turns out that a construction subgroup of a nearring under certain finiteness conditions is contained in one of these generalisations of the Jacobson radical (c.f. Proposition 4.4.1).

Much work has also been done to generalise quasiregularity from rings to nearrings. Beidleman [6] describes a generalisation of quasiregularity, which is very similar to that in ring theory. Meldrum [17] uses a more general definition, which includes Beidleman's concept. Both notions are described in Section 4.1.2, since some results only hold for the more restrictive definition of Beidleman [6].

A short section of Chapter 4 deals with nearfields, since they are needed to describe the structure of local nearrings in Chapter 5.

In Section 4.3, the *prime ring* of a nearring R is introduced. A prime ring is defined to be the subnearring of R generated by its identity element. The structure of the prime ring of a nearring R gives some information about the whole nearring R. For instance, it is very easy to show that there exists up to isomorphism exactly one nearring with identity element over a finite cyclic additive group. It is shown that prime rings are always isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some positive integer n or to a certain subring of $\mathbb{Q}$ (c.f. Lemmas 4.3.3 and 4.3.4). In Theorem 4.3.7 the construction subgroups of a prime ring are described.

A nearring R is called *local*, if the set L_R of all elements of R, which are not right invertible, forms a subgroup of the additive group R^+. These nearrings are especially useful for the construction of triply factorized groups, since in a local nearring R the set L_R is a construction subgroup. Local nearrings were first investigated by Maxson [16]. Their structure is described in Chapter 5.

It still seems to be unknown if the group L_R is always an ideal of the local nearring R, although this holds in many cases. It is shown that if a local nearring R exists, in which

L_R is not an ideal, then there also exists a simple local nearring, i.e. a local nearring which does not have any ideals other than the trivial ones. Simple local nearrings are studied in Section 5.1.5.

In Section 5.2.1 the prime rings of local nearrings are investigated. It turns out that the prime ring of a local nearring is local as well. If L_R is a normal subgroup of the additive group of a local nearring R, the additive group $L_R + P_R$ is also a local nearring, where P_R is the prime ring of R. For the construction of triply factorized groups this nearring is sufficient, since it contains the construction subgroup L_R and the identity element of R.

The nearfield R/L_R for a local nearring R is examined in Section 5.2.3. It is shown that for every skewfield K there is a local nearring R which is not a ring, such that R/L_R is isomorphic to K. Moreover, in Example 5.2.12 a local nearring R is given, in which the nearfield R/L_R is not a skewfield. This example was constructed using a C++-program which calculates the whole multiplication table of the nearring starting with a few predefined products. This program also checks that the calculated multiplication indeed leads to a local nearring. The program is explained in detail in Appendix A.

If R is a zero-symmetric local nearring satisfying certain finiteness conditions, the subgroup L_R is a nilpotent nearring. The structure of a local nearring R with nilpotent L_R is investigated in Section 5.3. These results are used in Chapter 8 for the classification of local nearrings with dihedral groups of units. For these investigations the annihilator series of a local nearring is introduced (c.f. Definition 5.3.1), which leads to the following criterion for L_R to be nilpotent.

Theorem 5.3.4.
If R is a local nearring, then the R-subgroup L_R is nilpotent if and only if R possesses an annihilator series.

It is well-known that the additive group of a finite local nearring is always a p-group for a prime p (c.f. Maxson [16]). Therefore using finite local nearrings only triply factorized p-groups can be constructed. In order to obtain more general triply factorized groups, in Section 5.4 subdirect products of local nearrings are studied. It is shown in Corollary 5.4.2 that a subdirect product of local nearrings is in fact a direct product of suitable local nearrings under certain finiteness conditions. These direct products can be used to obtain nearrings which are not local, but contain construction subgroups which need not be p-groups.

The construction subgroups L_R of most of the examples of local nearrings that can be found in literature are abelian. To obtain also examples of local nearrings R, in which the construction subgroup L_R is not abelian, a method for constructing local nearrings with non-abelian construction subgroup L_R is described in Chapter 6. The following is proved.

Theorem 6.1.5.
Given an arbitrary p-group N of finite exponent, where p is a prime number, there exists always a local nearring R such that N is isomorphic to a subgroup of L_R.

In Section 6.2 the additive and the multiplicative structure of the nearring in Theorem 6.1.5 is investigated. Also the operation of $L_R + 1$ on L_R is described, which is important to know the structure of the resulting triply factorized groups.

All triply factorized groups constructible by using local nearrings of order p^3 for a prime number p are presented in Chapter 7. It is well-known that for every prime p there exist exactly 5 non-isomorphic groups of order p^3. These are treated separately, where the case $p = 2$ requires a special consideration. It is clear that the triply factorized groups that can be constructed by local nearrings of order p^3 must have order p^4. Moreover, there are two different triply factorized groups of order p^4 for every prime p. It is surprising that if the additive group R^+ is non-abelian of exponent p^2 there is no local nearring such that the triply factorized group obtained by R is a non-trivial semidirect product of the elementary abelian group of order p^2 with itself, if $p \geq 5$, whereas for $p = 3$ there is such a local nearring whose additive group is non-abelian of exponent 9 (c.f. Theorem 7.6.2).

In Chapter 8 all local nearrings with dihedral group of units are classified. It is shown that the additive group of such a local nearring is always a finite p-group for $p = 2$ or $p = 3$. Moreover, the order of R does not exceed 9, if R^+ is a 3-group. The structure of a local nearring with dihedral multiplicative group is rather restricted, as the following result shows.

Theorem 8.3.11.
There is no local nearring with dihedral multiplicative group, whose order is larger than 16.

This is proved by considering the structure of all groups of order 32. It is shown that none of these groups can occur as the additive group of a local nearring with dihedral multiplicative group. Some of the calculations in the proof of Theorem 8.3.11 were done using the computer algebra system GAP [9]. This system contains a large library of “small” groups and their automorphism groups. The programs used in the proof of this theorem are described in detail in Appendix B.

Notation

General notation

Symbol	Description
$\varnothing$	The empty set
$\mathbb{N}$	Set of positive integers $\{1, 2, 3, \ldots\}$
$\mathbb{N}_0$	Set of non-negative integers ($\mathbb{N} \cup \{0\}$)
$\mathbb{Z}$	Ring of integers
$\mathbb{Z}/n\mathbb{Z}$	Ring of integers modulo n
$\mathbb{Q}$	Field of rational numbers
$\mathbb{Q}_p$	Ring of rationals whose denominator is not divisible by the prime p
$\mathbb{F}_q$	Field of order q (q a prime power)
$(F)_n$	Ring of $n \times n$-matrices over the field F
C_n	Cyclic group of order n
E_{p^n}	Elementary abelian group of order p^n for a prime p; additive group of $\mathbb{F}_{p^n}$
Q_{2^n}	(Generalized) quaternion group of order 2^n
D_n	Dihedral group of order n
$GL(n, p)$	Group of automorphisms of E_{p^n}

Symbol	Description
$H \leq G$	H is a subgroup of the group G; H is a subnearring of the nearring G
$H < G$	H is a proper subgroup of the group G; H is a proper subnearring of the nearring G
$A \trianglelefteq B$	A is a normal subgroup of the group B; A is an ideal of the nearring B
$A \triangleleft B$	A is a proper normal subgroup of the group B; A is a proper ideal of the nearring B
$G \cong H$	G and H are isomorphic
$G \cong_R H$	G and H are isomorphic as R-modules
$\|M\|$	Cardinality of the set M
$\|G : U\|$	Index of the subgroup U in the group G
$\exp(G)$	Exponent of the group G
$o(g)$	Order of the group element g
$\mathbf{Z}(G)$	Centre of the group G
$\mathbf{C}_G(U)$	Centraliser of U in the group G
$\mathbf{N}_G(U)$	Normalizer of U in the group G
$\mathrm{Stab}_G(\Omega)$	Stabilizer of Ω in G
$\mathrm{End}(G)$	Semigroup of endomorphisms of G
$\mathrm{Aut}(G)$	Group of automorphisms of G
$\mathrm{Inn}(G)$	Group of inner automorphisms of G
$\langle A_i \mid i \in I\rangle$	Group generated by the subsets A_i of a group, $i \in I$
$\langle a_i \mid i \in I\rangle$	Group generated by the elements a_i of a group, $i \in I$

Symbol	**Description**
$[a, b]$	Commutator of the group elements a and b, i.e. $-a - b + a + b$ for additively written groups, $a^{-1}b^{-1}ab$ for multiplicatively written groups
$[A, B]$	$\langle [a, b] \mid a \in A,\, b \in B \rangle$
G'	Derived subgroup $[G, G]$ of the group G
$A \times B$	Direct product of the groups A and B; Cartesian product of the sets A and B
$R \oplus S$	Direct sum of the nearrings R and S
$A + B$	$\{a + b \mid a \in A,\, b \in B\}$ for subsets A and B of an additively written group
AB	$\{ab \mid a \in A,\, b \in B\}$ for subsets A and B of a semigroup
$A \ltimes M$, $M \rtimes A$	Semidirect product of the group A with the group M, where M is the normal subgroup
$\alpha : A \to B$	α is a mapping from A in B
$\alpha : a \mapsto b$	$a\alpha = b$
id_M	The identity mapping on the set M
$\alpha\|_U$	Restriction of the mapping $\alpha : M \to N$ to the subset U of M
$\mathrm{Ker}(\alpha)$	Kernel of the homomorphism α
$\mathrm{Im}(\alpha)$	Image of the mapping α
$\mathrm{Hom}(G, H)$	Set of all homomorphisms from G in H
X^n	Set of all products of n elements of the subset X of a nearring
$\mathcal{J}(R)$	The Jacobson radical of the ring R

Special notation

Symbol	Description	Definition	Page
$G(R)$	Triply factorized group constructed by the radical ring R	1.2.2	16
R^+	Additive group of the nearring R	2.1.1	18
$M(G)$	Nearring of mappings from the group G in G	2.1.4	19
$M_0(G)$	Nearring of zero-symmetric mappings of the group G	2.1.4	19
$M_c(G)$	Nearring of constant mappings of the group G	2.1.4	19
R_0	The zero-symmetric part of the nearring R	2.1.6.(a)	20
R_c	The constant part of the nearring R	2.1.6.(b)	20
$R^\times$	Group of units of the nearring R	2.1.6.(g)	20
$o^+(r)$	Additive order of the nearring element r	2.1.6.(h)	20
$o^\times(r)$	Multiplicative order of the unit r of a nearring	2.1.6.(h)	20
$\mathfrak{A}_R(X)$	Annihilator of X in R	2.2.4	23
G_R	G is an R-module	2.2.5	23
R_R	The regular R-module R	2.2.8	24
$I \trianglelefteq_\ell R$	I is a left ideal of the nearring R	2.3.1	24
$I \trianglelefteq_r R$	I is a right ideal of the nearring R	2.3.1	24
$U \leq_R G$	U is a submodule of the R-module G	2.3.1	24
$U \trianglelefteq_R G$	U is an R-ideal of the R-module G	2.3.1	24
$B \leq_\ell R$	B is a left R-subgroup of the nearring R	2.3.5	26
$B \leq_r R$	B is a right R-subgroup of the nearring R	2.3.5	26

Symbol	Description	Definition	Page
$(X : Y)$	$\{r \in R \mid \forall y \in Y : yr \in X\}$ for a nearring R and non-empty subsets X and Y of an R-module G	2.3.8	26
$[X : Y]$	$\{g \in G \mid \forall y \in Y : gy \in X\}$ for a nearring R, a non-empty subset X of an R-module G, and a non-empty subset Y of R	2.3.8	26
$\mathfrak{C}_Y(X)$	$\{y \in Y \mid Xy \subseteq R_c\}$ for a nearring R and non-empty subsets X and Y of R	2.3.11	27
$G(R, U, N)$	Triply factorized group constructed by the construction subgroup U of the nearring R and the normal subgroup N of U	3.1.4	30
$G(R, U)$	Triply factorized group constructed by the construction subgroup U of the nearring R	3.1.4	30
$\mathcal{J}_\nu(R)$	Intersection of all annihilators of R-modules of type ν for a nearring R; the ν-radical of R	4.1.5	37
P_R	The prime ring of the nearring R	4.3.1	41

Chapter 1.

Triply factorized groups

1.1. Factorized groups

In the theory of factorized groups, triply factorized groups play an important rôle. Many problems concerning factorized groups can be reduced to triply factorized groups.

1.1.1 Definition (c.f. Amberg, de Giovanni, Franciosi [2])
A group G 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. On the other hand, a subgroup S of G need not be factorized by a subgroup of A and a subgroup of B.

1.1.2 Example
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 of A and a subgroup of B.

A subgroup S of a factorized group $G = AB$ is called *factorized*, if $S = (A \cap S)(B \cap S)$ and $A \cap B \subseteq S$ (c.f. [2]). It can easily be shown that the intersection of arbitrarily many factorized subgroups of G is factorized (c.f. [2, Lemma 1.1.2]). Thus, the intersection $X(S)$ of all factorized subgroups of G which contain the subgroup S of G is the smallest factorized subgroup of G containing S. $X(S)$ is called the *factorizer* of S. If N is a normal subgroup of G, the factorizer $X(N)$ has an interesting triple factorization.

1.1.3 Lemma (Amberg, de Giovanni, Franciosi [2, 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, $X(N) = (A \cap BN)N = (B \cap AN)N = (A \cap BN)(B \cap AN)$.

1.1.4 Example
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 $B \cap AS = \langle xy^3\rangle$.

Since the factorizer of a normal subgroup N of a factorized group G always has a triple factorization by Lemma 1.1.3, in order to obtain information on the structure of N, in many cases one has to consider groups with a triple factorization. If G is a group which has a triple factorization of the form $G = AB = AM = BM$ with subgroups A and B of G and an abelian normal subgroup M of G, then $C = (A \cap M)(B \cap M)$ is a normal subgroup of G. In this case,

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

1.1.5 Definition
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.

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. A connection between triply factorized groups and radical rings

If $G = A \ltimes M = B \ltimes M = AB$ is a triply factorized group with an abelian normal subgroup M, there is an interesting connection to radical rings in the sense of Jacobson [12].

1.2.1 Definition
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* $a \circ b = ab + a + b$ for all a, $b \in R$. Obviously, a radical ring does not contain an identity element.

The following construction, due to Ya. Sysak, is for instance described in [2].

1.2.2 Construction (Sysak [20])
Let R be a radical ring, embedded in an arbitrary way into the ring R_1 with identity element. Then the group R° is isomorphic to the subgroup $R + 1$ of the group of units of R_1.

Let U be a left ideal of R and $M = R/U$ as 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 $G = G(R) = A \ltimes M$,

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

is a complement of M with the property

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

i.e. G is a triply factorized group.

This construction raises the question, if 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 next theorem shows that this is the case, if A, B, and M are abelian and if $A \cap B = 1$.

1.2.3 Theorem (Sysak, in [2, Proposition 6.1.4])
If $G = A \ltimes M = B \ltimes M = AB$ is a triply factorized group with abelian subgroups A, B, and M, and with $A \cap B = \{1\}$, then there is a commutative radical ring R with $G \cong G(R)$.

In [4, Example 2.4] it is also shown that Theorem 1.2.3 need not be true, if A and B are nilpotent of class 2.

Since the group M in Construction 1.2.2 is the additive group of an R-module, it is always abelian. To obtain triply factorized groups $G = A \ltimes M = B \ltimes M = AB$ with a possibly nonabelian group M, one can use nearrings instead of rings.

Chapter 2.

Nearrings

2.1. Basics about nearrings

First some basic facts about nearrings are given. Most results in this chapter can be found in Meldrum [17], Pilz [18], and Clay [7].

2.1.1 Definition (c.f. Meldrum [17])

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

(N1) $(R, +)$ is a (not necessarily abelian) group with neutral element 0; $(R, +)$ often is written as R^+;

(N2) $(R, \cdot)$ is a semigroup, i.e. the multiplication is associative;

(N3) the left distributive law holds, i.e. $x \cdot (y + z) = x \cdot y + x \cdot z$ for all x, y, $z \in R$.

As usual, for $x \cdot y$ one often only writes 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 a *nearring with identity*. A nearring with $xy = 0$ for all x, $y \in R$ is called a *zero nearring*, and a nearring is called *constant nearring*, if $xy = y$ for all x, $y \in R$.

If instead of the axiom (N3) in R the axiom

(N3′) $(x + y) \cdot z = x \cdot z + y \cdot z$ for all x, y, $z \in R$.

holds, then R is called a *right nearring*. Right nearrings are used by some authors (e.g. Pilz [18]), and all results about left nearrings always have an analogue for right nearrings and vice versa.

2.1.2 Convention

Let R be a nearring, $r \in R$ and $n > 0$ a positive integer. Then for $\underbrace{r + \cdots + r}_{n \text{ times}}$ in the sequel will always be written rn and *never* nr. Analogously, for negative integers m, rm

will mean $-(r(-m))$. The reason for this are nearrings with identity. If integral factors are written on the right, they can be considered as multiples of the identity element.[1] Conversely, nr will mean $(1+\cdots+1)r$, 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 all $n \in \mathbb{Z}$, even if R does not have an identity element.

2.1.3 Remark

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 $1 \neq 0$.

2.1.4 Examples

(a) Let G be a (not necessarily abelian) additively written group with neutral element 0. Then
$$M(G) = \{\alpha : G \to G\},$$
the set of all mappings from G in G, is a left nearring under pointwise addition (i.e. $g(\alpha+\beta) = g\alpha + g\beta$) and composition of mappings ($g(\alpha\beta) = (g\alpha)\beta$)). (If one writes the mapping on the left of the element it operates on, then $M(G)$ becomes a right nearring.)

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

- $M_0(G) = \{\alpha : G \to G \mid 0\alpha = 0\}$
- $M_c(G) = \{\alpha : G \to G \mid \alpha = \text{const}\}$
- $M_c^0(G) = \big\{\alpha : G \to G \;\big|\; \alpha\,|_{G\setminus\{0\}} = \text{const and } 0\alpha = 0\big\}$

2.1.5 Remarks

As for rings, one can show that the following equalities hold in any nearring:

(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′) $0r = 0$

(b′) $(-r)s = -(rs)$.

The following definitions are very useful when dealing with nearrings. In particular, part (e) is important, since the terms *commutative* and *abelian* in the theory of nearrings have different meanings.

[1] In powers the exponent is also written on the right.

2.1.6 Definition

Let R be a nearring.

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

(b) $R_c = \{r \in R \mid 0r = r\} = \{r \in R \mid \forall x \in R: xr = r\}$ (c.f. Lemma 2.1.10) is called the *constant part* of R.

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

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

(e) R is called *commutative*, if $(R, \cdot)$ is commutative; R is called *abelian*, if $(R, +)$ is abelian.

(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, one often writes $R = (R, S)$.

(g) If R is a nearring with identity, the group of units of R is referred to by $R^\times$.

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

Weinert [23] deals with distributive nearrings. One important result of this article is that a distributive nearring with identity always is a ring.

2.1.7 Lemma (Weinert [23])

If $R = R_d$ is a distributive nearring, then

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

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

If one is familiar with rings, especially the constant part R_c appears unusual, since rings are always zero-symmetric nearrings. The following theorem gives an important description of the structure of the additive group of a nearring. Moreover, although a constant element r of a nearring R has the property that $sr = r$ for *all* $s \in R$, Lemma 2.1.10 shows that it is enough to consider $0r$, if one wants to check if r is contained in R_c or not.

2.1.8 Theorem (Meldrum [17, Theorem 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 $0r \in R_c$.

2.1.9 Corollary

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

2.1.10 Lemma (Meldrum [17, Lemma 1.12])

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 is of special interest. In this context it is useful to know that the multiplicative inverse of a zero-symmetric element is zero-symmetric as well. Moreover, the subsequent 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 $R_c + 1$.

2.1.11 Proposition

Let R be a nearring with identity 1 and $r \in R^\times \cap R_0$. 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 2.1.10, and thus both must be 0. Hence, $0r^{-1} = 0$ and $r^{-1} \in R_0$. □

2.1.12 Lemma (c.f. [3, Lemma 2.5])

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

Proof. It is not difficult to see that the mapping $\sigma : {R_c}^+ \to (R_c + 1)^\times$, $x \mapsto -x + 1$, is a group isomorphism. Moreover, if $r \in R^\times$, by Theorem 2.1.8 there are elements $c \in R_c$ and $z \in R_0$ such that $r = c + z = z(c + 1)$. Since $R_0 \cap R_c = \{0\}$ and $1 \in R_0$, it is clear that ${R_0}^\times \cap (R_c + 1) = \{1\}$. □

For the construction of triply factorized groups using nearrings, the operation of the group of units on the additive group is important. For the investigation of the structure of the constructed triply factorized groups the following result is useful.

2.1.13 Proposition

Let R be a nearring with identity element 1. Then $R^\times$ is isomorphic to a subgroup of $\mathrm{Aut}(R^+)$, i.e. $R^\times$ operates faithfully on R^+.

Proof. For $r \in R^\times$ consider the mapping $\sigma_r : R \to R$ with $x \mapsto rx$ for all $x \in R$. Since $(x + y)\sigma_r = r(x + y) = rx + ry = x\sigma_r + y\sigma_r$ for all x, $y \in R$, σ_r is an endomorphism of R^+. Obviously, σ_r is bijective, hence $\sigma_r \in \mathrm{Aut}(R^+)$. Since $\sigma_r\sigma_s = \sigma_{sr}$ for all r, $s \in R^\times$, the mapping $\sigma : R^\times \to \mathrm{Aut}(R^+)$ with $r \mapsto \sigma_{r^{-1}}$ for all $r \in R^\times$ 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 $r = 1$. This means that the kernel of σ is trivial and hence σ is a monomorphism. It follows that $R^\times$ is isomorphic to $\mathrm{Im}(\sigma)$. □

Given a nearring R with identity element 1, the additive order of units always is equal to the exponent of the additive group. In particular, a group which does not contain an element whose order is equal to the exponent of the group cannot be the additive group of a nearring with identity.

2.1.14 Theorem

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, $o^+(xr) \mid o^+(r)$. □

2.1.15 Corollary

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

Proof. First let $\exp(R^+) < \infty$ and $r \in R^\times$. Then $o^+(r) \mid \exp(R^+) = n$. Now 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 $\exp(R^+) = \infty$, since if $o^+(r) = n < \infty$ for some $r \in R^\times$, for all $s \in R$ would hold $s \cdot o^+(r) = 0$. □

2.2. Homomorphisms and modules

2.2.1. Nearring homomorphisms

Homomorphisms are a well-known and useful tool for the investigation of any kind of algebraic structures. As known from rings or groups, nearring homomorphisms can be used to embed nearrings into other nearrings and in this way to achieve information about the structure of the nearrings under consideration.

2.2.1 Definition

Let R and S be nearrings, $\alpha : R \to S$ a group homomorphism from R^+ to S^+. The mapping α is called *nearring homomorphism*, if for all r, $r' \in R$ the following equation holds: $(rr')\alpha = (r\alpha)(r'\alpha)$. The terms *kernel*, *monomrophism*, *epimorphism*, *isomorphism*, *endomorphism*, and *automorphism* are defined as usual.

2.2.2 Remark
Let R be a nearring and $\alpha : R \to M(R^+)$ the mapping with $r(s\alpha) = rs$. It is easily checked, that α is a nearring homomorphism with $\mathrm{Ker}(\alpha) = \{r \in R \mid Rr = 0\}$. In particular, every nearring with $\mathrm{Ker}(\alpha) = \{0\}$ can be embedded into the nearring $M(R^+)$.

It is well-known that any ring R can be embedded into a ring R_1 with identity element, such that R is an ideal in R_1. For nearrings, this is not always possible, but the following theorem shows that it is at least possible to embed a given nearring into a nearring with identity as a subnearring.

2.2.3 Theorem (Clay [7, Theorem 1.3.27])
Every nearring can be embedded into a nearring with identity.

2.2.2. Nearring modules

In ring theory, the concept of modules is very important. For nearrings, a similar concept exists. Because of the lack of right distributivity, left and right modules lead to essentially different theories. For the construction of triply factorized groups only right modules are important, and thus in the following only right modules will be introduced. Of course, authors using right nearrings also use left modules.

2.2.4 Definition (R-modules)

(a) Let $(G, +)$ be a group and R a nearring. G is called a *(right) R-module*, if there is a nearring homomorphism $\theta : (R, +, \cdot) \to (M(G), +, \circ)$. Such a homomorphism is called *representation* of R. A representation θ of R is called *faithful*, if $\mathrm{Ker}(\theta) = \{0\}$.

(b) Let R be a nearring and G an R-module. For $Y \subseteq G$, the set

$$\mathfrak{A}_R(Y) = \{x \in R \mid Yx = 0\}$$

is called the *annihilator* of Y. If θ is a representation of R, then θ is faithful, if and only if $\mathfrak{A}_R(G) = \mathrm{Ker}(\theta) = \{0\}$.

Note that some authors (e.g. Pilz [18]) use the term “R-group” instead of “R-module”.

2.2.5 Remark
Often one finds a definition of R-modules, which is equivalent to Definition 2.2.4: Let $(G, +)$ be a group with neutral element 0 and R a nearring. Let $\mu : G \times R \to G$, $(g, r) \mapsto gr$. Then, (G, μ) is called *R-module*, if for all $g \in G$, r, $s \in R$:

(M1) $g(r + s) = gr + gs$, and

(M2) $g(rs) = (gr)s$.

If there is no danger of confusion, one often writes G instead of (G, μ). Some authors also use the notation G_R (or ${}_RG$, if they are using right nearrings).

The following definition is very useful if one deals with nearrings with identity.

2.2.6 Definition
Let R be a nearring with identity, G an R-module. If $g1 = g$ for all $g \in G$, then G is called *unital*.

Also for nearring modules homomorphisms are defined in the usual way.

2.2.7 Definition
Let R be a nearring, G and H R-modules. Let $\tau : G \to H$ be a group homomorphism from G^+ to H^+. Then τ is called *R-module homomorphism* or short *R-homomorphism*, if $(gr)\tau = (g\tau)r$ for all $g \in G$ and all $r \in R$. The terms *kernel*, *R-monomrophism*, *R-epimorphism*, *R-isomorphism*, *R-endomorphism*, and *R-automorphism* are defined as usual.

2.2.8 Remarks

(a) Let R be a nearring. Then R is an R-module, which is called the *regular R-module*, and is often denoted by R_R.

(b) Let G be a group. Then G is an $M(G)$-module in the obvious way.

(c) The following statements are very easy to check:

  (i) $g0_R = 0_G$ for all $g \in G$.

  (ii) $g(-r) = -(gr)$ for all $g \in G$ and all $r \in R$.

  (iii) $0_G r = 0_G$ for all $r \in R_0$.

  (iv) $gr = 0_G r$ for all $g \in G$ and $r \in R_c$.

2.3. Ideals and special subgroups

2.3.1. Nearring and module ideals

In ring theory ideals of rings play an important rôle. Note that ideals, as for rings, in the theory of nearrings are defined as the kernels of homomorphisms, but the criterion for a subgroup of the additive group of a nearring does not look as simple as in ring theory. In particular, since the additive group of a nearring need not be abelian, ideals have to be normal subgroups of the additive group. It is also a very important difference between rings and nearrings that one has to distinguish between module ideals and submodules. While module ideals are the kernels of module homomorphisms, submodules are subsets of modules which are modules themselves under the module operations.

2.3.1 Definition (Ideals and submodules)
Let R be a nearring and G an R-module.

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

  (i) $RI \subseteq I$

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

  If I only has property (i), it is called *left ideal* (denoted $I \trianglelefteq_\ell R$); if I only has 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 $g \in G$, all $n \in N$, and 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 $U \leq G^+$ is called *R-submodule* of G (denoted $U \leq_R G$), if $UR \subseteq U$.

Factor nearrings and *factor modules* are defined in the usual way. It is easy to check, that ideals (R-ideals) are exactly the kernels of nearring homomorphisms (R-homomorphisms). Note that for an R-module M the factor module M/N is only defined for R-ideals N, not for R-submodules N.

A nearring is called *simple*, if R and $\{0\}$ are the only ideals in R. An R-module is called *simple*, if it has no non-trivial R-ideals (c.f. Pilz [18]).

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 ideals, right ideals, and R-ideals are defined analogously.

2.3.2 Example

Let R be a nearring. Then the zero-symmetric part R_0 is a right ideal of R. By Theorem 2.1.8, ${R_0}^+ \trianglelefteq R^+$, thus it suffices 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 $0((r+z)s - rs) = (0r + 0z)s - 0rs = 0rs - 0rs = 0$.

As known for rings, the sum of two nearring ideals again is an ideal. The subsequent theorem shows that the factor nearring R/I of a nearring R modulo an ideal I, as expected, is zero-symmetric if the constant part R_c is contained in the ideal I.

2.3.3 Lemma (Meldrum [17, Theorem 1.30])

(a) The group-theoretical sum of two right ideals again is a right ideal.

(b) The group-theoretical sum of two left ideals again is a left ideal.

(c) The group-theoretical sum of two ideals again is an ideal.

2.3.4 Theorem

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

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

2.3.2. R-subgroups

In ring theory, (left or right) ideals often are introduced as subgroups of the additive group of a ring, which are invariant under left or right multiplication (or both) with arbitrary ring elements. As stated above, for nearrings ideals are defined in a slightly different way. But also for nearrings R the R-invariant subgroups are important.

2.3.5 Definition
Let R be a nearring and $H \leq R^+$ a subgroup of the additive group R^+.

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

(b) H is called *right R-subgroup* of R (denoted $H \leq_r R$), 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, "R-subgroup" will always mean "right R-subgroup". R-subgroups are exactly the R-submodules of R_R. Maximal (left, right, two-sided) R-subgroups are defined in the usual way.

2.3.6 Example
Let R be a nearring. Then the constant part R_c is an (R, R)-subgroup of R, since for $r \in R$ and $c \in R_c$ one has $0rc = c = rc$ and $0cr = cr$. Thus, by Lemma 2.1.10, rc, $cr \in R_c$.

If one considers only zero-symmetric nearrings, it is a useful fact that in this case right ideals always are right R-subgroups. From this point of view, zero-symmetric nearrings are a bit closer to rings than general nearrings.

2.3.7 Lemma (Meldrum [17, 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 an (R, R)-subgroup of R.

2.3.3. Generalised annihilators

Annihilators are an important concept in ring theory. For nearrings and nearring modules, annihilators are introduced in a more general context. Here it is not necessary that certain products are zero, but only that they are contained in some given set.

2.3.8 Definition
Let R be a nearring and G an R-module. Let X and Y be non-empty subsets of G. Then one defines

$$(X : Y) = \{r \in R \mid \forall y \in Y : yr \in X\} .$$

For $\varnothing \neq X \subseteq G$ and $\varnothing \neq Y \subseteq R$ one defines

$$[X : Y] = \{g \in G \mid \forall y \in Y : \, gy \in X\} \, .$$

Note that $(X : Y)$ is a subset of R, while $[X : Y]$ is a subset of G. In most cases there is no danger of confusion, but if G is a submodule of the regular module R_R, it is important to distinguish these two cases.

Since these sets are more general than annihilators, one cannot expect that they are ideals in general. But depending on the special structure of the subsets X and Y of the R-module G, also structural facts about the sets $(X : Y)$ can be stated.

2.3.9 Theorem (Meldrum [17, Theorem 2.31])
Let R be a nearring and G an R-module, X, $Y \subseteq G$. Then the following statements hold.

(a) If $X^+ \leq G^+$, then $(X : Y)^+ \leq R^+$.

(b) If $X^+ \trianglelefteq G^+$, then $(X : Y)^+ \trianglelefteq R^+$.

(c) If $X \leq_R G$, then $(X : Y) \leq_r R$.

(d) If $X^+ \leq G^+$ and $YR \leq Y$, then $(X : Y) \leq_\ell R$.

(e) If $X \trianglelefteq_R G$, then $(X : Y) \trianglelefteq_r R$.

From this it follows that the annihilators of arbitrary subsets of R-modules always are right ideals of R, and the annihilators of submodules of an R-module are ideals of the nearring R.

2.3.10 Corollary (Meldrum [17, Corollary 2.32])
Let R be a nearring and Y a subset of the R-module G. Then $(0 : Y) = \mathfrak{A}_R(Y) \trianglelefteq_r R$ and $\mathfrak{A}_R(G) \trianglelefteq R$.

The following definition is useful for generalising results concerning nilpotency in zero-symmetric nearrings to general nearrings (c.f. Theorem 4.1.13).

2.3.11 Definition
Let R be a nearring and $\varnothing \neq X, Y \subseteq R$. Then define $\mathfrak{C}_Y(X) = \{y \in Y \mid Xy \subseteq R_c\}$. Then $\mathfrak{C}_R(X) = (R_c : X)$ and by Theorem 2.3.9, $\mathfrak{C}_R(X) \leq_r R$.

2.3.4. Properties of ideals and R-subgroups

As in ring theory, also nearrings with identity element always contain maximal ideals. Since all rings are nearrings, it is clear that also in the case of nearrings it is essential that the nearring under consideration contains an identity element.

2.3.12 Lemma

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

Proof. Let $\mathfrak{M} = \{K \trianglelefteq R \mid K \neq R, I \subseteq K\}$. Since $I \in \mathfrak{M}$, $\mathfrak{M} \neq \varnothing$, and $\mathfrak{M}$ is partially ordered by inclusion. Now let $\mathfrak{k}$ be a chain in $\mathfrak{M}$, and let $J = \bigcup\{K \mid K \in \mathfrak{k}\}$. Since R has an identity element, which is contained in no $K \in \mathfrak{k}$ because $K \neq R$ for all $K \in \mathfrak{M}$, one has $J \neq R$. Moreover, since $\mathfrak{k}$ is a chain, it is easy to check that $J \trianglelefteq R$. By Zorn's Lemma, $\mathfrak{M}$ contains a maximal element M. □

In a similar way one can show that a nearring R with identity always contains maximal left and right ideals.

Chapter 3.

Constructing triply factorized groups

3.1. Construction of triply factorized groups

It was shown Construction 1.2.2, how triply factorized groups can be constructed by using radical rings. This construction will now be generalised using nearrings. For this the following definition is needed.

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

If U is a construction subgroup of the nearring R, then $1 \notin U$, since otherwise $0 \in U+1$, which is not invertible. For the construction of triply factorized groups it is not only important that $U+1$ is a multiplicative group if U is a construction subgroup, but also that U is invariant under left multiplication with elements from $U+1$. The following result shows that this is always the case.

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

Proof. Let $A = U+1 \leq R^\times$. Since U is an additive group, for every a, $b \in A$ one has $a-b = a-1+1-b = (a-1)-(b-1) \in U$, 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, $a \in A$. □

3.1.3 Examples

(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 $R_c + 1 \leq R^\times$ by Lemma 2.1.12.

(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.

(e) A large class of nearrings containing less trivial construction subgroups than these examples are the local nearrings (c.f. Maxson [16]), which will be described in detail in Chapter 5.

Using construction subgroups it is possible to construct triply factorized groups in a very similar way as in Construction 1.2.2. In fact, it is not difficult to see that Construction 1.2.2 is a special case of the following construction.

3.1.4 Construction

Let R be a nearring with identity element, U a construction subgroup of R, and $N^+ \trianglelefteq U^+$ a normal subgroup of U^+ with $(U+1)\,N \subseteq N$. Let $M = U^+/N$ and $A = (U+1)^\times$. Then A operates on M via the rule

$$(u+N)^{(v+1)} = (v+1)^{-1}\,u + N$$

for all $u+N \in M$ and all $v+1 \in A$. Next, form the semidirect product $G = G(R,U,N) = A \ltimes M = \{(u+1, v+N) \mid u,v \in U\}$ and let

$$B = \left\{\left((u+1)^{-1}, u+N\right) \mid u \in U\right\}.$$

Then $G = A \ltimes M = B \ltimes M = AB$ is a triply factorized group. In the following, $G(R,U)$ will be written instead of $G(R,U,\{0\})$.

Proof. It is clear, that A operates on M^+ via the above rule.

(a) B is a group:

Let $\left((u+1)^{-1}, u+N\right), \left((w+1)^{-1}, w+N\right) \in B$. Then

$$\begin{aligned}
&\left((u+1)^{-1}, u+N\right)\left((w+1)^{-1}, w+N\right)\\
&= \left((u+1)^{-1}(w+1)^{-1}, u^{(w+1)^{-1}} + w + N\right)\\
&= \left(((w+1)(u+1))^{-1}, (w+1)\,u + w + N\right)\\
&= \left(((w+1)\,u + w + 1)^{-1}, (w+1)\,u + w + N\right) \in B
\end{aligned}$$

and $\left((u+1)^{-1}, u+N\right)^{-1} = \left(u+1, (u+1)^{-1} - 1 + N\right) \in B$, because $u+1 = \left((u+1)^{-1} - 1 + 1\right)^{-1}$ and

$$\begin{aligned}
&\left((u+1)^{-1}, u+N\right)\left(u+1, (u+1)^{-1} - 1 + N\right)\\
&= \left((u+1)^{-1}(u+1), (u+1)^{-1}u + (u+1)^{-1} - 1 + N\right)\\
&= \left(1, (u+1)^{-1}(u+1) - 1 + N\right)\\
&= (1, N)
\end{aligned}$$

(b) $G = B \ltimes M$:

(i) $B \cap M = \{(1, N)\}$:
Let $B \ni \left((u+1)^{-1}, u+N\right) \in M = \{(1, u+N) \mid u \in U\}$. Then $u+1 = 1$, and thus $u = 0$.

(ii) $G = BM$:
Let $g = (k+1, l+N) \in G$. Then one gets $g = bm$ with the elements $b = \left(k+1, (k+1)^{-1} - 1 + N\right) \in B$ and $m = \left(1, 1 + (k+1)^{-1} + l + N\right) \in M$.

(c) $G = AB$.
Let $g = (k+1, l+N) \in G$. If one chooses $a = ((k+1)(l+1), N) \in A$ and $b = \left((l+1)^{-1}, l+N\right) \in B$, one gets $ab = g$.

Thus $G = A \ltimes M = B \ltimes M = AB$ is triply factorized. □

3.1.5 Proposition
Let R be a nearring and U a construction subgroup of R. If the operation of $U+1$ on U is trivial, i.e. if $(u+1)v = v$ for all u, $v \in U$, then $U^+ \cong (U+1)^\times$.

Proof. Let $\alpha : U \to U+1$ with $u\alpha = -u+1$ for all $u \in U$. Clearly, α is a bijection, hence it suffices to show that α is a group homomorphism. Let u, $v \in U$. Then

$$\begin{aligned}(u\alpha)(v\alpha) &= (-u+1)(-v+1)\\ &= (-u+1)(-v) + (-u+1)\\ &= -v-u+1\\ &= -(u+v)+1\\ &= (u+v)\alpha.\end{aligned}$$ □

3.2. Triply factorized groups constructible by nearrings

In Theorem 1.2.3 it was shown that a triply factorized group $G = A \ltimes M = B \ltimes M = AB$ with $A \cap B = 1$ can always be constructed using a radical ring, if A, B, and M are abelian groups. Within nearring theory, one can even show that every triply factorized group with $A \cap B = 1$ and an arbitrary subgroup M can be obtained from a construction subgroup of $M(M)$ (c.f. Example 2.1.4).

Let $G = A \ltimes M = B \ltimes M = AB$ a triply factorized group with $A \cap B = 1$. In the following, the elements of G will be written as tuples (a, m) with $a \in A$ and $m \in M$. For A, B, and G the multiplicative notation will be used, while M will be written additively. Furthermore, let $\tilde{\pi} : G \to A$, $(a, m) \mapsto a$, be the canonical epimorphism from G onto A, and let $\pi = \tilde{\pi}|_B$. Finally, let $\tilde{\mu} : G \to M$, $(a, m) \mapsto m$ and $\mu = \tilde{\mu}|_B$. (Clearly, μ need not be a homomorphism in general.)

3.2.1 Lemma
(a) μ is a bijection between B and M.

(b) π is an isomorphism from B onto A.

Proof. (a) Let $b_i = (a_i, m) \in B$, $i = 1$, 2, with $b_1\mu = b_2\mu = m$. Then

$$\begin{aligned} b_1{b_2}^{-1} &= (a_1, m)\,(a_2, m)^{-1} \\ &= (a_1, m)\left({a_2}^{-1}, -m^{{a_2}^{-1}}\right) \\ &= \left(a_1{a_2}^{-1}, m^{{a_2}^{-1}} - m^{{a_2}^{-1}}\right) \\ &= \left(a_1{a_2}^{-1}, 0\right) \in A \cap B = \{1\} \end{aligned}$$

Hence $a_1 = a_2$, i.e. $b_1 = b_2$, and thus μ is injective.

Now let $m \in M$. Since $G = AB$, there is an $a \in A$ and a $b \in B$ with $m = ab$, i.e. $(1, m) = (a, 0)\,(b\pi, b\mu) = (a\,(b\pi)\,, b\mu)$. Thus $m = b\mu$ and hence μ is also surjective.

(b) Let $a \in A$. Since $G = B \ltimes M$, there are elements $b \in B$ and $m \in M$ with $a = bm$. Thus one has $a = a\tilde{\pi} = (bm)\,\tilde{\pi} = b\tilde{\pi}m\tilde{\pi} = b\tilde{\pi} = b\pi$, since $\mathrm{Ker}(\tilde{\pi}) = M$. Hence π is surjective.

Now let $b_i = (a, m_i) \in B$, $i = 1$, 2, with $b_1\pi = b_2\pi$. Then

$$\begin{aligned} b_1{b_2}^{-1} &= (a, m_1)\,(a, m_2)^{-1} \\ &= (a, m_1)\left(a^{-1}, -{m_2}^{a^{-1}}\right) \\ &= \left(aa^{-1}, m_1^{a^{-1}} - {m_2}^{a^{-1}}\right) \\ &= \left(1, (m_1 - m_2)^{a^{-1}}\right) \in B \cap M = 1. \end{aligned}$$

Hence $(m_1 - m_2)^{a^{-1}} = 0$, i.e. $m_1 = m_2$ and thus $b_1 = b_2$. This means that π is injective. □

Now let $\delta : A \to M$, $a \mapsto a\pi^{-1}\mu$, which is a bijection by Lemma 3.2.1.

3.2.2 Lemma
Let a, $b \in A$. Then $(ab)\,\delta = (a\delta)^b + b\delta$. In particular, $1\delta = 0$ and $(a^{-1})\,\delta = -\,(a\delta)^{a^{-1}}$.

Proof. Let a, $b \in A$ with $a\pi^{-1} = (a, m) \in B$, and $b\pi^{-1} = (b, n) \in B$. Then $a\delta = m$ and $b\delta = n$. But $ab = (a, m)\,(b, n) = \left(ab, m^b + n\right) \in B$, and hence $(ab)\,\delta = (ab)\,\pi^{-1}\mu = m^b + n = (a\delta)^b + b\delta$.

Moreover, $1\delta = (1 \cdot 1)\,\delta = (1\delta)^1 + 1\delta = 1\delta + 1\delta$, and thus $1\delta = 0$. Finally, $0 = 1\delta = (a \cdot a^{-1})\,\delta = (a\delta)^{a^{-1}} + (a^{-1})\,\delta$. It follows that $(a^{-1})\,\delta = -\,(a\delta)^{a^{-1}}$. □

Next let $\gamma : A \to M\,(M)$, $a \mapsto \gamma_a$ with $\gamma_a : M \to M$, $x \mapsto \left(a^{-1}\left(x\delta^{-1}\right)\right)\delta$.

3.2.3 Lemma

(a) $\gamma_1 = \mathrm{id}_M$, *where* id_M *is the identity mapping on* M*.*

(b) $\gamma_a\gamma_b = \gamma_{ab}$ *for all* a, $b \in A$*.*

(c) γ_a *is bijective for all* $a \in A$*.*

(d) γ *is a group monomorphism from* A *in* $M(M)^{\times}$*. In particular,* $A \cong \mathrm{Im}(\gamma)$*.*

Proof. (a) Let $x \in M$. Then $x\gamma_1 = \left(1^{-1} \cdot x\delta^{-1}\right)\delta = x$, and hence $\gamma_1 = \mathrm{id}_M$.

(b) Let $x \in M$. Then

$$\begin{aligned} x\gamma_a\gamma_b &= \left(a^{-1}\left(x\delta^{-1}\right)\right)\delta\gamma_b \ = \left(b^{-1}\left(a^{-1}\left(x\delta^{-1}\right)\right)\delta\delta^{-1}\right)\delta \\ &= \left(b^{-1}a^{-1}\left(x\delta^{-1}\right)\right)\delta = \left((ba)^{-1}\left(x\delta^{-1}\right)\right)\delta \\ &= x\gamma_{ab}. \end{aligned}$$

Thus $\gamma_a\gamma_b = \gamma_{ab}$.

(c) It follows immediately from (a) and (b) that $\gamma_{a^{-1}} = {\gamma_a}^{-1}$.

(d) That γ is a group homomorphism follows from (c) and (b). So let $a \in \mathrm{Ker}(\gamma)$, i.e. $\gamma_a = \mathrm{id}_M$. Then $0 = 0\gamma_a = \left(a^{-1}\left(0\delta^{-1}\right)\right)\delta = a^{-1}\delta$. Hence $a^{-1} = 0\delta^{-1} = 1$, that is $a = 1$. □

Since $0\gamma_a = a^{-1}\delta$, γ_a is uniquely determined by $0\gamma_a$, because of the bijectivity of γ. Let $V = \mathrm{Im}(\gamma)$ and $U = V - \mathrm{id}_M$. Then the following lemma holds.

3.2.4 Lemma

(a) U *is a group with respect to addition.*

(b) The mapping $\xi : M \to U$, $m \mapsto \gamma_{(m\delta^{-1})^{-1}} - \mathrm{id}_M$*, is a group isomorphism.*

(c) U *is a construction subgroup of* $M(M)$*.*

(d) ${\gamma_a}^{-1}(m\xi) = (m^a)\,\xi$ *for all* $a \in A$ *and all* $m \in M$*.*

Proof. (a) Let $\nu_i = \gamma_{a_i} - \mathrm{id}_M \in U$, $i = 1, 2$. It suffices to show that $\nu_1 - \nu_2 \in U$, i.e. $\nu_1 - \nu_2 + \mathrm{id}_M = \gamma_{a_1} - \mathrm{id}_M + \mathrm{id}_M - \gamma_{a_2} + \mathrm{id}_M = \gamma_{a_1} - \gamma_{a_2} + \mathrm{id}_M \in V$. Let $c = \left(\left({a_1}^{-1}\delta - {a_2}^{-1}\delta\right)\delta^{-1}\right)^{-1}$. Then, for all $x \in M$,

$$\begin{aligned}
x\left(\gamma_{a_1} - \gamma_{a_2} + \mathrm{id}_M\right) &= \left({a_1}^{-1}\left(x\delta^{-1}\right)\right)\delta - \left({a_2}^{-1}\left(x\delta^{-1}\right)\right)\delta + x \\
&= \left({a_1}^{-1}\delta\right)^{x\delta^{-1}} + x - x - \left({a_2}^{-1}\delta\right)^{x\delta^{-1}} + x \\
&= \left({a_1}^{-1}\delta\right)^{x\delta^{-1}} - \left({a_2}^{-1}\delta\right)^{x\delta^{-1}} + x \\
&= \left({a_1}^{-1}\delta - {a_2}^{-1}\delta\right)^{x\delta^{-1}} + x \\
&= \left(c^{-1}\delta\right)^{x\delta^{-1}} + x \\
&= \left(c^{-1}\left(x\delta^{-1}\right)\right)\delta \\
&= x\gamma_c
\end{aligned}$$

It follows that $\gamma_{a_1} - \gamma_{a_2} + \mathrm{id}_M = \gamma_c \in V$ and hence U^+ is a group.

(b) First $0\,(m\xi) = 0\gamma_{(m\delta^{-1})^{-1}} - \mathrm{id}_M = \left(m\delta^{-1}\left(0\delta^{-1}\right)\right)\delta = m$ for all $m \in M$, i.e. the mapping $m\xi$ is uniquely determined by $0(m\xi)$. Then $0(m\xi + n\xi) = m + n = 0((m+n)\xi)$, i.e. $(m+n)\xi = m\xi + n\xi$. Thus ξ is a group homomorphism. Since ξ is bijective (the mapping $\gamma_a - \mathrm{id}_M \mapsto \left(a^{-1}\right)\delta$ is an inverse of ξ), ξ is an isomorphism and hence $M \cong U^+$.

(c) By (a), U is an additive group. By construction of U, the set $U+1$ is a multiplicative group. Hence U is a construction subgroup of $M(M)$.

(d) Let $a \in A$ and $m \in M$. Then

$$\begin{aligned}
0\left({\gamma_a}^{-1}\left(m\xi\right)\right) &= 0\left(\gamma_{a^{-1}}\left(m\xi\right)\right) \\
&= \left(a\delta\right)\left(m\xi\right) \\
&= \left(a\delta\right)\left(\gamma_{(m\delta^{-1})^{-1}} - \mathrm{id}_M\right) \\
&= \left(m\delta^{-1}\left(a\delta\delta^{-1}\right)\right)\delta - a\delta \\
&= \left(m\delta^{-1}a\right)\delta - a\delta \\
&= \left(m\delta^{-1}\delta\right)^a + a\delta - a\delta \\
&= m^a = 0\left(m^a\xi\right),
\end{aligned}$$

and thus ${\gamma_a}^{-1}\left(m\xi\right) = m^a\xi$. □

By Construction 3.1.4, U leads to a triply factorized group $V \ltimes U$, which is isomorphic to G via the group isomorphism $\alpha : G \to V \ltimes U$, $(a, m) \mapsto (\gamma_a, m\xi)$.

Proof. Let $(a,m)\,,\,(b,n) \in G$. Then

$$\begin{aligned}
((a,m)\,(b,n))\,\alpha &= \big(ab, m^b + n\big)\,\alpha \\
&= \big(\gamma_{ab}, \big(m^b + n\big)\,\xi\big) \\
&= \big(\gamma_a\gamma_b, \big(m^b\big)\,\xi + n\xi\big) \\
&= \big(\gamma_a\gamma_b, {\gamma_b}^{-1}\,(m\xi) + n\xi\big) \\
&= (\gamma_a, m\xi)\,(\gamma_b, n\xi) \\
&= (a,m)\,\alpha \cdot (b,n)\,\alpha.
\end{aligned}$$

Moreover, α is bijective, since γ and ξ are. □

In summary it follows that the group G can be constructed from the construction subgroup $U \leq M(M)$. Thus the following theorem is proved.

3.2.5 Theorem

If $G = A \ltimes M = B \ltimes M = AB$ is a triply factorized group with $A \cap B = 1$, then the nearring $M(M)$ contains a construction subgroup U with $G \cong G(R,U)$.

Chapter 4.

More on nearrings

4.1. Radical theory

4.1.1. Monogenic R-modules and modules of type ν

In ring theory the Jacobson radical $\mathcal{J}(R)$ of a ring R plays an important rôle (c.f. e.g. Jacobson [12]). There are several different characterisations of the Jacobson radical in ring theory. Unfortunately, these characterisations lead to different concepts when generalised to nearrings. In the following, a few useful generalisations of the Jacobson radical for nearrings are introduced. These are closely connected to quasiregularity for nearrings, as the usual quasiregularity is connected to the Jacobson radical in ring theory. For these generalisations, first monogenic R-modules of type ν have to be defined.

4.1.1 Definition (Meldrum [17, Definition 3.1])
Let R be a nearring and let G be an R-module. G will be called *monogenic*, if there exists a $g \in G$ such that $gR = G$, i.e. $G = \{gr \mid r \in R\}$. An element $g \in G$ such that $G = gR$ is called a *generator* of G.

4.1.2 Proposition
If G is a monogenic R-module and R a nearring with identity, then $g1 = g$ for all $g \in G$, i.e. G is a unital module.

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 $g1 = (hr)1 = h(r1) = hr = g$. □

4.1.3 Definition (Meldrum [17, Definition 3.4])
Let G be a monogenic R-module. Then

- G is an R-module of *type 0*, if G is simple, i.e. it has no 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 no 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.

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

Proof. For every $g \in G$, the set gR is a submodule of G, since for r, $s \in R$ always $gr + gs = g(r + s) \in gR$ 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 is now possible to define the radicals $\mathcal{J}_\nu(R)$ for a zero-symmetric nearring R. Note that these three radicals coincide with the Jacobson radical of R if R is a ring.

4.1.5 Definition (Meldrum [17, Definition 5.4])
Let R be a nearring. For $\nu \in \{0, 1, 2\}$ the *ν-radical* $\mathcal{J}_\nu(R)$ is

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

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

4.1.6 Remark
For zero-symmetric nearrings R, Beidleman [6] defines the radical $\mathcal{J}(R)$ as the intersection of all right ideals of R which are maximal as R-subgroups. Using Lemma 4.1.4 it is easy to see that $\mathcal{J}(R) = \mathcal{J}_2(R)$.

4.1.2. Quasiregularity

The ring theoretical quasiregularity may also be generalised to nearrings. Because of the lack of the right distributive law, the definition of quasiregularity seems to be somewhat more complicated than in ring theory.

4.1.7 Definition (Meldrum [17, Definition 5.19])

(a) 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 $\{x - zx \mid x \in R\}$

(b) A subset X of R is called *quasiregular* if every element of X is right quasiregular.

4.1.8 Remark
If R is a zero-symmetric nearring with identity element 1, Beidleman [6] calls the element $z \in R$ right quasiregular, if there exists an element $r \in R$ such that $(1 - z)r = 1$. In this case, z is also right quasiregular in the sense of Meldrum [17].

Proof. Let z be right quasiregular in the sense of Beidleman [6], $r \in R$ with $(1-z)r = 1$, and let I be the right ideal of R 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 Lemma 2.3.7. Hence $z = 1 \cdot z = (1-z)rz \in I$. □

Note that the definitions of Beidleman [6] and Meldrum [17] are not equivalent, even for zero-symmetric nearrings with identity. An example for an element which is right quasiregular in the sense of Meldrum [17], but not in the sense of Beidleman [6] is given in a more general context below in Remark 4.4.4.

As for rings, one may define nil and nilpotent subsets for nearrings, as well as nilpotent elements. Nilpotent construction subgroups will be of special interest when local nearrings are investigated in Chapter 5.

4.1.9 Definition (Beidleman [6, Definition 6.1])
Let R be a nearring.

(a) An element $x \in R$ is called *nilpotent*, if there is a positive integer n such that $x^n = 0$.

(b) A subset $X \subseteq R$ is called *nil*, if all elements of X are nilpotent.

(c) A subset $X \subseteq R$ is called *nilpotent*, if there is a positive integer n such that

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

i.e. each product of n elements of X is zero. Clearly, every nilpotent subset of R is nil.

Although Meldrum [17] and Beidleman [6] only consider zero-symmetric nearrings, most statements about nilpotent elements and nil subsets also hold in general nearrings, since obviously nilpotent elements are always contained in the zero-symmetric part of a nearring.

The following lemma and the subsequent theorem are well-known in ring theory, but hold also for nearrings. Since Meldrum [17] only considers zero-symmetric nearrings, here the proof for the general case is given.

4.1.10 Lemma (see Meldrum [17, Lemma 5.20 and Corollary 5.21])
A nilpotent element of a nearring R is right quasiregular. In paricular, 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 theorems taken from Meldrum [17] hold for zero-symmetric nearrings.

4.1.11 Theorem (Meldrum [17, Theorem 5.23])
If B is a quasiregular R-subgroup of the zero-symmetric nearring R, then $B \subseteq \mathcal{J}_2(R)$.

4.1.12 Theorem (Meldrum [17, 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 generalised as follows.

4.1.13 Theorem
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 $H + 1 \subseteq R^\times$. 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

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

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 $K = H_n$ and show that $K = H \cap R_c$ – this is sufficient to show the theorem.

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 $K_2 = K$. Next 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 $K \neq H \cap R_c$, $K^2 \neq H \cap R_c$ and 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 $K^2 \subseteq \mathfrak{C}_R(m) \leq_r R$, and hence $\mathfrak{C}_R(m) \supseteq K_2 = K$ (c.f. Definition 2.3.11). 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 $xr - r \in \mathfrak{A}_R(m)$ for all $r \in R$. Since $H + 1 \subseteq R^\times$, $-x + 1 \in \mathfrak{A}_R(m) \cap R^\times$. It follows

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

But then $mk \in R_c$ for all $k \in K$ and thus $mK = H \cap R_c$, a contradiction. Hence $K = H \cap R_c$. □

4.2. Nearfields

Nearfields are an important class of nearrings. They first appear in Dickson [8]. For the construction of triply factorized groups, nearfields do not play a very important rôle, but they appear as factor nearrings of local nearrings, which will be described in detail in Chapter 5. An overview about the theory of nearrings can be found in Wähling [22].

4.2.1 Definition

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

4.2.2 Proposition (Pilz [18, Proposition 8.1])

If F is a nearfield then either $F \cong M_c(C_2)$ or F is a zero-symmetric nearring with identity.

4.2.3 Remark

Note that $F = M_c(C_2)$ is not a nearring with identity. Let ι be the neutral element of the group $F \setminus \{0\}$. Then ι is not an identity element of F, since $0\iota = \iota \neq 0$.

On the other hand, if F is a zero-symmetric nearring, then the neutral element 1 of $F \setminus \{0\}$ is an identity element. In the following only zero-symmetric nearfields will be considered.

As the next lemma and the subsequent theorem show, nearfields are much closer to rings than general nearrings.

4.2.4 Lemma (Wähling [22, Satz I.2.2])

Let F be a nearfield and x, $y \in F$. Then the following holds:

(a) $xy = 0$ *if and only if* $x = 0$ *or* $y = 0$.

(b) $x^2 = 1$ *if and only if* $x = 1$ *or* $x = -1$.

(c) $(-1)x = x(-1)$.

(d) $(-x)y = -xy = x(-y)$.

4.2.5 Theorem (Wähling [22, Satz I.2.3])

The additive group F^+ of a nearfield F is abelian.

4.3. Prime rings

The prime field of a field is the subfield generated by the identity element. For nearrings with identity, this concept may be generalised. One cannot expect that the subnearring generated by the identity element in general is a field, but it turns out that it is a commutative ring. In the following the subnearring generated by the identity element is less important than the nearring containing also the inverses of the invertible elements.

4.3.1 Definition

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

4.3.2 Lemma

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

Proof. Let n, $m \in E$, i.e. there are integers $\tilde{n}$, $\tilde{m}$ with $n = 1 \cdot \tilde{n}$ 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 $\tilde{m} < 0$, $nm = -(n(-m)) \in E_R$. 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 Lemma 2.1.7.

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, $y \in E_R \cap R^\times$. 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 Lemma 2.1.7. □

The following two lemmas describe the structure of E_R and P_R in detail. It turns out that the structure of these rings is not very complicated.

4.3.3 Lemma

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 $E_R = P_R$. □

4.3.4 Lemma

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 $D = \mathbb{Z} \setminus (\bigcup_{p \in \pi_R} p\mathbb{Z})$, i.e.

$$P_R \cong \left\{ \frac{n}{m} \in \mathbb{Q} \;\middle|\; \forall p \in \pi_R : p \nmid m \right\}.$$

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

Proof. If $o^+(1) = \infty$, it is clear that $E_R \cong \mathbb{Z}$. Now let $n \in \mathbb{Z}$ such that n is invertible in R. Then for every prime p with $p \mid n$, also p must be invertible in R. On the other hand, if n is not invertible, then there is a prime divisor p of n which is not invertible. But if p is a prime which is not invertible in R, then for every $z \in \mathbb{Z}$ the element pz is not invertible – hence $p\mathbb{Z} \cap R^\times = \varnothing$. Now let π_R be the set of all primes which are not invertible in R. Then all elements of $\bigcup_{p \in \pi_R} p\mathbb{Z}$ are not invertible, while all elements of $D = \mathbb{Z} \setminus (\bigcup_{p \in \pi_R} p\mathbb{Z})$ are invertible. An easy calculation shows that $P_R \cong \mathbb{Z}D^{-1}$, where $\mathbb{Z}D^{-1}$ is the ring of quotients over $\mathbb{Z}$ with set of denominators D. □

4.3.5 Definition

Let R be a nearring with identity 1. Then P_R is called the *prime ring* of R. Note that by Lemmas 4.3.3 and 4.3.4 P_R is always contained in R_0.

In the following, the construction subgroups of prime rings will be investigated. In particular, prime rings always contain a unique maximal construction subgroup. The following definition is needed for the description of construction subgroups of finite prime rings.

4.3.6 Definition

Let n be a positive integer with $n = \prod\limits_{i=1}^{k} p_i^{\alpha_i}$, where p_i are pairwise distinct primes, $\alpha_i > 0$, and $k \geq 0$. Then let $\kappa(n) = \prod\limits_{i=1}^{k} p_i$, the greatest square-free divisor of n. For negative integers let $\kappa(n) = \kappa(-n)$.

4.3.7 Theorem

Let R be a nearring with identity.

(a) If $o^+(1) = n < \infty$ then $U \leq {P_R}^+$ is a construction subgroup of P_R if and only if $U^+ = \langle k \rangle^+$ with $k \mid n$ and $\kappa(k) = \kappa(n)$.

(b) If $o^+(1) = \infty$ and π_R is the set of all prime numbers in E_R which are not invertible in R, then U is a construction subgroup of P_R if and only if there is an integer x with $p \mid x$ for all $p \in \pi_R$ and

$$U \cong \mathbb{Q}_x = \left\{ \frac{n}{m} \in \mathbb{Q} \;\middle|\; x \mid n,\, (x, m) = 1 \right\}.$$

In particular, if π_R is finite and $q = \prod\limits_{p \in \pi_R} p$, then $K = \mathbb{Q}_q = qP_R$ is the unique maximal construction subgroup of P_R. If π_R is infinite, there is no non-trivial construction subgroup of P_R.

Proof. (a) Let U be a construction subgroup of P_R. By Lemma 4.3.3, $P_R \cong \mathbb{Z}/n\mathbb{Z}$ and hence U^+ is generated by a divisor of n. First show that $(lk + 1,\, n) = 1$ for all $l \in \mathbb{Z}$ if and only if $\kappa(n) = \kappa(k)$.

To see this $\kappa(k) = \kappa(n)$, $l \in \mathbb{Z}$, and let $1 \neq t$ be an arbitrary divisor of n. Then $\kappa(t) \mid lk$ and hence $\kappa(t) \nmid lk + 1$. Thus $t \nmid lk - 1$ and since this holds for any divisor t of n, one has $(lk + 1, n) = 1$. An easy calculation shows that in this case $U + 1 \leq {P_R}^\times$.

On the other hand, if $k \mid n$ with $\kappa(k) \neq \kappa(n)$ then there is a prime p with $p \mid n$ and $p \nmid k$. Hence $(p, k) = 1$. Then there are elements x, $y \in \mathbb{Z}$ with $xp + yk = 1$, i.e. $xp = (-y)k + 1$. Thus $p \mid (-y)k + 1$ and $(-y)k + 1$ is not invertible in P_R.

(b) First let U be a construction subgroup of P_R, and let $\frac{a}{b} \in U$ with $(a,b) = 1$. Assume that there is an element $p \in \pi_R$ with $p \nmid a$. Then there exists an integer k with $ka \equiv -1 \pmod{p}$, and hence $p \mid ka+1$. Thus $ka + 1 \notin {P_R}^{\times}$. But this is a contradiction, since $\frac{a}{b} \in U$ and therefore $\frac{a}{b} \cdot kb = ka \in U$. Hence $p \mid a$ for all $p \in \pi_R$. Thus, if π_R is finite, $U \leq K$, and if π_R is infinite, a is divisible by an infinite number of primes and hence a must be zero, such that the trivial subgroup of ${P_R}^+$ is the only construction subgroup of P_R.

For the remainder of this proof let π_R be a finite set and let $q = \prod\limits_{p \in \pi_R} p$.

Now show that $\mathbb{Q}_x$ is a construction subgroup of P_R if $q \mid x$ (which is equivalent to the condition that $p \mid x$ for all $p \in \pi_R$). It is clear that $\mathbb{Q}_x$ is a subgroup of ${P_R}^+$. If $\frac{xa}{b}$, $\frac{xr}{s} \in \mathbb{Q}_x$ with $(xa,b) = (xr,s) = 1$, then $\frac{xa}{b} + 1 = \frac{xa+b}{b} \in {P_R}^{\times}$, since $p \nmid xa + b$ for all $p \in \pi_r$. Furthermore,

$$\begin{aligned} \left(\frac{xa}{b} + 1\right) \cdot \left(\frac{xr}{s} + 1\right)^{-1} &= \frac{xa+b}{b} \cdot \frac{s}{xr+s} \\ &= \frac{xas + bs}{xbr + bs} = \frac{xas - xbr}{xbr + bs} + 1 \in \mathbb{Q}_x + 1, \end{aligned}$$

since $x \mid xas - xbr$ and $(x, bs) = 1$. Hence, $\mathbb{Q}_x + 1$ is a group under multiplication and thus a construction subgroup of P_R.

Next let U be a construction subgroup of P_R. Then $U + 1$ is a multiplicative group. In particular, for every $x \in U$ also $1 - (x+1)^{-1}$ and $1 - (-x+1)^{-1}$ are contained in U. It will be shown by induction, that for every $n \in \mathbb{N}_0$ the elements $\frac{a}{b \pm na}$ lie in U, if $\frac{a}{b} \in U$. For $n = 0$ this is clear. Now assume that $\frac{a}{b \pm (n-1)a} \in U$ for some $n \in \mathbb{N}_0$. Then

$$\begin{aligned} \frac{a}{b+na} &= 1 - \left(1 + \frac{a}{b+(n-1)a}\right)^{-1} \in U \\ \text{and} \quad \frac{a}{b-na} &= 1 - \left(-\frac{a}{b-(n-1)a} + 1\right)^{-1} \in U. \end{aligned}$$

Since if $\frac{a}{b} \in U$ also $a \in U$, one has $\frac{a}{1+na} \in U$ for all $n \in \mathbb{Z}$. Now let $\frac{ar}{s} \in \mathbb{Q}_a$ with $(ar, s) = 1$. Then $s + a\mathbb{Z} \in (\mathbb{Z}/a\mathbb{Z})^{\times}$, such that there is an integer t with $st \equiv 1 \pmod{a}$, or, in other words, $st = 1 + na$ for a suitable $n \in \mathbb{Z}$. By what was shown above, $\frac{a}{st} = \frac{a}{1+na} \in U$, and hence $\frac{ar}{s} = \frac{a}{1+na} \cdot rt \in U$. Thus, $\mathbb{Q}_a \leq U$.

Finally, let $\mathrm{Num}(U) = \left\{a \in \mathbb{Z} \;\middle|\; \exists b \in \mathbb{Z} : (a,b) = 1 \wedge \frac{a}{b} \in U\right\}$ be the set of all numerators of the elements of U (clearly, $\mathrm{Num}(U) \neq \varnothing$). As shown above, $q \mid a$ and $\mathbb{Q}_a \leq U$ for all $a \in \mathrm{Num}(U)$. Let $\tilde{q}$ be the greatest common divisor of the elements of $\mathrm{Num}(U)$. (In the sequel, the greatest common divisor of the elements of the set $M \subseteq \mathbb{Z}$ will be denoted as $\gcd M$.) Then it has to be shown that $U = \mathbb{Q}_{\tilde{q}}$.

Clearly, $\mathrm{Num}(U) \subseteq U$, and there is a finite number of elements $a_i \in \mathrm{Num}(U)$, $1 \leq i \leq n$, with $\gcd\{a_i \mid 1 \leq i \leq n\} = \tilde{q}$. Hence, there are integers $z_1, \ldots, z_n$ with $\tilde{q} = \sum_{i=1}^{n} a_i z_i$, such that $\tilde{q} \in U$ and thus $\mathbb{Q}_{\tilde{q}} \leq U$. If on the other hand $\frac{a}{b} \in U$ with $(a, b) = 1$, then $a \in \mathrm{Num}(U)$, and hence $\tilde{q} \mid a$. Furthermore, $(\tilde{q}, b) = 1$, such that $\frac{a}{b} \in \mathbb{Q}_{\tilde{q}}$. Hence $U \leq \mathbb{Q}_{\tilde{q}}$ and thus $U = \mathbb{Q}_{\tilde{q}}$. □

4.4. More on construction subgroups

In the following, the structure of construction subgroups is investigated. In particular, for zero-symmetric nearrings some useful facts are given.

4.4.1 Proposition

Let R be a zero-symmetric nearring with identity. If U is a construction subgroup, then U is quasiregular. 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 2.3.7, and thus $I = R$. Hence $x \in I$ and so x is a right quasiregular element. The rest follows immediately from Theorem 4.1.11. □

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

4.4.2 Theorem

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

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

4.4.3 Lemma

Let R be a zero-symmetric nearring with identity, $K \trianglelefteq_r R$ a quasiregular right ideal of R in the sense of Beidleman [6] (c.f. Remark 4.1.8). 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 [6], for every $k \in K$ the element $1 - k$ is right invertible, and since K is a right ideal, one has $K + 1 = 1 + K$ and all elements of $K + 1$ have a right inverse.

Thus it suffices 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, $r \in R$ 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 leads to $1-(1+k)r+(1+k)r-r = 1-r \in K \Leftrightarrow r-1 \in K$, 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. □

4.4.4 Remark

The following example shows that Lemma 4.4.3 is not true if $K \trianglelefteq_r R$ is only quasiregular in the sense of Meldrum [17] as defined in Definition 4.1.7. Let $R^+ = \langle 1, a\rangle \cong E_4$ be Klein's Four Group and define a multiplication on R via the following multiplication table.

$\cdot$	0	1	a	$1+a$
0	0	0	0	0
1	0	1	a	$1+a$
a	0	a	0	a
$1+a$	0	$1+a$	0	$1+a$

It is not difficult to see that this multiplication leads to a zero-symmetric nearring with identity element. Now, consider the annihilator $K = \mathfrak{A}_R(a) = \{0, a\}$ which is a right ideal of R by Corollary 2.3.10. But since $(1+a)-a(1+a) = 1+a-a = 1$, the right ideal of R generated by the set $\{x - ax \mid x \in R\}$ is equal to R and hence a is a quasiregular element of R in the sense of Definition 4.1.7. But since $xa = 0$ for $x \neq 1$, the element 1 is the only invertible element in R. Hence R does not contain non-trivial construction subgroups, in particular, K is not a construction subgroup of R.

Moreover, a is an example for a right quasiregular element of a zero-symmetric nearring, which is not right quasiregular in the sense of Beidleman [6] (c.f. Remark 4.1.8).

The following two lemmas describe the behaviour of construction subgroups under the forming of factor nearrings and sums of subgroups.

4.4.5 Lemma

Let R be a nearring, U 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 is an element $v \in U$ with $(u+1)(v+1) = 1$, and hence $((u+I)+(1+I))((v+I)+(1+I)) = (u+1)(v+1)+I = 1+I$. □

4.4.6 Lemma

Let R be a nearring with identity, and let U and V be 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 $U+V=V+U$, which it follows that $U+V$ is an additive group. Let $u, u' \in U$ and $v, v' \in V$. Then

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

Moreover, since $RU \subseteq U$ and since U and V are construction subgroups, $(v+1)^{-1}u+1$ is contained in $U+1$ and therefore

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

i.e. all elements of $U+V+1$ are left invertible. But since $\left((v+1)^{-1}u+1\right)^{-1} \in U+1$ and $(v+1)^{-1} \in V+1$, it follows that $\left((v+1)^{-1}u+1\right)^{-1}(v+1)^{-1} \in U+V+1$. 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. □

As one might expect, the ascending or descending chain condition for subgroups in $R^\times$ is related to the ascending or descending chain condition for construction subgroups.

4.4.7 Lemma

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

Proof. Let $R^\times$ satisfy the ascending chain condition for subgroups. Furthermore, let $U_0 \leq U_1 \leq U_2 \leq \dots$ be an ascending chain of construction subgroups of R. Then $U_0+1 \leq U_1+1 \leq U_2+1 \leq \dots$ is an ascending chain of subgroups of $R^\times$ and hence there is an $n \in \mathbb{N}$ with $U_n+1 = U_m+1$ for all $m \geq n$. Thus $U_n = U_m$ for $m \geq n$. The proof is the similar for the descending chain condition. □

If R is a nearring and U a construction subgroup of R, then $U+1$ is a subgroup of $R^\times$ by the definition of construction subgroups. The following lemma shows that if U is also an ideal of R, $U+1$ is a normal subgroup of $R^\times$. In the subsequent remark it is shown that the converse need not be true, i.e. if $U+1$ is a normal subgroup of $R^\times$, U need not be an ideal of R.

4.4.8 Lemma

Let R be a nearring with identity and U a construction subgroup of R which is an ideal of R. Then $U+1 \trianglelefteq R^\times$.

PROOF. Since U is an ideal of R, the canonical epimorphism $\sigma : R \to R/U$ can be restricted to the set $R^\times$. Since σ is a nearring homomorphism, $\sigma\mid_{R^\times}$ is a group homomorphism $R^\times \to (R/U)^\times$. Clearly, $U+1$ is the kernel of $\sigma\mid_{R^\times}$, and hence $U+1 \trianglelefteq R^\times$.□

4.4.9 Remark

The converse of Lemma 4.4.8 is not true. Let $C_3 = \{0,1,2\}$ be the cyclic group of order 3, and $R = M(C_3)$. For $\sigma \in R$ write $(0\sigma, 1\sigma, 2\sigma)$, i.e. for example, if $0\sigma = 1\sigma = 1$ and $2\sigma = 2$, then $\sigma = (1,1,2)$.

Now, let $U = \{(x,x,x) \in R \mid x \in C_3\}$. Then, since $R^\times \cong S_3$,

$$V = U + 1 = \{(0,1,2),\ (1,2,0),\ (2,0,1)\} \trianglelefteq R^\times.$$

Hence, U is a construction subgroup of R with $U+1 \trianglelefteq R^\times$. But U is not an ideal of R, because for instance for $r = (1,1,0)$, $s = (1,1,2)$, and $u = (1,1,1) \in U$,

$$\begin{aligned}(r+u)s - rs &= ((1,1,0)+(1,1,1))\cdot(1,1,2) - (1,1,0)\,(1,1,2)\\ &= (2,2,1)\,(1,1,2) - (1,1,1)\\ &= (2,2,1) - (1,1,1)\\ &= (1,1,0) \notin U.\end{aligned}$$

4.5. Subdirect sums and products

Subdirect sums and products are well-known group and ring theoretical notions. For nearrings, these concepts are defined in a similar way. Most of the results in this section can be found in Pilz [18]. These results will be used in Section 5.4 below, where subdirect products of local nearrings are investigated.

4.5.1 Definition (Pilz [18, Definition 1.54])

Let R_i, $i \in I$, be a family of nearrings.

(a) The set $\mathop{\times}\limits_{i\in I} R_i$ with component-wise defined operations "+" and "·" is called the *direct product* $\prod\limits_{i\in I} R_i$ of the nearrings R_i, $i \in I$.

(b) The subnearring of $\prod\limits_{i\in I} R_i$ consisting of those elements where all but a finite number of components are zero, is called the *(external) direct sum* $\bigoplus\limits_{i\in I} R_i$ of the R_i, $i \in I$.

4.5.2 Definition (Pilz [18, Definition 1.55])

Let R_i, $i \in I$, be a family of nearrings, R a subnearring of $\prod\limits_{i\in I} R_i$. If all projection maps $\pi_i : R \to R_i$, $i \in I$, are surjective, then R is called a *subdirect product* of the R_i, $i \in I$. R is called *subdirect sum*, if R also is a subnearring of the direct sum of the R_i, $i \in I$.

4.5.3 Remark (Pilz [18, Remark 1.58], c.f. Grätzer [11])

If R is a subdirect product of nearrings R_i, $i \in I$, then the R_i are homomorphic images of R. If $K_i = \operatorname{Ker}(\pi_i)$ for the projection mappings $\pi_i : R \to R_i$, then $(K_i)_{i\in I}$ is a family of ideals of R with zero intersection.

Conversely, if a family of ideals $(K_i)_{i\in I}$ of some nearring R with $\bigcap_{i\in I} = \{0\}$ is given, R is isomorphic to a subdirect product of the nearrings $R_i = R/K_i$.

4.5.4 Definition (Pilz [18, Definition 1.59])

A subdirect product R of nearrings R_i, $i \in I$ is called *trivial*, if there is an index $i \in I$ for which π_i is an isomorphism. A nearring R is called *subdirectly irreducible*, if R is not isomorphic to a non-trivial subdirect product of nearrings.

4.5.5 Theorem (Pilz [18, Theorem 1.60], c.f. Grätzer [11])

The following conditions for a nearring $R \neq \{0\}$ are equivalent:

(a) R is subdirectly irreducible;

(b) If $(K_i)_{i\in I}$ is a family of ideals of R with zero-intersection, then there is an index $i \in I$ with $K_i = \{0\}$;

(c) $\bigcap\limits_{\{0\}\neq I \trianglelefteq R} I \neq \{0\}$;

(d) R contains a unique minimal ideal, contained in all other non-zero ideals.

4.5.6 Example

The ring $\mathbb{Z}/p^\ell\mathbb{Z}$ for a prime p and a positive integer ℓ is subdirectly irreducible.

4.5.7 Corollary (Pilz [18, Corollary 1.61])

Each simple nearring is subdirectly irreducible.

4.5.8 Theorem (Grätzer [11, page 124])

Each nearring is isomorphic to a subdirect product of subdirectly irreducible nearrings.

Chapter 5.

Local nearrings

5.1. Definition and basic properties

Local nearrings form 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 [16] as a generalisation of local rings. In the following, basic properties of local nearrings are described. In particular, the structure of prime rings and the groups of units of local nearrings are investigated. Later certain nilpotency conditions for local nearrings are exhibited and at the end of this chapter subdirect products of local nearrings are considered.

5.1.1. Definition of local nearrings

In the following, only nearrings R with identity 1 are considered, but in general they are not zero-symmetric as in Maxson [16]. Therefore, some of the proofs have to be adapted.

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

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

5.1.2 Definition (Maxson [16, Definition 2.1])
The nearring R is called a *local nearring*, if L_R is an R-subgroup of R.

5.1.3 Theorem (Maxson [16, Theorem 2.2])
Since no element of a proper R-subgroup of R can have a right inverse, L_R is the unique maximal R-subgroup of R, if R is a local nearring,

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

5.1.4 Theorem (Maxson [16, Theorem 2.3])
The nearring R is local if and only if L_R is a subgroup of R^+.

The next lemma shows that a local nearring R is the set theoretical union of the group $R^\times$ of units of R and the R-subgroup L_R. This is a useful property of local nearrings, since every element of R is either a unit or contained in L_R.

5.1.5 Lemma (Maxson [16, Lemma 2.4])
Let R be a local nearring. Then the elements of L_R do not have left inverses, and the elements of $R \setminus L_R$ are units.

Proof. Assume, $l \in L_R$ has a left inverse r, i.e. $rl = 1$. Then $lr \in L_R$ and hence $1 - lr \notin L_R$. Therefore there is 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 2.1.8, a contradiction. Thus, the elements of L_R do not have left inverses.

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

5.1.6 Corollary (Maxson [16, Corollary 2.6])
If R is a local nearring, then L_R is an (R, R)-subgroup of R.

The following proposition shows that local nearrings can be used for the construction of triply factorized groups.

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

Proof. It is clear that $L_R + 1 \subseteq R^\times$. 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 multiplication. □

5.1.2. Basic properties of local nearrings

Maxson [16] considers only zero-symmetric local nearrings. The following lemma shows that there is no big difference, to allow local nearrings to have a non-trivial constant part, since the constant part R_c of a nearring R is always contained in L_R (c.f. Lemma 2.1.12).

5.1.8 Lemma
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 $1 = yx = x \in R_c$. But by Corollary 2.1.9, $1 \in R_0$, and by Theorem 2.1.8, $R_0 \cap R_c = \{0\}$, a contradiction to $1 \neq 0$. □

5.1.9 Corollary

If L_R is nil, then R is zero-symmetric, since no non-trivial constant element can be nilpotent.

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

5.1.10 Proposition

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

Proof. It is clear that $l \in L_R \cap R_0$ implies $l \in L_{R_0}$. Now let $l \in L_{R_0}$. Then l cannot be a unit in R, since the inverses of zero-symmetric units are also zero-symmetric by Proposition 2.1.11. Hence $l \in L_R$, and thus $L_{R_0} = L_R \cap R_0$ is an additive group. By Theorem 5.1.4, R_0 is local. □

5.1.11 Remark

By Lemma 5.1.8, $R_c \subseteq L_R$. By Lemma 2.1.12, $R_c + 1 \subseteq R^\times$. In fact it is easy to check that then $(c+1)^{-1} = -c + 1$.

It is well-known that for local rings R the group L_R always is 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.

5.1.12 Lemma (Maxson [16, Lemma 2.9])

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 Remark 4.1.8 and hence is contained in $\mathcal{J}_2(R)$ by Theorem 4.1.11. □

5.1.13 Corollary

(a) *If R is a zero-symmetric local nearring with descending chain condition for R-subgroups, then L_R is nilpotent by Theorem 4.1.12.*

(b) *If R is a local nearring with descending chain condition for R-subgroups, then by Theorem 4.1.13 and Lemma 5.1.8 there is an $n \in \mathbb{N}_0$ with ${L_R}^n = R_c$.*

As for rings one can show that non-trivial factor nearrings of local nearrings are likewise local.

5.1.14 Lemma

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 $r \in R^\times$, $(r+I)(r^{-1}+I) = 1+I$, and hence $r+I \in (R/I)^\times$. Now, let $l \in L_R$ and assume 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. It seems that there is up to now neither a proof that a local nearring R always is different from $\mathcal{J}_2(R)$, nor an example for a local nearring R with $R = \mathcal{J}_2(R)$. Because of this, many authors (e.g. Gorodnik [10]) define local nearrings R to be different from the radical $\mathcal{J}_2(R)$.

5.1.15 Theorem (Maxson [16, Theorem 2.10])
If R is a zero-symmetric nearring with $\mathcal{J}_2(R) \neq R$, then R is local if and only if $L_R = \mathcal{J}_2(R)$. L_R is an ideal of R if and only if $R \neq \mathcal{J}_2(R)$.

5.1.16 Corollary (c.f. Maxson [16, 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.

5.1.3. Properties of the additive group R^+

5.1.17 Definition (Maxson [16])
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 *Property (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 $1 \cdot n_i \in R^\times = R \setminus L_R$ for $i \in \{1, 2\}$ and hence $1 \cdot n_0 = 1 \cdot (n_1 n_2) = (1 \cdot n_1)(1 \cdot n_2) \in R^\times$, a contradiction. Thus n_0 is a prime.

From this it follows that R fulfils Property (P) if and only if there is a prime p with $1 \cdot p \in L_R$.

5.1.18 Proposition (Maxson [16])
Let R be a local nearring satisfying Property (P), and let n, m be positive integers with $1 \cdot n$, $1 \cdot m \in L_R$. 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 lemma shows that if L_R has finite exponent and is non-trivial, it follows that R satisfies Property (P). If R is a nearfield, i.e. a local nearring with trivial R-subgroup L_R, one can not obtain much information about R from the structure of L_R.

5.1.19 Lemma

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

Proof. Assume that R is not a nearfield, i.e. $L_R \neq \{0\}$. Let $n = \exp({L_R}^+)$ and assume, R does not satisfy Property (P). Then $1 \cdot n \in R^\times$, 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 2.1.9, $1 \cdot n$ is zero-symmetric, so that by Proposition 2.1.11 also 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 Property (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-groups for some prime number p.

5.1.20 Theorem (Maxson [16, Theorem 7.4])

If R is a local nearring with descending chain condition for R-subgroups and Property (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 [16, 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 $1 - l_1 \in R^\times$, 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 2.1.10. By Corollary 2.1.9, $(1 \cdot p)^k = 1 \cdot p^k \in R_0$, i.e. $0x = (1 \cdot p)^k \in R_c \cap R_0 = \{0\}$. Hence $o^+(1) \mid p^k$, and by Corollary 2.1.15 R^+ is a p-group. □

5.1.21 Corollary (Maxson [16, Corollary 7.6])

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 R-subgroups of R lie in L_R. But since L_R is finite, R has descending chain condition on R-subgroups. By Lemma 5.1.19, R satisfies Property (P), and hence R^+ is a p-group by Theorem 5.1.20. If R is finite, R satisfies Property (P) as well as the descending chain condition for R-subgroups, even if L_R is trivial. □

5.1.22 Corollary
Let R be a local nearring. Then $|R^{\times}|$ is odd, if and only if R is a finite nearfield of characteristic 2.

Proof. If R is a finite nearfield of characteristc 2, it is clear that $|R^{\times}|$ is odd.

Let $|R^{\times}|$ be odd, in particular finite. Because of $L_R + 1 \subseteq R^{\times}$ and $|L_R + 1| = |L_R|$, also L_R and hence R is finite. By Corollary 5.1.21, $|R| = p^n$ and $|L_R| = p^m$ for a prime p and non-negative integers n and m with $m < n$. This means that $|R^{\times}| = p^n - p^m = p^m(p^{n-m} - 1) \equiv 1 \pmod 2$. 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. □

In the investigation of zero-symmetric local nearrings, those local nearrings R with nil or even nilpotent L_R play an important rôle. The following result exhibits a useful connection between the nilpotency of L_R and the exponent of the additive group ${L_R}^+$.

5.1.23 Proposition
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, one has $0 = 1 \cdot p^l \in L_R$ 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}. □

5.1.4. 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^+.

5.1.24 Lemma
Let R be a local nearring in which the additive group ${L_R}^+$ is not normal in the additive group R^+. Then ${L_R}^+$ coincides with its normalizer $\mathbf{N}_{R^+}({L_R}^+)$.

Proof. Since ${L_R}^+$ is not normal in R^+ there is an element $r \in R^{\times}$ and a $k \in L_R$ with $-r + k + r \notin L_R$. This means that $r^{-1}(-r + k + r) = -1 + r^{-1}k + 1 \in R^{\times}$. Hence, for arbitrary $s \in R^{\times}$, one gets $-s + s(r^{-1}k) + s \notin L_R$. But $s(r^{-1}k) \in L_R$, hence $R^{\times} \cap \mathbf{N}_{R^+}({L_R}^+) = \varnothing$, and thus ${L_R}^+ = \mathbf{N}_{R^+}({L_R}^+)$. □

5.1.25 Theorem (c.f. [3])
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 one has $l^{n-1}t = l^{n-1}(r + l)s - l^{n-1}rs = (l^{n-1}r + l^n)s - l^{n-1}rs = l^{n-1}rs - l^{n-1}rs = 0$. But if

$t \in R^{\times}$, one can multiply this with t^{-1} from the right and obtains $l^{n-1} = 0$, 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 all $l \in L_R$, with $r = -1$ and $s = 1$ one sees that $-1 + l + 1 \in L_R$ for all $l \in L_R$. By Lemma 5.1.24 it follows that ${L_R}^+ \trianglelefteq R^+$. □

5.1.26 Corollary

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 5.1.12 and hence nilpotent by Theorem 4.1.12. Thus, $L_R \trianglelefteq R$ by Theorem 5.1.25. □

5.1.27 Lemma

Let R be an 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 5.1.16, 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. In particular, to investigate local nearring in which L_R is not an ideal, one can restrict the investigations to zero-symmetric nearrings. Moreover, it is shown in Corollary 5.1.30 that in a finite local nearring R the R-subgroup L_R is always an ideal.

5.1.28 Theorem (c.f. [3, Lemma 3.3])

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 5.1.25 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 an (R,R)-subgroup of R by Corollary 5.1.6, 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, $s \in R^{\times}$. 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 $l \in L_R$ and all $s \in {R_0}^{\times}$.

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 $(1+l_c)s - s \in R^\times$, there is an element $x \in R^\times$ with $1 = x((1+l_c)s - s) = (x+l_c)s - xs$. From this it follows 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 $(1+l_c)s - s \in R^\times$. Hence $L_R \trianglelefteq R$. □

5.1.29 Corollary

Let R be a local nearring with descending chain condition for R-subgroups. Then $L_R \trianglelefteq R$.

Proof. By Corollary 5.1.26, $L_{R_0} \trianglelefteq R_0$. Hence by Theorem 5.1.28 $L_R \trianglelefteq R$. □

5.1.30 Corollary

Let R be a finite local nearring. Then $L_R \trianglelefteq R$.

5.1.31 Remark

It seems to be unknown, if there is a local nearring with $L_R \ntrianglelefteq R$, and hence it is unknown, if it can happen that ${L_R}^+ \ntrianglelefteq R^+$. Corollary 5.1.30 shows, that such a local nearring must be infinite, if it exists.

Moreover, if R is a local nearring with $L_R \ntrianglelefteq R$, then let I be a maximal ideal in R (by Lemma 2.3.12, such an ideal exists). Then R/I is a simple local nearring, and $L_{R/I} \ntrianglelefteq R/I$. Thus, if there is a local nearring with $L_R \ntrianglelefteq R$, then there also exists a *simple* local nearring with this property. Simple local nearrings are investigated in Section 5.1.5.

If R is a distributively generated local nearring (c.f. Definition 2.1.6.(f)), it suffices to show that L_R is a normal subgroup of the additive group R^+ to ensure that L_R is an ideal of R, as the next lemma shows.

5.1.32 Lemma

Let (R,S) be a distributively generated local nearring with ${L_R}^+ \trianglelefteq R^+$. Then $L_R \trianglelefteq R$.

Proof. Let $l \in L_R$ and $r, s \in R$, where $s = \sum_{i=1}^n s_i$ with $s_i \in S$ or $-s_i \in S$. Then it suffices to show that $(l+r)s - rs \in L_R$.

First, let $n = 1$. Then

$$\begin{aligned}(l+r)s - rs &= (l+r)s_1 - rs_1 \\ &= \begin{cases} ls_1 + rs_1 - rs_1, & s_1 \in S \\ rs_1 + ls_1 - rs_1, & -s_1 \in S \end{cases} \\ &= \begin{cases} ls_1, & s_1 \in S \\ (ls_1)^{-rs_1}, & -s_1 \in S \end{cases} \in L_R\end{aligned}$$

Here, x^y means additive conjugation, i.e. $x^y = -y+x+y$. Next assume that $(l+r)s-rs \in L_R$ for all s with $n = k-1$. Then for $n = k$ one has

$$\begin{aligned}
(l+r)\,s - rs &= (l+r)\sum_{i=1}^{k} s_i - r\sum_{i=1}^{k} s_i \\
&= \sum_{i=1}^{k} (l+r)\,s_i - \sum_{i=1}^{k} rs_i \\
&= \sum_{i=1}^{k-1} (l+r)\,s_i + (l+r)\,s_k - rs_k - \sum_{i=1}^{k-1} rs_i \\
&= \sum_{i=1}^{k-1} (l+r)\,s_i + \underbrace{\left\{\begin{matrix} ls_k + rs_k, & (s_k \in S) \\ rs_k + ls_k, & (-s_k \in S) \end{matrix}\right\} - rs_k}_{\in L_R} - \sum_{i=1}^{k-1} rs_i \\
&= \underbrace{\sum_{i=1}^{k-1} (l+r)\,s_i - \sum_{i=1}^{k-1} rs_i}_{\in L_R} + \underbrace{((l+r)\,s_k - rs_k)^{\left(-\sum_{i=1}^{k-1} rs_i\right)}}_{\in L_R} \in L_R.
\end{aligned}$$

Hence $(l+r)s - rs \in L_R$ and thus $L_R \trianglelefteq R$. □

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

5.1.33 Lemma

Let R be a local nearring. If there is an $r \in R^\times$ such that $r \in \mathbf{C}_{R^+}({L_R}^+)$, then $R^\times \subseteq \mathbf{C}_{R^+}({L_R}^+)$ and ${L_R}^+$ is abelian. Hence $L_R \leq \mathbf{Z}(R^+)$.

Proof. Let $r \in R^\times \cap \mathbf{C}_{R^+}({L_R}^+)$. 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, $1 \in \mathbf{C}_{R^+}({L_R}^+)$ and thus $R^\times \subseteq \mathbf{C}_{R^+}({L_R}^+)$.

Now, $l+k+1 = l+(k+1) = (k+1)+l = k+(1+l) = k+l+1$. Hence ${L_R}^+$ is abelian. □

In Proposition 5.1.7 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.

5.1.34 Lemma

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

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

5.1.35 Lemma

Let R be a local nearring, $I \lhd R$ a proper ideal of R. Then $I+1 \trianglelefteq R^{\times}$.

Proof. Since $I \lhd R$, I is a proper left R-subgroup of R and hence by Lemma 5.1.34 a construction subgroup of R. By Lemma 4.4.8, $I+1$ is a normal subgroup of $R^{\times}$. □

In Remark 4.4.9 it was shown that the converse of Lemma 4.4.8 does not hold in general. The following theorem shows that for the construction subgroup L_R of a local nearring R the converse of this lemma indeed holds. Moreover, this gives another criterion for L_R to be an ideal of R.

5.1.36 Theorem

Let R be a local nearring. $L_R + 1$ is a normal subgroup of $R^{\times}$ if and only if $L_R \trianglelefteq R$.

Proof. If $L_R \trianglelefteq R$ then $L_R + 1 \trianglelefteq R^{\times}$ by Lemma 5.1.35.

On the other hand, if $L_R + 1 \trianglelefteq R^{\times}$, for every $l \in L_R$ and every $r \in R^{\times}$ 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

$$\begin{aligned} k_{l,-1}+1 = \quad & (-1)(l+1)(-1) = ((-1)l-1)(-1) \quad = 1-(-1)l \\ \Longleftrightarrow \quad & (-1)l = -1 - k_{l,-1} + 1 \\ \Longleftrightarrow \quad & l = (-1)(-1-k_{l,-1}+1) = 1-(-1)k_{l,-1}-1 \\ \Longleftrightarrow \quad & -1+l+1 = -(-1)k_{l,-1} \in L_R. \end{aligned}$$

Hence $1 \in \mathbf{N}_{R^+}({L_R}^+)$. By Lemma 5.1.24, ${L_R}^+ \trianglelefteq R^+$.

(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, $s \in R^{\times}$. Then

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

□

5.1.37 Corollary

Let R be a finite local nearring. Then $L_R + 1 \in \mathrm{Syl}_p(R^\times)$ for some prime p. By Theorem 5.1.30, $L_R \lhd R$, so that $L_R + 1$ is normal in $R^\times$. This is the only Sylow-p-subgroup of $R^\times$, and every p-element of $R^\times$ 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, $|R^\times| = p^n - p^m = p^m(p^{n-m} - 1)$. Because $|L_R + 1| = |L_R| = p^m$, it follows that $L_R + 1 \in \mathrm{Syl}_p(R^\times)$. □

The following theorem shows that if R is a local nearring in which the group ${L_R}^+$ is normal in R^+, R contains a local subnearring N such that $L_N = L_R$ and L_N is an ideal in N. Since this subnearring contains the whole construction subgroup L_R, in this situation one can restrict the consideration to N for the construction of triply factorized groups.

5.1.38 Theorem ([3, Lemma 3.6])

Let R be a local nearring with ${L_R}^+ \trianglelefteq R^+$. Then $N = L_R \cup \mathbf{N}_{R^\times}(1 + L_R)$ is a local nearring with $L_N \trianglelefteq N$.

The next theorem shows that a local nearring with cyclic additive group is finite. In Section 5.2.1 it will be shown that these local nearrings even coincide with their prime rings and hence are completely classified in Section 4.3.

5.1.39 Theorem

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

Proof. Assume that R is infinite, i.e. $R^+ = \mathbb{Z}^+$. Then there is a non-negative integer k with $L_R = k\mathbb{Z}$.

Let $0 \neq E$ be the identity element of R, which need not coincide with the generator 1 of the additive group $\mathbb{Z}^+$. For every $n \in R^\times$ there is an element $x \in R^\times$ with $E = xn \in n\mathbb{Z}$ (without loss of generality, $n > 0$ in $\mathbb{Z}$). Now let q be a prime with $q \nmid k$, if $k \neq 0$; if $k = 0$, let q be an arbitrary prime. 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. □

5.1.5. Simple local nearrings

If R is a local nearring, it still seems to be unknown whether L_R is always an ideal of R or not. This section 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 5.1.28 $L_R \trianglelefteq R$ if and only if $L_{R_0} \trianglelefteq R_0$, in the following R will be assumed to be zero-symmetric. By Corollary 5.1.26,

R cannot satisfy the descending chain condition. Clearly, every proper (right) ideal of R is contained in L_R. Since R has an identity, it contains maximal (right) ideals by Lemma 2.3.12. Since the sum of two (right) ideals is likewise a (right) ideal by Lemma 2.3.3 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 a simple local nearring which is not a nearfield. Obviously, $L_{R/I}$ is not an ideal of R/I.

5.1.40 Remark
Without loss of generality one may assume in the following that R is simple.

5.1.41 Theorem
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 an R-module with $I \leq \mathfrak{A}_R(G) \trianglelefteq R$. Since $I \neq \{0\}$ and since R is simple, $\mathfrak{A}_R(G) = R$, a contradiction to $1 \in R$ ($(I+1) \cdot 1 = I + 1 \neq I$). □

5.1.42 Theorem
R has no zero-divisors.

Proof. Assume $kl = 0$ for $k,\ l \in R \backslash \{0\}$. Then $\mathfrak{A}_R(k) \trianglelefteq_r R$ and $0 \neq l \in \mathfrak{A}_R(k)$. By Theorem 5.1.41, $\mathfrak{A}_R(k) = R$, 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.

5.1.43 Theorem
G is isomorphic to the regular R-module R_R.

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

(1) α is a group homomorphism:

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

(2) α is an 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 $G \cong_R R$. □

5.1.44 Corollary

G is a simple R-module.

Proof. By Theorem 5.1.43, 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 5.1.41. □

Thus G is an 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 $0 < gR < G$. Theorem 5.1.43 and Corollary 5.1.44 applied to gR, gives an infinite descending chain of R-submodules of G:

$$G = lR \supset l_1R \supset l_2R \supset l_3R \supset \dots$$

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

$$\begin{aligned} \alpha : R &\to M_0(G) \\ r &\mapsto \alpha_r \\ (ls)\alpha_r &= l(sr) \end{aligned}$$

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.

5.1.45 Proposition

α_r is surjective if and only if $r \in R^\times$.

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 5.1.42 $sr = 1$. Hence $r \in R^\times$. The converse is trivial. □

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

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

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

5.2. The structure of local nearrings

5.2.1. Prime rings of local nearrings

In this section, the structure of the prime rings of local nearrings will be investigated. It turns out that these prime rings are local and, as an extension of Theorem 5.1.20, that the additive group R^+ of a local nearring R is a p-group for a prime p, if R^+ has finite exponent.

5.2.1 Lemma

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 $P_R \cong \mathbb{Q}_p = \left\{\frac{n}{m} \in \mathbb{Q} \mid p \nmid m\right\}$, if there is a prime p with $1 \cdot p \in L_R$, and $P_R \cong \mathbb{Q}$, if there is no such 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 then it is both a nearfield and a ring.*

Proof. (a) By Lemma 4.3.3, $P_R \cong \mathbb{Z}/m\mathbb{Z}$. Since $o^+(1) < \infty$, R has Property (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 addition, and all elements of P_R which are not contained in L_R are invertible in P_R by Lemma 4.3.3. Hence P_R is local and thus m is a prime power.

(b) Consider the mapping $\sigma : P_R \to \mathbb{Q}$ with $(1 \cdot n)(1 \cdot m)^{-1} \mapsto \frac{n}{m}$. Again, 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. $\mathrm{Im}(\sigma) = \mathbb{Q}_p$. If there is no such 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 obvious. □

Now Theorem 5.1.20 may be extended.

5.2.2 Corollary

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 5.1.20 ${P_R}^+$ 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 5.2.2 is of course 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 2.1.15 it follows that $\exp(R^+) = p^n < \infty$.

5.2.3 Remark

In Theorem 5.1.39 it was shown that a local nearring with a cyclic additive group must be finite. Since by Corollary 2.1.15 the nearring R must coincide with $\langle 1\rangle^+$ in this case, Lemma 5.2.1 implies that $R = P_R$, and so there is a prime number p and a positive integer ℓ such that $R \cong \mathbb{Z}/p^\ell\mathbb{Z}$. In particular, R is zero-symmetric.

Figure 5.1 describes the structure of a local nearring with $L_R \trianglelefteq R$. Here P_R is the prime ring of R, and K is the prime field of the nearfield R/L_R.
Lemma 5.2.5 shows that for $L_R \trianglelefteq R$ the group $P_R + L_R$ is a local nearring. This raises the following question: Let F be a nearfield with primefield K, and R a local nearring with $L_R \trianglelefteq R$ and $R/L_R \cong K$. Is there a nearring $\tilde{R}$ with $L_{\tilde{R}} \cong L_R$ and $\tilde{R}/L_{\tilde{R}} \cong F$?
However, the following example shows that this is not always the case.

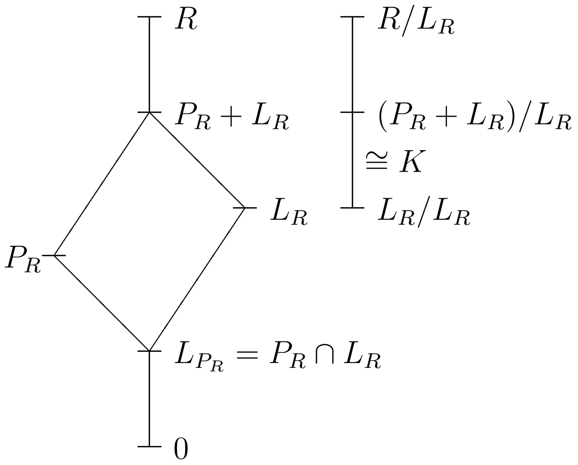


Figure 5.1.: Local nearring with $L_R \trianglelefteq R$

5.2.4 Example

Let $R = \mathbb{Z}/4\mathbb{Z}$ be a local nearring and $F = \mathbb{F}_4$. Then there is no local nearring $\tilde{R}$ with $R \leq \tilde{R}$, $L_R = L_{\tilde{R}}$ and $\tilde{R}/L_{\tilde{R}} \cong F$.

Proof. Assume, $\tilde{R}$ is such a local nearring. Since $|L_R| = 2$ and $|\tilde{R}/L_{\tilde{R}}| = 4$, the group $\tilde{R}^+$ has order 8. Moreover, $\exp(\tilde{R}^+) = 4$, since $\tilde{R}^+$ has a cyclic subgroup of order 4. But this group cannot be cyclic itself, since it has a factor group isomorphic to Klein's four group. Since $|L_R| = 2$, one has $|R^\times| = 6$, and thus R^+ must have at least 6 elements of order 4 by Corollary 2.1.15. Hence $\tilde{R}^+ \cong Q_8$. But by Malone [14, Corollary 4] there is no nearring with identity over Q_8. □

5.2.5 Lemma

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

Proof. Let $N = L_R \cup \mathbf{N}_{R^\times}(L_R + 1)$. By Theorem 5.1.38, 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 2.3.3 $P_R + L_R$ is a subnearring of N with $L_R \trianglelefteq P_R + L_R$.

Let $r = p + l \in (P_R + L_R) \setminus L_R$. Then $r^{-1} \in R$ exists. 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 needed. Hence it suffices to consider the subnearring of R generated by $U+1$. Thus, if ${L_R}^+ \trianglelefteq R^+$ for a local nearring R, for the construction of triply factorized groups using local nearrings, one may assume that $R = P_R + L_R$.

5.2.2. The multiplicative group $R^\times$

In this section 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 the nearfield R/L_R. Moreover, it will turn out that if the group of units of a local nearring R is a torsion group, also the additive group of R is periodic and hence has finite exponent by Corollary 2.1.15.

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

Proof. Clearly, the mapping $\alpha : (R/L_R)^\times \to R^\times/(L_R+1)^\times$ with $(L_R+r)\alpha = (L_R+1)r$ is a group isomorphism. □

5.2.7 Lemma
Let R be a finite local nearring. Then $R^\times \cong (L_R+1)^\times \rtimes (R/L_R)^\times$.

Proof. Let $|R| = p^n$, p a prime, $n \in \mathbb{N}$. Moreover, let $|L_R| = p^m$ $(0 < m < n)$. Then $|R^\times| = p^n - p^m = p^m(p^{n-m}-1)$. Since $p^m \nmid p^{n-m}-1$, the group L_R+1 has a complement B in $R^\times$ by the Schur-Zassenhaus Theorem (c.f. Robinson [19, Theorem 9.1.2]). But since $B \cong R^\times/(L_R+1)^\times \cong (R/L_R)^\times$, it follows that $R^\times \cong (L_R+1)^\times \rtimes (R/L_R)^\times$. □

5.2.8 Lemma
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 Property (P).

(c) If $|R : L_R| < \infty$, R has Property (P).

(d) If $R^\times$ is periodic, so is R^+.

Proof. (a) By Corollary 2.1.15, $\exp(R^+) = o^+(1) < \infty$.

(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 Property (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 Property (P).

(d) Let $R^\times$ be periodic. Assume that $\exp(R^+) = \infty$. By Lemma 5.2.1, 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 ${P_R}^\times \leq R^\times$. □

The next theorem holds for general nearrings, although it is formulated only for finite local nearrings in Maxson [16].

5.2.9 Theorem

If R is a local nearring which is not a nearfield, then $|R| \leq |L_R|^2$ (c.f. Maxson [15, Theorem 2.1]).

Proof. By Corollary 2.3.10, for every $y \in R$, the annihilator $\mathfrak{A}_R(y)$ is a right ideal of R. Since $1 \notin \mathfrak{A}_R(y)$, this yields $\mathfrak{A}_R(y) \leq L_R$. Now let $0 \neq l \in L_R$. Define $\lambda_l : R \to lR$ by $x\lambda_l = lx$ for all $x \in R$. This is an R-endomorphism of the regular module R_R with $\operatorname{Ker}(\lambda_l) = \mathfrak{A}_R(l)$. Hence, $R_R/\mathfrak{A}_R(l) \cong_R \operatorname{Im}(\lambda_l)$. Since $\operatorname{Im}(\lambda_l) \subseteq lR \subseteq L_R$, $|R| = |R_R| = |\operatorname{Ker}(\lambda_l)| \cdot |\operatorname{Im}(\lambda_l)| \leq |L_R| \cdot |L_R| = |L_R|^2$. □

5.2.10 Corollary

(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 5.2.9 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 5.2.9 . 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 [14, Corollary 4] no generalised 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. This result will be used in Chapter 8, where local nearrings with dihedral groups of units are investigated.

5.2.11 Corollary

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 2.1.15 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 $1 \notin L_R$. □

5.2.3. The nearfield R/L_R

In the following only local nearrings R with $L_R \trianglelefteq R$ will be considered, since only in this case R/L_R has a meaning. In most examples of local nearrings that appear in literature the nearfield R/L_R is a field, in many cases even a prime field. The next two examples show that every skewfield and even proper nearfields, i.e. nearfields which are not skewfields, can occur as R/L_R.

5.2.12 Examples

(a) Let K be a skewfield. Then there is an abelian local nearring R with $R/L_R \cong K$. Let $R^+ = K^+ \times K^+$ and define a multiplication on this group as follows:

$$(g_1, f_1) \cdot (g_2, f_2) = \begin{cases} (g_1 f_2, 0), & f_1 = 0 \\ (g_2 + g_1 f_2, f_1 f_2), & f_1 \neq 0 \end{cases}.$$

Then $(R, +, \cdot)$ is a local nearring with $L_R = \{(g, 0) \mid g \in K\}$ and identity element $(0, 1)$. To see this, only the associative and left distributive laws have to be checked. In the case $f_1 \neq 0 \neq f_2$ only the associativity will be verified, since the other cases are similar and even easier. Also the left distributivity is very easy and will be skipped. Let g_i, $f_i \in K$ for $i \in \{1, 2, 3\}$.

$$\begin{aligned} \big((g_1, f_1)(g_2, f_2)\big)\,(g_3, f_3) &= (g_2 + g_1 f_2, f_1 f_2) \\ &= (g_3 + (g_2 + g_1 f_2) f_3, f_1 f_2 f_3) \\ &= (g_3 + g_2 f_3 + g_1 f_2 f_3, f_1 f_2 f_3) \end{aligned}$$

$$\begin{aligned} (g_1, f_1)\,\big((g_2, f_2)(g_3, f_3)\big) &= (g_1, f_1)(g_3 + g_2 f_3, f_2 f_3) \\ &= (g_g + g_2 f_3 + g_1 f_2 f_3, f_1 f_2 f_3) \end{aligned}$$

Here it is necessary that K is a skewfield, since the right distributivity of K is used.

To show that $L_R = \{(g, 0) \mid g \in K\}$, let g_1, $g_2 \in K$. Then $(g_1, 0)(g_2, 0) = (0, 0)$, and hence the elements of the given set cannot be invertible. On the other hand, if $(g, f) \in R$ with $f \neq 0$, consider the element $(-gf^{-1}, f^{-1})$. Then

$$(-gf^{-1}, f^{-1})(g, f) = (0, 1),$$

and hence (g, f) is right invertible. Thus, the set claimed to be L_R is indeed the set of elements of R which are not right invertible.

Obviously, L_R is an additive group, and hence R is a local nearring. An easy calculation shows that L_R is an ideal of R. Moreover, R is not right distributive in general. If char $K \neq 2$, one gets

$$\begin{aligned} \big((1, 1) + (1, 1)\big)\,(1, 1) &= (2, 2)(1, 1) \\ &= (3, 2) \end{aligned}$$

$$\begin{aligned} (1, 1)(1, 1) + (1, 1)(1, 1) &= (2, 1) + (2, 1) \\ &= (4, 2) \end{aligned}$$

Finally, by the definition of the operations on R, it is clear that $R/L_R \cong K$.

(b) In the examples for local nearrings given so far, the nearfield R/L_R always is a skewfield. The next example shows that R/L_R may be a proper nearfield.

Let $R^+ = \langle 1,\, a \mid 9 = a \cdot 9 = [1,\, a] = 0 \rangle \cong C_9 \times C_9$, and define a multiplication on R by $x \cdot 1 = x$ for every $x \in R$. Furthermore, for all $x \in R$ the product xa has to be defined. If this is done, all products in R can be determined by the left distributive law.

Define xa for all $x \in L$, where $L = R \cdot 3$, by the following table.

x	xa	x	xa	x	xa
0	0	3	$a \cdot 3$	-3	$-a \cdot 3$
$a \cdot 3$	-3	$3 + a \cdot 3$	$3 - a \cdot 3$	$-3 + a \cdot 3$	$3 + a \cdot 3$
$-a \cdot 3$	3	$3 - a \cdot 3$	$-3 - a \cdot 3$	$-3 - a \cdot 3$	$-3 + a \cdot 3$

Now let $(a \cdot 2)a = -2$ and $(1 - a \cdot 2)a = -2 - a \cdot 4$. These definitions are sufficient to calculate the whole multiplication. Let $a \in R^+$ be an arbitrary element. Then define n_x and k_x such that $x = n_x + ak_x$. Then n_x and k_x are uniquely defined modulo 9.

Let x and y be elements of R for which the products xa and ya are already known. Then the product of x and y is $xy = x(n_y + ak_y) = xn_y + (xa)k_y$. Moreover, also the product $(xy)a$ can be determined in a similar way: $(xy)a = x(ya) = xn_{ya} + (xa)k_{ya}$. Thus, all products xa for $x \in R \setminus L$ can be calculated successively (actually, the calculations were done by a C++-program, which is explained in Appendix A). These calculations lead to the following table.

x	xa	x^{-1}	x	xa	x^{-1}
a	-1	$-a$	$a \cdot 2$	-2	$a \cdot 4$
$a \cdot 4$	-4	$a \cdot 2$	$-a \cdot 4$	4	$-a \cdot 2$
$-a \cdot 2$	2	$-a \cdot 4$	$-a$	1	a
1	a	1	2	$a \cdot 2$	-4
$1 + a$	$1 - a$	$-4 - a \cdot 4$	$2 + a$	$4 - a \cdot 2$	$-2 - a$
$1 + a \cdot 2$	$-4 - a$	$-4 + a$	$2 + a \cdot 2$	$2 - a \cdot 2$	$-2 - a \cdot 2$
$1 + a \cdot 3$	$3 + a \cdot 4$	$1 - a \cdot 3$	$2 + a \cdot 3$	$3 - a \cdot 4$	$-4 - a \cdot 3$
$1 + a \cdot 4$	$4 + a \cdot 2$	$-4 - a$	$2 + a \cdot 4$	$1 - a \cdot 2$	$-2 - a \cdot 4$
$1 - a \cdot 4$	$2 - a$	$-4 - a \cdot 2$	$2 - a \cdot 4$	$-4 + a$	$-2 + a$
$1 - a \cdot 3$	$-3 - a \cdot 2$	$1 + a \cdot 3$	$2 - a \cdot 3$	$-3 - a$	$-4 + a \cdot 3$
$1 - a \cdot 2$	$-2 - a \cdot 4$	$-4 + a \cdot 2$	$2 - a \cdot 2$	$-2 - a \cdot 2$	$-2 + a \cdot 2$
$1 - a$	$-1 - a$	$-4 + a \cdot 4$	$2 - a$	$-1 + a \cdot 4$	$-2 + a \cdot 4$
$3 + a$	$2 - a \cdot 3$	$-3 - a \cdot 4$	$3 + a \cdot 2$	$1 - a \cdot 3$	$-3 + a$

x	xa	x^{-1}	x	xa	x^{-1}
$3+a\cdot 4$	$-1-a\cdot 3$	$-3-a$	$3-a\cdot 4$	$-2-a\cdot 3$	$-3+a\cdot 4$
$3-a\cdot 2$	$-4-a\cdot 3$	$-3+a\cdot 2$	$3-a$	$4-a\cdot 3$	$-3-a\cdot 2$
4	$a\cdot 4$	-2	-4	$-a\cdot 4$	2
$4+a$	$1+a\cdot 2$	$-1-a\cdot 4$	$-4+a$	$-2+a\cdot 4$	$1+a\cdot 2$
$4+a\cdot 2$	$-1-a\cdot 4$	$-1+a\cdot 4$	$-4+a\cdot 2$	$2+a$	$1-a\cdot 2$
$4+a\cdot 3$	$3-a\cdot 2$	$-2-a\cdot 3$	$-4+a\cdot 3$	$3-a$	$2-a\cdot 3$
$4+a\cdot 4$	$4-a\cdot 4$	$-1-a$	$-4+a\cdot 4$	$4+a\cdot 4$	$1-a$
$4-a\cdot 4$	$-4-a\cdot 4$	$-1+a$	$-4-a\cdot 4$	$-4+a\cdot 4$	$1+a$
$4-a\cdot 3$	$-3+a$	$-2+a\cdot 3$	$-4-a\cdot 3$	$-3+a\cdot 2$	$2+a\cdot 3$
$4-a\cdot 2$	$-2-a$	$-1+a\cdot 2$	$-4-a\cdot 2$	$1+a\cdot 4$	$1-a\cdot 4$
$4-a$	$2-a\cdot 4$	$-1-a\cdot 2$	$-4-a$	$-1-a\cdot 2$	$1+a\cdot 4$
$-3+a$	$-4+a\cdot 3$	$3+a\cdot 2$	$-3+a\cdot 2$	$4+a\cdot 3$	$3-a\cdot 2$
$-3+a\cdot 4$	$2+a\cdot 3$	$3-a\cdot 4$	$-3-a\cdot 4$	$1+a\cdot 3$	$3+a$
$-3-a\cdot 2$	$-1+a\cdot 3$	$3-a$	$-3-a$	$-2+a\cdot 3$	$3+a\cdot 4$
-2	$-a\cdot 2$	4	-1	$-a$	-1
$-2+a$	$1-a\cdot 4$	$2-a\cdot 4$	$-1+a$	$1+a$	$4-a\cdot 4$
$-2+a\cdot 2$	$2+a\cdot 2$	$2-a\cdot 2$	$-1+a\cdot 2$	$2+a\cdot 4$	$4-a\cdot 2$
$-2+a\cdot 3$	$3+a$	$4-a\cdot 3$	$-1+a\cdot 3$	$3+a\cdot 2$	$-1-a\cdot 3$
$-2+a\cdot 4$	$4-a$	$2-a$	$-1+a\cdot 4$	$-2+a$	$4+a\cdot 2$
$-2-a\cdot 4$	$-1+a\cdot 2$	$2+a\cdot 4$	$-1-a\cdot 4$	$-4-a\cdot 2$	$4+a$
$-2-a\cdot 3$	$-3+a\cdot 4$	$4+a\cdot 3$	$-1-a\cdot 3$	$-3-a\cdot 4$	$-1+a\cdot 3$
$-2-a\cdot 2$	$-2+a\cdot 2$	$2+a\cdot 2$	$-1-a\cdot 2$	$4+a$	$4-a$
$-2-a$	$-4+a\cdot 2$	$2+a$	$-1-a$	$-1+a$	$4+a\cdot 4$

The computer program described in Appendix A also checks the associative and left distributive laws. Obviously the product of every two elements of L is zero, such that these elements cannot be invertible, while the elements not contained in L are units. Hence $L = L_R$ and R is a local nearring.

Now let $x = a\cdot 2$ and $y = 1 - a\cdot 2$. Then $o^\times(x) = o^\times(y) = 12$ and $x^6 = y^6 = -1$. Moreover, one finds that $\langle x\rangle^\times \cap \langle y\rangle^\times = \langle -1\rangle^\times$ and $yx = xy^{-1}$. But

$$|\langle x\rangle \cdot \langle y\rangle| = \frac{|\langle x\rangle| \cdot |\langle y\rangle|}{|\langle x\rangle \cap \langle y\rangle|} = \frac{12\cdot 12}{2} = 72 = \left|R^\times\right|,$$

and hence $R^\times = \langle x,\, y \mid x^{12} = 1,\, x^6 = y^6,\, yx = xy^{-1}\rangle$.

To verify that R/L_R is a proper nearfield, consider the expression

$$(1+a)a - (a+a^2) = (1+a)a - a^2 - a = 1 - a - (-1) - a = 2 - a\cdot 2 \notin L_R.$$

This means that

$$\big((1+L_R) + (a+L_R)\big)\,(a+L_R) \neq (1+L_R)(a+L_R) + (a+L_R)(a+L_R)$$

and so R/L_R is not distributive, i.e. R/L_R is not a skewfield.

5.3. Local nearrings with nilpotent L_R

In the following let R be a local nearring with the additional property ${L_R}^n = 0$ but ${L_R}^{n-1} \neq 0$ for some non-negative integer n. In particular, R is zero-symmetric and $L_R \trianglelefteq R$ by Theorem 5.1.25. Local nearrings R with nilpotent R-subgroup L_R are of special interest, because e.g. finite zero-symmetric nearrings belong to this class by Corollary 5.1.13. The main goal of this section is to define annihilator series, which are used to investigate local nearrings with dihedral groups of units in Chapter 8.

5.3.1 Definition

(a) A series
$$0 = I_k \lhd I_{k-1} \lhd \cdots \lhd I_1 = L_R$$
of ideals of R is called an *annihilator series*, if $I_j \subseteq (I_{j+1} : L_R)$ for $1 \leq i \leq k-1$.

(b) Let L_n be the ideal of R generated by $(L_R)^i$, the set of all products of i elements of L_R. Then $L_n = \{0\}$.

(c) Define recursively
$$\mathfrak{A}_0 = \mathfrak{A}_0(R) = \{0\}$$
$$\mathfrak{A}_i = \mathfrak{A}_i(R) = (\mathfrak{A}_{i-1}(R) : L_R)$$

Since L_j is an ideal of R, so is $(L_j : L_R)$. Clearly, $L^j \subseteq (L_{j+1} : L_R)$, so that $L_j \subseteq (L_{j+1} : L_R)$ for $1 \leq j \leq n-1$, and hence
$$0 = L_n \lhd L_{n-1} \lhd \cdots \lhd L_1 = L_R$$
is an annihilator series.

5.3.2 Lemma

Let $0 = I_k \lhd I_{k-1} \lhd \cdots \lhd I_1 = L_R$ be an annihilator series of R. Then $L_j \subseteq I_j$ for all $1 \leq j \leq k$.

Proof. The case $j = 1$ is clear, since $L_1 = I_1 = L_R$. Now assume that $L_j \subseteq I_j$. Since $I_j \subseteq (I_{j+1} : L_R)$, $li \in I_{j+1}$ for all $i \in I_j$ and for all $l \in L_R$. But ${L_R}^j \subseteq L_j \subseteq I_j$, and so ${L_R}^{j+1} \subseteq I_{j+1}$. Since $I_{j+1} \lhd R$, $L_{j+1} \subseteq I_{j+1}$. □

The series $0 = L_n \lhd L_{n-1} \lhd \cdots \lhd L_1 = L_R$ is called the *lower annihilator series.*

5.3.3 Lemma

Let $0 = I_k \lhd I_{k-1} \lhd \cdots \lhd I_1 = L_R$ be an annihilator series of R. Then $I_{k-j} \subseteq \mathfrak{A}_j$ for $0 \leq j < k$.

Proof. For $j = 0$ this is true, because $I_k = \mathfrak{A}_0 = \{0\}$. Assume that $I_{k-(j-1)} \subseteq \mathfrak{A}_{j-1}$. Since $I_{k-j} \subseteq (I_{k-(j-1)} : L_R) = \{r \in R \mid \forall l \in L_R : lr \in I_{k-(j-1)}\}$ and $\mathfrak{A}_j = (\mathfrak{A}_{j-1} : L_R)$ one has

$$I_{k-j} \subseteq (I_{k-(j-1)} : L_R) \subseteq (\mathfrak{A}_{j-1} : L_R) = \mathfrak{A}_j$$

and hence $I_{k-j} \subseteq \mathfrak{A}_j$. □

Because of the last lemma, the series

$$0 = \mathfrak{A}_0 \lhd \mathfrak{A}_1 \lhd \cdots \lhd \mathfrak{A}_{n-1} = L_R$$

is called the *upper annihilator series* of R.

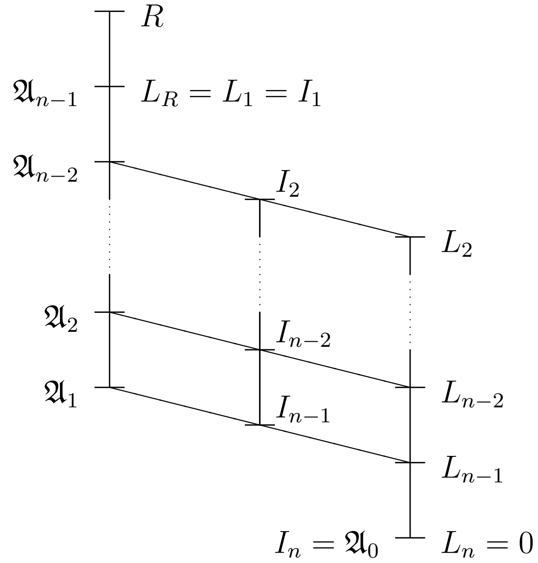


Figure 5.2.: An annihilator series of R in the case $k = n$

From the above considerations one gets the following result.

5.3.4 Theorem

Let R be a local nearring. L_R is nilpotent if and only if R has an annihilator series.

5.4. Subdirect products of local nearrings

Subdirect sums and products of nearrings were introduced in Section 4.5. In the following, subdirect products of local nearrings are investigated. It turns out that under certain finiteness conditions subdirect products of local nearrings are in fact direct products of local nearrings. These direct products are needed for the construction of triply factorized groups, since they have non-trivial construction subgroups with less structural restrictions than the construction subgroups of local nearrings.

5.4.1 Theorem

Let R_i, $i \in I$, be a family of local nearrings and R a subdirect product of the R_i, i.e. the projection maps $\pi_i : R \to R_i$ are surjective, or, in other words, for every $r_i \in R_i$ there is an $r \in R$ with $r\pi_i = r_i$. Furthermore, let R have an identity element 1_R.

Let $\varnothing \neq J \subseteq I$ and $j_0 \in J$ with the following property:

$$\text{If } r\pi_{j_0} \in L_{R_{j_0}}, \text{ then } r\pi_j \in L_{R_j} \text{ for every } j \in J. \tag{5.1}$$

(a) $1_R\pi_i = 1_{R_i}$ for all $i \in I$.

(b) For all $j \in J$, $r\pi_j \in L_{R_j}$ implies that $r\pi_k \in L_{R_k}$ for all $k \in J$.

(c) Let $r \in R$ with $r\pi_j \in R_j^\times$ for some $j \in J$. Then $r\pi_k \in R_k^\times$ for all $k \in J$ and if $|J| < \infty$, there is an element $s \in R$ with $s\pi_k = (r\pi_k)^{-1}$ for all $k \in J$.

(d) Let $R_J = \{(r\pi_j \mid j \in J) \mid r \in R\}$. Then R_J is a subdirect product of the R_j, $j \in J$, and for a finite set J, the nearring R_J is local.

(e) If $|J| < \infty$, then R is isomorphic to a subdirect product of the local nearring R_J and the R_i, $i \in I \setminus J$.

(f) If I is finite and (5.1) *implies that $|J| = 1$, then R is the direct product of the R_i, $i \in I$.*

Proof. (a) For every $r_i \in R_i$ there is an $r \in R$ with $r\pi_i = r_i$. Hence, $r_i = r\pi_i = (r1_R)\pi_i = (r\pi_i)(1_R\pi_i) = r_i(1_R\pi_i)$. Similarly, one sees that $(1_r\pi_i)r_i = r_i$ for every $r_i \in R_i$. Thus, $1_R\pi_i = 1_{R_i}$.

(b) Let $j \in J$ and $r \in R$ with $r\pi_j \in L_{R_j}$. First it is shown that then $r\pi_{j_0} \in L_{R_{j_0}}$. Assume, this is not the case. Then there is an element $s \in R$ with $s\pi_{j_0} = (r\pi_{j_0})^{-1}$. Hence $(rs)\pi_{j_0} = 1$ and $(rs-1)\pi_{j_0} = 0 \in L_{R_{j_0}}$. For brevity let $r_j = r\pi_j$ and $s_j = s\pi_j$. Since $r_j \in L_{R_j}$, the element $(rs-1)\pi_j = r_js_j - 1 \in R_j^\times$, which contradicts (5.1).

Thus $r\pi_{j_0} \in L_{R_{j_0}}$, and (5.1) implies that $r\pi_k \in L_{R_k}$ for all $k \in J$.

(c) By (b), $r\pi_k \in R_k^\times$ for all $k \in J$. Furthermore, there are elements $s^{(k)} \in R$ with $s^{(k)}\pi_k = (r\pi_k)^{-1}$ for all $k \in J$.

Now, let $|J| = n < \infty$. Without loss of generality let $J = \{1, \ldots, n\}$. It is shown by induction that the $s^{(k)}$ can be chosen such that $s^{(1)} = \cdots = s^{(n)}$. For $n = 1$ this is clear. Next assume that $s^{(1)} = \cdots = s^{(k-1)} = t$ for $k < n$ and a suitable $t \in R$, i.e. $t\pi_l = (r\pi_l)^{-1}$, and hence $(1 - rt)\pi_l = 0$ for $1 \leq l \leq k-1$.

Let $t' = s^{(k)}(1 - rt) + t$. Then for $1 \leq l \leq k-1$

$$\begin{aligned} t'\pi_l &= \left(s^{(k)}\left(1 - rt\right) + t\right)\pi_l \\ &= s^{(k)}\pi_l\left(1 - rt\right)\pi_l + t\pi_l \\ &= t\pi_l = \left(r\pi_l\right)^{-1}, \end{aligned}$$

and furthermore

$$\begin{aligned} t'\pi_k &= \left(s^{(k)}\left(1-rt\right)+t\right)\pi_k \\ &= s^{(k)}\pi_k\left(1-rt\right)\pi_k + t\pi_k \\ &= \left(r\pi_k\right)^{-1}\left(1-\left(r\pi_k\right)\left(t\pi_k\right)\right)+t\pi_k \\ &= \left(r\pi_k\right)^{-1} - \left(t\pi_k\right) + t\pi_k \\ &= \left(r\pi_k\right)^{-1}. \end{aligned}$$

Hence the elements $s^{(l)}$ can be replaced by t' for all $1 \le l \le k$. Thus it may be assumed by induction that $s^{(k)} = s$ for all $k \in J$. But then $(rs)\pi_j = 1$ for all $j \in J$.

(d) It is clear that R_J is a subdirect product of the R_j, $j \in J$. Next, consider the set

$$L = \left\{ r \in R_J \;\middle|\; \forall j \in J:\ r\pi_j \in L_{R_j} \right\}.$$

By (5.1), $r \in L$ if and only if $r\pi_j \in L_{R_j}$ for some $j \in J$. Furthermore, L is an additive group, and by (c), $r \in R_J \setminus L$ is invertible with inverse in R_J, since all components $r\pi_j$ are invertible. Hence, $L = L_{R_J}$ and R_J is a local nearring.

(e) Let $P = R_J \oplus \prod_{i \in I\setminus J} R_i$, i.e.

$$P = \left\{ \left(\left(r\pi_j \mid j \in J,\, r \in R\right), \left(r_i \mid r_i \in R_i,\, i \in I \setminus J\right) \right) \right\}.$$

For all $i \in I$, define the mappings

$$\begin{aligned} \sigma_i : P &\to R_i \\ \left(\left(r\pi_j \mid j \in J,\, r \in R\right), \left(r_i \mid r_i \in R_i,\, i \in I \setminus J\right) \right) &\mapsto \begin{cases} r\pi_i, & i \in J \\ r_i, & i \in I \setminus J \end{cases} \end{aligned}$$

Let $\tilde{R}$ be the set of all $\tilde{r} \in P$ such that there is an element $\hat{r} \in R$ with $\tilde{r}\sigma_i = \hat{r}\pi_i$ for all $i \in I$. It is clear that $\tilde{R} \cong R$, and since R is a subdirect product, so is $\tilde{R}$.

(f) Let $i \in I$ be fixed. Then for every $j \in I \setminus \{i\}$ there is an element $r_j \in R$ with $r_j\pi_i \in L_{R_i}$ and $r_j\pi_j \in R_j^\times$, since there is no $J \subseteq I$ with Property (5.1) and $|J| \ge 2$. Hence there is an element $s_j \in R$ with $(r_js_j)\pi_j = 1$. Since $(r_js_j - 1)\pi_i \in R_i^\times$ and $(r_js_j - 1)\pi_j = 0$, there exists an element $s_{ij} \in R$ with $s_{ij}\pi_i = 1$ and $s_{ij}\pi_j = 0$ for each i and $j \in I$ with $i \ne j$ (take an arbitrary element $s' \in R$ with $s'\pi_i = ((r_js_j - 1)\pi_i)^{-1}$ – then let $s_{ij} = s(r_js_j - 1)$). Hence for every $i \in I$ the element

$$e_i = \prod_{j \in I\setminus\{i\}} s_{ij}$$

satisfies the relation $e_i\pi_j = 0$ for $i \ne j$ and $e_i\pi_i = 1$ (e_i exists since $|I| < \infty$). Thus for every $i \in I$ and every $r_i \in R_i$ there is an element $r \in R$ with $r\pi_i = r_i$ and $r\pi_j = 0$ for $j \ne i$. This means that R is the complete direct product of the R_i, $i \in I$. □

5.4.2 Corollary

Let $R_1, \dots, R_n$, $n \in \mathbb{N}$, be local nearrings, R a subdirect product of the R_i, $1 \leq i \leq n$, and let R have an identity element. Then R is a direct product of local nearrings. If the set $\{1, \dots, n\}$ has Property (5.1), then R itself is a local nearring by Theorem 5.4.1.(d).

Proof. If there exists a subset $J \subseteq \{1, \dots, n\}$ which satisfies Property (5.1) and $|J| \geq 2$, the nearrings R_j, $j \in J$, can be replaced by R_J. Since there are only finitely many R_i, the nearring R can be written as a subdirect product of a smaller number of local nearrings. After finitely many steps, all J with Property (5.1) will be of cardinality 1. Hence, R is a direct product of local nearrings by Theorem 5.4.1.(f). □

5.4.3 Example

In Corollary 5.4.2 it is necessary that only finitely many local nearrings are used. Consider the ring $\mathbb{Z}$ of integers and let p be an arbitrary prime. For $n \in \mathbb{N}$ let I_n be the ideal $p^n\mathbb{Z}$ of $\mathbb{Z}$. Then $\bigcap\limits_{n \in \mathbb{N}} I_n = \{0\}$, and hence $\mathbb{Z}$ is isomorphic to a subdirect product of the $\mathbb{Z}/I_n$ by Remark 4.5.3. But the $\mathbb{Z}/I_n$ are local nearrings, whereas $\mathbb{Z}$ is not a direct sum of local nearrings.

Moreover, consider $R_n = \mathbb{Z}/p^n\mathbb{Z}$ for a prime p. The mapping

$$\begin{aligned} \sigma : \mathbb{Z} &\to \prod_{n \in \mathbb{N}} R_n \\ z &\mapsto (1_{R_n} \cdot z \mid n \in \mathbb{N}) \end{aligned}$$

is an embedding of $\mathbb{Z}$ into the direct product of the R_n and all projection mappings are surjective. Hence $\mathbb{Z}\sigma$ is a subdirect product of the R_n, and is indeed isomorphic to $\mathbb{Z}$. Since $z\sigma\pi_i \in L_{R_i}$ if and only if p divides z, the index set $\mathbb{N}$ satisfies (5.1). Thus, also in the second statement of Theorem 5.4.1.(d) the finiteness of J is required, since $\mathbb{Z}$ is not local.

In Example 5.4.3 it was shown that $\mathbb{Z}$ is isomorphic to a subdirect product of the local nearrings $\mathbb{Z}/p^n\mathbb{Z}$, $n \in \mathbb{N}$, where p is a prime. Similarly it can be shown that the ring $p\mathbb{Z}$ is isomorphic to a subdirect product of these rings. All of the rings $\mathbb{Z}/p^n\mathbb{Z}$ have an identity element, but $p\mathbb{Z}$ does not. The following theorem shows that this cannot happen for subdirect products of finitely many nearrings R_i with periodic groups of units.

5.4.4 Theorem

Let R_i, $i \in I$, be local nearrings. If $|I| < \infty$ and ${R_i}^\times$ is periodic for all $i \in I$, then every subdirect product R of the R_i, $i \in I$, has an identity element.

Proof. Without loss of generality, let $I = \{1, \dots, n\}$, $n \in \mathbb{N}$. Since R is a subdirect product, there is an element $r_1 \in R$ with $r_1\pi_1 = 1$, where π_i is the projection mapping $R \to R_i$. Now assume that $r_{k-1} \in R$ with $r_{k-1}\pi_j = 1$ for $1 \leq j \leq k-1$. If $r_{k-1}\pi_k \in {R_k}^\times$, put $r_k = r_{k-1}^m$, where $m = o^\times(r_{k-1}\pi_k)$ is a positive integer. Then $r_k\pi_j = 1$ for $1 \leq j \leq k$.

Next assume that $r_{k-1}\pi_k \in L_{R_k}$. Then there is an element $s \in R$ with $s\pi_k = 1$. Then $(r_{k-1}s - s)\pi_j = 0$ for $1 \leq j \leq k-1$, and $(r_{k-1}s - s)\pi_k = r_{k-1}\pi_k - 1$. Since $r_{k-1}\pi_k - 1 \in {R_k}^{\times}$, there is an element $t \in R$ with $t\pi_k = 1$ and $t\pi_j = 0$ for $1 \leq j \leq k-1$. But then $(r_{k-1} + t)\pi_j = 1$ for $1 \leq j \leq k-1$, and $(r_{k-1} + t)\pi_k = r_{k-1}\pi_k + 1 \in {R_k}^{\times}$. As above, this gives an element $r_k \in R$ with $r_k\pi_j = 1$ for $1 \leq j \leq k$.

By induction, there is an element $r_n \in R$ with $r_n\pi_i = 1$ for all $i \in I$. This is an identity element for R. □

5.4.5 Theorem

Every local nearring is a subdirect sum of subdirectly irreducible local nearrings.

Proof. By Theorem 4.5.8 every nearring R is a subdirect sum of subdirectly irreducible nearrings, which are isomorphic to epimorphic images of R. But non-trivial epimorphic images of local nearrings are local by Lemma 5.1.14. □

Chapter 6.

An example for a local nearring

In this chapter a method to construct a local nearring R is described, such that the group L_R contains a subgroup isomorphic to a given p-group N of finite exponent, where p is a prime. With this construction it is possible to obtain examples of local nearrings with non-abelian construction subgroups L_R, which lead to the construction of triply factorized groups $G = A \ltimes M = B \ltimes M = AB$ with a non-abelian group M.

6.1. Construction of a local nearring R

Let p be a prime, N^+ an additively written, not necessarily abelian p-group of exponent p^ℓ, $\ell \in \mathbb{N}$. Then N with zero the multiplication is a nearring. This nearring can be embedded into a nearring with identity as follows.

Let $G = N \oplus \mathbb{F}_p$. Then N can be embedded into $M_0(G)$ by Theorem 2.2.3:

$$\begin{aligned} \varphi : N &\to M_0(G) \\ n &\mapsto \theta_n \end{aligned}$$

Here, $g\theta_n = \begin{cases} n, & g \notin N \\ 0, & g \in N \end{cases}$ for all $g \in G$. Thus $N\varphi$ is a subnearring of $M_0(G)$ isomorphic to N, which will be identified with N in the sequel. Note that if $g = n + f \in G = N \oplus \mathbb{F}_p$ then $g \in N \Leftrightarrow f = 0$. Next let

$$R = \left\{ \sum_{j=1}^{r} \left(\mathrm{id}_G a_j + \theta_{n_j} \right) \;\middle|\; a_j \in \mathbb{Z}/p^\ell\mathbb{Z},\, n_j \in N,\, r \in \mathbb{N}_0 \right\}, \tag{6.1}$$

where id_G is the identity of $M_0(G)$. In the following it will be shown that R is a local nearring, whose R-subgroup L_R contains a subgroup isomorphic to N.

Beacuse of left distributivity, to determine the multiplication on R, it is sufficient to know the product of an element of R with an element of $N\varphi$.

6.1.1 Lemma

Let $x = \sum_{j=1}^{r} \left(\mathrm{id}_G a_j + \theta_{n_j}\right) \in R$ and $m \in N$. Then

$$x\theta_m = \begin{cases} \theta_m, & \sum_{j=1}^{r} a_j \not\equiv 0 \pmod{p} \\ 0, & \sum_{j=1}^{r} a_j \equiv 0 \pmod{p} \end{cases}$$

Proof. Let $g \in G$. Then

$$\begin{aligned} g\left(\sum_{j=1}^{r} \left(\mathrm{id}_G a_j + \theta_{n_j}\right)\right)\theta_m &= \left(\sum_{j=1}^{r} \left(g a_j + g\theta_{n_j}\right)\right)\theta_m \\ &= \begin{cases} \left(\sum_{j=1}^{r} (g a_j + n_j)\right)\theta_m, & g \notin N \\ \left(\sum_{j=1}^{r} g a_j\right)\theta_m, & g \in N \end{cases} \\ &= \begin{cases} \left(\sum_{j=1}^{r} (g a_j + n_j)\right)\theta_m, & g \notin N \\ 0, & g \in N \end{cases}. \end{aligned}$$

It is shown next that $\sum_{j=1}^{r} (g a_j + n_j) \in N$ if and only if $\sum_{j=1}^{r} a_j \equiv 0 \pmod{p}$. Let $g = n + f$ with $n \in N$ and $f \in \mathbb{F}_p$. Then

$$\begin{aligned} \sum_{j=1}^{r} (g a_j + n_j) &= \sum_{j=1}^{r} ((n+f)a_j + n_j) \\ &= \sum_{j=1}^{r} (n a_j + n_j) + \sum_{j=1}^{r} f a_j. \end{aligned}$$

But this expression lies in N if and only if $\sum_{j=1}^{r} a_j f = 0$, which is equivalent to $\sum_{j=1}^{r} \equiv 0 \pmod{p}$. Since this condition is independent of the choice of g, the lemma is proved. □

6.1.2 Theorem

R is a zero-symmetric nearring.

Proof. It is trivial that R is an additive group, since N has finite exponent. By Lemma 6.1.1, R is closed under multiplication, since $x(\mathrm{id}_G a) = xa$ and $x\theta_m \in R$ for every $x \in R$, $a \in \mathbb{Z}$, and $m \in N$. The nearring R is zero-symmetric, since $R \subseteq M_0(G)$.□

The next step is to determine the set L_R of elements of R which are not right invertible. This is done in the following lemma and the subsequent theorem. The last step then is to show that L_R is indeed a subgroup of R^+.

6.1.3 Lemma
Let $\kappa : G \to G$ with $(n+f)\kappa = \begin{cases} [na_0, m_0], & f \neq 0 \\ 0, & f = 0 \end{cases}$, where $m_0 \in N$, $a_0 \in \mathbb{Z}/p^\ell\mathbb{Z}$, and $[na_0, m_0] = -na_0 - m_0 + na_0 + m_0$ is the additive commutator of na_0 and m_0. Then $\kappa \in R$. In particular, all mappings of the form

$$n + f \mapsto \begin{cases} \sum_{k=1}^{s} [na_k, m_k], & f \neq 0 \\ 0, & f = 0 \end{cases} \tag{6.2}$$

are contained in R.

Proof. It is easy to see that $\kappa = [a_0 \mathrm{id}_G, \theta_{m_0}] \in R$. □

6.1.4 Theorem
Let $x = \sum_{j=1}^{r} \left(\mathrm{id}_G a_j + \theta_{n_j}\right) \in R$. Then x is right invertible if and only if $\sum_{j=1}^{r} a_j \not\equiv 0 \pmod{p}$.

Proof. If $\sum_{j=1}^{r} a_j \equiv 0 \pmod{p}$, it is clear that x is not injective and hence has no right inverse. Thus let $a = \sum_{j=1}^{r} a_j \not\equiv 0 \pmod{p}$ and $m = \sum_{j=1}^{r} n_j$. Then $a \in \left(\mathbb{Z}/p^\ell\mathbb{Z}\right)^{\times}$, i.e. $a^{-1} \in \mathbb{Z}/p^\ell\mathbb{Z}$ exists. Let $\tilde{y} = \mathrm{id}_G a^{-1} + \theta_{-ma^{-1}}$. Then

$$\begin{aligned}
(n+f)x\tilde{y} &= \begin{cases} \left(\sum_{j=1}^{r} (na_j + n_j) + \sum_{j=1}^{r} fa_j\right) \tilde{y}, & f \neq 0 \\ \left(\sum_{j=1}^{r} na_j\right) \tilde{y}, & f = 0 \end{cases} \\
&= \begin{cases} \left(\sum_{j=1}^{r} (na_j) + \sum_{j=1}^{r} n_j + \tilde{k}(n) + \sum_{j=1}^{r} fa_j\right) \tilde{y}, & f \neq 0,\ \tilde{k}(n) \in N' \\ naa^{-1}, & f = 0 \end{cases} \\
&= \begin{cases} \left(n\left(\sum_{j=1}^{r} a_j\right) + \sum_{j=1}^{r} n_j + \tilde{k}(n)\right) a^{-1} + f\left(\sum_{j=1}^{r} a_j\right) a^{-1} - ma^{-1}, & f \neq 0 \\ n, & f = 0 \end{cases} \\
&= \begin{cases} naa^{-1} + ma^{-1} + \hat{k}(n) - ma^{-1} + faa^{-1}, & f \neq 0,\ \hat{k}(n) \in N' \\ n, & f = 0 \end{cases} \\
&= \begin{cases} n + f + k(n), & f \neq 0,\ k(n) \in N' \\ n, & f = 0 \end{cases}
\end{aligned}$$

Here the commutator expressions $\tilde{k}(n)$, $\hat{k}(n)$ and $k(n)$ appear since the order of the summands which need not commute is changed. These expressions are as in (6.2). By Lemma 6.1.3 the mapping $\kappa : G \to G$ with $(n+f)\kappa = \begin{cases} k(n), & f \neq 0 \\ 0, & f = 0 \end{cases}$ lies in R, and hence so does the right inverse $y = \tilde{y} - \kappa$ of x. □

6.1.5 Theorem
The nearring R is local, where

$$L_R = \left\{ \sum_{k=1}^{s} (\mathrm{id}_G a_k + \theta_{n_k}) \in R \;\middle|\; \sum_{k=1}^{s} a_k \equiv 0 \pmod{p} \right\} \tag{6.3}$$

Proof. By Theorem 6.1.4, the set given in (6.3) is the set L_R of all not right-invertible elements of R. Thus it is sufficient to show that L_R is a subgroup of R^+, but this is trivial, since N and hence R^+ have finite exponent. □

6.2. The examination of the structure of R

To examine the structure of R, the following definitions are needed.

6.2.1 Definition

(a) The mapping $\sigma : R \to \mathbb{Z}/p^\ell\mathbb{Z}$ is defined by $\sum_{j=1}^r \left(\mathrm{id}_G a_j + \theta_{n_j}\right) \mapsto \sum_{j=1}^r a_j$. It is clear that σ is a nearring homomorphism, since by Lemma 6.1.1 $(x\theta_n)\,\sigma = 0$.

(b) The group homomorphism $\tau : R \to N$ is given by $\sum_{j=1}^r \left(\mathrm{id}_G a_j + \theta_{n_j}\right) \mapsto \sum_{j=1}^r \theta_{n_j}$.

(c) Let $x = \sum_{j=1}^r \left(\mathrm{id}_G a_j + \theta_{n_j}\right) \in R$. By changing the order of the summands one gets

$$\begin{aligned} x &= \mathrm{id}_G \left(\sum_{j=1}^r a_j\right) + \sum_{j=1}^r \theta_{n_j} + \kappa_x \\ &= \mathrm{id}_G(x\sigma) + x\tau + \kappa_x, \end{aligned}$$

where κ_x is an element of the commutator subgroup R' of R^+. Thus one can define the mapping $\kappa : R \to R'$ by $x\kappa = \kappa_x = -x\tau - \mathrm{id}_G(x\sigma) + x$.

Since the representations of elements of R given in (6.1) are not unique, it has to be checked that these mappings are well-defined. Since for $g = 0 + 1 \in G$ one has $gx = 0 + x\tau$, τ is well-defined. Moreover, $nx = n \cdot (x\sigma)$ for all $n \in N$, thus also σ is well-defined. This implies that κ is well-defined.

6.2.1. The additive group R^+

For the investigation of the structure of R^+, first consider the set

$$\tilde{N} = \{-\mathrm{id}_G + \theta_n + \mathrm{id}_G \mid n \in N\}.$$

It is clear that $\tilde{N}$ is a subgroup of R^+ isomorphic to N.

6.2.2 Lemma

$N \cap \tilde{N} = \mathbf{Z}(N) = \mathbf{Z}(\tilde{N})$.

Proof. Let $x = -\mathrm{id}_G + \theta_{\tilde{n}} + \mathrm{id}_G \in N \cap \tilde{N}$, i.e. there is an $n \in N$ with $x = \theta_n$. For $g = m + f \in G$ this means

$$gx = \begin{cases} -g + \tilde{n} + g, & g \notin N \\ 0, & g \in N \end{cases}$$

$$= \begin{cases} -f - m + \tilde{n} + m + f, & g \notin N \\ 0, & g \in N \end{cases}$$

$$= \begin{cases} -m + \tilde{n} + m, & g \notin N \\ 0, & g \in N \end{cases},$$

but also

$$gx = \begin{cases} n, & g \notin N \\ 0, & g \in N \end{cases},$$

thus $-m + \tilde{n} + m = n$ for all $m \in N$; for $m = 0$ it follows that $\tilde{n} = n$, and hence $n \in \mathbf{Z}(N)$. Thus $N \cap \tilde{N} \subseteq \mathbf{Z}(N) = \mathbf{Z}(\tilde{N})$. The inclusion $\mathbf{Z}(N) \subseteq N \cap \tilde{N}$ is obvious. □

The following lemma shows that in the local nearring R the R-subgroup L_R is always nilpotent. The smallest number n for which ${L_R}^n = 0$ only depends on the exponent of the group N, from which R was constructed.

6.2.3 Lemma

For $1 \leq n \leq \ell$, the set ${L_R}^n \subseteq \{x \in R \mid x\sigma \equiv 0 \pmod{p^n}\}$. Moreover, ${L_R}^{\ell+1} = \{0\}$.

Proof. For $n = 1$ the lemma is trivial. So let $y = \sum_{j=1}^{r} \left(\mathrm{id}_G a_j + \theta_{n_j}\right)$ with $y\sigma \equiv 0 \pmod{p^{n-1}}$ and $x \in L_R$. Then $xy = \sum_{j=1}^{r} \left(xa_j + x\theta_{n_j}\right) = \sum_{j=1}^{r} xa_j = x(y\sigma)$, and because of $x\sigma \equiv 0 \pmod{p}$ one gets $(xy)\sigma \equiv 0 \pmod{p^n}$.

If $y\sigma \equiv 0 \pmod{p^{n-1}}$, i.e. $y\sigma = 0$, then $xy = x(y\sigma) = 0$. □

6.2.4 Corollary

(a) $R' \subseteq \mathrm{Ker}(\sigma)$.

(b) Let x, $y \in R'$. Then $xy = 0$.

Proof. The first statement follows directly from the definition of σ. The second follows from the proof of Lemma 6.2.3. □

Now the structure of ${L_R}^+$ and of R^+ may be described.

6.2.5 Theorem

Let $M = L_R \cap \mathrm{Ker}(\tau)$. Then ${L_R}^+ = N \ltimes M$ and $R^+ = N \ltimes \mathrm{Ker}(\tau)$.

Proof. It is clear that $N \cap \mathrm{Ker}(\tau) = \{0\}$. Now let $x = x\tau + (\mathrm{id}_G(x\sigma) + \tilde{\kappa}_x) \in R$. Then $\mathrm{id}_G(x\sigma) = \tilde{\kappa}_x \in \mathrm{Ker}(\tau)$. It is also clear that $\mathrm{id}_G(x\sigma) + \tilde{\kappa}_x \in M$ for $x \in L_R$. □

Depending on the structure of N, the structure of the additive group R^+ can be quite complicated. For nilpotent N of nilpotency class 2, the calculations in R^+ can be simplified, as the following lemma shows. In this case it is also easier to describe the groups R^+ and ${L_R}^+$.

6.2.6 Lemma

If N is nilpotent of class 2, the following statements hold:

(a) Let n, m, $k \in N$, a, $b \in \mathbb{Z}/p^\ell\mathbb{Z}$ with $a+b \in \mathbb{Z}/p^\ell\mathbb{Z}^\times$. Then there are elements r, $s \in N$ with

$$\theta_n + \mathrm{id}_G a + \theta_m + \mathrm{id}_G b + \theta_k = \theta_r + \mathrm{id}_G(a+b) + \theta_s,$$

where $r = n+m+k-\tilde{m}(a+b)^{-1}$ and $s = \tilde{m}(a+b)^{-1}$ with $\tilde{m} = ma + k(a+b)$.

(b) Let n, m, $k \in N$, a, $t \in \mathbb{Z}/p^\ell\mathbb{Z}$. Then there are elements r and $s \in N$ with

$$\theta_n + \mathrm{id}_G(pt-a) + \theta_m + \mathrm{id}_G a + \theta_k = \theta_r + \mathrm{id}_G(pt+1) + \theta_s - \mathrm{id}_G,$$

where $r = n+m+k+ma$ and $s = -ma$.

Proof. Let n, m, $k \in N$.

(a) Put $\tilde{m} = ma + k(a+b)$. Then

$$\begin{aligned}
&\theta_n + \mathrm{id}_G a + \theta_m + \mathrm{id}_G b + \theta_k \\
&= \theta_{n+m} + \mathrm{id}_G(a+b) + \theta_k + [\mathrm{id}_G a, \theta_m] \\
&= \theta_{n+m+k} + \mathrm{id}_G(a+b) + [\mathrm{id}_G, \theta_m \cdot a] + [\mathrm{id}_G(a+b), \theta_k] \\
&= \theta_{n+m+k} - \theta_s + \theta_s + \mathrm{id}_G(a+b) + \big[\mathrm{id}_G,\ \theta_{ma+k(a+b)}\big] \\
&= \theta_{n+m+k-s} + \mathrm{id}_G(a+b) + \theta_s + [\mathrm{id}_G, \theta_{\tilde{m}}] + [\theta_s, \mathrm{id}_G(a+b)] \\
&= \theta_r + \mathrm{id}_G(a+b) + \theta_s + [\mathrm{id}_G, \theta_{\tilde{m}}] + \big[\theta_{s(a+b)}, \mathrm{id}_G\big] \\
&= \theta_r + \mathrm{id}_G(a+b) + \theta_s + [\mathrm{id}_G, \theta_{\tilde{m}}] + [\theta_{\tilde{m}}, \mathrm{id}_G] \\
&= \theta_r + \mathrm{id}_G(a+b) + \theta_s.
\end{aligned}$$

(b) Let $r = n+m+k+ma$ and $s = -ma$. Then

$$\begin{aligned}
&\theta_n + \mathrm{id}_G(pt-a) + \theta_m + \mathrm{id}_G a + \theta_k \\
&= \theta_n + \mathrm{id}_G pt + [\mathrm{id}_G a, \theta_{-m}] + \theta_m + \theta_k \\
&= \theta_{n+m+k} + \mathrm{id}_G pt + [\mathrm{id}_G, \theta_{-ma}] \\
&= \theta_{n+m+k} + \mathrm{id}_G pt + [\theta_{-ma}, -\mathrm{id}_G] \\
&= \theta_{n+m+k} + \mathrm{id}_G pt + \theta_{ma} + \mathrm{id}_G + \theta_{-ma} - \mathrm{id}_G \\
&= \theta_{n+m+k+ma} + \mathrm{id}_G pt + \mathrm{id}_G + \theta_s - \mathrm{id}_G \\
&= \theta_r + \mathrm{id}_G(pt+1) + \theta_s - \mathrm{id}_G.
\end{aligned}$$

□

6.2.7 Corollary
In the situation of Lemma 6.2.6 one has

$$L_R = \left\{\theta_n + \mathrm{id}_G(pt+1) + \theta_m - \mathrm{id}_G \;\middle|\; n,\, m \in N,\ t \in \mathbb{Z}/p^\ell\mathbb{Z}\right\}, \tag{6.4}$$

and

$$R^\times = \left\{\theta_n + \mathrm{id}_G c + \theta_m \;\middle|\; n,\, m \in N,\ c \in \mathbb{Z}/p^\ell\mathbb{Z}^\times\right\}. \tag{6.5}$$

Proof. Both statements follow by successive application of Lemma 6.2.6. □

6.2.2. The multiplicative group $R^\times$

For the investigation of the group of units of R it is convenient to consider the sets

$$N_1 = \{\mathrm{id}_G + \theta_n \mid n \in N\} \quad \text{and} \quad N_2 = \{\theta_n + \mathrm{id}_G \mid n \in N\}.$$

From Lemma 6.1.1 it follows that these are subgroups of $R^\times$ isomorphic to N. First one sees that N_1N_2 is the central product of N_1 and N_2.

6.2.8 Lemma
$N_1 \cap N_2 = \mathbf{Z}(N_1) = \mathbf{Z}(N_2)$.

Proof. Let $x = \mathrm{id}_G + \theta_n = \theta_m + \mathrm{id}_G \in N_1 \cap N_2$. Then $(k+1)x = (k+1)+n = m+(k+1)$ for all $k \in N$, hence $k+n = m+k$. For $k=0$ one can see that $n=m$, and this implies that $n \in \mathbf{Z}(N)$, hence $\mathrm{id}_G + \theta_n \in \mathbf{Z}(N_1)$ and $\theta_n + \mathrm{id}_G \in \mathbf{Z}(N_2)$. Thus it follows $N_1 \cap N_2 \subseteq \mathbf{Z}(N_1) = \mathbf{Z}(N_2)$. The inclusion $\mathbf{Z}(N_1) \subseteq N_1 \cap N_2$ also follows immediately. □

6.2.9 Lemma
For all $x \in N_1$ and all $y \in N_2$ the equation $xy = yx$ holds.

Proof. Let $x = \mathrm{id}_G + \theta_n$ and $y = \theta_m + \mathrm{id}_G$. Then

$$\begin{aligned}(\mathrm{id}_G + \theta_n)(\theta_m + \mathrm{id}_G) &= (\mathrm{id}_G + \theta_n)\theta_m + \mathrm{id}_G + \theta_n \\ &= \theta_m + \mathrm{id}_G + \theta_n \\ &= \theta_m + \mathrm{id}_G + (\theta_m + \mathrm{id}_G)\theta_n \\ &= (\theta_m + \mathrm{id}_G)(\mathrm{id}_G + \theta_n).\end{aligned}$$

□

6.2.10 Corollary
$N_1N_2 = \{\theta_n + \mathrm{id}_G + \theta_m \mid n,\, m \in N\}$ is the central product of N_1 and N_2 (c.f. e.g. Robinson [19, Section 5.3]).

As the next two lemmas show, also the group of units $R^\times$ can be written as a semidirect product.

6.2.11 Lemma
Let x, $y \in R$. Then

$$xy = \begin{cases} x(y\sigma), & x \in L_R \\ x(y\sigma) + y\tau + x\kappa_y, & x \in R^\times \end{cases}.$$

Proof. Since $y = \mathrm{id}_G(y\sigma) + y\tau + \kappa_y$, this follows immediately from Lemma 6.1.1. □

In Definition 6.2.1, the nearring homomorphism σ is defined. The restriction

$$\sigma^* : R^\times \to \mathbb{Z}/p^\ell\mathbb{Z}^\times$$

with $\sigma^* = \sigma|_{R^\times}$ is a group-epimorphism.

6.2.12 Lemma
(a) The multiplicative group $S = \left\{\mathrm{id}_G c \,\middle|\, c \in \mathbb{Z}/p^\ell\mathbb{Z}^\times\right\}$ is isomorphic to $\mathbb{Z}/p^\ell\mathbb{Z}^\times$.

(b) $R^\times = S \ltimes K$, where $K = \mathrm{Ker}(\sigma^*)$.

Proof. Statement (a) is clear. It is also clear that $S \cap K = 1$ and $K \trianglelefteq R$. Let $x \in R^\times$. Then $x_1 = \mathrm{id}_G\,(x\sigma^*)^{-1} \cdot x \in K$. Moreover, $\mathrm{id}_G\,(x\sigma^*) \in S$ and $x = \mathrm{id}_G\,(x\sigma^*) \cdot x_1$. This implies (b). □

6.2.3. The operation of $L_R + 1$ on L_R

For the construction of triply factorized groups by local nearrings the operation of L_R+1 on $L_R{}^+$ is important, since L_R is a construction subgroup as needed in Construction 3.1.4. In particular, it is interesting under which circumstances this operation is trivial. It turns out that this is the case if and only if N N is an elementary abelian group.

6.2.13 Lemma
The subgroup $L_R + 1 \leq R^\times$ operates trivially on L_R if and only if N is an elementary abelian group.

Proof. First let $\exp(N) = p^\ell$ with $\ell \geq 2$. Then $0 \neq y = \mathrm{id}_G p \in L_R$. Now let $x = \theta_n + \mathrm{id}_G \in L_R + 1$ with $np \neq 0$. Then $xy = (\theta_n + \mathrm{id}_G)p$, and thus for $g = m + f \in G$ one gets

$$\begin{aligned} g(xy) &= \begin{cases} (n+g)p, & g \notin N \\ gp, & g \in N \end{cases} \\ &= \begin{cases} (n+m)p + fp, & g \notin N \\ gp, & g \in N \end{cases} \\ &= \begin{cases} (n+m)p, & g \notin N \\ gp, & g \in N \end{cases}. \end{aligned}$$

If m is chosen such that $o^+(m) \neq p = o^+(n+m)$, then $(\theta_m + \mathrm{id}_G)y \neq 0$, but also $(\theta_m + \mathrm{id}_G)(xy) = 0$. Hence $xy \neq y$ and $L_R + 1$ does not operate trivially on L_R.

Now let N be such that for all x, $y \in L_R$ the equation $(x + \mathrm{id}_G)y = y$ holds. By the above considerations, $\exp(N) = p$. Moreover,

$$\begin{aligned} -\mathrm{id}_G + \theta_m + \mathrm{id}_G &= (\theta_n + \mathrm{id}_G)(-\mathrm{id}_G + \theta_m + \mathrm{id}_G) \\ &= -\mathrm{id}_G - \theta_n + \theta_m + \theta_n + \mathrm{id}_G \\ &= -\mathrm{id}_G + \theta_{-n+m+n} + \mathrm{id}_G \end{aligned}$$

for all n, $m \in N$, and this implies that $\theta_{-n+m+n} = \theta_m$, i.e. $-n+m+n = m$. Hence N must be abelian.

On the other hand, if N is elementary abelian, it follows from (6.3) that $L_R = N$, and hence, by Lemma 6.1.1, $L_R + 1$ operates trivially on L_R. □

Chapter 7.

Triply factorized groups constructed by local nearrings of order p^3

7.1. Preliminary results

In the following, all groups $G(R, L_R)$ will be determined, where R is a local nearring of order p^3 for a prime p (c.f. Construction 3.1.4). Since $|L_R| \geq |R : L_R|$ by Theorem 5.2.9, one has $|L_R| = p^2$ and hence $|G(R, L_R)| = p^4$. The following lemma shows that for $p \geq 3$ the group $G(R, L_R)$ has the form $E_{p^2} \ltimes E_{p^2}$, if ${L_R}^+$ is elementary abelian. The case ${L_R}^+$ cyclic will be described in Section 7.2.

7.1.1 Lemma
Let $p \geq 3$, $A = C_{p^2}$, $M = E_{p^2}$, and $G = A \ltimes M$. Then M has no complement B in G such that $G = AB$, i.e. G is not triply factorized by A, B, and M.

Proof. Let $A = \langle a \rangle$, and let $\alpha : M \to M$, $m \mapsto m^a$. Then $\alpha \in \mathrm{Aut}(M)$. Since $\mathrm{Aut}(M) = GL(2, p)$ does not contain elements of order p^2, the order of α must be 1 or p.

First consider the case $\alpha = \mathrm{id}_M$, i.e. $G = A \times M$, and let B be another complement of M in G. Assume that $G = AB$. Then the intersection of A and B is be trivial, because $p^4 = |G| = |AB| = \frac{|A|\cdot|B|}{|A\cap B|} = \frac{p^2 \cdot p^2}{|A \cap B|}$. But since G is abelian, this means that $G = A \times B$. This is impossible, since $C_{p^2} \times C_{p^2}$ and $C_{p^2} \times E_{p^2}$ are not isomorphic.

Let $o(\alpha) = p$. Since $\mathrm{Aut}(M) \cong GL(2, p)$, α may be considered as a 2×2-matrix over $\mathbb{F}_p$, and since $o(\alpha) = p$, the minimal polynomial of α is a divisor of $x^p - 1 = (x - 1)^p$, and thus the characteristic polynomial of α is $f_\alpha = (x - 1)^2$. Hence there is a basis of M such that the matrix α is $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ for some $0 \neq x \in \mathbb{F}_p$. This means that there are elements m_1, $m_2 \in M$ such that $M = \langle m_1, m_2 \rangle$, $m_1\alpha = m_1$, and $m_2\alpha = {m_1}^x m_2$.

Now assume that G is triply factorized by A, B, and M. Then $B = \langle b \rangle$ with $b = a^i m$ for some $m \in M$. Without loss of generality one may assume that $i = 1$, i.e. $b = am$.

By induction one sees that $b^n = a^i m g_n(\alpha)$, where $g_n \in \mathbb{F}_p[x]$ is the polynomial $\frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + x + 1$. For $n = 1$, this is clear. Now let $n > 1$. Then

$$\begin{aligned} b^{n+1} = b^n b \qquad\qquad\qquad\qquad\qquad & = a^n m g_n(\alpha) a m \\ = a^{n+1}\left(m g_n(\alpha)\right)\alpha m \qquad\qquad & = a^{n+1}\left(m\alpha^{n-1}\, m\alpha^{n-2} \cdots m\alpha\, m\right)\alpha m \\ = a^{n+1}\left(m\alpha^n\, m\alpha^{n-1} \cdots m\alpha^2\, m\alpha\right) m & = a^{n+1} m g_{n+1}(\alpha). \end{aligned}$$

But g_p is the zero polynomial, and hence $b^p = a^p$. It follows that $|A \cap B| > 1$, which contradicts $G = AB$. □

It is well-known that for every prime p there are exactly five groups of order p^3, three of which are abelian. In the following, these five cases for R^+ will be considered separately.

7.2. The case R^+ cyclic

First it will be shown that ${L_R}^+$ is a cyclic group if and only if R^+ is cyclic. To prove this, the following lemma is needed.

7.2.1 Lemma

Let p be a prime and G a group of order p^3 and exponent p^2. If G contains exactly $p^3 - p$ elements of order p^2, then $p = 2$ and $G \cong Q_8$.

Proof. First assume that G is abelian, i.e. $G \cong C_{p^2} \times C_p$. Write the elements of this group as pairs of the form (x, y) with $x \in C_{p^2}$ and $y \in C_p$. Since $y^{p^2} = y^p = 1$ for all $y \in C_p$, the element (x, y) has order p^2 in G if and only if x has order p^2 in C_{p^2}. Moreover, there are exactly $p^2 - p$ elements of order p^2 in C_{p^2}. Hence G contains exactly $p(p^2 - p)$ elements of order p^2. Now $p(p^2 - p) = p^3 - p^2$ is always different from $p^3 - p$. Hence G cannot be abelian.

Assume that G is non-abelian and $p \geq 3$. Since $\exp(G) = p^2$, one has

$$G = \left\langle a, b \;\middle|\; a^{p^2} = b^p = 1,\, a^b = a^{p+1} \right\rangle.$$

Thus, $(a^p)^b = a^{p^2+p} = a^p$. Hence, if $g = a^{ip} b^j \in G$ with $0 \leq i,\, j \leq p-1$, it follows that $g^p = a^{ip^2} b^{jp} = 1$, i.e. $g = 1$ or $o(g) = p$. Thus G contains at most $p^3 - p^2$ elements of order p^2, but $p^3 - p^2 < p^3 - p$. Hence also $p \geq 3$ is impossible.

This means that G is non-abelian and $p = 2$. There are only two non-abelian groups of order 2^3, both of which have exponent 2^2. But the dihedral group D_8 contains only two elements of order 4, whereas Q_8 indeed contains $2^3 - 2 = 6$ elements of order 4. □

If ${L_R}^+$ is a cyclic group, then $\exp(R^+) \geq p^2$ and for all $r \in R^\times$ one has $o^+(r) = \exp(R^+)$ by Lemma 2.1.15. Assume that $\exp(R^+) = p^2$. Then R^+ has exactly

$$\underbrace{p^3 - p^2}_{|R^\times|} + \underbrace{p^2 - p}_{\in L_R} = p^3 - p$$

elements of order p^2. By Lemma 7.2.1 it follows that $p = 2$ and $R^+ \cong Q_8$. But by Malone [14, Corollary 4] there exists no nearring with identity whose additive group is isomorphic to Q_8. Hence, if ${L_R}^+$ is cyclic, also R^+ must be cyclic.

If R is a local nearring additive group is cyclic, $R \cong \mathbb{Z}/p^3\mathbb{Z}$ because of $R = P_R$ and Theorem 5.1.39. In this case, $L_R = \langle p \rangle^+$, and $L_R + 1$ is a cyclic group of order p^2, if $p \geq 3$. If $p = 2$, it is isomorphic to E_4. The operation of $L_R + 1$ on L_R is well-known: for $l = pn \in L_R$ and $k = pm + 1 \in L_R + 1$ one has $kl = (pm + 1)pn = p^2mn + pn$. Thus, in the case $p = 2$, $G(R, L_R) \cong E_4 \ltimes C_4$, and for $p \geq 3$, one has $G(R, L_R) \cong C_{p^2} \ltimes C_{p^2}$.

7.3. The case R^+ elementary abelian

First the structure of $L_R + 1$ and how $L_R + 1$ can operate on L_R will be determined.

Let $R^+ = \langle 1,\, a,\, b \rangle$, where $L_R = \langle a,\, b \rangle$. Then for every $r \in R$ the mapping $\alpha_r : R \to R$ with $x\alpha_r = rx$ is an endomorphism of R^+; if $r \in R^\times$, it is even an automorphism. Moreover, if $\alpha_r = \alpha_s$ for $r,\, s \in R$, then $rx = sx$ for all $x \in R$. For $x = 1$ this yields $r = s$. This means that $\alpha : R^\times \to \mathrm{Aut}(R^+) \cong GL(3, p)$, $x \mapsto \alpha_x$ is a monomorphism. Now consider the group $(L_R + 1)^\times$ of order p^2, which is isomorphic to a subgroup of $GL(3, p)$. If $p \geq 3$, by Lemma 7.1.1 $(L_R + 1)^\times$ cannot be cyclic and hence must be elementary abelian. If $p = 2$, $(L_R + 1)^\times$ may also be cyclic.

The next lemma is needed to describe all semidirect products $E_{p^2} \ltimes E_{p^2}$.

7.3.1 Lemma

For every prime p there are exactly two non-isomorphic semidirect products $E_{p^2} \ltimes E_{p^2}$, one of which is abelian.

Proof. Clearly the direct product $E_{p^2} \times E_{p^2}$ is abelian. Thus consider a non-trivial semidirect product $E_{p^2} \ltimes E_{p^2}$. In the following, E_{p^2} will be considered as a 2-dimensional vector space over $\mathbb{F}_p$, and identify the automorphism group of E_{p^2} with $GL(2, p)$.

Let G and H be elementary abelian groups of order p^2, and let $\alpha \in \mathrm{Hom}(G, GL(2, p))$, so that $\mathrm{Ker}(\alpha) \neq G$. Since $|GL(2, p)| = p(p+1)(p-1)^2$, the kernel of α cannot be trivial, i.e. $|\,\mathrm{Ker}(\alpha)| = p$. Thus there is an element $a \in G$ with $a\alpha \neq E$, where E is the identity of $GL(2, p)$ (of course, $o(a\alpha) = p$). Moreover, there is an element $1 \neq b \in G$ with $b\alpha = E$.

Now let $A = a\alpha$. Since $A^p - E = 0$, the minimal polynomial of A is a divisor of $x^p - 1 = (x - q)^p$, and hence the characteristic polynomial of A is $f_a = (x - 1)^2$, so that there is a basis $(x,\, y)$ of H such that the matrix representation of A has triangular form. Moreover, 1 is the only eigenvalue of A. Thus A can be represented by

$$A = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

where $0 \neq n \in \mathbb{F}_p$. Now let $m = n^{-1} \in \mathbb{F}_p$ (or, more precisely, let $m \in \mathbb{N}$ with $nm \equiv 1 \pmod{p}$). Then

$$A^m = (a^m)\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Replacing a by $\tilde{a} := a^m$, one has $G = \langle \tilde{a},\, b \rangle$ and $H = \langle x,\, y \rangle$, and in $G \ltimes H$ it follows that $x^{\tilde{a}} = x$, $x^b = x$, $y^{\tilde{a}} = xy$, and $y^b = y$. Thus every two non-abelian semidirect products $E_{p^2} \ltimes E_{p^2}$ are isomorphic. □

Subcase 1: $p \geq 3$

In this case, $(L_R + 1)^\times$ is elementary abelian. Thus $G(R, L_R) \cong E_{p^2} \ltimes E_{p^2}$. Since there is a large number of nearrings of order p^3, not all local nearrings over E_{p^3} will be determined. But for every possible semidirect product $G = E_{p^2} \ltimes E_{p^2}$ a local nearring R with $R^+ \cong E_{p^3}$ and $G(R, L_R) \cong G$ will be given.

Consider the matrix ring R over $\mathbb{F}_p$ generated by the elements

$$M_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then $o^\times(M_1) = o^\times(M_2) = p$. Then it is not difficult to see that

$$R = \left\{ \begin{pmatrix} n & x & y \\ 0 & n & 0 \\ 0 & 0 & n \end{pmatrix} \;\middle|\; n,\, x,\, y \in \mathbb{F}_p \right\},$$

and hence it is clear that $|R| = p^3$. Since R is a subring of the matrix ring $(\mathbb{F}_p)_3$, it follows that $R^+ \cong E_{p^3}$. Moreover, $L_R = \{M \in R \mid \det(M) = 0\}$, i.e. all matrices in R with zeroes in the main diagonal. Thus it is clear that R is local. Finally, the operation of $(L_R + 1)^\times$ on L_R is trivial, which means that $G(R, L_R) \cong E_{p^2} \times E_{p^2}$.

Next, consider the matrix ring R over $\mathbb{F}_p$ generated by

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Again, it is easy to check that

$$R = \left\{ \begin{pmatrix} n & x & y \\ 0 & n & x \\ 0 & 0 & n \end{pmatrix} \;\middle|\; n,\, x,\, y \in \mathbb{F}_p \right\}$$

is a local nearring with $R^+ \cong E_{p^3}$ and $L_R = \{M \in R \mid \det(M) = 0\}$. Simple calculations show that $L_R = \langle X,\, Y\rangle^+$, where

$$X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

and $L_R + 1 = \langle A,\, B\rangle^\times$, where

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Moreover, it is not difficult to verify that $AX = X$, $AY = X + Y$, $BX = X$, and $BY = Y$, and hence, $G(R, L_R)$ is isomorphic to the non-abelian semidirect product $E_{p^2} \ltimes E_{p^2}$ by Lemma 7.3.1.

Subcase 2: $p = 2$

First consider the groups of the form $E_4 \ltimes E_4$. If R is the subnearring R of $(\mathbb{F}_2)_3$ generated by

$$M_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

then one has

$$R = \left\{ \begin{pmatrix} n & 0 & x \\ 0 & n & y \\ 0 & 0 & n \end{pmatrix} \;\middle|\; n\, x,\, y \in \mathbb{F}_2 \right\}.$$

Here $L_R + 1$ operates trivially on L_R, and it follows that $G(R, L_R) \cong E_4 \times E_4$.

On the other hand, there is no local nearring R with $R^+ \cong E_8$ and $G(R, L_R) = E_4 \ltimes E_4$ non-abelian, as the following lemma and its corollary show.

7.3.2 Lemma

The non-abelian group $G = E_4 \ltimes E_4$ does not have a normal subgroup $M \cong E_4$, which has two complements A and B, such that G is triply factorized by A, B, and M.

Proof. By Lemma 7.3.1 the group G can be written as $\langle a,\, b,\, x,\, y\rangle$ with $x^a = x$, $y^a = xy$, $x^b = x$, and $y^b = y$. Let $M = \langle x,\, y\rangle \trianglelefteq G$, and let $E = \langle a,\, b,\, x\rangle \cong E_8$.

Let U be a subgroup of G which is isomorphic to E_4. If U contains one of the elements x, y, or xy, then $|U \cap M| \geq 2$, and hence U cannot be a complement of M. If U contains one of the elements bx or bxy, then a cannot be contained in U, since U is abelian, but $by^a = bxy$ and $bxy^a = by$. Now y, xy, by, and bxy are the only elements of order 2 of G which are not contained in E. Thus, all complements of M are contained in E. But then, if A and B are complements of M, one has $AB \leq E < G$. This means that G cannot be triply factorized by M and two of its complements. □

7.3.3 Corollary
Let R be a local nearring with $R \cong E_8$ and ${L_R}^+ \cong (L_R+1)^\times \cong E_4$. Then $(k+1)l = l$ for all k, $l \in L_R$ and hence $G(R, L_R) \cong E_4 \times E_4$.

Proof. By Lemma 7.3.2 there is no nearring R which has a construction subgroup U such that $U^+ \cong (U+1)^\times \cong E_4$ and the operation of $U+1$ on U is non-trivial. □

In order to find local nearrings R with $R^+ \cong E_8$ and a cyclic group $(L_R+1)^\times$, in the following lemma all possible semidirect products $C_4 \ltimes E_4$ are determined.

7.3.4 Lemma
Up to isomorphism there are exactly two different semidirect products $C_4 \ltimes E_4$, one of which is abelian.

Proof. Obviously, the direct product $C_4 \times E_4$ is abelian. Hence it suffices to show that all non-trivial semidirect products $C_4 \ltimes E_4$ are isomorphic.

Let $G = \langle a \rangle \cong C_4$, $H \cong E_4$, and let $\alpha : G \to \mathrm{Aut}(H) \cong GL(2,2)$ be a non-trivial homomorphism, so that $a\alpha$ is not the identity mapping on H. Since $|GL(2,2)| = 6$, one has $o(a\alpha) = 2$. Hence, as in the proof of Lemma 7.3.1, one can find elements x, $y \in H$ such that $x^a = x$ and $y^a = xy$. Thus every two non-trivial semidirect products $C_4 \ltimes E_4$ are isomorphic. □

If R is a local nearring with ${L_R}^+ \cong E_4$ and $(L_R+1)^\times \cong C_4$, then L_R+1 cannot operate trivially on ${L_R}^+$ by Proposition 3.1.5. Moreover, it is easy to see that the group $C_4 \times E_4$ is not triply factorized. Thus only the group $C_4 \ltimes E_4$ can occur as $G(R, L_R)$. Let

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in (\mathbb{F}_2)_3.$$

Then $o^\times(M) = 4$ and the subring R of $(\mathbb{F}_2)_3$ generated by M has order 8. More precisely,

$$R = \left\{ \begin{pmatrix} n & x & y \\ 0 & n & x \\ 0 & 0 & n \end{pmatrix} \;\middle|\; n,\, x,\, y \in \mathbb{F}_2 \right\},$$

and it is easy to see that R is in fact a local nearring with ${L_R}^+ \cong E_4$ and $(L_R+1)^\times \cong C_4$. Hence $G(R, L_R) \cong C_4 \ltimes E_4$ is a non-trivial semidirect product.

7.4. The case R^+ abelian of exponent p^2

If $\exp(R^+) = p^2$ and R^+ is abelian, then

$$R^+ = \left\langle 1,\, a \;\middle|\; 1 \cdot p^2 = a \cdot p = [1, a] = 0 \right\rangle. \tag{7.1}$$

In this case, $L_R = \langle p,\, a\rangle$, i.e. ${L_R}^+ \cong E_{p^2}$. By Lemma 7.1.1 $(L_R + 1)^\times$ is elementary abelian if $p \geq 3$.

The first lemma in this section gives a criterion for a ring over the additive group given in (7.1) to be local.

7.4.1 Lemma

Let R be a ring over the group given in (7.1), *where the multiplication is given by $1 \cdot x = x \cdot 1 = x$ for all $x \in R$ and the product $a \cdot a$ (note that a ring over an abelian group is determined uniquely if the products of the generators of the group are known). If $a \cdot a \in \langle p\rangle^+$, R is local with $L_R = \langle a,\, 1 \cdot p\rangle^+$.*

Proof. Let $a \cdot a \in \langle p\rangle^+$, so that $a \cdot a = pt$ for some $t \in \mathbb{Z}$. Since the elements of $\langle p\rangle^+$ cannot be invertible because of $p^2 = 0$, it suffices to show that every $x \in R \setminus \langle a,\, p\rangle^+$ has a multiplicative inverse. Let $x \in R \setminus \langle a,\, p\rangle^+$, so that $x = n + am$ for some $n,\, m \in \mathbb{Z}$ and $p \nmid n$. Then

$$x^k = n^k + \sigma(k)ptm^2n^{k-2} + akmn^{k-1}$$

for $k \geq 2$, where $\sigma(k) = \frac{k(k-1)}{2}$, i.e. $\sigma(1) = 0$ and $\sigma(k+1) = k + \sigma(k)$. This can be seen by induction as follows. First,

$$\begin{aligned} x^2 = (n+am)^2 \qquad\qquad &= n^2 + a \cdot 2nm + a^2m^2 \\ = n^2 + ptm^2 + a \cdot 2mn &= n^2 + \sigma(2)ptmn^0 + a \cdot 2mn^2. \end{aligned}$$

Now, let $k \geq 2$. Then

$$\begin{aligned} x^{k+1} &= x \cdot x^k \\ &= (n+am)\left(n^k + \sigma(k)ptm^2n^{k-2} + akmn^{k-1}\right) \\ &= n^{k+1} + \sigma(k)ptm^2n^{k-1} + akmn^k \\ &\quad + amn^k + \underbrace{ap\sigma(k)tm^3n^{k-2}}_{=0} + \underbrace{a^2km^2n^{k-1}}_{=ptkm^2n^{k-1}} \\ &= n^{k+1} + ptm^2n^{k-1}(\sigma(k) + k) + a(k+1)mn^k \\ &= n^{k+1} + \sigma(k+1)ptm^2n^{k-1} + a(k+1)mn^k. \end{aligned}$$

Since $|R \setminus \langle a,\, p\rangle^+| = p^3 - p^2 = p^2(p-1)$, it follows that

$$\begin{aligned} x^{p^2(p-1)} &= n^{p^2(p-1)} + \sigma(p^2(p-1))ptm^2n^{p^2(p-1)-2} + \underbrace{ap^2(p-1)mn^{p^2(p-1)-1}}_{=0} \\ &= n^{p^2(p-1)} + \frac{p^2(p-1)(p^2(p-1)-1)}{2} \cdot ptm^2n^{p^2(p-1)-2} \\ &= n^{p^2(p-1)} + \frac{p(p-1)}{2} \cdot \underbrace{p^2(p^2(p-1)-1)tm^2n^{p^2(p-1)-2}}_{=0} \\ &= n^{p^2(p-1)}. \end{aligned}$$

But since $P_R \cong \mathbb{Z}/p^2\mathbb{Z}$ and so $|{P_R}^\times| = p^2 - p = p(p-1)$, one has $n^{p^2(p-1)} = 1$ because of $n \in {P_R}^\times$, i.e. $x^{p^2(p-1)} = 1$. This means that x is invertible, and hence $L_R = \langle a,\, p\rangle^+$. Thus it follows that R is a local ring. □

By Lemma 7.1.1 $L_R + 1$ is elementary abelian, if $p \geq 3$. If $p = 2$ and $L_R + 1$ is elementary abelian, by Lemma 7.3.2 the operation of $L_R + 1$ on L_R must be trivial. For every prime p, a nearring R with $G(R, L_R) \cong E_{p^2} \times E_{p^2}$ is for instance given by the ring with multiplication defined by $1 \cdot 1 = 1$, $1 \cdot a = a \cdot 1 = a$, and $a \cdot a = 0$, where 1 and a are the generators of R^+ given in (7.1) (this ring is local by Lemma 7.4.1).

If $p \geq 3$, the operation of $L_R + 1$ on L_R need not be trivial. Consider for example the ring given by the multiplication defined via $a^2 = p$, which is again local by Lemma 7.4.1. In this case, $a^3 = 0$, and hence $l^3 = 0$ for all $l \in L_R$, since

$$(an + pm)^3 = a^3n^3 + a^2n^2pm \cdot 3 + anp^2m^2 \cdot 3 + p^3m^3 = 0$$

for $0 \leq n,\, m < p$. Moreover, $(an + pm)^2 = a^2n^2 + anpm \cdot 2 + p^2m^2 = a^2n^2 = n^2 \cdot p$.

Now

$$(a+1)^n = \sum_{i=0}^{n} a^i \binom{n}{i} = a^2\binom{n}{2} + a\binom{n}{1} + \binom{n}{0} = \frac{n(n-1)}{2} \cdot p + an + 1$$

for $n \geq 2$, and

$$\begin{aligned}(a+p+1)^n = \sum_{i=0}^{n} (a+p)^i \binom{n}{i} \qquad &= (a+p)^2\binom{n}{2} + (a+p)\binom{n}{1} + \binom{n}{0} \\ = \frac{n(n-1)}{2} \cdot p + an + pn + 1 &= \frac{n(n+1)}{2} \cdot p + an + 1.\end{aligned}$$

Thus, if $(a+1)^n = (a+p+1)^m$ for $n,\, m \in \mathbb{Z}$, one has

$$\begin{aligned} & \frac{n(n-1)}{2} \cdot p + an + 1 = \frac{m(m+1)}{2} \cdot p + am + 1 \\ \iff \quad & \left(\frac{n(n-1)}{2} - \frac{m(m+1)}{2}\right) \cdot p = a(m-n) \in \langle p\rangle \cap \langle a\rangle \,. \end{aligned}$$

Since $\langle p\rangle \cap \langle a\rangle = \{0\}$, it follows that $a(n-m) = 0$ and hence $n \equiv m \pmod{p}$. Thus $\langle a+1\rangle^\times \cap \langle a+p+1\rangle^\times = \{1\}$ and so $L_R + 1 = \langle a+1, a+p+1\rangle$. But

$$(a+1)a = a^2 + a = p + a \neq a,$$

which means that $L_R + 1$ operates non-trivially on L_R. Thus $G(R, L_R) = E_{p^2} \times E_{p^2}$.

If $p = 2$, $L_R + 1$ may also be cyclic. Again consider the ring defined by $a^2 = 2$. Then $L_R + 1$ is cyclic, since $(a+1)^2 = a^2 + a \cdot 2 + 1 = 2 + 1 = 3 \neq 1$.

7.5. The case R^+ non-abelian of exponent p

In this case $p \geq 3$, since groups of exponent 2 are always abelian. As there is (up to isomorphism) exactly one non-abelian group of order p^3 and exponent p for every odd prime p, in this case $R^+ = \left\langle a,\, b \;\middle|\; a \cdot p = b \cdot p = 0,\, [a,b]^a = [a,b]^b = [a,b] \right\rangle$. Now $(R^+)'$ is always a left R-subgroup of the nearring R. Therefore in a local nearring the group $(R^+)'$ must be contained in L_R unless R^+ is a perfect group by Lemma 5.1.27.(a). Since finite p-groups are not perfect, in a finite local nearring R one must have $1 \notin (R^+)'$. This means that without loss of generality

$$R^+ = \left\langle 1,\, a \;\middle|\; 1 \cdot p = a \cdot p = 0,\, [1,a]^1 = [1,a]^a = [1,a] \right\rangle, \tag{7.2}$$

so that $L_R = \langle a,\, [1,a] \rangle^+$. Since $x \cdot 1 = x$ for every $x \in R$ and because of the left distributivity of R, the multiplication of R is determined uniquely, whenever $x \cdot a$ is known for all $x \in R$. Moreover, $P_R \cap \langle a,\, [1,a] \rangle^+ = \{0\}$. Thus for all $x \in R$ there is an $n \in P_R$ and an $l \in L_R$ such that $x = n + l$.

Since R^+ is a nilpotent group of class 2, the following rules hold for all $x,\, y,\, z \in R$ and all $n \in P_R$:

$$\begin{aligned} [x+y,z] &= [x,z] + [y,z], & [x,y+z] &= [x,y] + [x,z], \\ [xn,y] &= [x,y]n = [x,yn], & [x,y] &\in \mathbf{Z}(R^+). \end{aligned}$$

In the following these relations are used without further reference.

By Lemma 7.1.1 the group $(L_R + 1)^\times$ must be elementary abelian. Hence in this case $G(R, L_R)$ can only be a semidirect product of the form $E_{p^2} \ltimes E_{p^2}$.

7.5.1 Theorem
Let R be a nearring whose additive group is as in (7.2) *and whose multiplication is given by $1 \cdot x = x \cdot 1 = x$ for all $x \in R$ and $(n + l)a = an$ for all $n \in P_R = \langle 1 \rangle^+$ and all $l \in \langle a,\, [1,a] \rangle^+$. Then R is a local nearring with $L_R = \langle a,\, [1,a] \rangle^+$, and $G(R, L_R) \cong E_{p^2} \times E_{p^2}$.*

Proof. By the definition of the multiplication one has $na = an$ for all $n \in P_R$. Moreover, for all $x,\, y,\, z \in R$ the identity $x[y,z] = [xy, xz]$ holds in every nearring R.

By the left distributive law this multiplication can be extended to the whole group R^+. Now has only to be checked that the associative law holds. This is now done in several steps. Since $p \geq 3$, one has $2 \in {P_R}^\times$. Let $z = 2^{-1} \in P_R$, and let $L = \langle a,\, [1,a] \rangle^+$. Note that L is an abelian group.

(1) $(n + k)[1,a] = [1,a]n^2$ for all $n \in P_R$ and $l \in L$:

$$\begin{aligned} (n+k)[1,a] = [n+k, (n+k)a] &= [n+k, an] &&= [n,an] + [k,an] \\ = [n,an] \qquad\qquad &= [n,a]n &&= [1,a]n^2. \end{aligned}$$

(2) $(n+k)[1,a] = n[1,a]$ for all $n \in P_R$ and $k \in L$:

$(n+k)[1,a] = [n+k, an] = [n, na] + [k, na] = n[1,a]$.

(3) $(n+k)l = nl$ for all $n \in P_R$ and $l \in L$:

Let $l = ax + [1,a]y \in L$ with x, $y \in P_R$. Then

$$\begin{aligned}(n+k)l &= (n+k)(ax+[1,a]y) = (n+k)(ax) + (n+k)([1,a]y)\\ &\overset{(2)}{=} nax + n[1,a]y \qquad\quad = n(ax+[1,a]y)\\ &= nl.\end{aligned}$$

(4) $(n+k)m = nm + km + [k,n]zm(m-1)$ for all n, $m \in P_R$ and $k \in L$:

Since $m \in P_R$, there is a positive integer $\tilde{m}$ with $m = 1 \cdot \tilde{m}$. Apply induction on $\tilde{m}$. For $\tilde{m} = 1$ one has $m = 1$ and hence $nm+km+[k,n]zm(m-1) = n+k+0 = n+k$. Now let $\tilde{m} \geq 1$. Then $m+1 = 1 \cdot (\tilde{m}+1)$ and one has

$$\begin{aligned}(n+k)(m+1) &= (n+k)m + n + k\\ &= nm + km + [k,n]zm(m-1) + n + k\\ &= nm + km + n + k + [k,n]zm(m-1)\\ &= nm + n + km + k + [km,n] + [k,n]zm(m-1)\\ &= n(m+1) + k(m+1) + [k,n]m + [k,n]zm(m-1)\\ &= n(m+1) + k(m+1) + [k,n](m + zm(m-1))\\ &= n(m+1) + k(m+1) + [k,n](2zm + zm(m-1))\\ &= n(m+1) + k(m+1) + [k,n]zm(2+m-1)\\ &= n(m+1) + k(m+1) + [k,n]zm(m+1)\\ &= n(m+1) + k(m+1) + [k,n]z(m+1)m\end{aligned}$$

(5) $(n+k)(m+l) = nm+km+nl+[k,n]zm(m-1)$ for all n, $m \in P_R$ and all k, $l \in L$:

$(n+k)(m+l) = (n+k)m + (n+k)l = nm + km + [k,n]zm(m-1) + nl = nm + km + nl + [k,n]zm(m-1)$ by (3) and (4).

(6) $\big((n+k)(m+l)\big)\,h = nmh$ for all n, $m \in P_R$ and all k, l, $h \in L$:

This follows immediately from (5) and (3).

(7) For every n, m, $r \in P_R$ and every k, $l \in L$ the following holds:

$$\begin{aligned}&\big((n+k)(m+l)\big)\,r\\ &= nmr + kmr + nlr + \big[k\,\big(zr(m-1) + mzr(r-1)\big) + nlzr(r-1), nm\big] :\end{aligned}$$

By (4) and (5) one has

$$\begin{aligned}
&\big((n+k)(m+l)\big)\, r\\
&\overset{(5)}{=} \big(nm+km+nl+\big[k,n\big]\, zm(m-1)\big)\, r\\
&\overset{(4)}{=} nmr+kmr+nlr+\big[k,n\big]\, zmr(m-1)+\big[km+nl,nm\big]\, zr(r-1)\\
&= nmr+kmr+nlr+\big[k,nm\big]\, zr(m-1)+\big[(km+nl)zr(r-1),nm\big]\\
&= nmr+kmr+nlr+\big[kzr(m-1),nm\big]+\big[kmzr(r-1)+nlzr(r-1),nm\big]\\
&= nmr+kmr+nlr+\big[kzr(m-1)+kmzr(r-1)+nlzr(r-1),nm\big]\\
&= nmr+kmr+nlr+\big[k\left(zr(m-1)+mzr(r-1)\right)+nlzr(r-1),nm\big]
\end{aligned}$$

(8) For every n, m, $r \in P_R$ and every k, l, $h \in L$ the following holds:

$$\begin{aligned}
&\big((n+k)(m+l)\big)\,(r+h)\\
&= nmr+kmr+nlr+nmh+\big[k\left(zr(m-1)+zmr(r-1)\right)+nlzr(r-1),nm\big]
\end{aligned}$$

This follows immediately from (6) and (7).

(9) For every n, m, $r \in P_R$ and every k, l, $h \in L$ the following holds:

$$\begin{aligned}
&(n+k)\,\big((m+l)(r+h)\big)\\
&= nmr+kmr+nlr+nmh+\big[nlzr(r-1)+kzr(mr-1),nm\big]
\end{aligned}$$

Using (5) one obtains

$$\begin{aligned}
&(n+k)\,\big((m+l)(r+h)\big)\\
&= (n+k)\,\big(mr+lr+mh+\big[l,m\big]\, zr(r-1)\big)\\
&= nmr+kmr+n\left(lr+mh+\big[l,m\big]\, zr(r-1)\right)+\big[k,n\big]\, zmr(mr-1)\\
&= nmr+kmr+nlr+nmh+\big[nl,nm\big]\, zr(r-1)+\big[k,nm\big]\, zr(mr-1)\\
&= nmr+kmr+nlr+nmh+\big[nlzr(r-1)+kzr(mr-1),nm\big]
\end{aligned}$$

(10) Since $zr(m-1)+zmr(r-1)=zr(mr-1)$, the multiplication on R is associative by (8) and (9).

By the definition of the multiplication it is clear that $kl = 0$ for all k, $l \in L$. Hence the elements of L cannot be right invertible. Thus it suffices to show that $R^\times = R \setminus L$ in order to see that R is local with $L_R = L$.

Let $x \in R \setminus L$. Then there are elements $n \in {P_R}^\times$ and $l \in L$ such that $x = n + l$. Moreover, there exists an $m \in {P_R}^\times$ with $nm = 1$. Then

$$\begin{aligned}&(n+k)\big(m - mkm - \big[mk,1\big]\, zm(m-1)\big)\\ &\overset{(5)}{=} nm + km - nmkm - \big[nmk,n\big]\, zm(m-1) + \big[k,n\big]\, zm(m-1)\\ &= 1 + km - km - \big[k,1\big]\, z(m-1) + \big[k,1\big]\, z(m-1)\\ &= 1\end{aligned}$$

Hence x is right invertible, and this means that R is a local nearring with $L_R = L$. Moreover, for every k, $l \in L$ by the definition of the multiplication it follows

$$(k+1)l = (1 + k + [k,1])l = l,$$

i.e. $L_R + 1$ operates trivially on L_R. Thus $G(R, L_R) \cong E_{p^2} \times E_{p^2}$. □

7.5.2 Theorem

Let R be a nearring with R^+ as in (7.2) and multiplication given by $1 \cdot x = x \cdot 1 = x$ for all $x \in R$ and $(an + cm + k)a = ak^2 + ckn$, where $c = [1, a]$, and n, m, $k \in \mathbb{N}$. Then R is a local nearring with $L_R = \langle a,\, [1,a]\rangle^+$, and $G(R, L_R)$ is isomorphic to the non-trivial semidirect product $E_{p^2} \ltimes E_{p^2}$.

Proof. It is clear that every $x \in R$ can be written as $an + cm + 1 \cdot k = an + cm + k$, where $c = [1, a]$ and n, m, $k \in \mathbb{N}$ are unique modulo p, and that the given rules lead to a well-defined multiplication which is left distributive. It has only to be checked that the multiplication is associative. This is done in several steps.

(1) $(an + cm + k)c = ck^3$:

$$\begin{aligned}(an+cm+k)c &= (an+cm+k)[1,a] &&= [an+cm+k, (an+cm+k)a]\\ &= [an+k, ak^2+ckn] &&= [an+k, ak^2]\\ &= [an, ak^2] + [k, ak^2] &&= [k, ak^2]\\ &= [1,a]k^3 &&= ck^3.\end{aligned}$$

(2) $(an + cm + k)r = anr + c\left(mr + kn\frac{r(r-1)}{2}\right) + kr$ for all $r \in \mathbb{N}_0$:

Apply induction on r. For $r = 0$ this is clear. Thus let $r > 0$. Then

$$\begin{aligned}(an+cm+k)r &= (an+cm+k)(r-1+1)\\ &= an(r-1) + c\left(m(r-1) + kn\frac{(r-1)(r-2)}{2}\right) + k(r-1)\\ &\quad + an + cm + k\end{aligned}$$

$$\begin{aligned}
&= an(r-1) + c\left(mr + kn\frac{(r-1)(r-2)}{2}\right) + an \\
&\quad + k(r-1) + [k(r-1), an] + k \\
&= anr + c\left(mr + kn\frac{(r-1)(r-2)}{2}\right) + [1,a]k(r-1)n + kr \\
&= anr + c\left(mr + kn\left(\frac{(r-1)(r-2)}{2} + r - 1\right)\right) + kr \\
&= anr + c\left(mr + kn\frac{r(r-1)}{2}\right) + kr
\end{aligned}$$

(3) $(an+cm+k)(ar+cs+t) = a\left(k^2r+nt\right) + c\left(knr + k^3s + mt + kn\frac{t(t-1)}{2}\right) + kt$:

$$\begin{aligned}
&(an+cm+k)(ar+cs+t) \\
&= (an+cm+k)ar + (an+cm+k)cs + (an+cm+k)t \\
&= \left(ak^2 + ckn\right)r + ck^3s + ant + c\left(mt + kn\frac{t(t-1)}{2}\right) + kt \\
&= ak^2r + cknr + ck^3s + ant + c\left(mt + kn\frac{t(t-1)}{2}\right) + kt \\
&= a\left(k^2r + nt\right) + c\left(knr + k^3s + mt + kn\frac{t(t-1)}{2}\right) + kt
\end{aligned}$$

(4) The multiplication is associative:

Let $an+cm+k$, $ar+cs+t$, $ax+cy+z \in R$. Then, on one hand,

$$\begin{aligned}
&\left((an+cm+k)(ar+cs+t)\right)(ax+cy+z) \\
&= \left(a\left(k^2r+nt\right) + c\left(knr + k^3s + mt + kn\frac{t(t-1)}{2}\right) + kt\right)(ax+cy+z) \\
&= a\left(k^2t^2x + k^2rz + ntz\right) \\
&\quad + c\left(kt\left(k^2r+nt\right)x + k^3t^3y + \left(knr + k^3s + mt + kn\frac{t(t-1)}{2}\right)z\right. \\
&\qquad \left. + kt\left(k^2r+nt\right)\frac{z(z-1)}{2}\right) \\
&\quad + ktz
\end{aligned}$$

$$\begin{aligned}
&= a\left(k^2t^2x + k^2rz + ntz\right) \\
&\quad + c\left(k^3rtx + nkt^2x + k^3t^3y + nkrz + k^3sz + mtz + nktz\frac{t-1}{2}\right. \\
&\qquad\left. + k^3rtz\frac{z-1}{2} + nkt^2z\frac{z-1}{2}\right) \\
&\quad + ktz \\
&= a\left(k^2t^2x + k^2rz + ntz\right) \\
&\quad + c\left(k^3rtx + nkt^2x + k^3t^3y + nkrz + k^3sz + mtz\right. \\
&\qquad\left. + k^3rtz\frac{z-1}{2} + nktz\left(\frac{t-1}{2} + \frac{t(z-1)}{2}\right)\right) \\
&\quad + ktz \\
&= a\left(k^2t^2x + k^2rz + ntz\right) \\
&\quad + c\left(k^3rtx + nkt^2x + k^3t^3y + nkrz + k^3sz + mtz\right. \\
&\qquad\left. + k^3rtz\frac{z-1}{2} + nktz\frac{tz-1}{2}\right) \\
&\quad + ktz,
\end{aligned}$$

and on the other hand,

$$\begin{aligned}
&(an + cm + k)\left((ar + cs + t)(ax + cy + z)\right) \\
&= (an + cm + k)\left(a\left(t^2x + rz\right) + c\left(trx + t^3y + sz + tr\frac{z(z-1)}{2}\right) + tz\right) \\
&= a\left(k^2t^2x + k^2rz + ntz\right) \\
&\quad + c\left(kn\left(t^2x + rz\right) + k^3\left(trx + t^3y + sz + tr\frac{z(z-1)}{2}\right)\right. \\
&\qquad\left. + mtz + kn\frac{tz(tz-1)}{2}\right) \\
&\quad + ktz \\
&= a\left(k^2t^2x + k^2rz + ntz\right) \\
&\quad + c\left(nkt^2x + nkrz + k^3rtx + k^3t^3y + k^3sz + k^3rtz\frac{z-1}{2}\right. \\
&\qquad\left. + mtz + nktz\frac{tz-1}{2}\right) \\
&\quad + ktz
\end{aligned}$$

It is easy to see that these two expressions are equal. Thus R is a left nearring under the given multiplication.

Furthermore $L_R = \langle a,\, c\rangle$, since for $k \not\equiv 0 \pmod p$ the inverse of $an+cm+k$ is $ar+cs+t$, where $t \in \mathbb{N}$ with $kt \equiv 1 \pmod p$, $r \equiv -nt^3 \pmod p$, and $s \equiv -t^2nr - mt^4 - n\frac{t^3(t-1)}{2}$ (mod p). For $k = 0$ the element $an + cm + k$ cannot be right invertible. Hence the nearring R is local.

It is clear that $|L_R + 1| = p^2$. From Lemma 7.1.1 it follows that $(L_R + 1)^\times \cong E_{p^2}$. Moreover, it is easy to see that $(a+1)a = a+c$. Hence the semidirect product $G(R, L_R)$ is non-trivial. □

7.6. The case R^+ non-abelian of exponent p^2

If R^+ is non-abelian of exponent p^2, the case $p = 2$ is impossible, since there are no local nearrings over Q_8 (c.f. Malone [14, Corollary 4]) or D_8 (c.f. Corollary 5.2.11).

Hence $p \geq 3$ and $R^+ = \left\langle a,\, b \;\middle|\; a \cdot p^2 = b \cdot p = 0,\, a^b = a \cdot (p+1)\right\rangle$. Since $o^+(1) = \exp(R^+)$ in every nearring by Corollary 2.1.15, one has without loss of generality

$$R^+ = \left\langle 1,\, b \;\middle|\; p^2 = b \cdot p = 0,\, -b + 1 + b = p + 1\right\rangle . \tag{7.3}$$

In this case, $[1, b] = p$. If R is a local nearring over the additive group given in (7.3), it is clear that $b \in L_R$; moreover, one has $L_R = \langle b,\, p\rangle$. Furthermore, $L_R + 1$ is elementary abelian by Lemma 7.1.1. Since $(p + 1)^n = pn + 1$ for all $n \in \mathbb{N}$ (this holds since $P_R \cong \mathbb{Z}/p^2\mathbb{Z}$), one has $(L_R + 1)^\times = \langle b + 1,\, p + 1\rangle$. As in Section 7.5, R^+ is a nilpotent group of class 2, such that the following rules hold for all $x,\, y,\, z \in R$ and all $n \in P_R$ and will be used without further reference:

$$\begin{aligned} &[x + y, z] = [x, z] + [y, z], && [x, y + z] = [x, y] + [x, z], \\ &[xn, y] = [x, y]n = [x, yn], && [x, y] \in \mathbf{Z}(R^+). \end{aligned}$$

For the understanding of the structure of local nearrings over R^+ as in (7.3), the following calculation rules are useful.

7.6.1 Lemma

Let R be a local nearring over the additive group given in (7.3). Then the following holds:

(a) For all $n,\, k,\, r \in \mathbb{N}_0$ one has

$$(bn + k)r = bnr + k\left(r + pn\frac{r\,(r-1)}{2}\right) \tag{7.4}$$

Note that every element of R^+ can be written as $bn + k$ for suitable n and k.

(b) $(b+1)p = p$

(c) $(p+1)p = p$

(d) $(p+1)b = b$

(e) *There is an element* $x \in \mathbb{F}_p$ *such that*

$$(b+1)b = b + px. \tag{7.5}$$

This x *will be fixed until the end of this section.*

(f) $(b+1)^k b = b + pkx$ *for all* $k \in \mathbb{N}_0$.

(g) $(b+1)^n = bn + px\frac{n(n-1)}{2} + 1$ *for all* $n \in \mathbb{N}_0$.

(h) $(b+1)^k(p+1)^l = bk + p\left(l + x\frac{k(k-1)}{2}\right)$.

Proof. (a) For $r = 0$ this is trivial. Now let $r \geq 1$. Then

$$\begin{aligned}
(bn+k)r &= (bn+k)(1+r-1)\\
&= bn + k + (bn+k)(r-1)\\
&= bn + k + bn(r-1) + k\left(r - 1 + pn\frac{(r-1)(r-2)}{2}\right)\\
&= bn + bn(r-1) + k + [k, bn(r-1)] + k\left(r - 1 + pn\frac{(r-1)(r-2)}{2}\right)\\
&= bnr + k + \underbrace{[1,b]}_{=p} kn(r-1) + k\left(r - 1 + pn\frac{(r-1)(r-2)}{2}\right)\\
&= bnr + k\left(1 + pn(r-1) + r - 1 + pn\frac{(r-1)(r-2)}{2}\right)\\
&= bnr + k\left(r + pn\left(\frac{(r-1)(r-2)}{2} + r - 1\right)\right)\\
&= bnr + k\left(r + pn\frac{(r-1)(r-2) + 2(r-1)}{2}\right)\\
&= bnr + k\left(r + pn\frac{r(r-1)}{2}\right).
\end{aligned}$$

(b) This follows immediately from (a).

(c) Since P_R is a ring one has $(p+1)p = p^2 + p = p$.

(d) Since $(L_R+1)^\times \cong E_{p^2}$ is an abelian group, one obtains

$$\begin{aligned} && (p+1)(b+1) &= (b+1)(p+1) \\ \iff && (p+1)b+p+1 &= (b+1)p+b+1 \\ \iff && (p+1)b+p+1 &= p+b+1 \\ \iff && (p+1)b &= p \end{aligned}$$

(e) Since $b \in L_R$, it is clear that there are elements x_1, $x \in \mathbb{F}_p$ such that $(b+1)b = bx_1 + px \in L_R$. Using (b) it follows

$$\begin{aligned} p = (b+1)p \quad &= (b+1)[1,b] = [b+1,(b+1)b] \\ = [b+1, bx_1+px] &= [b+1, bx_1] \;\; = [b, bx_1] + [1, bx_1] \\ = [1,b]x_1 \quad &= px_1 \end{aligned}$$

Thus $x_1 = 1$.

(f) This follows by induction immediately from (e).

(g) For $n = 0$ this is clear. So let $n \geq 1$. Then

$$\begin{aligned} (b+1)^n &= (b+1)(b+1)^{n-1} \\ &= (b+1)\left(b(n-1) + px\frac{(n-1)(n-2)}{2} + 1\right) \\ &= (b+1)b(n-1) + (b+1)px\frac{(n-1)(n-2)}{2} + b + 1 \\ &\overset{(e)}{=} (b+px)(n-1) + px\frac{(n-1)(n-2)}{2} + b + 1 \\ &= b(n-1) + px\left(n - 1 + \frac{(n-1)(n-2)}{2}\right) + b + 1 \\ &= bn + px\frac{n(n-1)}{2} + 1 \end{aligned}$$

(h) Using the previous rules, one obtains

$$\begin{aligned} (b+1)^k(p+1)^l &= (b+1)^k(pl+1) \\ &= (b+1)^k pl + (b+1)^k \\ &= pl + bk + px\frac{k(k-1)}{2} + 1 \\ &= bk + p\left(l + x\frac{k(k-1)}{2}\right) + 1. \end{aligned}$$ □

It is well-known that $(\mathbb{Z}/p^2\mathbb{Z})^\times \cong C_{p(p-1)}$. Hence there is an element $z \in {P_R}^\times$ with $o^\times(z) = p-1$. Since $zb \in L_R$, there are elements y_1, $y \in \mathbb{F}_p$ with $zb = by_1 + py$. But

$$\begin{aligned} pz = zp \qquad\qquad &= z[1,b] \;= [z, zb] \;\;\; = [z, by_1 + py] \\ = [z, by_1] + [z, py] &= [z, by_1] = [1,b]zy_1 = pzy_1, \end{aligned}$$

and hence $y_1 = 1$. This means that

$$zb = b + py, \tag{7.6}$$

which leads to the following.

$$\begin{aligned} z^{-1}(b+1)z &= \left(z^{-1}b + z^{-1}\right) z \\ &= \left(b - pyz^{-1} + z^{-1}\right) z \\ &= bz + \left(z^{-1} - pyz^{-1}\right)\left(z + p\frac{z(z-1)}{2}\right) \\ &= bz - py + p\frac{z-1}{2} + 1 \end{aligned}$$

On the other hand, by Lemma 7.6.1 (h)

$$\begin{aligned} (b+1)^z(p+1)^{(1-xz)\frac{z-1}{2}-y} &= (b+1)^z\left(p\left((1-xz)\frac{z-1}{2} - y\right) + 1\right) \\ &= p\left((1-xz)\frac{z-1}{2} - y\right) + (b+1)^z \\ &= p\left((1-xz)\frac{z-1}{2} - y\right) + bz + px\frac{z(z-1)}{2} + 1 \\ &= bz + p\left(\frac{z-1}{2} - x\frac{z(z-1)}{2} - y + x\frac{z(z-1)}{2}\right) + 1 \\ &= bz + p\left(\frac{z-1}{2} - y\right) + 1 \\ &= bz - py + p\frac{z-1}{2} + 1. \end{aligned}$$

Hence

$$z^{-1}(b+1)z = (b+1)^z(p+1)^{(1-xz)\frac{z-1}{2}-y}. \tag{7.7}$$

7.6.2 Theorem

(a) For every prime $p \geq 3$ there is a local nearring R over R^+ given in (7.3) such that $G(R, L_R) = E_{p^2} \times E_{p^2}$, i.e. $L_R + 1$ operates trivially on L_R.

(b) For $p = 3$ there is a local nearring R over R^+ such that $L_R + 1$ operates non-trivially on L_R. For $p \geq 5$ there is no local nearring over R^+ with a non-trivial operation of $L_R + 1$ on L_R.

PROOF. (a) Defining $rb = b$ for all $r \in R$, the left distributive law yields

$$\begin{aligned}(bn+l)(br+k) &= (bn+l)br + (bn+l)k \\ &\overset{(7.4)}{=} br + bnk + l\left(k + pn\frac{k(k-1)}{2}\right) \\ &= b(r+nk) + pnl\frac{k(k-1)}{2} + lk.\end{aligned}$$

The associativity of this multiplication has to be checked. For A, B, C, D, E, $F \in \mathbb{N}$ one has on one hand

$$\begin{aligned}&((bA+B)(bC+D))(bE+F) \\ &= \left(b\left(C+AD\right) + pAB\frac{D\left(D-1\right)}{2} + BD\right)\left(bE+F\right) \\ &= b\left(E+CF+ADF\right) \\ &\quad + p\left(C+AD\right)\left(pAB\frac{D\left(D-1\right)}{2} + BD\right)\frac{F\left(F-1\right)}{2} \\ &\quad + \left(pAB\frac{D\left(D-1\right)}{2} + BD\right)F \\ &= b\left(E+CF+ADF\right) \\ &\quad + p\left(C+AD\right)BD\frac{F\left(F-1\right)}{2} + pABF\frac{D\left(D-1\right)}{2} + BDF \\ &= b\left(E+CF+ADF\right) \\ &\quad + p\left(BCD\frac{F\left(F-1\right)}{2} + ABD^2\frac{F\left(F-1\right)}{2} + ABF\frac{D\left(D-1\right)}{2}\right) \\ &\quad + BDF \\ &= b\left(E+CF+ADF\right) \\ &\quad + p\left(BCD\frac{F\left(F-1\right)}{2} + ABDF\left(\frac{DF-D}{2} + \frac{D-1}{2}\right)\right) \\ &\quad + BDF \\ &= b\left(E+CF+ADF\right) + p\left(BCD\frac{F\left(F-1\right)}{2} + ABDF\frac{DF-1}{2}\right) + BDF,\end{aligned}$$

and on the other hand

$$\begin{aligned}&(bA+B)((bC+D)(bE+F)) \\ &= (bA+B)\left(b\left(E+CF\right) + pCD\frac{F\left(F-1\right)}{2} + DF\right)\end{aligned}$$

$$
\begin{aligned}
&= b\left(E + CF + A\left(pCD\frac{F(F-1)}{2} + DF\right)\right) \\
&\quad + pAB\frac{\left(pCD\frac{F(F-1)}{2} + DF\right)\left(pCD\frac{F(F-1)}{2} + DF - 1\right)}{2} \\
&\quad + B\left(pCD\frac{F(F-1)}{2} + DF\right) \\
&= b(E + CF + ADF) \\
&\quad + pAB\frac{DF(DF-1)}{2} + pBCD\frac{F(F-1)}{2} + BDF \\
&= b(E + CF + ADF) + p\left(BCD\frac{F(F-1)}{2} + ABDF\frac{DF-1}{2}\right) + BDF.
\end{aligned}
$$

Thus the multiplication is associative. Moreover, since $(p+1)p = p$, $(p+1)b = b$, $(b+1)b = b$, and $(b+1)p = bp + p + p\frac{p(p-1)}{2} = p$ by (7.4), the operation of $L_R + 1$ on L_R is trivial.

(b) By (7.6), one has $z^{-1}b = b - pyz^{-1}$. Thus, on one hand, using Lemma 7.6.1 one gets

$$
\begin{aligned}
z^{-1}(b+1)^2 &= z^{-1}(b2 + px + 1) \\
&= z^{-1}b2 + z^{-1}px + z^{-1} \\
&= \left(b - pyz^{-1}\right)\cdot 2 + pxz^{-1} + z^{-1} \\
&= b2 - p2yz^{-1} + pxz^{-1} + z^{-1} \\
&= b2 + p\left(xz^{-1} - 2yz^{-1}\right) + z^{-1},
\end{aligned}
$$

but also

$$
\begin{aligned}
z^{-1}(b+1)^2 &= z^{-1}(b+1)zz^{-1}(b+1) \\
&= (b+1)^z(p+1)^{(1-xz)\frac{z-1}{2}-y}\left(z^{-1}b + z^{-1}\right) \\
&= (b+1)^z(p+1)^{(1-xz)\frac{z-1}{2}-y}\left(b - pyz^{-1} + z^{-1}\right) \\
&= (b+1)^z\left(b - pyz^{-1} + (p+1)^{(1-xz)\frac{z-1}{2}-y}z^{-1}\right) \\
&= (b+1)^z\left(b - pyz^{-1} + \left(p\left((1-xz)\frac{z-1}{2} - y\right) + 1\right)z^{-1}\right) \\
&= (b+1)^z\left(b + p\left((z^{-1} - x)\frac{z-1}{2} - 2yz^{-1}\right) + z^{-1}\right) \\
&= (b+1)^z b + p\left((z^{-1} - x)\frac{z-1}{2} - 2yz^{-1}\right) + (b+1)^z z^{-1} \\
&= b + pxz + p\left((z^{-1} - x)\frac{z-1}{2} - 2yz^{-1}\right) + (b+1)^z z^{-1}
\end{aligned}
$$

$$\begin{aligned}
&= b + p\left(xz + (z^{-1} - x)\frac{z-1}{2} - 2yz^{-1}\right) + (b+1)^z z^{-1} \\
&= b + p\left(xz + (z^{-1} - x)\frac{z-1}{2} - 2yz^{-1}\right) \\
&\quad + \left(bz + px\frac{z(z-1)}{2} + 1\right) z^{-1} \\
&= b + p\left(xz + (z^{-1} - x)\frac{z-1}{2} - 2yz^{-1}\right) \\
&\quad + bzz^{-1} + \left(px\frac{z(z-1)}{2} + 1\right)\left(z^{-1} + pz\frac{z^{-1}(z^{-1}-1)}{2}\right) \\
&= b2 + p\left(xz + (z^{-1} - x)\frac{z-1}{2} - 2yz^{-1}\right) \\
&\quad + \underbrace{\left(px\frac{z(z-1)}{2} + 1\right)}_{=(p+1)^{x\frac{z(z-1)}{2}}}\left(z^{-1} + p\frac{z^{-1}-1}{2}\right) \\
&= b2 + p\left(xz + (z^{-1} - x)\frac{z-1}{2} - 2yz^{-1}\right) \\
&\quad + \left(px\frac{z(z-1)}{2} + 1\right) z^{-1} + p\frac{z^{-1}-1}{2} \\
&= b2 + p\left(xz + z^{-1}\frac{z-1}{2} - x\frac{z-1}{2} - 2yz^{-1}\right) \\
&\quad + pxz^{-1}\frac{z(z-1)}{2} + z^{-1} + p\frac{z^{-1}-1}{2} \\
&= b2 + p\left(xz + \frac{1-z^{-1}}{2} - 2yz^{-1}\right) - px\frac{z-1}{2} \\
&\quad + px\frac{z-1}{2} + p\frac{z^{-1}-1}{2} + z^{-1} \\
&= b2 + p\left(xz - \frac{z^{-1}-1}{2} - 2yz^{-1} + \frac{z^{-1}-1}{2}\right) + z^{-1} \\
&= b2 + p\left(xz - 2yz^{-1}\right) + z^{-1}.
\end{aligned}$$

Hence $xz^{-1} - 2yz^{-1} = xz - 2yz^{-1}$, i.e. $xz^{-1} = xz$ or $x = xz^2$. This means that either $x = 0$ or $z^2 \equiv 1 \pmod{p}$. The first case leads to a trivial operation of $L_R + 1$ on L_R, and this means that in the case of a non-trivial operation of $L_R + 1$ on L_R one has $x \neq 0$. Hence, $z^2 \equiv 1 \pmod{p}$, which means that $z^{2p} = 1$, since $(pn+1)^p \equiv 1 \pmod{p^2}$ for all $n \in \mathbb{N}$. But $o^{\times}(z) = p-1$, and hence $z^{p-1} = 1$. Thus, $1 = z^{2p}z^{-2(p-1)} = z^{2p-2(p-1)} = z^2$. It follows that $o^{\times}(z) = p - 1 \mid 2$. Since $z \neq 1$ this means that $p = 3$.

If $p = 3$, one can choose $x = 1$ to obtain a local nearring in which $L_R + 1$ operates non-trivially on L_R. □

Chapter 8.

Local nearrings with dihedral multiplicative group

8.1. General results

In this section local nearrings with dihedral multiplicative group are investigated. Most of these results can also be found in [3]. The first lemma on the structure of dihedral groups is well-known and will not be proved here.

8.1.1 Lemma

Let D be a dihedral group and $N \trianglelefteq D$. Then one of the following holds:

(1) $|D : N| = 2$ and N is a dihedral group.

(2) $D = N$.

(3) N is a cyclic group.

The next two lemmas and the subsequent theorem can also be found in detail in [3].

8.1.2 Lemma ([3, Lemma 4.1])

If R is a nearfield with (non-trivial)[1] *dihedral multiplicative group, then $|R| = 3$ and hence $R \cong \mathbb{F}_3$.*

Proof. By Lemma 4.2.4 (b) the equation $x^2 = 1$ has only the two solutions $x = 1$ and $x = -1$ in R. Hence $|R^\times| < 4$, which means that $|R^\times| = 2$. Thus $|R| = 3$, and so $R \cong \mathbb{F}_3$. □

8.1.3 Lemma ([3, Lemma 4.2])

Let R be a local nearring. If $L_R + 1$ is a cyclic group, then L_R is finite.

8.1.4 Theorem ([3, Theorem 4.3])

Let R be a local nearring whose multiplicative group $R^\times$ is dihedral. Then R is finite.

[1] The trivial group is not really a dihedral group, but sometimes it is useful to consider it as a dihedral group. The cyclic group of order 2 and Klein's Four Group both are dihedral groups throughout this section.

8.2. Nearrings of odd order

First local nearrings of odd order are considered. It turns out that the order of a local nearring of odd order with dihedral multiplicative group cannot be larger than 9. In the following, all these nearrings will be determined. In Lemma 8.1.2 it was shown, that there is exactly one local nearring of order 3 with dihedral multiplicative group. It will be shown in Theorem 8.2.2 that there are up to isomorphism exactly two local nearrings of order 9 with dihedral multiplicative group. Since $\mathbb{Z}/9\mathbb{Z}$ is the only nearring with identity element over the additive group C_9, and since $(\mathbb{Z}/9\mathbb{Z})^\times$ is not dihedral, it is clear that the additive group of these two local nearrings is elementary abelian.

8.2.1 Theorem ([3, Theorem 4.4])
Let R be a finite local nearring of odd order. If $R^\times$ is dihedral, then either $R \cong \mathbb{F}_3$ or R^+ is an elementary abelian group of order 9.

Proof. By Corollary 5.1.30, $L_R \trianglelefteq R$. Since R/L_R is a nearfield whose multiplicative group is isomorphic to $R^\times/(L_R + 1)$, this group is dihedral and so $R/L_R \cong \mathbb{F}_3$ by Lemma 8.1.2. Therefore, $3 \in L_R$ and hence R^+ is a 3-group by [3, Lemma 3.9]. Thus $L_R + 1$ is a normal 3-subgroup of $R^\times$ and so a cyclic group whose elements are inverted by -1. In particular, since $4 \in L_R + 1$, it follows that $4 = (-1) \cdot 4 \cdot (-1) = 4^{-1}$, so that $16 = 1$ and hence $3 = 0$. Therefore $\exp(R^+) = 3$. Next $(L_R + 1) \ltimes L_R$ is a product of two cyclic 3-groups by Construction 3.1.4, so that L_R is cyclic by [21, Lemma 6]. Hence $|L_R| = 3$ and so $R^+ \cong E_9$. □

8.2.2 Theorem
There are exactly two local nearrings over E_9 whose multiplicative groups are dihedral, one of which is zero-symmetric.

Proof. Let R be a local nearring over E_9 with dihedral multiplicative group, and let $0 \neq a \in L_R$. Then $R^+ = \langle 1, a\rangle$. To determine the multiplication in R it suffices to consider the products ra for all $r \in R$.

Since $|L_R| = 3$, also $(L_R + 1)^\times \cong C_3$. Hence $o^\times(a+1) = 3$ and $(a+1)^2 = a \cdot 2 + 1$. It follows that $(a+1)a = (a \cdot 2 + 1)a = a$. Since $-1 \notin L_R + 1$, one has $R^\times = \langle -1, a+1\rangle$ and $(-1)(a+1)(-1) = (a+1)^{-1} = a \cdot 2 + 1$. But on the other hand,

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

This yields $-(-1)a = -1 + a \cdot 2 + 1 = a \cdot 2$, and so $(-1)a = a$. Thus $ra = a$ for all $r \in R^\times$.

Since $a^2 \in L_R$, there are the following three possibilities for a^2:

(1) $a^2 = 0$:

In this case $a \notin R_c$. But ${R_c}^+ \leq {L_R}^+$ by Lemma 5.1.8, and hence $R_c = \{0\}$. Thus L_R is nilpotent by Corollary 5.1.13, which means that also $(a + a)a = 0$.

(2) $a^2 = a$:

In this case, $a \in R_c$, because otherwise R would be zero-symmetric as in (1) and hence L_R is nilpotent. Thus $R_c = L_R$ and $ra = a$ for all $a \in R$. But this implies that $a^2 = 0$, a contradiction.

(3) $a^2 = a + a$:

In (1) was shown that L_R is nilpotent and hence $a^2 = 0$, if $a \notin R_c$. This means that $a \in R_c$ and hence $a^2 = a$. But then $a^2 = a + a$ is impossible since $a + a \neq a$.

Thus there are at most two local nearrings with dihedral multiplicative group over E_9, one of which is zero-symmetric. Indeed, both possibilities for the multiplication lead to local nearrings. Only the associativity of the operations has to be checked. Thus let $b \in E_9$ and consider the mappings α_1 and α_2 with

$$\begin{aligned} \alpha_1 : E_9 &\to E_9 \\ x &\mapsto \begin{cases} 0, & x \in \langle b \rangle \\ b, & x \notin \langle b \rangle \end{cases}, \\ \alpha_2 : E_9 &\to E_9 \\ x &\mapsto b. \end{aligned}$$

Let R_i be the subnearring of $M(E_9)$ generated by the identity mapping of E_9 and α_i for $i \in \{1, 2\}$. Then it is not difficult to see that $R_i{}^\times \cong D_6$, where R_i is local, R_1 is zero-symmetric, but R_2 is not. □

Thus all local nearrings with dihedral multiplicative groups of odd order are classified.

8.3. Nearrings of even order

Now local nearrings of even order will be studied. In [3] it was shown that a local nearring of even order has order at most 32, if its group of units is dihedral. An investigation of all possible additive groups of order 32 shows that there is no local nearring of order 32 whose multiplicative group is dihedral. Thus Theorem 8.3.11 improves the main result of [3]. Moreover, in this section several cases for the structure of local nearrings of even order with dihedral groups of units are treated and illustrated by examples.

8.3.1 Lemma ([3, Lemma 5.1])
Let R be a local nearring of order 2^{n+1} with dihedral multiplicative group. Then $|R : L_R| = 2$, in particular $R^\times = L_R + 1$ is a dihedral group of order 2^n. Furthermore, $\exp(R^+) \leq 8$.

Proof. Since R/L_R is a nearfield of even order, it cannot be isomorphic to $\mathbb{F}_3$. Thus, by Lemma 8.1.2, $(R/L_R)^\times$ cannot be dihedral and hence must be trivial. That 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 Lemma 4.3.3. Hence ${P_R}^\times \cong C_2 \times C_{2^{l-2}}$ is an abelian subgroup of $R^\times$. This means that $|{P_R}^\times| \leq 4$, which is equivalent to $|P_R| \leq 8$. Thus $\exp(R^+) \leq 8$. □

8.3.2 Lemma ([3, Lemma 5.4])

Let R be a local nearring of even order with dihedral multiplicative group such that $R^\times$ 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, $|R| \leq 16$.

8.3.3 Corollary

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

Proof. By Lemma 8.3.2 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 $R \cong \mathbb{Z}/8\mathbb{Z}$ by Lemma 4.3.3. 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 $\mathrm{Stab}_{R^\times}(L_R) = \langle -3\rangle^\times$ in this case). □

8.3.4 Theorem ([3, Theorem 5.7])

Let R be a local nearring of order 2^n with $n \geq 1$, and let $R^\times$ 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.

In the following let R be a local nearring of order 2^{n+1} with dihedral mutliplicative group. Then, by Lemma 8.3.1, $R^\times = L_R + 1 \cong D_{2^n}$ and $|R : L_R| = 2$. Let $L_R + 1 = \langle k+1, l+1\rangle^\times$ for suitable k, $l \in L_R$, and let

$$K = \mathrm{Stab}_{R^\times}(L_R) = \left\{ r \in R^\times \;\middle|\; \forall l \in L_R : rl = l \right\}. \tag{8.1}$$

Of course, $K \trianglelefteq R^\times$, so that by Lemma 8.1.1 there are the following three cases. Other than in [3], the nearrings under consideration will now be investigated depending on these three cases.

(1) $K = R^\times$;

(2) $|R^\times : K| = 2$ and K is not cyclic;

(3) K is cyclic.

Case (1): $K = R^\times$

In this case, $L_R + 1$ operates trivially on L_R, and hence ${L_R}^+$ is a dihedral group of order 2^n. Because of the trivial operation and since $-1 \in L_R + 1$ and $2 \in L_R$, one has $-2 = (-1)2 = 2$, i.e. $4 = 0$, and so $\exp(R^+) \leq 4$. This means that $|L_R| \leq 8$ and thus $|R| \leq 16$.

The following lemma is needed to investigate the structure of the additive group R^+. With this result it will be possible to show that a nearring with $K = R^\times$ has at most 8 elements.

8.3.5 Lemma

Let G be a group of order 16 and exponent 4, $D = \langle a, c \mid a^2 = c^4 = 1, c^a = c^{-1}\rangle$ a subgroup of G isomorphic to D_8. Then there is an element $h \in G \setminus D$ with $o(h) = 2$.

Proof. Let $d \in G \setminus D$ with $o(d) = 4$ (if there is no such element, there is nothing to prove). Since D is a normal subgroup of G of index 2, the element d^2 is contained in D. Then $G = \langle a, c, d\rangle$. Since $C = \langle c\rangle$ is characteristic in D, it follows $C \trianglelefteq G$. Hence $c^d \in C$, i.e. $c^d \in \{c, c^{-1}\}$. This means that d^2 commutes with c, and since $d^2 \in D$, it follows that $d^2 \in C$. Moreover, since $o(d^2) = 2$, $d^2 = c^2$. Next, $a^d \in D$, but $a^d \notin C$, since $c^{a^d} = c^{-1}$. Now consider two cases:

(i) $c^d = c$:

In this case $(dc)^2 = d^2c^2 = c^4 = 1$, i.e. $o(dc) = 2$. But $dc \in G \setminus D$, and so one can let $h = dc$.

(ii) $c^d = c^{-1}$:

Here $[c, da] = 1$, and hence $(dac)^2 = (da)^2c^2$. Since $(da)^2 \in D$ and $[c, (da)^2] = 1$, $(da)^2 \in C$. Without loss of generality one may assume that $o(da) = 4$ (otherwise put $h = da$) and hence $(da)^2 = c^2$. It follows that $o(dac) = 2$. Since $dac \in G \setminus D$, one can put $h = dac$.

Thus in every case there is an element $h \in G \setminus D$ with $o(h) = 2$. □

Now suppose that $|R| = 16$. Then R^+ is a group of order 16 with $\exp(R^+) = 4$ and ${L_R}^+$ is a subgroup of R^+ isomorphic to D_8. But then $R \setminus L_R = R^\times$ contains an element h with $o^+(h) = 2$, contradicting Corollary 2.1.15. Hence $|R| \leq 8$.

8.3.6 Examples

(a) If $|R| = 4$, there are two possibilities for R^+. If R^+ is cyclic, then $R \cong \mathbb{Z}/4\mathbb{Z}$, and indeed in this local nearring the operation of $L_R + 1$ on L_R is trivial. If R^+ is elementary abelian, i.e. $R^+ = \langle 1, b\rangle$ with $L_R = \langle b\rangle$, then $1 \cdot b = (b + 1)b = b$. Since $b^2 \in L_R$, there are exactly two possibilities for b^2, both of which lead to a local nearring. Since R in this case is very small, the possible multiplications can be given by the following tables:

$b^2 = 0$

$\cdot$	0	b	1	$b+1$
0	0	0	0	0
b	0	0	b	b
1	0	b	1	$b+1$
$b+1$	0	b	$b+1$	1

$b^2 = b$

$\cdot$	0	b	1	$b+1$
0	0	b	0	b
b	0	b	b	0
1	0	b	1	$b+1$
$b+1$	0	b	$b+1$	1

(b) If $|R| = 8$, then R^+ is abelian since it is not possible to define a local nearring on D_8 by Corollary 5.2.11 or on Q_8 by Malone [14, Corollary 4]. First, if R^+ is cyclic, then $R \cong \mathbb{Z}/8\mathbb{Z}$ and $R^\times$ is isomorphic to the dihedral group of order 4. But in $\mathbb{Z}/8\mathbb{Z}$ the operation of $L_R + 1$ on L_R is not trivial since $(-1) \cdot 2 = -2 \neq 2$. Thus there are only the following two possibilities in this case:

(1) $R^+ = \langle 1, b \rangle \cong C_4 \times C_2$:

Here $L_R = \{0, b, 2, b+2\}$. Since $L_R + 1$ operates trivially on L_R, the equation $rb = b$ holds for every $r \in R^\times$. If R is not zero-symmetric, $R_c = \langle b \rangle$, since $2 \notin R_c$. This means that $rb = b$ for every $r \in R$. By left distributivity, this multiplication may be extended to a multiplication on the whole of R. It can easily be checked that this multiplication is associative (indeed this nearring is isomorphic to the subnearring of $M(R^+)$ generated by the identity mapping and the constant mapping which maps all elements to b).

Now let R be zero-symmetric. Then L_R is nilpotent by Corollary 5.1.13, and there are the two cases ${L_R}^2 = 0$ and ${L_R}^2 \neq 0$. In both cases ${L_R}^3 = 0$ by Lemma 5.3.3 since $|L_R| = 4$. If ${L_R}^2 = 0$, the multiplication is completely defined by $rb = \begin{cases} 0, & r \in L_R \\ b, & r \in R^\times \end{cases}$. It is not difficult to check that this nearring is a ring.

If ${L_R}^2 \neq 0 = {L_R}^3$, one has $1 < |\mathfrak{A}_R(L_R)| < 4$, and since $2 \in \mathfrak{A}_R(L_R)$, it follows that $\mathfrak{A}_R(L_R) = \{0, 2\}$. Since the ideal L_2 generated by ${L_R}^2$ (c.f. Definition 5.3.1), is a subset of $\mathfrak{A}_R(L_R)$ by Lemma 5.3.3, the elements b^2 and $(b+1)b$ are contained in $\mathfrak{A}_R(L_R)$. Furthermore, $L_2 = \mathfrak{A}_R(L_R)$ since otherwise $L_2 = 0$ and so ${L_R}^2 = 0$. Thus $2 \cdot b \in L_3 = 0$ and hence $2 \cdot b = 0$. If $b^2 = 0$, then $(b+2)b = 2$, since otherwise ${L_R}^2 = 0$. But then $(b+2)((b+1)b) = (b+2)b = 2$, whereas on the other hand $((b+1)(b+1))b = ((b+1)b+b+1)b = (2+b+2)b = b^2 = 0$. This contradicts the associativity of the multiplication. Hence $b^2 = 2$. Considering the associativity of $b(b+1)b$ on sees that $(b+2)b = 0$ is also impossible. Thus $(b+2)b = 2$. Again using the mapping $\beta : x \mapsto xb$ it is easy to see that the above multiplication is associative and the nearring generated by the identity mapping on R^+ and β generate a local nearring as described above.

(2) $R^+ = \langle 1,\, a,\, b\rangle \cong E_8$:

Here a and b can be chosen such that $L_R = \langle a,\, b\rangle$. Since $r \cdot 1 = r$ for all $r \in R$, only the products ra and rb must be defined for every $r \in R$. If R is zero-symmetric, then L_R is nilpotent, and hence there are the following two possibilities.

(i) ${L_R}^2 = 0$:

In this case, $la = lb = 0$ for all $l \in L_R$. Consider the mappings

$$\begin{aligned} \alpha : R^+ &\to R^+ \\ x &\mapsto \begin{cases} 0, & x \in \langle a,\, b\rangle \\ a, & \text{otherwise} \end{cases} \end{aligned} \qquad\qquad \begin{aligned} \beta : R^+ &\to R^+ \\ x &\mapsto \begin{cases} 0, & x \in \langle a,\, b\rangle \\ b, & \text{otherwise} \end{cases} \end{aligned}$$

and let id_R be the identity mapping on R^+. Then the subnearring $\tilde{R}$ of $M(R^+)$ generated by id_R, α, and β is a local nearring of order 8, whose group of units is isomorphic to D_4 and $L_{\tilde{R}} + 1$ operates trivially on $L_{\tilde{R}}$. Moreover, ${L_{\tilde{R}}}^2 = 0$.

(ii) ${L_R}^2 \neq 0 = {L_R}^3$:

In this case $\mathfrak{A}_R(L_R)$ is a subgroup of order 2 of L_R, so that without loss of generality $\mathfrak{A}_R(L_R) = \langle a\rangle^+$. Now b^2, $(a + b)b \in \mathfrak{A}_R(L_R)$. If $b^2 = 0$, then $(a + b)b \neq 0$ since $b \notin \mathfrak{A}_R(L_R)$. Hence in this case $(a + b)b = a$. But this means that $(a + b)((b + 1)b) = (a + b)b = a$, whereas $((a + b)(b + 1))b = (a + a + b)b = b^2 = 0$, a contradiction to the associativity. Similarly one shows that $(a + b)b \neq 0$. Hence $b^2 = (a + b)b = a$, and thus for all $r \in R$ the products ra and rb are defined. This multiplication can be extended to a multiplication on the whole of R. It is not difficult to check that this indeed leads to an associative multiplication and a local nearring with dihedral group of units.

If R is not zero-symmetric, $R_c \leq L_R$ and hence $|R_c| \in \{2,\, 4\}$. If $|R_c| = 4$, the products ra and rb are defined for all $r \in R$, and it is not difficult to check that the resulting multiplication is indeed associative. Finally consider the case $|R_c| = 2$. Without loss of generality $R_c = \langle a\rangle^+$. But then R_0 is a local nearring by Proposition 5.1.10. Since ${R_0}^\times \leq R^\times$ and $|R_0| = 4$, the case $|L_{R_0}| = 1$ is impossible and hence $|L_{R_0}| = 2$. Thus L_{R_0} contains a non-trivial element of L_R, and without loss of generality this element is b. By Corollary 5.1.13 L_{R_0} is nilpotent and hence $b^2 = 0$. Now $a((a+1)b) = ab$ since $L_R + 1$ operates trivially on L_R. But by associativity and since $b \in R_0$ one has

$$\begin{aligned} a((a + 1)b) = (a(a + 1))b &= (a^2 + a)b = (a + a)b \\ = 0b \qquad &= 0, \end{aligned}$$

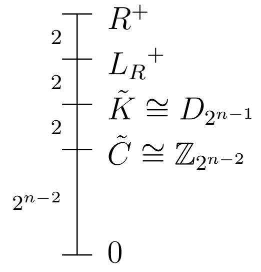
hence $ab = 0$. Similarly,

$$\begin{aligned}(a+b)b &= (a+b)((a+1)b) = ((a+b)(a+1))b = ((a+b)a+a+b)b \\ &= (a+a+b)b \qquad = b^2 \qquad\qquad\qquad = 0.\end{aligned}$$

Thus all products rb for $r \in R$ are defined. As above one can check that the multiplication on R given by this and left distributivity is indeed associative.

Thus all local nearrings of even order with dihedral multiplicative group and a trivial operation of $L_R + 1$ on L_R are described.

Case (2): $|R^\times : K| = 2$ and K not cyclic


R^+
$L_R{}^+$
$\tilde{K} \cong D_{2^{n-1}}$
$\tilde{C} \cong \mathbb{Z}_{2^{n-2}}$
0
2
2
2
2^{n-2}

In this case K is isomorphic to the dihedral group $D_{2^{n-1}}$. Since $(k+1)l = l$ for every $k+1 \in K$ and every $l \in L_R$, the set $\tilde{K} = \{k \in L_R \mid k+1 \in K\}$ is a subgroup of $L_R{}^+$, which is isomorphic to K. Thus R^+ is a group of order 2^{n+1} which has a subgroup $L_R{}^+$ of index 2 and a dihedral subgroup $\tilde{K}$ of index 4, such that $o^+(r) = \exp(R^+)$ for all $r \in R \setminus L_R$. Since R^+ is not cyclic, $\exp(R^+) \leq 2^n$. The following lemma shows that in this case $|R| \leq 32$.

By Theorem 8.3.4, $|R| \leq 32$ in general. In the case under consideration, the following lemma gives another proof for this result.

8.3.7 Lemma

Let G be a group, $U \trianglelefteq G$, and $D \trianglelefteq U$ with $|G : U| = |U : D| = 2$ and $D \cong D_{2^{n-1}}$. If $o(g) = \exp(G)$ for every $g \in G \setminus U$, then $n \leq 4$, i.e. $|G| = 2^{n+1} \leq 2^5 = 32$.

Proof. Let G be such a group with $o(g) = \exp(G)$ for each $g \in G \setminus U$. The exponent of G is 2^{n-k}, where $k \in \{0, 1, 2\}$, since $|G| = 2^{n-1}$, G is not cyclic and $\exp(D) = 2^{n-2}$.

Without loss of generality let $n \geq 4$ (otherwise there is nothing to show). Let T be the cyclic subgroup of order 2^{n-2} of D. If for every $g \in G \setminus U$ the order of $T \cap \langle g \rangle$ would be at least 4, then the subgroup of order 4 of T would be in the centre of G, which is not possible. Thus there exists an element $h \in G \setminus U$ with $|T \cap \langle h \rangle| \leq 2$. This means that

$$|T\langle h \rangle| \geq \frac{2^{n-2} \cdot 2^{n-k}}{2} = 2^{2n-3-k}.$$

Since $|G| = 2^{n+1}$, one has $2n-3-k \leq n+1$, so that $n \leq 4+k$. But $k \leq 2$, and hence $n \leq 4+k \leq 6$. Thus the order of G is at most 2^7.

$n = 6$**:** This is only possible if $k = 2$, i.e. $\exp(G) = 2^{n-2}$. In this case, $G = T\langle h \rangle$, and hence $D = T\langle h^4 \rangle$. But since $h \in G \setminus U$, $o(h) = 2^4$, and so $o(h^4) = 2^2 = 4$. This is a contradiction, since all elements of D which of 4 are contained in T.

$n=5$**:** If in this case $\exp(G)=2^{n-1}$, then one gets the same contradiction as above. Thus only the case $\exp(G)=2^{n-2}$ has to be considered. Let G be a group of order 64 and exponent 8, and let $D \leq U \leq G$ with $|G:U|=|U:D|=2$ and $D \cong D_{16}$. Let $D=\langle a,\, c \mid a^2=c^8=c^ac=1\rangle$, $U=\langle a,\, c,\, u\rangle$, and $G=\langle a,\, c,\, u,\, x\rangle$. Moreover, let $C=\langle c\rangle$. Without loss of generality, one may assume that $o(x)=8$, because otherwise there is nothing to show. Then there is an element $h \in G \setminus U$ with $o(h)<8$, i.e. $h^4=1$. To show this, the following two cases have to be considered.

(1) $D \trianglelefteq G$:

In this case, $C \trianglelefteq G$, since C is a characteristic subgroup of D. Thus $c^x \in \{c^{\pm 1},\, c^{\pm 3}\}$ and hence $c^{x^2}=c$, i.e. $[c,x^2]=1$. Since $x^4 \in D$, $o(x^4)=2$, and $[c,x^4]=1$, it follows that $x^4=c^4$. Similarly way one sees that $[c,(xa)^2]=1$ and $(xa)^4=c^4$, if $o(xa)=8$ (otherwise there is nothing to prove). Now consider the four cases for c^x.

(a) $c^x=c$:
Here $[c,x]=1$ and hence $(xc)^4=x^4c^4=c^4c^4=1$.

(b) $c^x=c^{-1}$:
In this case, $[c,xa]=c^{-1}ax^{-1}cxa=c^{-1}ac^{-1}a=c^{-1}c=1$, and hence $(xac)^4=(xa)^4c^4=c^4c^4=1$.

(c) $c^x=c^3$:
Because $a \notin C$, also $a^x \notin C$, say $a^x=ac^n$. Then $(xa)^2=xaxa=x^2a^xa=x^2ac^na=x^2c^{-n}$. It follows that $(xa)^3=(xa)^2xa=x^2c^{-n}xa=x^3c^{-3n}a=x^3ac^{3n}$, and hence $(xa)^4=(xa)^3xa=x^3ac^{3n}xa=x^3axc^na=x^4ac^nac^{-n}=c^4c^{-2n}=c^{4-2n}$. But $(xa)^4=c^4$, and thus $c^4=c^{4-2n}$. It follows that $c^{2n}=1$. Since $c^{xa}=(c^3)^a=c^{-3}$, from this one gets $(xac)^2=(xa)c(xa)c=(xa)^2c^{xa}c=(xa)^2c^{-2}=x^2c^{-2-n}$, and this leads to $(xac)^4=(x^2c^{-2-n})^2=x^4c^{-4-2n}=c^4c^{-4}=1$.

(d) $c^x=c^{-3}$:
Here $(xc)^2=x^2c^xc=x^2c^{-2}$, and thus $(xc)^4=x^4c^{-4}=c^4c^{-4}=1$.

(2) $D \not\trianglelefteq G$:

In this case $U=\mathbf{N}_G(D)$ since $D \trianglelefteq U$. If $g \in G \setminus U$ with $g^2 \in U \setminus D$, there is an element $d \in D$ with $d^g=ue$ for some $e \in D$, because $g \notin \mathbf{N}_G(D)$. Thus there is an element $g \in G \setminus U$ with $g^2 \in D$. Hence $(gd)^2=g^2d^gd=g^2ue$. But $g^2,\, u \in U \setminus D$, and so $g^2u \in D$. Therefore $(gd)^2 \in D$ and without loss of generality one may assume that $x^2 \in D$. Moreover, in the following $o(xa)=8$ will be assumed, since otherwise the claim is proved.

Now $x^2 \in D$ and $o(x^2)=4$, and thus $x^2=c^{\pm 2}$. If $x^2=c^{-2}$, replace x by x^{-1}, so that in any case $x^2=c^2$.

First assume $c^x \notin D$. If $a^x \notin D$, then $(ac)^x \in D$ and one can replace a by ac. Thus let $a^x \in D$, so that $a^x=a^jc^l$ for some $j,\, l \in \mathbb{N}$. If $j=0$, one has $l=4$

since $o(a) = o(a^x) = 2$, i.e. $a^x = c^4$. But then $(xa)^2 = x^2a^xa = c^2c^4a = ac^2$ and hence $(xa)^4 = 1$, a contradiction to $o(xa) = 8$. Thus $a^x \notin C$, and so $a^x = ac^l$. Hence $(xa)^2 = x^2a^xa = c^2ac^la = c^{2-l}$. Since $o(xa) = 8$, $(xa)^2 = c^{\pm 2}$ and hence $l = 0$ or $l = 4$. But if $l = 0$, one has $ac^4 = a^{c^2} = a^{x^2} = a$, a contradiction. On the other hand, $l = 4$ leads to $ac^4 = a^{c^2} = a^{x^2} = (ac^4)^x = a^x(c^4)^x = ac^4(c^4)^x$ and hence $(c^4)^x = 1$, which is contradiction. This means that $c^x \in D$ and hence $a^x \notin D$.

Since $o(c^x) = 8$, $c^x \in \{c^{\pm 1}, c^{\pm 3}\}$. But then $c^xc \in \langle c^2 \rangle$. If $o(xc) = 8$, $o((xc)^2) = 4$. But $(xc)^2 = x^2c^xc = c^2c^xc \in \langle c^2 \rangle$, and hence $(xc)^2 = c^{\pm 2}$. If $(xc)^2 = c^2$, one has $c^2c^xc = (xc)^2 = c^2$ and hence $c^x = c^{-1}$. But this leads to $c^2 = x^2 = (x^2)^x = (c^2)^x = c^{-2}$, a contradiction to $o(c) = 8$. Thus $(xc)^2 = c^{-2}$, and hence $c^x = c^3$. As above, this leads to the contradiction $c^2 = x^2 = (x^2)^x = (c^2)^x = c^6 = c^{-2}$.

In summary it is shown that in every case there is an element $g \in G \setminus U$ with $o(g) < 8$.

It follows that $n \leq 4$ and hence $|G| \leq 32$. □

The following lemma will be used in Example 8.3.9.(d) to show that also in the case under consideration there is no local nearring R with $|R| = 32$.

8.3.8 Lemma

Let G be a group of order 32 which has a subgroup D isomorphic to D_8. For every $g \in G$ let $\mathcal{S}_g = \{(dg)^2 \mid d \in D\}$, the set of squares of the elements of the right coset Dg. Then $|\mathcal{S}_g| \geq 2$ for every $g \in G$.

Proof. Let $D = \langle a, c \mid a^2 = c^4 = c^ac = 1 \rangle$ and assume that there is an element $g \in G$ such that $|\mathcal{S}_g| = 1$. Let s be the unique element of $\mathcal{S}_g$. Then $(dg)^2 = s$ for all $d \in D$. But this means that $s = (dg)^2 = dgdg = dd^{g^{-1}}g^2 = dd^{g^{-1}}s$ and hence $dd^{g^{-1}} = 1$ for all $d \in D$, or in other words $d^{g^{-1}} = d^{-1}$ for every $d \in D$. In particular, $ac^{-1} = a^{-1}c^{-1} = a^{g^{-1}}c^{g^{-1}} = (ac)^{g^{-1}} = (ac)^{-1} = ac$ and hence $c = c^{-1}$, a contradiction. Hence $|\mathcal{S}_g| \geq 2$. □

8.3.9 Examples

(a) If $|R| = 4$, L_R is cyclic of order 2. Thus there is an element $b \in L_R$ with ${L_R}^+ = \langle b \rangle^+$. But since $rb \neq 0$ for all $r \in R^\times$, the operation of $L_R + 1$ on L_R must be trivial. Hence in Case (2) there are no local nearrings of order 4.

(b) Next consider the case $|R| = 8$. If R^+ is cyclic, i.e. $R \cong \mathbb{Z}/8\mathbb{Z}$, it is not difficult to see that $K = \langle -3 \rangle$. This means that $\mathbb{Z}/8\mathbb{Z}$ belongs to Case (2). As mentioned above, the additive group of a local nearring of order 8 must be abelian. Consider the non-cyclic abelian groups of order 8. If R^+ is not cyclic, both $R^\times$ and ${L_R}^+$ are elementary abelian of order 4. But then for every $l \in L_R$ one has $1 = (l+1)^2 = (l+1)l+l+1$ and so $(l+1)l = -l = l$ for each $l \in L_R$. Now consider $k, l \in L_R$ with $k \neq 0 \neq l$ and $k \neq l$.

Then $(k+1)(l+1) \notin \{1,\, k+1,\, l+1\}$ and hence $l+k+1 = (k+1)(l+1) = (k+1)l+k+1$. It follows that $(k+1)l = l$ for all k, $l \in L_R$ and hence $L_R + 1$ operates trivially on L_R. Thus in Case (2) there is only one local nearring of order 8.

(c) Using GAP [9] with SONATA [1] one can check that there are 185 local nearrings of order 16 with dihedral group of units such that $|L_R + 1 : K| = 2$. These nearrings will not all be described here. Only two examples will be given here.

(1) Let $R^+ = \langle 1,\, a \mid 8 = a \cdot 2 = [1, a] = 0\rangle \cong C_8 \times C_2$. Clearly, then $L_R = \langle 2,\, a\rangle^+ \cong C_4 \times C_2$. If one defines $(-1)a = (a-1)a = a+4$, one gets $(a-1)^2 = (a-1)a - (a-1) = a+4+1-a = 5 = -3$. This leads to $o^\times(a-1) = 4$ and $(a-1)^{-1} = a+3$. Moreover, $(-1)(a-1)(-1) = (-1)(1-a) = -1-(a+4) = a+3 = (a-1)^{-1}$. Hence $R^\times \cong D_8$. It is also clear that $R^\times \neq K$, and since $-3 = (a-1)^2 \in K$ and $(-1)(a-1) = a-3 \in K$, one has $|K| = 4$. Of course, K is not cyclic. If one defines $la = 0$ for every $l \in L_R$, the products ra are defined for every $r \in R$. To see that this leads to an associative multiplication on R it suffices to check the subnearring of $M(R^+)$ generated by id_{R^+} and the mapping $\alpha : R^+ \to R^+$ with $x \mapsto xa$ where xa is as defined above.

(2) Consider the non-abelian group

$$R^+ = \langle 1,\, a_1,\, a_2 \mid 4 = a_1 \cdot 2 = a_2 \cdot 2 = [1, a_2] = [a_1, a_2] = 0, \\ -1 + a_1 + 1 = a_1 + a_2\rangle\,.$$

Then it can be checked that $|R^+| = 16$ and $\exp(R^+) = 4$ (R^+ is the non-abelian semidirect product $C_4 \ltimes E_4$ as described in Lemma 7.3.4). Now a multiplication on R^+ has to be introduced such that R becomes a local nearring. Then $L_R = \langle 2,\, a_1,\, a_2\rangle^+ \cong E_8$. Now define $kl = 0$ for all k, $l \in L_R$ and $ra_1 = a_1$ and $ra_2 = a_2$ for all $r \in R \setminus L_R$. To check the associativity of this multiplication consider the following mappings:

$$\alpha_1 : R^+ \to R^+ \qquad\qquad \alpha_2 : R^+ \to R^+$$

$$x \mapsto \begin{cases} 0, & x \in L_R \\ a_1, & \text{otherwise} \end{cases} \qquad\qquad x \mapsto \begin{cases} 0, & x \in L_R \\ a_2, & \text{otherwise} \end{cases}$$

It can easily be checked that the subnearring of $M(R^+)$ generated by id_{R^+}, α_1, and α_2 has order 16 and the multiplication is as described above.

Now $(a_1-1)^2 = (a_1-1)a_1 - (a_1-1) = a_1 + 1 - a_1 = a_1 + a_2 + 1$ and hence $(a_1-1)^4 = (a_1+a_2+1)^2 = (a_1+a_2+1)a_1 + (a_1+a_2+1)a_2 + a_1 + a_2 + 1 = a_1 + a_2 + a_1 + a_2 + 1 = 1$. Moreover, $(-1)(a_1-1)(-1) = a_1 + a_2 - 1 = (a_1-1)^{-1}$. Hence $R^\times \cong D_8$. Since $ra_i = a_i$ for $i = 1, 2$ and all $r \in R^\times$, one has $r \in K$ if and only if $r \cdot 2 = r$. Thus $a_1 - 1 \notin K$, i.e. $|K| \leq 4$. But since $-1 \in K$ and $a_2 + 1 \in K$, $|K| \geq 4$. Because of $(-1)^2 = (a_2+1)^2 = 2$, K cannot be cyclic, and this means that R belongs to Case (2).

(d) Assume that $|R| = 32$. Then $|L_R| = 16$ and $K \cong D_8$. Moreover, $D = K - 1$ is a subgroup of ${L_R}^+$ which is also isomorphic to D_8. Now consider the homomorphism $\sigma : R^\times \to \mathrm{Aut}({L_R}^+)$ with $r \mapsto \sigma_r$, where $l\sigma_r = rl$ for all $l \in L_R$. Then of course $K = \mathrm{Ker}(\sigma)$. Hence $|\,\mathrm{Im}(\sigma)| = 2$ and there is an automorphism $\alpha \in \mathrm{Aut}({L_R}^+)$ with $o(\alpha) = 2$ and $r\sigma = \alpha$ for all $r \in R^\times \setminus K$. Clearly $2 \in L_R$ and so

$$r + r = r \cdot 2 = 2\alpha \tag{8.2}$$

for each $r \in R^\times \setminus K$. But since $|R : D| = 4$, the group D has four right cosets in R, two of which are contained in L_R and one coinciding with K. This means that $R^\times \setminus K$ is a right coset of D. Thus there is an element $s \in R^\times \setminus K$ such that $R^\times \setminus K = D + s$. By (8.2) there is an element $z = 2\alpha$ with $(d + s) \cdot 2 = z$ for all $d \in D$. But this is a contradiction to Lemma 8.3.8, since R^+ satisfies the hypothesis of that lemma. Hence there are no local nearrings of order 32 in Case (2).

Case (3): K is cyclic

First some examples will be given. It turns out that for $|R| \in \{4, 8\}$ there are no additional nearrings not covered by the previous cases. For $|R| = 16$ one example is given to demonstrate that there are local nearrings of order 16 which do not belong to Case (1) or Case (2). In Theorem 8.3.11 all groups of order 32 are considered to show that there are no local nearrings of order 32 with dihedral group of units.

8.3.10 Examples

(a) If $|R| = 4$, $R^\times$ is cyclic and hence so is K. But as mentioned above, $L_R + 1$ operates trivially on L_R and so this case is identical to Case (1).

(b) If $|R| = 8$, then $R^\times \cong D_4$. If $K \neq 1$ is cyclic, then $K \cong C_2 = D_2$; this case is treated as Case (2). Thus only the case $K = 1$ remains. But this case is not possible, since K is the kernel of a homomorphism $R^\times \to \mathrm{Aut}({L_R}^+)$ and $\mathrm{Aut}({L_R}^+) \cong S_3$ does not contain a subgroup isomorphic to E_4.

(c) Let $R^+ = \langle 1, a, b \mid 4 = a \cdot 2 = b \cdot 2 = [1, a] = [1, b] = [a, b] = 0\rangle \cong C_4 \times E_4$. Define a multiplication on R by $r \cdot 1 = r$ for all $r \in R$ and the following rules:

$$ra = \begin{cases} 0, & r \in \langle 2\rangle^+ \\ 2, & r \in L_R \setminus \langle 2\rangle^+ \\ a, & r \in \langle 2 + a\rangle^+ + 1 \\ 2 + a, & r \in \langle a\rangle^+ + b - 1 \\ 2 + a + b, & r \in \langle a + b\rangle^+ + 1 + a \\ a + b, & r \in \langle 2 + a + b\rangle^+ - 1 \end{cases} \qquad rb = \begin{cases} 0, & r \in L_R \\ b, & r \in \langle 2, b\rangle^+ + 1\ . \\ 2 + b, & \text{otherwise} \end{cases}$$

Considering the mappings $\alpha : R \to R$, $r \mapsto ra$ and $\beta : R \to R$, $r \mapsto rb$ as defined above, one can see that the subnearring of $M(R^+)$ generated by α, β, and the identity mapping on R^+ is a local nearring of order 16 over R^+ with $R^\times \cong D_8$ and $|K| = 1$.

In the following theorem all groups of order 32 are considered to show that they cannot be the additive group of a local nearring with a dihedral group of units. There are 51 groups of order 32, but not all have to be considered separately. Most of the groups of order 32 cannot occur as R^+, since for example their exponent is larger than 8. Altogether there are seven groups of order 32 left, which will be treated separately.

8.3.11 Theorem

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

Proof. Assume there exists a local nearring R of order 32, whose multiplicative group $R^\times$ is isomorphic to D_{16}. Then, R belongs to Case (3), i.e. the group K as defined in (8.1) is cyclic. Let $C = \{k - 1 \mid k \in K\}$. Then C is a cyclic subgroup of ${L_R}^+$ isomorphic to K. Since $\exp(R^+) \leq 8$ by Lemma 8.3.1, also $|K|$ is not larger than 8. By Lemma 8.3.2, $|K| \geq 1$. Proposition 2.1.13 implies that $\mathrm{Aut}(R^+)$ contains a subgroup isomorphic to D_{16}; in particular, R^+ is a group of order 32 with an automorphism of order 8. By Baginski, Malinowska [5], there are 23 groups of order 32, which have an automorphism of order 8. Using GAP [9] (but also by simple calculation) one can see that 16 of these groups have exponent not larger than 8 and an automorphism group which has a subgroup isomorphic to D_{16}. The GAP-programs used to obtain these informations are described in detail in Appendix B.

Moreover, ${L_R}^+$ is a subgroup of index 2 of R^+, such that $o^+(r) = \exp(R^+)$ for every $r \in R \setminus L_R$. Among the 16 groups under consideration, seven have such a subgroup of index 2. These are the following:

$$G_1 = E_{32}$$

$$G_2 = C_4 \times E_8$$

$$G_3 = \langle a,\, b,\, c \mid a \cdot 4 = c \cdot 4 = [b, c] = 0,\, a \cdot 2 = b \cdot 2,\, b^a = -b,\, c^a = -c \rangle$$

$$\begin{aligned} G_4 = \langle a,\, b,\, c,\, d \mid\ & a \cdot 4 = c \cdot 2 = d \cdot 2 = [a, c] = [a, d] = [b, c] = 0, \\ & [b, d] = [c, d] = 0,\, a \cdot 2 = b \cdot 2,\, b^a = -b \rangle \end{aligned}$$

$$G_5 = \langle a,\, b,\, c \mid a \cdot 8 = b \cdot 2 = c \cdot 2 = [b, c] = 0,\, [a, b] = c,\, a^c = -a \cdot 3 \rangle$$

$$\begin{aligned} G_6 = \langle a,\, b,\, c \mid\ & a \cdot 8 = b \cdot 4 = c \cdot 2 = [b, c] = 0,\, a \cdot 4 = b \cdot 2, \\ & [a, b] = c,\, [a, c] = a \cdot 4 \rangle \end{aligned}$$

$$G_7 = \langle a,\, b \mid a \cdot 8 = b \cdot 8 = 0,\, a \cdot 4 = b \cdot 4,\, b^a = b \cdot 3 \rangle$$

Here, the groups G_2, G_3, and G_4 have exponent 4, whereas the groups G_5, G_6, and G_7 have exponent 8.

Now consider the mapping

$$\begin{aligned} \tau : R^\times &\to \operatorname{Aut}(R^+) \\ r &\mapsto \tau_r, \end{aligned} \tag{8.3}$$

where $x\tau_r = rx$, and let $D = \operatorname{Im}(\tau)$. By Proposition 2.1.13, τ is a monomorphism and $D \cong D_{16}$. Let $r \in R^\times$ and $\alpha_1, \alpha_2 \in D$ with $r\alpha_1 = r\alpha_2$. Then there are elements $s_1, s_2 \in R^\times$ with $\alpha_i = s_i\tau$ and $r\alpha_i = s_i r$ for $i \in \{1, 2\}$. Hence $s_1 r = s_2 r$, and right multiplication with r^{-1} leads to $s_1 = s_2$. Thus $\alpha_1 = \alpha_2$. This means that for all $r \in R^\times$ the following holds

$$\bigl|\{r\delta \mid \delta \in D\}\bigr| = 16. \tag{8.4}$$

First assume that R^+ is elementary abelian. Let $S \in \operatorname{Syl}_2(\operatorname{Aut}(R^+))$ and $\mathcal{D} = \{D \le S \mid D \cong D_{16}\}$. Then $|S| = 1024$ and $|\mathcal{D}| = 16$. It can be checked that for every $r \in R$ and every $D \in \mathcal{D}$ there is an $\alpha_{r,D} \in D$, such that $\alpha_{r,D} \ne \mathrm{id}_R$ and $r\alpha_{r,D} = r$. Hence $\bigl|\{r\delta \mid \delta \in D\}\bigr| < 16$. Now let $r \in R^\times$ and let D_1 be an arbitrary subgroup of $\operatorname{Aut}(R^+)$ isomorphic to D_{16}. Then there is a $\beta \in \operatorname{Aut}(G)$ such that $D_1 \le S^\beta$, such that $D_1 = {D_0}^\beta$ for some $D_0 \in \mathcal{D}$. Let $s = r\beta^{-1}$ and $\gamma = \alpha_{s,D_0}$. Then $\gamma^\beta \in D_1$ and $r\gamma^\beta = r\beta^{-1}\gamma\beta = s\gamma\beta = s\beta = r$. Hence for every $r \in R$ and every $D \le \operatorname{Aut}(R^+)$ with $D \cong D_{16}$ one obtains $\bigl|\{r\delta \mid \delta \in D\}\bigr| < 16$, a contradiction to (8.4). Thus R^+ cannot be elementary abelian, and there are only six groups left to be checked.

In the following, let $\mathcal{L}(G) = \bigl\{U \le G \bigm| |G:U| = 2 \wedge \forall g \in G \setminus U : o(g) = \exp(G)\bigr\}$, and $\mathcal{D}(G) = \{D \le \operatorname{Aut}(G) \mid D \cong D_{16}\}$. Then $\mathcal{L}(G)$ is the set of all subgroups of G which are candidates for L_R in a local nearring R with $R^+ \cong G$. Moreover, for $U \in \mathcal{L}(G)$ let $\mathcal{D}_U(G) = \{D \in \mathcal{D}(G) \mid U \text{ is } D\text{-invariant}\}$. All the calculations in the following have been done using **GAP** [9], but of course they could also be done by direct calculation. The groups of order 32 are described in detail in [13].

(1) $R^+ = G_2 = \langle a\rangle \times \langle b, c, d\rangle \cong C_4 \times E_8$:

In this case, $|\mathcal{L}(R^+)| = 1$ and hence there is only one possibility for L_R. It turns out that $L = \langle a \cdot 2, b, c, d\rangle$ is the only group in $\mathcal{L}(R^+)$. Moreover, one can check that $|\mathcal{D}(R^+)| = 336$. But an elementary calculation shows that $\bigl|\{r\delta \mid \delta \in D\}\bigr| = 8$ for every $r \in R \setminus L$ and every $D \in \mathcal{D}(R^+)$, a contradiction to (8.4). Thus there is no local nearring R with dihedral group of units over G_2.

(2) $R^+ = G_3 = \langle a, b, c \mid a \cdot 4 = c \cdot 4 = [b, c] = 0,\ a \cdot 2 = b \cdot 2,\ b^a = -b,\ c^a = -c\rangle$:

In this case $|\mathcal{L}(R^+)| = 7$ and $|\mathcal{D}(R^+)| = 16$. But the only group $L \in \mathcal{L}(R^+)$ for which there is a $D \in \mathcal{D}(R^+)$ such that L is D-invariant is $L = \langle a \cdot 2, b, c\rangle$; for this group $\mathcal{D}_L(R^+) = \mathcal{D}(R^+)$. But again it turns out that $\bigl|\{r\delta \mid \delta \in D\}\bigr| = 8$ for each $r \in R \setminus L$ and each $D \in \mathcal{D}(R^+)$. This contradiction to (8.4) shows that there is no local nearring R with dihedral group of units over G_3.

(3) $R^+ = G_4$:

Here, $|\mathcal{L}(R^+)| = 3$ and $|\mathcal{D}(R^+)| = 144$. Also in this case it turns out that for every $L \in \mathcal{L}(R^+)$, every $r \in R^+ \setminus L$ and every $D \in \mathcal{D}_L(R^+)$ one gets $\big|\{r\delta \mid \delta \in D\}\big| = 8$. Thus by (8.4) there is no local nearring with the desired properties over G_4.

(4) $R^+ = G_5 = \langle a,\, b,\, c \mid a \cdot 8 = b \cdot 2 = c \cdot 2 = [b, c] = 0,\, [a, b] = c,\, a^c = -a \cdot 3\rangle = \langle a,\, b\rangle$:

In this case $|\mathcal{D}(R^+)| = 4$, $|\mathcal{L}(R^+)| = 1$, and $L_R = \langle a \cdot 2,\, b,\, c\rangle \in \mathcal{L}(R^+)$. Clearly, L_R is a characteristic subgroup of R^+. Since for every $r \in R \setminus L_R$ the relation $r^{[r,b]} = -r \cdot 3$ holds, without loss of generality a is the identity element 1 of R.

Since the group $P_R = \langle 1\rangle^+$ is not normal in R^+, the group ${R_0}^+$ must be a normal subgroup of R^+ which properly contains P_R. Assume that R is not a zero-symmetric nearring. Then ${R_0}^+ = \mathbf{N}_{R^+}(P_R)$, since it is the only proper normal subgroup of R^+ containing P_R. But then $|R_c| = 2$ and there is an $x \in R_c$, $x \neq 0$, with $rx = x$ for all $r \in R$. In particular, if $r \in R^\times$, one gets $x = rx = x(r\tau)$, where τ is the mapping defined in (8.3). This means that there exists a group $D \in \mathcal{D}(R^+)$ such that $x\delta = x$ for all $\delta \in D$. But there is no $D \in \mathcal{D}(R^+)$ such that $x\delta = x$ for all $\delta \in D$ and some $x \notin \mathbf{N}_{R^+}(P_R)$ with $o^+(x) = 2$. Thus the nearring R must be zero-symmetric. In particular, L_R is nilpotent by Corollary 5.1.13.

It is not difficult to see that ${L_R}' = \langle 4\rangle^+$. In particular, $l[k, m] = 0$ for all k, l, $m \in L_R$, since $\exp({L_R}^+) = 4$. Moreover, if $l \in L_R$, then $l \cdot 2 \in \langle 4\rangle^+$, i.e. $l \cdot 2 = 4n'$ for some $n' \in \mathbb{N}$. By Theorem 2.1.14, $o^+(lb) \mid o^+(b) = 2$. The elements of R^+ whose orders divide 2 are 0, c, b, $b + c$, $2 + b$, $2 + b + c$, 4, $4 + c$, $4 + b$, $4 + b + c$, $-2 + b$, and $-2 + b + c$. Then $lb \in \{0,\, c,\, 4,\, 4 + c\}$ for all $l \in L_R$, since all other possibilities lead to a contradiction to the nilpotency of L_R:

1. $lb = b$: This would mean $l^2b = b$, and so $l^nb = b \neq 0$ for all $n \in \mathbb{N}$.
2. $lb = b + c$: This would lead to $l^2b = l(b + c) = lb + lc = b + c + [l, lb] \neq 0$, and hence $l^3b = l(b + c + [l, lb]) = l(b + c) = l^2b$. Thus $l^nb = l^2b \neq 0$ for all $n \geq 2$.
3. $lb = 2 + b$: This would mean $l^2b = l(2 + b) = l \cdot 2 + lb = 4n' + 2 + b \neq 0$, hence $l^3b = l(4n' + 2 + b) = l(2 + b) = l^2b \neq 0$ and thus $l^nb = l^2b \neq 0$ for all $n \geq 2$.
4. $lb = 2 + b + c$: This would mean $l^2b = l(2 + b + c) = l \cdot 2 + lb + lc = 4n' + 2 + b + c + [l, lb] \neq 0$, hence $l^3b = l(4n' + 2 + b + c + [l, lb]) = l(2 + b + c) = l^2b$ and thus $l^nb = l^2b \neq 0$ for all $n \geq 2$.
5. $lb = 4 + b$: This would mean $l^2b = l(4 + b) = lb \neq 0$, hence $l^nb = lb \neq 0$ for all $n \in \mathbb{N}$.
6. $lb = 4 + b + c$: This would mean $l^2b = l(4 + b + c) = lb + lc = 4 + b + c + [l, lb] \neq 0$, hence $l^3b = l(4 + b + c + [l, lb]) = l(4 + b + c) = l^2b$ and thus $l^nb = l^2b \neq 0$ for all $n \geq 2$.
7. $lb = -2 + b$: This would mean $l^2b = l(-2 + b) = 2l \cdot 2 + lb = 4n' - 2 + b \neq 0$, hence $l^3b = l(4n' - 2 + b) = l(-2 + b) = l^2b$ and thus $l^nb = l^2b \neq 0$ for all $n \geq 2$.

8. $lb = -2 + b + c$: This would mean $l^2 b = l(-2 + b + c) = -l \cdot 2 + lb + lc = 4n' - 2 + b + c + [l, lb] \neq 0$, hence $l^3 b = l(4n' - 2 + b + c + [l, lb]) = l(-2 + b + c) = l^2 b$ and thus $l^n b = l^2 b \neq 0$ for all $n \geq 2$.

Since all eight cases lead to contradictions to the nilpotency of L_R, only the four possibilities given above remain. Since $c = [1, b]$, one gets $lc = [l, lb]$ for every $l \in L_R$. But since all possibilities for lb are contained in the centre of ${L_R}^+$, it follows that $lc = 0$ in every case. Now let k, $l \in L_R$ with $l = 2x + by + cz$ and $k \cdot 2 = 4w$. Then $kl = k(2x + by + cz) = 4wx + kby + kcz = 4wx + kby \in \langle 4,\, c\rangle^+$. Hence $klm = 0$ for all k, l, $m \in L_R$ and thus ${L_R}^3 = 0$.

Therefore $\langle 4,\, c\rangle^+ \leq \mathfrak{A}_R(L_R)$. Since $\exp({L_R}^+) = 4$, it is also clear that $2 \notin \mathfrak{A}_R(L_R)$. There are three normal subgroups of R^+ which contain 4 and c and do not contain 2. These are the candidates for $\mathfrak{A} = \mathfrak{A}_R(L_R)^+$.

(A) $\mathfrak{A} = \langle 4,\, c\rangle^+$ $(|\,\mathfrak{A}\,| = 4)$:

In this case is $(R/\,\mathfrak{A})^+ \cong C_4 \times C_2$. As shown above, there are two zero-symmetric local nearrings over this group whose multiplicative groups are dihedral. In both cases the operation of $(R/\,\mathfrak{A})^\times$ on $L_{R/\,\mathfrak{A}}$ is trivial, such that $rb \in b + \mathfrak{A}$ for every $r \in R^\times$. But there is no $D \in \mathcal{D}(R^+)$ such that $b\alpha \in b + \mathfrak{A}$ for each $\alpha \in D$. Thus this case is impossible.

(B) $\mathfrak{A} = \langle 4,\, b,\, c\rangle^+$ $(|\,\mathfrak{A}\,| = 8)$:

In this case $(R/\,\mathfrak{A})^+$ is cyclic of order 4. There is only one nearring with one over this group, and this is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. This is a local nearring with dihedral group of units, and the operation of $(R/\,\mathfrak{A})^\times$ on $L_{R/\,\mathfrak{A}}$ is trivial. But again, there is no $D \in \mathcal{D}(R^+)$ such that $b\alpha \in b + \mathfrak{A}$ for all $\alpha \in D$. Therefore also this case is impossible.

(C) $\mathfrak{A} = \langle 4,\, 6 + b,\, c\rangle^+$ $(|\,\mathfrak{A}\,| = 8)$:

As in the last case, $(R/\,\mathfrak{A})^+$ is cyclic of order 4, and there is no $D \in \mathcal{D}(R^+)$ such that $b\alpha \in b + \mathfrak{A}$ for all $\alpha \in D$. Thus also this case is impossible.

Therefore no local nearring with dihedral group of units exists over G_5.

(5) $R^+ = G_6 = \langle a,\, b\rangle$:

In this case $|\mathcal{L}(R^+)| = 1$ and $|\mathcal{D}(R^+)| = 4$. If such a local nearring exists, then $L_R = \langle a \cdot 2,\, b,\, c\rangle$. Since $R^+ = \langle a,\, b\rangle$ and the relations between a and b are satisfied by every $r \in R^\times$, without loss of generality $1 = a$.

Assume that R is not zero-symmetric. The group ${P_R}^+$ is not normal in R^+, but it is contained in the zero-symmetric part R_0. Hence ${R_0}^+ = \mathbf{N}_{R^+}({P_R}^+)$, since this is the only proper normal subgroup of R^+ containing P_R, because $|R : P_R| = 4$. But this normalizer does not have a complement in R^+, a contradiction to Theorem 2.1.8. Hence R must be zero-symmetric.

Since ${L_R}' = \langle 4\rangle^+$ and $\exp({L_R}^+) = 4$, it follows that $k[l, m] = 0$ for every k, l, $m \in L_R$. Moreover, $l \cdot 2 \in \langle 4\rangle^+$ for every $l \in L_R$. From $4 = b \cdot 2$ it follows that $(lb) \cdot 2 = l(b \cdot 2) = l \cdot 4 = 0$ for every $l \in L_R$. Hence $lb \in \langle 4,\, c\rangle^+$, because $o^+(l) = 4$ for all $l \in L_R \backslash \langle 4,\, c\rangle^+$. But since $\langle 4,\, c\rangle^+ = \mathbf{Z}({L_R}^+)$, this yields $lc = l[1, b] = [l, lb] = 0$ for every $l \in L_R$. Thus $\langle 4,\, c\rangle^+ \leq \mathfrak{A}_R(L_R) \trianglelefteq R$. Since $2 \notin \mathfrak{A}_R(L_R)$, there are the following possibilities for $\mathfrak{A} = \mathfrak{A}_R(L_R)$:

(A) $\mathfrak{A} = \langle 4,\, c\rangle$, $(|\,\mathfrak{A}\,| = 4)$:
In this case, $(R/\,\mathfrak{A})^+ \cong C_4 \times C_2$. As shown above, the operation of $(R/\,\mathfrak{A})^\times$ on $L_{R/\,\mathfrak{A}}$ must be trivial, i.e. there must be a $D \in \mathcal{D}(R^+)$ with $b\alpha + \mathfrak{A} = b + \mathfrak{A}$ for every $\alpha \in D$. It is easy to check that this is not the case, and hence this case is impossible.

(B) $\mathfrak{A} = \langle b,\, c\rangle$, $(|\,\mathfrak{A}\,| = 8)$:
Since here $(R/\,\mathfrak{A})^+ \cong C_4$, also in this case the operation of $(R/\,\mathfrak{A})^\times$ on $L_{R/\,\mathfrak{A}}$ must be trivial. Again, there is no $D \in \mathcal{D}(R^+)$ such that $b\alpha + \mathfrak{A} = b + \mathfrak{A}$ for every $\alpha \in D$. Hence also this case is impossible.

(C) $\mathfrak{A} = \langle 2 - b,\, c\rangle$, $(|\,\mathfrak{A}\,| = 8)$:
Again, $(R/\,\mathfrak{A})^+ \cong C_4$. But as in the last case it turns out that this group $\mathfrak{A}$ cannot be the annihilator of L_R in R.

As none of the possible normal subgroups of R^+ can be the annihilator of L_R in R^+, this local nearring cannot exist.

(6) $R^+ = G_7 = \langle a,\, b \mid a \cdot 8 = b \cdot 8 = 0,\, a \cdot 4 = b \cdot 4,\, b^a = b \cdot 3\rangle$:

For this group one obtains $|\mathcal{L}(R^+)| = 3$ and $|\mathcal{D}(R^+)| = 8$. The groups $L_1 = \langle a,\, b \cdot 2\rangle$ and $L_2 = \langle a + b \cdot 3,\, b \cdot 2\rangle$ are both contained in $\mathcal{L}(R^+)$, but one can check that $\mathcal{D}_{L_i}(R^+) = \varnothing$ for $i \in \{1,\, 2\}$. Thus, if a local nearring with dihedral group of units exists over this group, $L_R = \langle a \cdot 2,\, b\rangle$. Since then for every $r \in R^\times$ the relations $r \cdot 4 = b \cdot 4$ and $b^r = b \cdot 3$ hold, without loss of generality $1 = a$. Again, the group ${P_R}^+ = \langle 1\rangle^+$ is not normal in R^+ and the normalizer $\mathbf{N}_{R^+}({P_R}^+)$ has no complement in R^+, such that R must be a zero-symmetric nearring. By Corollary 5.1.13, L_R must be nilpotent.

Since $\exp({L_R}^+) = 8$, the element 4 cannot be contained in the annihilator $\mathfrak{A}_R(L_R)$. Let $n \in \mathbb{N}$ such that ${L_R}^{n-1} \neq 0 = {L_R}^n$. Then $n \geq 4$ by Proposition 5.1.23. As in Definition 5.3.1, L_{n-1} is the ideal of R generated by ${L_R}^{n-1}$. This is contained in $\mathfrak{A}_1 = \mathfrak{A}_R(L_R)$ by Lemma 5.3.3. The group R^+ contains exactly three elements of order 2; namely 4, $2 + b \cdot 2$, and $2 - b \cdot 2$. Since it is already known that $4 \notin \mathfrak{A}_1$, let $x \in \{2 \pm b \cdot 2\}$ and let N_x be the normal closure of $\langle x\rangle^+$. Since $\mathfrak{A}_1$ must contain at least one element x of order 2 and since ${\mathfrak{A}_1}^+ \trianglelefteq R^+$, this group must also contain the normal closure N_x. But for both possible choices for x it turns out that $4 \in N_x$. Thus the desired nearring also does not exist in this case.

Since a local nearring with dihedral group of units cannot exist over any group of order 32, the theorem is proved. □

8.3.12 Corollary

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

Appendix A.
C++-Program used in Example 5.2.12

In Example 5.2.12 a nearring over a group isomorphic to $C_9 \times C_9$ was defined. In this example $R^+ = \langle 1,\, a \mid 9 = a \cdot 9 = [1,\, a] = 0 \rangle$, and a multiplication on this group is given such that R becomes a local nearring with $L_R = R \cdot 3$. By the left distributive law it is clear that only the products $x \cdot 1$ and $x \cdot a$ have to be defined for all $x \in R$. In order that 1 becomes the identity element of R, it is clear that $x \cdot 1 = x$ for all $x \in R$. Then, the products $l \cdot a$ are defined for all $l \in L_R$. Furthermore let $(a \cdot 2)a = -2$ and $(1 - a \cdot 2)a = -2 - a \cdot 4$. Then it has to be checked that these products define the whole multiplication on R and that this multiplication is well-defined and an associative left distributive nearring multiplication. This check has been done by a C++-program, which is described here.

First a class for the elements of R is defined (the line numbers given here are the numbers of the code lines in the source code file, which is as a whole given at the end of this appendix).

```
class Nearring_Element
```

This class contains two member variables in the range from 0 to 8, which describe the element. Thus the element constructed by the constructor

```
     // Constructor:
     // The element constructed is the tuple (E,A) in the additive group
     // C9 x C9.
25   Nearring_Element(int E,
                      int A) :
       e(E%9),
       a(A%9)
     {
30     if (e < 0)
         e += 9;
       if (a < 0)
         a += 9;
     }
```

is the element $\texttt{e} \cdot 1 + \texttt{a} \cdot a$ in the group. The function body of this constructor ensures that the member variables are in fact in the desired range.

Moreover, the elements of the group can be numbered from 0 to 80. This is necessary to define the multiplication later. The constructor

```
// Constructor:
// The additive group has order 81.  The elements are numbered from
// 0 to 80, and the element constructed is the element with the
// number i.
Nearring_Element(int i) :
  e((i/9)%9),
  a(i%9)
{
  if (e < 0)
    e += 9;
  if (a < 0)
    a += 9;
}
```

constructs the element with the number `i`, while the member function

```
// This function returns the number of a nearring element.
int
num() const
{
  return e*9+a;
}
```

returns the number of an element of R.

Also an addition for the elements is needed, as well as the possibility to multiply an element with an integer. This is done by the following two member functions.

```
// Addition of two nearring elements
Nearring_Element
operator+(const Nearring_Element &f) const
{
  return Nearring_Element(e+f.e, a+f.a);
}

// Multiplication of a nearring element with an integer
Nearring_Element
operator*(int i) const
{
  return Nearring_Element(e*i, a*i);
}
```

Multiplication is defined outside this class, because a global array is needed for this. As described above, only the products $x \cdot a$ have to be defined. Thus, an array is created in the program, in which the numbers of the elements xa are given, indexed by the number of x. As long as these products are not yet defined, the value -1 is put into the array to indicate that the products are unknown. Here the member functions `n()` and `k()` are used. These functions return the values of the two member variables of the class, i.e. if `x = Nearring_Element(u,v)` one has `x.n() = u` and `x.k() = v`. This means that x.n() = n_x and x.k() = k_x as defined in Example 5.2.12.(b) on page 67.

```
///////////////////////////////////////////////////////////////////////
//
// Multiplication table
//
// In this table the product x*a for all nearring elements is stored.
// If this product is still unknown, -1 is stored.  The element
// mtab[i] is the number of the nearring element
// Nearring_Element(i)*a.
//
///////////////////////////////////////////////////////////////////////
static int mtab[81] = {
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1
};

// Multiplication operator for two nearring elements.
Nearring_Element
operator*(const Nearring_Element &x,
          const Nearring_Element &y)
{
  return x*y.n() + Nearring_Element(mtab[x.num()])*y.k();
}
```

In the `main()` function, first the products already defined are put into the multiplication table.

```
  // First put the already known products for the non-invertible
  // elements into the table.
  mtab[Nearring_Element(0,0).num()]   // 0a = 0
    = Nearring_Element(0,0).num();
  mtab[Nearring_Element(0,3).num()]   // (a3)a = -3
    = Nearring_Element(-3,0).num();
  mtab[Nearring_Element(0,-3).num()]  // (-a3)a = 3
    = Nearring_Element(3,0).num();
  mtab[Nearring_Element(3,0).num()]   // 3a = a3
    = Nearring_Element(0,3).num();
  mtab[Nearring_Element(3,3).num()]   // (3+a3)a = 3-a3
    = Nearring_Element(3,-3).num();
  mtab[Nearring_Element(3,-3).num()]  // (3+a-3)a = -3-a3
    = Nearring_Element(-3,-3).num();
  mtab[Nearring_Element(-3,0).num()]  // -3a = -a3
    = Nearring_Element(0,-3).num();
  mtab[Nearring_Element(-3,3).num()]  // (-3+a3)a = 3+a3
    = Nearring_Element(3,3).num();
  mtab[Nearring_Element(-3,-3).num()] // (-3-a3)a = -3+a3
    = Nearring_Element(-3,3).num();

  // Next also put the two known products for the invertible elements
  // into the table
  mtab[Nearring_Element(0,2).num()]  // (a2)a = -2
    = Nearring_Element(-2,0).num();
  mtab[Nearring_Element(1,-2).num()] // (1-a2)a = -2-a4
    = Nearring_Element(-2,-4).num();
```

After this initialisation the remaining products are determined. This is done in a loop which runs until all products are known. As described in Example 5.2.12, if the products xa and ya are known, the product xya can be determined. Whenever two elements x and y are found for which the products xa and ya are already known, the value of xya is determined and stored in the multiplication table. If also the product xya is already known, it is checked if there is a contradiction to previously determined products. It is also verified that the multiplication table can be filled completely.

```
// The remaining products are determined successively using the
// already known products.  This is done as long as not all products
// are known.
while (number_of_non_defined_products() > 0) {
  // Count the unknown products
  int before = number_of_non_defined_products();

  // Loop over all nearring elements x for which the product xa is
  // already known
  for (int xnum = 0; xnum < 81; ++xnum) {
    if (mtab[xnum] == -1)
      continue;
    Nearring_Element x(xnum);
    Nearring_Element xa(mtab[xnum]);

    // Loop over all nearring elements y for which the product ya is
    // already known
    for (int ynum = 0; ynum < 81; ++ynum) {
      if (mtab[ynum] == -1)
        continue;
      Nearring_Element y(ynum);
      Nearring_Element ya(mtab[ynum]);

      // Determine xy and xya
      Nearring_Element xy = x*y.n() + xa*y.k();
      Nearring_Element xya = x*ya.n() + xa*ya.k();

      // Check if this product leads to a contradiction
      if (mtab[xy.num()] != -1) {
        if (mtab[xy.num()] != xya.num()) {
          // If yes, tell about the contradiction
          std::cerr << "Contradiction:"
                    << "␣␣x␣=␣" << x
                    << "␣␣xa␣=␣" << xa
                    << "␣␣y␣=␣" << y
                    << "␣␣ya␣=␣" << ya
                    << "␣␣xy␣=␣" << xy
                    << "␣␣xya␣=␣" << xya
                    << "␣␣In␣the␣table:␣"
                    << Nearring_Element(mtab[xy.num()])
                    << std::endl;
        }
      }
      else {
        // If there is no contradiction and the product xya is not
        // known up to now, put the newly determined product into
        // the table.
        mtab[xy.num()] = xya.num();
      }
    }
  }

  // Report an error if there were no new products determined.  This
  // means that the nearring multiplication is not completely
  // defined by the products defined initially.  In this case the
  // program has to be aborted.
  if (before == number_of_non_defined_products()) {
    std::cerr << "Did␣not␣find␣new␣products\n";
    std::abort();
  }
}
```

To ensure that the determined multiplication is indeed a nearring multiplication, a check for associativity and left distributivity is done next.

```
// Last the associativity and the left distributivity of the
// nearring multiplication is checked.
bool ass = true;
bool dis = true;
for (int i = 0; i < 81 && ass && dis; ++i) {
  Nearring_Element x(i);
  for (int j = 0; j < 81 && ass && dis; ++j) {
    Nearring_Element y(j);
    for (int k = 0; k < 81 && ass && dis; ++k) {
      Nearring_Element z(k);
      Nearring_Element D1 = x*(y+z);
      Nearring_Element D2 = (x*y)+(x*z);
      Nearring_Element A1 = (x*y)*z;
      Nearring_Element A2 = x*(y*z);
```

```
        // Check distributivity
        if (D1 != D2) {
          // Report any detected error
          std::cout << "Dis:␣" << x << "␣*␣(" << y << "␣+␣" << z
                    << ")␣=␣" << D1 << std::endl
                    << "␣␣␣␣␣" << x << "␣*␣" << y << "␣+␣" << x
                    << "␣*␣" << z << "␣=␣" << D2 << std::endl;
          dis = false;
        }

        // Check associativity
        if (A1 != A2) {
          // Report any detected error
          std::cout << "Ass:␣(" << x << "␣*␣" << y << ")␣*␣" << z
                    << "␣=␣" << A1 << std::endl
                    << "␣␣␣␣␣" << x << "␣*␣(" << y << "␣*␣" << z
                    << ")␣=␣" << A2 << std::endl;
          std::cout << "␣␣␣␣␣" << x << "␣*␣" << y << "␣=␣" << x*y
                    << std::endl << "␣␣␣␣␣" << y << "␣*␣" << z
                    << "␣=␣" << y*z << std::endl;
          ass = false;
        }
      }
    }
  }

  if (!dis) {
    std::cerr << "Distributivity␣error\n";
  }
  if (!ass) {
    std::cerr << "Associativity␣error\n";
  }
  if (!(ass && dis)) {
    std::abort();
  }
```

If the determined multiplication has passed all tests, a list of all products xa for all $x \in R$ is written to the standard output channel in LaTeX format, which can be used directly in the tables given on page 67. Also the inverses of the invertible elements of R are included in the table.

In the following the whole source code of the program is listed.

```
////////////////////////////////////////////////////////////////////////
//
// This program determines the multiplication of a nearring, if only a
// few products are defined.
//
////////////////////////////////////////////////////////////////////////

#include <iostream>
#include <string>
#include <sstream>
#include <cassert>
#include <cstdlib>

////////////////////////////////////////////////////////////////////////
//
// This class describes an element of the nearring.
//
////////////////////////////////////////////////////////////////////////
class Nearring_Element
{
public:
  // Constructor:
  // The element constructed is the tuple (E,A) in the additive group
  // C9 x C9.
  Nearring_Element(int E,
                   int A) :
    e(E%9),
    a(A%9)
  {
    if (e < 0)
      e += 9;
    if (a < 0)
      a += 9;
  }

  // Constructor:
  // The additive group has order 81.  The elements are numbered from
  // 0 to 80, and the element constructed is the element with the
  // number i.
  Nearring_Element(int i) :
    e((i/9)%9),
    a(i%9)
  {
    if (e < 0)
      e += 9;
    if (a < 0)
      a += 9;
  }

  // Addition of two nearring elements
```

```
Nearring_Element
operator+(const Nearring_Element &f) const
{
  return Nearring_Element(e+f.e, a+f.a);
}

// Multiplication of a nearring element with an integer
Nearring_Element
operator*(int i) const
{
  return Nearring_Element(e*i, a*i);
}

// Compare two nearring elements
bool
operator==(const Nearring_Element &f) const
{
  return e == f.e && a == f.a;
}

// The opposite of operator==
bool
operator!=(const Nearring_Element &f) const
{
  return e != f.e || a != f.a;
}

// This function returns the number of a nearring element.
int
num() const
{
  return e*9+a;
}

// This function checks if an element is contained in the subgroup L
// of R
bool
lr() const
{
  return e % 3 == 0 && a % 3 == 0;
}

// This function returns n for the nearring element n+ak
int
n() const
{
  return e;
}

// This function returns k for the nearring element n+ak
```

```
  int
  k() const
  {
    return a;
  }

private:
  int e, a;
};

///////////////////////////////////////////////////////////////////////////
//
// Multiplication table
//
// In this table the product x*a for all nearring elements is stored.
// If this product is still unknown, -1 is stored.  The element
// mtab[i] is the number of the nearring element
// Nearring_Element(i)*a.
//
///////////////////////////////////////////////////////////////////////////
static int mtab[81] = {
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1,
  -1, -1, -1, -1, -1, -1, -1, -1, -1
};

// Multiplication operator for two nearring elements.
Nearring_Element
operator*(const Nearring_Element &x,
          const Nearring_Element &y)
{
  return x*y.n() + Nearring_Element(mtab[x.num()])*y.k();
}

// Returns the multiplicative inverse of a nearring element, if it
// exists.  If the element is not invertible, the zero element is
// returned.
Nearring_Element
inverse(const Nearring_Element &f)
{
  // Check if the element is invertible
  if (f.lr())
    return Nearring_Element(0);

  // Search the inverse and return it.
  for (int i = 0; i < 81; ++i) {
    Nearring_Element x(i);
    if (f*x == Nearring_Element(1,0)) {
      return x;
    }
  }

  // This should never happen, because the inverse must have been
  // found previously.
  assert(false);
}

// Output operator
std::ostream &
operator<<(std::ostream &os, const Nearring_Element &f)
{
  return os << ’(’ << f.n() << ’,’ << f.k() << ’)’;
}

// This function returns LaTeX-code representing a nearring element.
std::string
latex(const Nearring_Element &f)
{
  // Get the data of the element
  int n = f.n();
  int k = f.k();

  // Special treatment for zero
  if (n == 0 && k == 0)
    return std::string("$0$");

  // Ensure that the absolute values of n and k are minimal
  if (n > 4)
    n -= 9;
  if (k > 4)
    k -= 9;

  // Build the LaTeX-Code
  std::ostringstream oss;
  oss << ’$’;
  if (n == 0) {
    if (k < 0) {
      if (k == -1) {
        oss << "-a";
      }
      else {
        oss << "-a␣\\cdot␣" << -k;
      }
    }
    else {
      if (k == 1) {
        oss << "a";
      }
      else {
        oss << "a␣\\cdot␣" << k;
      }
    }
  }
  else {
    oss << n;
    if (k != 0) {
      if (k < 0) {
        if (k == -1) {
          oss << "-a";
        }
        else {
          oss << "-a␣\\cdot␣" << -k;
        }
      }
      else {
        if (k == 1) {
          oss << "+a";
        }
        else {
          oss << "+a␣\\cdot␣" << k;
        }
      }
    }
  }
  oss << '$';

  // Return the generated LaTeX-Code
  return oss.str();
}

// This function counts how many products still are unknown
inline
int
number_of_non_defined_products()
{
  int res = 0;
  for (int i = 0; i < 81; ++i) {
    if (mtab[i] == -1)
      ++res;
  }
  return res;
}

// Main function
```

```
int main()
{
  // First put the already known products for the non-invertible
  // elements into the table.
  mtab[Nearring_Element(0,0).num()]   // 0a = 0
    = Nearring_Element(0,0).num();
  mtab[Nearring_Element(0,3).num()]   // (a3)a = -3
    = Nearring_Element(-3,0).num();
  mtab[Nearring_Element(0,-3).num()]  // (-a3)a = 3
    = Nearring_Element(3,0).num();
  mtab[Nearring_Element(3,0).num()]   // 3a = a3
    = Nearring_Element(0,3).num();
  mtab[Nearring_Element(3,3).num()]   // (3+a3)a = 3-a3
    = Nearring_Element(3,-3).num();
  mtab[Nearring_Element(3,-3).num()]  // (3+a-3)a = -3-a3
    = Nearring_Element(-3,-3).num();
  mtab[Nearring_Element(-3,0).num()]  // -3a = -a3
    = Nearring_Element(0,-3).num();
  mtab[Nearring_Element(-3,3).num()]  // (-3+a3)a = 3+a3
    = Nearring_Element(3,3).num();
  mtab[Nearring_Element(-3,-3).num()] // (-3-a3)a = -3+a3
    = Nearring_Element(-3,3).num();

  // Next also put the two known products for the invertible elements
  // into the table
  mtab[Nearring_Element(0,2).num()]  // (a2)a = -2
    = Nearring_Element(-2,0).num();
  mtab[Nearring_Element(1,-2).num()] // (1-a2)a = -2-a4
    = Nearring_Element(-2,-4).num();

  // The remaining products are determined successively using the
  // already known products.  This is done as long as not all products
  // are known.
  while (number_of_non_defined_products() > 0) {
    // Count the unknown products
    int before = number_of_non_defined_products();

    // Loop over all nearring elements x for which the product xa is
    // already known
    for (int xnum = 0; xnum < 81; ++xnum) {
      if (mtab[xnum] == -1)
        continue;
      Nearring_Element x(xnum);
      Nearring_Element xa(mtab[xnum]);

      // Loop over all nearring elements y for which the product ya is
      // already known
      for (int ynum = 0; ynum < 81; ++ynum) {
        if (mtab[ynum] == -1)
          continue;
        Nearring_Element y(ynum);
        Nearring_Element ya(mtab[ynum]);

        // Determine xy and xya
        Nearring_Element xy = x*y.n() + xa*y.k();
        Nearring_Element xya = x*ya.n() + xa*ya.k();

        // Check if this product leads to a contradiction
        if (mtab[xy.num()] != -1) {
          if (mtab[xy.num()] != xya.num()) {
            // If yes, tell about the contradiction
            std::cerr << "Contradiction:"
                      << "␣␣x␣=␣" << x
                      << "␣␣xa␣=␣" << xa
                      << "␣␣y␣=␣" << y
                      << "␣␣ya␣=␣" << ya
                      << "␣␣xy␣=␣" << xy
                      << "␣␣xya␣=␣" << xya
                      << "␣␣In␣the␣table:␣"
                      << Nearring_Element(mtab[xy.num()])
                      << std::endl;
          }
        }
        else {
          // If there is no contradiction and the product xya is not
          // known up to now, put the newly determined product into
          // the table.
          mtab[xy.num()] = xya.num();
        }
      }
    }

    // Report an error if there were no new products determined.  This
    // means that the nearring multiplication is not completely
    // defined by the products defined initially.  In this case the
    // program has to be aborted.
    if (before == number_of_non_defined_products()) {
      std::cerr << "Did␣not␣find␣new␣products\n";
      std::abort();
    }
  }

  // Last the associativity and the left distributivity of the
  // nearring multiplication is checked.
  bool ass = true;
  bool dis = true;
  for (int i = 0; i < 81 && ass && dis; ++i) {
    Nearring_Element x(i);
    for (int j = 0; j < 81 && ass && dis; ++j) {
      Nearring_Element y(j);
```

```
      for (int k = 0; k < 81 && ass && dis; ++k) {
        Nearring_Element z(k);
        Nearring_Element D1 = x*(y+z);
        Nearring_Element D2 = (x*y)+(x*z);
        Nearring_Element A1 = (x*y)*z;
        Nearring_Element A2 = x*(y*z);

        // Check distributivity
        if (D1 != D2) {
          // Report any detected error
          std::cout << "Dis:␣" << x << "␣*␣(" << y << "␣+␣" << z
                    << ")␣=␣" << D1 << std::endl
                    << "␣␣␣␣␣" << x << "␣*␣" << y << "␣+␣" << x
                    << "␣*␣" << z << "␣=␣" << D2 << std::endl;
          dis = false;
        }

        // Check associativity
        if (A1 != A2) {
          // Report any detected error
          std::cout << "Ass:␣(" << x << "␣*␣" << y << ")␣*␣" << z
                    << "␣=␣" << A1 << std::endl
                    << "␣␣␣␣␣" << x << "␣*␣(" << y << "␣*␣" << z
                    << ")␣=␣" << A2 << std::endl;
          std::cout << "␣␣␣␣␣" << x << "␣*␣" << y << "␣=␣" << x*y
                    << std::endl << "␣␣␣␣␣" << y << "␣*␣" << z
                    << "␣=␣" << y*z << std::endl;
          ass = false;
        }
      }
    }
  }

  if (!dis) {
    std::cerr << "Distributivity␣error\n";
  }
  if (!ass) {
    std::cerr << "Associativity␣error\n";
  }
  if (!(ass && dis)) {
    std::abort();
  }

  // Finally the multiplication table is written to standard output as
  // a table in LaTeX format.
  int column = 0;
  for (int e = 0; e < 9; e += 3) {
    for (int a = 0; a < 9; ++a) {
      Nearring_Element x(e,a);
      if (x.lr())
    continue;
   Nearring_Element xa(mtab[x.num()]);
   Nearring_Element x1 = inverse(x);
   std::cout << latex(x) << "␣&␣" << latex(xa)
        << "␣&␣" << latex(x1);
   ++column;
   if (column == 2) {
    std::cout << "␣\\\\\n\\hline\n";
    column = 0;
   }
   else {
    std::cout << "␣&␣";
   }
  }

  for (int a = 0; a < 9; ++a) {
   Nearring_Element x(e+1,a), y(e+2,a);
   Nearring_Element xa(mtab[x.num()]), ya(mtab[y.num()]);
   Nearring_Element x1 = inverse(x), y1 = inverse(y);
   std::cout << latex(x) << "␣&␣" << latex(xa) << "␣&␣"
        << latex(x1) << "␣&␣"
        << latex(y) << "␣&␣" << latex(ya) << "␣&␣"
        << latex(y1) << "␣\\\\\n\\hline\n";
  }
 }

 // Terminate program successfully
 return 0;
}
```

Appendix B.

GAP-programs used in the proof of Theorem 8.3.11

In the proof of Theorem 8.3.11 some calculations are used, which also could be done by hand, but they can be achieved much faster using a computer system. In this appendix the programs used to get the desired information are described.

The first problem is to determine all groups G of order 32 with $\exp(G) \leq 8$, such that $\mathrm{Aut}(G)$ contains a subgroup isomorphic to D_{16}. Since the automorphism group of E_{32} is very large ($|GL(5,2)| = 2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31 = 9999360$), this group is treated separately – it is well-known that $GL(5,2)$ contains a subgroup isomorphic to D_{16}. To check this using GAP, one does not have to check the whole group $GL(5,2)$, but only a Sylow-2-group. A subgroup of $GL(5,2)$ isomorphic to D_{16} is for example generated by the matrices

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The following GAP-program determines all groups of order 32 with the desired properties.

```
########################################################################
#
# Determine all groups of order 32 with exponent not larger than 8
#
########################################################################

Groups_List := Filtered(AllSmallGroups(32), G -> Exponent(G) <= 8);

########################################################################
#
# The following function checks if the group of automorphisms of the
# group G contains a dihedral subgroup of order 16.  Since it is known
# that GL(5,2) contains a dihedral subgroup of order 16, the case that
# G is elementary abelian is treated separately.
#
########################################################################

Aut_has_subgroup_D_16 := function(G)

    # Local variables

    local AutG, # For the group of automorphisms
          Ord2; # For the automorphisms of order 2

    # Check if G is elementary abelian

    if IsElementaryAbelian(G) then
        return true;
    fi;

    # Determine all automorphisms of order 2

    AutG := AutomorphismGroup(G);
    Ord2 := Filtered(AutG, a -> Order(a) = 2);

    # Return true if and only if there are two automorphisms a and b
    # of order 2, such that a*b has order 8.

    return ForAny(Combinations(Ord2, 2),
                  pair -> Order(Product(pair)) = 8);
end;

########################################################################
#
# Determine all groups G contained in Groups_List, such that the
# automorphism group of G has a dihedral subgroup of order 16.
#
########################################################################

Groups_List := Filtered(Groups_List, Aut_has_subgroup_D_16);
```

Now, `Groups_List` contains 16 groups. The next step is to check that the groups G considered in the proof of Theorem 8.3.11 must have a subgroup L of index 2, such that $o(g) = \exp(G)$ for each $g \in G \setminus L$. Since these subgroups are investigated in more detail, a function which returns all these candidates for L is defined. All groups for which this function returns the empty list are filtered out.

```
#########################################################################
#
# The following function returns a list of all subgroups L of G, such
# that the index of L in G is 2 and all elements of G not contained in
# L have order exp(G).  The fact is used that L has to be normal in G.
#
#########################################################################

Get_L_Candidates := function(G)

    # Local Variables

    local NormalSg; # For the normal subgroups of G

    # Determine all normal subgroups in G, which have index 2

    NormalSg := Filtered(NormalSubgroups(G), N -> Index(G, N) = 2);

    # Return all normal subgroups of G which have the desired
    # property.

    return Filtered(NormalSg,
                   N -> ForAll(G,
                           g -> g in N or Order(g) = Exponent(G)));
end;

#########################################################################
#
# Determine all groups in Groups_List for which Get_L_Candidates
# returns a non-empty list.
#
#########################################################################

Groups_List := Filtered(Groups_List, G -> Get_L_Candidates(G) <> []);
```

Next, Groups_List contains the seven groups which are investigated in detail in the proof of Theorem 8.3.11. Note that the sequence of groups in Groups_List differs from the sequence given in the proof on page 118; the groups in Groups_List are as follows: G_5, G_6, G_7, G_3, G_2, G_4, G_1. If one wants to check if a given group G, which is stored in the GAP-variable G, is contained in Groups_List, one can use the GAP-expression

```
  IdGroup(G) in List(Groups_List, IdGroup);
```

inside GAP. For example, to verify that the group G_3 is contained in Groups_List, the following GAP-code can be used. Note that groups in GAP are always written multiplicatively.

```
########################################################################
#
# Check that G_3 is contained in Groups_List.
#
########################################################################

# First construct the free group on three generators and assign the
# generators to the variables a, b, and c.

F := FreeGroup(["a", "b", "c"]);
a := F.1;
b := F.2;
c := F.3;

# Now define the relations of the group G_3 and construct the group
# G_3 using these relators.

Rel := [ a^4, c^4, Comm(b,c), a^2/b^2, b^a*b, c^a*c ];
G_3 := F/Rel;

# Check if G_3 is contained in Groups_List.

group_in_list := IdGroup(G_3) in List(Groups_List, IdGroup);
if group_in_list then
    Print("The group is contained in Groups_List.\n");
else
    Print("The group is not contained in Groups_List.\n");
fi;
```

After determining $\mathcal{L}(G)$ for a given group G using Get_L_Candidates the set $\mathcal{D}(G)$ has to be calculated. This is done by the following function.

```
########################################################################
#
# The following function returns a list of all subgroups of the
# automorphism group of G which are isomorphic to D_16.
#
########################################################################

Get_D16_Automorphism_Groups := function(G)

    # Local variables

    local AutG,  # The automorphism group of G
          Ord2,  # The automorphisms of order 2
          Pairs; # Pairs of automorphisms of order 2

    # Determine all automorphisms of G of order 2

    AutG := AutomorphismGroup(G);
    Ord2 := Filtered(AutG, a -> Order(a) = 2);
    # Determine all pairs of automorphisms of order 2 of G which
    # generate a dihedral group of order 16.

    Pairs := Combinations(Ord2, 2);
    Pairs := Filtered(Pairs, p -> Order(Product(p)) = 8);

    # Return the set of groups generated by the pairs of automorphisms
    # determined in the last step.  To avoid dublicates the function
    # Set is used instead of List.

    return Set(Pairs, Group);
end;
```

The first group to be checked by GAP is G_2. Since $|\mathcal{L}(G_2)| = 1$, there is only one possibility for L_R. The check of all 336 dihedral groups contained in $\mathcal{D}(G_2)$ is done by the following GAP-code.

```
# First select the group and determine L(G) and D(G).  L and Rx, the
# set of elements if G not contained in L, are also assigned.

G := Groups_List[5];
Ls := Get_L_Candidates(G);
L := Ls[1];
Rx := Filtered(G, g -> not g in L);
D_16_List := Get_D16_Automorphism_Groups(G);

# Print some information

Print("Number of candidates for L: ", Length(Ls), "\n");
Print("Number of dihedral automorphism groups of order 16: ",
      Length(D_16_List), "\n");

# For each D in D_16_List and each r in Rx determine the size of the
# set { r^delta | delta in D }.

res := Set(D_16_List,
           D -> Set(Rx, r -> Length(Set(D, delta -> r^delta))));
Print("Result: ", res, "\n");
```

The groups G_3 and G_4 are treated in a similar way.

Finally the verification of the argument that a certain normal subgroup $\mathfrak{A}$ of G cannot be the annihilator of L_R is explained. This applies for instance to G_5, for which it will be described here. The code for G_6 is nearly the same.

```
# First select G_5 and determine L and the generators of G

G := Groups_List[1];
Ls := Get_L_Candidates(G);
L := Ls[1];
Gens := [ G.1, G.2, G.3 ];
a := Gens[1];
b := Gens[2];
c := Gens[3];

# Determine D(G)

D16s := Get_D16_Automorphism_Groups(G);

# Determine the candidates for the annihilator of L

Anul_Cands := Filtered(NormalSubgroups(G),
                      N -> a^4 in N and c in N and not a^2 in N);

# Check if for one of the possible annihilators Anul there is a
# subgroup D of Aut(G) isomorphic to D_16, such that
#   b^delta + Anul = b + Anul
# for every delta in D.
# Note again that groups in GAP are written multiplicatively.

found := false;
for Anul in Anul_Cands do
    found := ForAny(D16s, D -> ForAll(D, delta -> b^delta/b in Anul));
    if found then
        Print("Found a candidate for the annihilator.\n");
        break;
    fi;
od;
if not found then
    Print("No candidate for the annihilator found.\n");
fi;
```

The GAP-calculations used to investigate G_1 and G_7 are elementary and need no further explanations.

Bibliography

[1] Erhard Aichinger, Franz Binder, Jürgen Ecker, Peter Mayr, and Christof Nöbauer. *SONATA – System of Nearrings and their Applications, Version 2.3.* Johannes Kepler Universität Linz, 2004. (`http://www.algebra.uni-linz.ac.at/Sonata/`).

[2] Bernhard Amberg, Silvana Franciosi, and Francesco de Giovanni. *Products of groups.* Oxford Mathematical Monographs. Clarendon Press, Oxford, 1992.

[3] Bernhard Amberg, Peter Hubert, and Yaroslav Sysak. Local nearrings with dihedral multiplicative group. *J. Algebra*, 273(2):700–717, 2004.

[4] Bernhard Amberg and Yaroslav Sysak. Radical rings and products of groups. In *Campbell, C. M. (ed.) et al., Groups St. Andrews 1997 in Bath. Selected papers of the international conference, Bath, UK, July 26–August 9, 1997. Vol. 1. Cambridge: Cambridge University Press. Lond. Math. Soc. Lect. Note Ser. 260, 1-19* . 1999.

[5] Czeslaw Baginski and Izabela Malinowska. On groups of order p^n with automorphisms of order p^{n-2}. *Demonstr. Math.*, 29(3):565–575, 1996.

[6] James C. Beidleman. Quasi-regularity in near-rings. *Math. Z.*, 89:224–229, 1965.

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

[8] Leonard Eugene Dickson. Definitions of a group and a field by independent postulates. *Trans. Amer. Math. Soc.*, 6:198–204, 1905.

[9] The GAP Group, Aachen, St Andrews. *GAP – Groups, Algorithms, and Programming, Version 4.4.3*, 2004. (`http://www-gap.dcs.st-and.ac.uk/~gap`).

[10] Alexander Gorodnik. Local near-rings with commutative groups of units. *Houston Journal of Mathematics*, 25:223–234, 1999.

[11] George Grätzer. *Universal algebra.* (The University Series in Higher Mathematics.) Princeton, N.J.-Toronto-London-Melbourne: D. Van Nostrand Company, Inc. XVI, 368 p., 1968.

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

[13] Marshall Hall jun. and James K. Senior. *The groups of order* 2^n $(n \leq 6)$. New York: The Macmillan Company; Toronto, Ontario: Collier-Macmillan Canada, Ltd. 255 p., 1964.

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

[15] Carlton J. Maxson. Local near-rings of cardinality p^2. *Can. Math. Bull.*, 11:555–561, 1968.

[16] Carlton J. Maxson. On local near-rings. *Math. Z.*, 106:197–205, 1968.

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

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

[19] Derek J. S. Robinson. *A course in the theory of groups.* Graduate Texts in Mathematics, 80. Springer-Verlag, New York Heidelberg Berlin, 1982.

[20] Yaroslav P. Sysak. Products of infinite groups. Preprint 82.53, Akad. Nauk. Ukrainy, Inst. Mat. Kiev, 1982.

[21] Yaroslav P. Sysak. Products of locally cyclic, torsion-free groups. *Algebra Logic*, 25(6):425–433, 1986.

[22] Heinz Wähling. *Theorie der Fastkörper.* Thales Verlag, Essen, 1987.

[23] Hanns Joachim Weinert. Ringe mit nichtkommutativer Addition. I. 1975.