Note di Matematica
Note Mat. 28 (2008), suppl. n. 2, 177-211
ISSN 1123-2536, e-ISSN 1590-0932
DOI 10.1285/i15900932v28n2supplp177
http://siba-ese.unisalento.it, © 2008 Università del Salento

Products of groups and local nearrings

Yaroslav P. Sysak
Institute of Mathematics,
Ukrainian National Academy of Science,
01601 Kiev, Ukraine
sysak@imath.kiev.ua

Abstract. Groups which can be written as a product $G = AB$ of two of its subgroups A and B have been studied by many authors. A particular role in such investigations play groups of the form $G = AB = AM = BM$ where M is a normal subgroup of G and $A \cap M = B \cap M = 1$. It turns out that there is a close connection between groups of this form and some nearrings, especially so called local nearrings, so that many problems concerning such nearrings can be reduced to questions about these groups. In the following we will discuss different aspects of this connection and, in addition, consider in detail certain structural questions arised in the case of almost cyclic subgroups A and B.

Keywords: factorized group; derivation; local nearring; multiplicative group.

MSC 2000 classification: MSC 2000 classification: Primary 16N20, 16U60. Secondary 20M25

1 Introduction

Let $G = AB = \{ab \mid a \in A, b \in B\}$ be a group factorized by two subgroups A and B and let N be a normal subgroup of G. Then $AN \cap BN = N(A \cap BN) = N(B \cap AN) = (A \cap BN)(B \cap AN)$ (see [1], Lemma 1.1.4). This means that many problems about factorized groups can be reduced to groups of the form $G = AB = AM = BM$ where M is a normal subgroup of G.

If M is abelian, then the intersections $A \cap M$ and $B \cap M$ are normal subgroups of G and so the subgroup $C = (A \cap M)(B \cap M)$ is normal in G. Passing to the factor group G/C, we arrive at a group $G = AB = AM = BM$ with $A \cap M = B \cap M = 1$. In this case A and B are complements to M in the semidirect product $G = M \rtimes A$, and M is a so-called radical A-module whose properties were in detail described by the author in [33] and can also be found in [3]. Although in the general case $A \cap M$ and $B \cap M$ need not be normal in G, the groups of the form $G = M \rtimes A = M \rtimes B = AB$ with a not necessarily abelian normal subgroup M and complements A and B have also some special properties and so are of interest. In what follows these groups will be called *triply factorized.* It turns out that they appear in a natural way during the study of nearrings, especially local nearrings. In the following we will discuss some aspects of a connection between such groups and nearrings. The reader is referred to the book by B. Amberg, S. Franciosi and F. de Giovanni [1] for many results about factorized groups and to the books by J. Clay [6], J. Meldrum [22] or G. Pilz [27] for terminology, definitions and basic facts of nearrings.

2 Products of groups close to be abelian

It seems intuitively clear that the structure of a group $G = AB$ factorized by two subgroups A and B should somehow be determined by that of the factors A and B. Unfortunately, without additional assumptions on G there exist only some few results in this direction. The first of them, obtained by a surprisingly simple commutator calculation more that fifty years ago, is a well-known theorem of Itô [17].

1 Theorem. *If $G = AB$ and the subgroups A and B are abelian, then the group G is metabelian, i.e. its derived subgroup G' is abelian.*

Since here G' coincides with the commutator subgroup $[A, B]$, the proof is reduced to verifying the relation $[a, b]^{x^{-1}y^{-1}} = [a, b]^{y^{-1}x^{-1}}$ for all $a, x \in A$ and $b, y \in B$ which is equivalent to the relation $[a, b][x, y] = [x, y][a, b]$ (see also [1], Theorem 2.1.1 for details).

Almost all results concerning the structure of the group $G = AB$ with abelian subgroups A and B are based on this theorem. One of the first is due to P. Cohn [8] who proved that in the case of infinite cyclic subgroups A and B there exists a non-trivial normal subgroup of G which is contained in A or B. A complete description of this case can be found in [31].

A first generalization of Itô's theorem for the case of central-by-finite subgroups A and B was obtained by N. Chernikov [5] after twenty five years.

2 Theorem. *If $G = AB$ is a group with central-by-finite subgroups A and B, then G is soluble-by-finite.*

The original proof of this theorem was also expounded in [1], Theorem 2.2.5. Since central-by-finite groups are finite-by-abelian by Schur's theorem, the following "non-symmetrical" generalization of D. Zaitsev [39] should be seen in relation with Theorem 2.

3 Theorem. *Let the group $G = AB$ be factorized by an abelian subgroup A and a finite-by-abelian subgroup B. Then G is soluble-by-finite. Moreover, if the subgroup B is nilpotent with derived subgroup B' of order n, then G is soluble with derived length at most $2 + 3 \log n$.*

This theorem was in fact derived by Zaitsev as a corollary from his more general result concerning groups factorized by an abelian subgroup A and an FC-subgroup B. Taking the center $Z(B)$ of B and developing Itô's approach for the commutator subgroup $[A, Z(B)]$, he established in [39] the following criterion for the nonsimplicity of such factorized groups. Recall that an FC-group is a group in which all conjugacy classes are finite.

4 Theorem. *Let $G = AB$ be a group factorized by an abelian subgroup A and an FC-subgroup B. If the center of B is non-trivial, then G contains a non-trivial normal FC-subgroup.*

As an application, from this criterion and a well-known theorem of Kegel and Wielandt about solubility of finite groups factorized by two nilpotent subgroups (see [1], Theorem 2.4.3) it follows that *every group factorized by an abelian subgroup and a locally nilpotent FC-subgroup is hyperabelian*, i.e it has an ascendant series of normal subgroups with abelian factors. Detailed proofs of these results can also be found in [1], Section 7.3.

Some other result in this direction was later proved by Jabara [12].

5 Theorem. *Let $G = AB$ be a group factorized by an elementary abelian 2-subgroup A and a periodic subgroup B without elements of even order. If B is hypercentral, i.e. it has an ascendant central series, then G is hyperabelian; moreover, if B is soluble with derived length d, then G has derived length at most $2d$.*

It should be noted that the theorems listed above are ones of the few results on factorized groups $G = AB$ with conditions imposed on subgroups A an B and without further restrictions (like solubility or finiteness conditions) on G.

In connection with Itô's theorem the following conjecture seems to be natural.

6 Conjecture. *Every group $G = AB$ with abelian-by-finite subgroups A and B is metabelian-by-finite.*

In such a form this conjecture was formulated by J. Wilson in [37] and confirmed him for the case when the group $G = AB$ is soluble-by-finite and minimax. As a question, Conjecture 6 is also contained in the book of B. Amberg, S. Franciosi and F. de Giovanni (see [1], Question 3). It was verified for linear groups by the author [32] (observe that every soluble-by-finite and minimax group is in fact linear) and for residually finite groups by J. Wilson (see [38] or [1], Theorem 2.3.4). However, without these restrictions on G untill recently there were no results known in this direction.

3 Linear products of abelian-by-finite groups

In this section it will be shown that the above conjecture is valid in the case of linear groups. It is assumed that the reader knows some basic definitions and simplest statements about linear algebraic groups and their Zariski topology. All of them can be found for instance in chapters 5 and 14 of the book of B.A.F. Wehrfritz [36].

7 Theorem. *Let the linear group $G = AB$ be the product of two abelian-by-finite subgroups A and B. Then G is metabelian-by-finite.*

Recall that for each linear group G there exist a positive integer n and an algebraically closed field F such that G can be viewed as a subgroup of the group $GL(n, F)$ of all invertible $n \times n$ matrices over F. Let $\bar{G}$ be the closure of G in the Zariski topology of $GL(n, F)$ and let $(\bar{G})_0$ be the connected component of $\bar{G}$ containing 1. It is well-known that $(\bar{G})_0$ is a normal subgroup of finite index in $\bar{G}$ and so if $G_0 = G \cap (\bar{G})_0$, then $\bar{G_0} = (\bar{G})_0$.

8 Lemma. *Let the linear group $G = AB$ be the product of two subgroups A and B. If G_0, A_0 and B_0 are the connected components containing* 1 *of G, A and B, respectively, then $G_0 \subseteq \bar{A}_0\bar{B}_0$.*

Proof. Clearly the subgroups A_0 and B_0 are contained in G_0 and there exist elements $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$ such that

$$G = \bigcup_{i=1}^{n} a_i A_0 B_0 b_i.$$

It is easy to see that, for each i, either $G_0 \cap a_i A_0 B_0 b_i = \emptyset$ or $a_i A_0 B_0 b_i \subseteq G_0$. Therefore

$$G_0 = \bigcup_{j=1}^{m} a_{i_j} A_0 B_0 b_{i_j}$$

and hence

$$\bar{G_0} = \bigcup_{j=1}^{m} a_{i_j} \overline{A_0 B_0} b_{i_j}.$$

As $\bar{G_0} = (\bar{G})_0$, this implies that $\bar{G_0} = \overline{A_0 B_0}$. Obviously $a_{i_j} \bar{A}_0 \bar{B}_0 b_{i_j} \subseteq \bar{G_0}$ and either

$$a_{i_j} \bar{A}_0 \bar{B}_0 b_{i_j} \cap a_{i_k} \bar{A}_0 \bar{B}_0 b_{i_k} = \emptyset$$

or

$$a_{i_j} \bar{A}_0 \bar{B}_0 b_{i_j} = a_{i_k} \bar{A}_0 \bar{B}_0 b_{i_k}.$$

By [36], Lemma 14.9, the set $\bar{A}_0 \bar{B}_0$ contains a non-empty open subset U of its closure $\overline{\bar{A}_0 \bar{B}_0} = \overline{A_0 B_0} = \bar{G_0}$. Since the intersection $U \cap aUb$ is non-empty for all $a, b \in \bar{G_0}$ and the subgroup $\bar{G_0}$ is connected, it follows that $a_{i_j} \bar{A}_0 \bar{B}_0 b_{i_j} = \bar{A}_0 \bar{B}_0$ for every j and so

$$G_0 = \bigcup_{j=1}^{m} a_{i_j} A_0 B_0 b_{i_j} \subseteq \bigcup_{j=1}^{m} a_{i_j} \bar{A}_0 \bar{B}_0 b_{i_j} = \bar{A}_0 \bar{B}_0,$$

as claimed. $\boxed{QED}$

The following lemma is another generalization of Itô's theorem obtained by a similar approach.

9 Lemma. *Let G be a group and A, B its abelian subgroups. If H is a subgroup of G contained in the set AB, then H is metabelian.*

Proof. It suffices to show that for any elements g, h, x, y of H the commutators $[g,h]$ and $[x,y]$ are permutable. Since $H = H^{-1} \subseteq BA$, it follows that every element $g \in H$ can be written in the form $g = a_g b_g = \bar{b}_g \bar{a}_g$ for some elements $a_g, \bar{a}_g$ of A and $b_g, \bar{b}_g$ of B. Therefore

$$[g,h] = [a_g b_g, a_h b_h] = [a_g, a_h b_h]^{b_g} [b_g, a_h b_h] = [a_g, b_h]^{b_g} [b_g, a_h]^{b_h} =$$
$$[b_g^{-1}(a_g b_g), b_h][b_g, b_h^{-1}(a_h b_h)] = [b_g^{-1}(\bar{b}_g \bar{a}_g), b_h][b_g, b_h^{-1}(\bar{b}_h \bar{a}_h)] = [\bar{a}_g, b_h][b_g, \bar{a}_h].$$

Similarly $[x,y] = [\bar{a}_x, b_y][b_x, \bar{a}_y]$ for some elements $\bar{a}_x, \bar{a}_y$ of A and b_x, b_y of B. Hence it remains to check that the commutators $[\bar{a}_g, b_h]$ and $[\bar{a}_x, b_y]$ are permutable.

Indeed, we have

$$\bar{a}_x b_h \bar{a}_x^{-1} = \bar{a}_x a_h^{-1}(a_h b_h)(\bar{a}_x^{-1} \bar{b}_x^{-1})\bar{b}_x = \bar{a}_x a_h^{-1}(hx^{-1})\bar{b}_x =$$
$$(\bar{a}_x a_h^{-1} a_{hx^{-1}})(b_{hx^{-1}} \bar{b}_x) = a_0 b_0$$

with $a_0 = \bar{a}_x a_h^{-1} a_{hx^{-1}} \in A$ and $b_0 = b_{hx^{-1}} \bar{b}_x \in B$. Next

$$b_y \bar{a}_g b_y^{-1} = b_y \bar{b}_g^{-1}(\bar{b}_g \bar{a}_g)(b_y^{-1} a_y^{-1})a_y = b_y \bar{b}_g^{-1}(gy^{-1})a_y =$$
$$(b_y \bar{b}_g^{-1} \bar{b}_{gy^{-1}})(\bar{a}_{gy^{-1}} a_y) = b_1 a_1$$

with $b_1 = b_y \bar{b}_g^{-1} \bar{b}_{gy^{-1}} \in B$ and $a_1 = \bar{a}_{gy^{-1}} a_y \in A$. Thus

$$[\bar{a}_g, b_h]^{\bar{a}_x^{-1} b_y^{-1}} = [\bar{a}_g, a_0 b_0]^{b_y^{-1}} = [b_y \bar{a}_g b_y^{-1}, b_0] = [b_1 a_1, b_0] = [a_1, b_0]$$

and similarly

$$[\bar{a}_g, b_h]^{b_y^{-1} \bar{a}_x^{-1}} = [b_1 a_1, b_h]^{\bar{a}_x^{-1}} = [a_1, \bar{a}_x b_h \bar{a}_x^{-1}] = [a_1, a_0 b_0] = [a_1, b_0].$$

Therefore $[\bar{a}_g, b_h]^{\bar{a}_x^{-1} b_y^{-1}} = [\bar{a}_g, b_h]^{b_y^{-1} \bar{a}_x^{-1}}$ and so $[\bar{a}_g, b_h]^{[\bar{a}_x, b_y]} = [\bar{a}_g, b_h]$, as desired. $\boxed{QED}$

Proof. of Theorem 7. Since the subgroups A and B of the group $G = AB \leq GL(n,F)$ are abelian-by-finite, their connected components A_0 and B_0 containing 1 are abelian. Let $\bar{A}_0$ and $\bar{B}_0$ be the closures of A_0 and B_0 in the Zariski topology of $GL(n,F)$. Then $\bar{A}_0$ and $\bar{B}_0$ are abelian subgroups of $GL(n,F)$ and $G_0 \leq \bar{A}_0 \bar{B}_0$ by Lemma 8. Hence the subgroup G_0 is metabelian by Lemma 9 and so the group G is metabelian-by-finite. $\boxed{QED}$

4 On products of cyclic-by-finite groups

The following theorem proved in [4] is a first result confirming Conjecture 6 in the case when no additional assumptions on the group $G = AB$ with abelian-by-finite subgroups A and B are given.

10 Theorem. *Let the group $G = AB$ be the product of two subgroups A and B each of which has a cyclic subgroup of index at most 2. Then G is metacyclic-by-finite and soluble.*

Recall that the structure of the finite group $G = AB$ satisfying the hypothesis of Theorem 10 was investigated by B. Huppert [16], W. Scott [29] and V. Monakhov [23, 24]. In particular, in [23] it was shown that in this case G is soluble.

It is easy to see that up to isomorphism there exists only one non-abelian infinite group with a cyclic subgroup of index 2, namely the infinite dihedral group. As dihedral groups have "enough" involutions, i.e. elements of order 2, an essential role in the proof of Theorem 10 is played by the well-known fact that every two involutions of a group generate a dihedral subgroup. A key role of involutions can partly be illustrated by the proof of the following lemma describing a situation in which infinite cyclic subgroups of the factors A and B of the group $G = AB$ are permutable.

11 Lemma. *Let G be a group of the form $G = AB$ with infinite dihedral subgroups A and B whose intersection $A \cap B$ is of order 2. If $<a>$ and $<b>$ are the cyclic subgroups of index 2 of A and B, respectively, then $<a><b>=<b><a>$.*

Proof. If c is the involution of $A \cap B$, then $cac = a^{-1}$ and $cbc = b^{-1}$, so that for all integers m, n the elements $a^m c$ and cb^n are involutions of G. Assume that the element $a^m b^n$ is also an involution for some non-zero m, n and show that then both m and n must be odd integers.

Indeed, otherwise one of the involutions $a^m c$ or cb^n is a conjugate of c because $a^{2k}c = a^k c a^{-k}$ and $cb^{2k} = b^{-k} c b^k$ for every integer k. Since $(a^m c)(cb^n) = a^m b^n = (a^m b^n)^{-1} = (cb^n)(a^m c)$, this implies that c is centralized by an involution which is different from c. On the other hand, $<c>= A \cap B$ and $N_A(A \cap B) = A \cap B = N_B(A \cap B)$, so that $N_G(A \cap B) = N_A(A \cap B) N_B(A \cap B) = A \cap B$. Therefore the subgroup $<c>$ is self-centralized and this means that both m and n are odd, as desired.

Show now that the subgroups $< a >$ and $< b >$ are permutable. As every element of G can uniquely be written in one of the forms $a^m cb^n$ or $a^m b^n$ for some m, n, it suffices to prove that for any integers k, l, m, n the equality $b^l a^k = a^m cb^n$ is impossible.

Indeed, in the other case for some k, l, m, n the following equalities hold:

$b^la^kb^{-n} = a^mc$, $a^{-m}b^la^k = cb^n$ and $b^{-l}a^mb^{-n} = a^kc$. As the elements a^mc, cb^n and a^kc are involutions, this implies the equalities $b^la^kb^{-n} = b^na^{-k}b^{-l}$, $a^{-m}b^la^k = a^{-k}b^{-l}a^m$ and $b^{-l}a^mb^{-n} = b^na^{-m}b^l$ which can be rewritten in the form $a^{-k}b^{n-l} = b^{l-n}a^k$, $a^{m-k}b^{-l} = b^la^{k-m}$ and $a^mb^{-l-n} = b^{l+n}a^{-m}$. Therefore the elements $a^{-k}b^{n-l}$, $a^{m-k}b^{-l}$ and a^mb^{-l-n} are involutions and hence the integers k, $m-k$ and m must simultaneously be odd by proved above. But if k and m are odd, then $m-k$ is even and this contradiction completes the proof. $\boxed{QED}$

Considering Theorem 10, one suspects that the following conjecture is valid.

12 Conjecture. *Every group $G = AB$ with cyclic-by-finite subgroups A and B is metacyclic-by-finite.*

It seems that a main problem here is to prove that G is soluble-by-finite because in this case G is polycyclic-by-finite by a theorem of Lennox, Roseblade and Zaitsev (see [1], Theorem 4.4.2). Since each cyclic-by-finite group contains a finite normal subgroup modulo which it is either cyclic or infinite dihedral, for this purpose it suffices to consider the case when at least one of these subgroups is finite-by-dihedral and so has "enough" involutions. Indeed, if both subgroups A and B are finite-by-cyclic, then they are central-by-finite and thus the group $G = AB$ is soluble-by-finite by Theorem 2. This gives a hope to confirm Conjecture 12 developing arguments used for the proof of Theorem 10.

5 Triply factorized groups with cyclic-by-finite complements

In this part Conjecture 12 will be verified for a special case of triply factorized groups $G = M \rtimes A = M \rtimes B = AB$ with a periodic normal subgroup M. The above remarks concerning this conjecture show that M must be finite if it is soluble-by-finite. Bearing in mind a subsequent application of these groups in studying of local nearrings, we will restrict here our attention to the case when M is a p-group. The following theorem gives for this case the same answer.

13 Theorem. *Let $G = M \rtimes A = M \rtimes B = AB$ be a triply factorized group whose subgroups A and B are cyclic-by-finite. If the normal subgroup M is a p-group, then it is finite.*

The proof of this theorem is divided in several lemmas. The first of them is elementary and describes the structure of cyclic-by-finite groups.

14 Lemma. *Let A be a cyclic-by-finite group. Then either A is central-by-finite or A contains a finite normal subgroup K such that the factor group A/K is infinite dihedral. Moreover, in the second case there exist elements a of* *infinite order and c of finite order of A such that $A = (K \rtimes <a>) <c>$ with $c^2 \in K$ and $c^{-1}ac = a^{-1}x$ for some $x \in K$ where $x = 1$ for the subgroup K of odd order.*

The next lemma is an immediate consequence of Theorem 2 and the remarks concerning Conjecture 12.

15 Lemma. *Let $G = M \rtimes A = M \rtimes B = AB$ be a triply factorized group with a periodic normal subgroup M and cyclic-by-finite subgroups A and B. If M is soluble-by-finite or A is central-by-finite, then M is finite.*

The following lemma deals with the case when M is a 2-group.

16 Lemma. *Let $G = M \rtimes A = M \rtimes B = AB$ be a group satisfying the hypothesis of Theorem 13 and let $A \cap B = 1$. If M is an infinite 2-group and A contains no subgroup of order 4, then there exists an infinite abelian subgroup Z of M normalized by a subgroup of finite index of G.*

Proof. The subgroup A is not central-by-finite by Lemma 15 and so it contains a finite normal subgroup K of odd order and an infinite cyclic subgroup $<a>$ such that $A = K \rtimes (<a> \rtimes <c>)$ for some involution $c \in A$ with $a^c = a^{-1}$ by Lemma 14. As $MK = M(B \cap (MK))$ and $M <a> = M(B \cap (M <a>))$, there exist a finite normal subgroup L of B and elements $y \in M$ and $b \in B$ such that $MK = ML$, $ay = b$ and $<b> = B \cap (M <a>)$. Furthermore, there exists an involution $d \in B$ such that $M <c> = M <d>$ and $cx = d$ for some $x \in M$. Clearly then $B = L \rtimes (<b> \rtimes <d>)$ with $b^d = b^{-1}$ and the elements y, x are non-trivial because $A \cap B = 1$.

Show first that every element $z \in M$ can be written in the form $ua^m cb^m dv$ or $ua^{-m}b^m v$ for some elements $u \in K$ and $v \in L$ such that $uv \in M$ and some integer m. As $G = AB$, the element z has to coincide with one of the elements $ua^m cb^n dv$, $ua^m cb^n v$, $ua^m b^n dv$ or $ua^m b^n v$ for some elements $u \in K$ and $v \in L$ and some integers m, n. Clearly the elements $a^m c \in A$ and $b^n d \in B$ are involutions for any m, n and so the elements $ua^m c \in A$ and $b^n dv \in B$ are of finite order. Therefore the equalities $z = ua^m cb^n v$ or $z = ua^m b^n dv$ are excluded. Indeed, otherwise there are non-zero integers m, n such that $b^n = (a^m c)u^{-1}zv^{-1} \in (MK)(a^m c)$ or $a^m = u^{-1}zv^{-1}(b^n d) \in (MK)(b^n d)$ from which $m = n = 0$. But then $z = ucv$ or $z = udv$ and hence $c = u^{-1}zv^{-1} \in MK$ or $d = u^{-1}zv^{-1} \in MK$ which is not the case. Thus z can coincide only with elements $ua^m cb^n dv$ or $ua^m b^n v$ for some m, n. Since $ay = b$ and so $a^m y_m = b^m$ for some element $y_m \in M$ and since $cx = d$, the equality $z = ua^m cb^n dv = ua^m ca^n y_n cxv = (ua^{m-n}v)(v^{-1}cy_n cxv)$ implies the inclusion $ua^{m-n}v = z(v^{-1}cy_n cxv)^{-1} \in M$ which is possible only if $m = n$ and $uv \in M$. Similarly, from $z = ua^m b^n v = ua^{m+n}y_n v$ it follows that $m = -n$ and $uv \in M$.

Thus

$$M = \{ua^m cb^m dv,\ ua^{-m}b^m v \mid m \in \mathbb{Z}\},\ u \in K,\ v \in L,\ uv \in M\},$$

as desired.

Show next that there exist infinitely many positive integers m such that the elements $a^{-m}b^m \in M$ are involutions. Clearly we may assume that M does not satisfy the minimal condition for abelian subgroups because otherwise it is a Chernikov 2-group by a result of Shunkov [30]. Then there exist an infinite elementary abelian subgroup E of M and two elements $u \in K$ and $v \in L$ with $uv \in M$ such that E contains the elements $ua^m cb^m dv$ or $ua^{-m}b^m v$ for infinitely many integers m. Assume that $m < n$ and both elements $ua^m cb^m dv$ and $ua^n cb^n dv$ belongs to E. Then $ua^m cb^m dv = v^{-1}b^m da^m cu^{-1}$ and so $(v^{-1}b^m da^m cu^{-1})(ua^n cb^n dv) = (v^{-1}db^{-m})(a^{m-n}b^{n-m})(b^m dv) \in E$. Therefore the element $a^{m-n}b^{n-m} \in E^{v^{-1}db^{-m}}$ is an involution for each $n > m$ with $ua^n cb^n dv \in E$. Similarly, if both $ua^{-m}b^m v$ and $ua^{-n}b^n v$ are contained in E, then $a^{m-n}b^{n-m} \in E^{v^{-1}b^{-m}}$ for each $n > m$ with $ua^{-n}b^n v \in E$.

Finally, let $z = a^{-m}b^m$ be the involution of M in which the positive integer m is minimal. If n is the least integer with $n > m$ such that the element $a^{-n}b^n \in M$ is an involution, then from the equalities $a^{-m}b^m = b^{-m}a^m$ and $a^{-n}b^n = b^{-n}a^n$ it follows that $a^{-m}b^{m-n}a^n = a^{-n}b^{n-m}a^m$ and so the element $a^{m-n}b^{n-m} = b^{m-n}a^{n-m}$ is also an involution of M with $0 < n - m < n$. Therefore $n - m = m$ by the choice of n and hence $n = 2m$. Arguing by induction on n, this implies that for each $k \geq 1$ the element $a^{-km}b^{km}$ is an involution of M. Since $a^m z = b^m$ and so $a^{-km}b^{km} = z^{a^{(k-1)m}} \cdots z^{a^m} z$, it follows that the involutions $z, z^{a^m}, \cdots, z^{a^{km}}, \cdots$ are permutable. Hence the subgroup $Z = < z^{a^{km}} \mid k \in \mathbb{Z} >$ is infinite abelian and normalized by the subgroups $< a^m >$ and $< b^m >$. Thus Z is normalized by the subgroup $< a^m, b^m >$ whose index in the group $G = AB$ is finite by [1], Lemma 1.2.5, as desired. $\boxed{QED}$

The final lemma reduces the proof to the case when A contains no subgroups of order 4.

17 Lemma. *Let $G = M \rtimes A = M \rtimes B = AB$ be a group satisfying the hypothesis of Theorem 13 and let its normal subgroup M be infinite periodic. If the subgroup A contains an involution i whose centralizer $C_A(i)$ in A is infinite, then i is contained in a finite normal subgroup of G.*

Proof. Clearly $C_A(i)$ is a subgroup of finite index in A and so the conjugacy class $\{i^a \mid a \in A\}$ of i in A is finite. If the centralizer $C_M(i)$ of i in M is finite, then the subgroup M is soluble-by-finite by a theorem of Shunkov [30] and so finite by Lemma 15 which is not the case. Therefore $C_M(i)$ is infinite and hence there exists an infinite subset $\mathcal{A}$ of A such that $C_M(i) = \{ab_a \mid a \in \mathcal{A},\ b_a \in B\}$.

Clearly $b_a \neq b_{a'}$ if $a \neq a'$, so that the set $\{b_a \mid a \in \mathcal{A}\}$ is also infinite. Since $i^{ab_a} = i$ for each $a \in \mathcal{A}$ and thus $i^a = i^{b_a^{-1}}$, the set $\{i^{b_a^{-1}} \mid a \in \mathcal{A}\}$ is finite because so is the conjugacy class $\{i^a \mid a \in A\}$. Therefore there exists an infinite subset $\mathcal{B}$ of $\{b_a^{-1} \mid a \in \mathcal{A}\}$ such that $i^b = i^{b'}$ for all $b, b' \in \mathcal{B}$. Then the set $\mathcal{B}b^{-1}$ with $b \in \mathcal{B}$ is also infinite and centralizers i. Hence the centralizer $C_B(i)$ is infinite and so has a finite index in B. But then the join $<C_A(i), C_B(i)>$ is a subgroup of finite index in G by [1, Lemma 1.2.5] and thus the conjugacy class $\{i^g \mid g \in G\}$ of i in G is finite. Therefore the normal subgroup generated by this class contains i and is finite by Dietzmann's lemma. $\boxed{QED}$

Proof. of Theorem 13 Assume that the theorem is false and choose a counterexample $G = M \rtimes A = M \rtimes B = AB$ with an infinite p-subgroup M and cyclic-by-finite subgroups A and B. Then A is not central-by-finite by Lemma 15 and so it contains a finite normal subgroup K such that the factor group A/K is infinite dihedral. Since A and so B satisfies the maximal condition on subgroups, the group $G = AB$ satisfies the maximal condition on normal subgroups by [1], Lemma 1.2.6. Therefore G contains a unique finite normal subgroup N of maximal order. Passing to the factor group $G/M \cap N$, one may be assumed that $M \cap N = 1$ and so $[M, N] = 1$. Clearly in this case the intersection $A \cap B \cap N$ is a normal subgroup of G. Factoring out this intersection, we arrive at a group $G = M \rtimes A = M \rtimes B = AB$ in which $A \cap B \cap N = 1$. Show that then A and so B has no subgroup of order 4.

Indeed, otherwise the finite normal subgroup K of A contains an involution i whose centralizer $C_A(i)$ is infinite. Hence $i \in N$ by Lemma 17 and so i centralizes M. Clearly $i = xj$ for some $x \in M$ and an involution $j \in B$, so that the centralizer $C_B(j)$ is isomorphic to $C_A(i)$. Therefore $j \in N$ by the same lemma and thus $x \in N$. But then $x = 1$ and so $i = j \in A \cap B \cap N$, contrary to the choice of G.

Thus A contains no subgroup of order 4 and hence its finite normal subgroup K consists of all elements of odd order of A. Similarly B and its normal subgroup $L = B \cap (KM)$ have the same property. Since the normalizers $N_A(K \cap L)$ and $N_B(K \cap L)$ are of finite index in A and B, respectively, the normal closure of the intersection $K \cap L$ in G is finite because the normalizer $N_G(K \cap L)$ is of finite index in G. Therefore $K \cap L \subseteq N$ and so $K \cap L = 1$. This implies that the intersection $A \cap B$ has no non-trivial elements of odd order and thus it must be finite of order at most 2.

If $A \cap B$ is of order 2 and i is its involution, then $N_G(A \cap B) = N_A(A \cap B)N_B(A \cap B)$ and thus the centralizer $C_G(i)$ is finite because so are the centralizers $C_A(i)$ and $C_B(i)$. But then the subgroup M is soluble-by-finite by the above-mentioned theorem of Shunkov and so finite, contrary to the choice of G. Hence $A \cap B = 1$ and thus M is a 2-group. Indeed, since A contains an involution i and $i = xj$ for some $x \in M$ and an involution $j \in B$, it follows that $<i, j>=<x> \rtimes <i>=<x> \rtimes <j>$, so that the involutions i and j are conjugate in $G = AB$ if M is a p-group with $p \neq 2$. But this is impossible because otherwise $i^{ab} = j$ for some $a \in A$ and $b \in B$ and so $i^a = j^{b^{-1}} \in A \cap B = 1$.

Thus M is an infinite 2-group and therefore it contains an infinite abelian subgroup Z whose normalizer $N_G(Z)$ is of finite index in G by Lemma 16. Hence Z is subnormal in M and so its normal closure F in G is an infinite nilpotent 2-subgroup. On the other hand, the factorizer $X(F) = AF \cap BF$ of F in $G = AB$ is a triply factorized group satisfying the hypothesis of Theorem 13 because $X(F) = F \rtimes (A \cap BF) = F \rtimes (AF \cap B) = (A \cap BF)(AF \cap B)$ by [1], Lemma 1.1.4. Therefore the subgroup F must be finite by Lemma 15 and this contradiction completes the proof. $\boxed{QED}$

6 Semidirect products of groups and derivations

Throughout this section let A be a group acting on a group M, i.e. a homomorphism from A into the automorphism group $\mathrm{Aut}(M)$ of M is given, and let $G = M \rtimes A$ be the semidirect product of M by A.

A mapping $\delta : A \to M$ is a *derivation* (or *1-cocycle*) from A into M if $(ab)^\delta = (a^\delta)^b b^\delta$ for all elements $a, b \in A$.

For instance, for each $m \in M$ the mapping $\delta : a \mapsto [a, m] = m^{-a}m$ with $a \in A$ is a derivation from A into M which is called *inner*. Since $a^\delta = a^\delta 1^\delta$ and $1^\delta = (aa^{-1})^\delta = (a^\delta)^{a^{-1}}(a^{-1})^\delta$, it follows that $1^\delta = 1$ and $(a^{-1})^\delta = a^{\delta^{-a^{-1}}}$. Therefore the kernel $\mathrm{Ker}\,\delta = \{a \mid a^\delta = 1,\, a \in A\}$ of δ is a subgroup of A. On the other hand, the image $\mathrm{Im}\,\delta = \{a^\delta \mid a \in A\}$ of A in M under δ need not be a subgroup of M. If for some subgroup N of M there exists a subgroup C of A such that $N = \{c^\delta \mid c \in C\}$, then we will say that N is a *derivation image* of C. Clearly if A acts trivially on M, then every derivation $\delta : A \to M$ is in fact a homomorphism from A into M.

It is well-known that the derivations from A into M correspond to the complements to M in $G = A \ltimes M$ (see for instance [1], p. 107, or [28], p. 304). The following theorem describes some properties of these derivations in terms of complements to M in $G = M \rtimes A$.

18 Theorem. *Let A be a group acting on a group M and $G = M \rtimes A$. If $\delta : A \to M$ is a derivation and $B = \{aa^\delta \mid a \in A\}$, then B is a complement to M in G and the following statements hold:*

1) The derivation δ is inner if and only if B is conjugate to A in G.

2) $\mathrm{Ker}\,\delta = A \cap B$ *and in particular δ is injective if and only if $A \cap B = 1$.*

3) The derivation δ is surjective if and only if $G = AB$. In other words, M is a derivation image of A if and only if $G = M \rtimes A = M \rtimes B = AB$ is a triply factorized group.

Proof. If δ is inner, then there exists $m \in M$ such that $a^\delta = m^{-a}m$ for every $a \in A$. Therefore $aa^\delta = a(m^{-a}m) = a^m$ and hence $B = A^m$. Conversely, if $B = A^m$ for some $m \in M$ and $a \in A$, then $a^m = bb^\delta$ for some $b \in A$. Since $a^{-1}bb^\delta = a^{-1}a^m \in M$, this implies $a^{-1}b = 1$ and so $a^\delta = m^{-a}m$. This proves 1).

Now, if $a^\delta = 1$ for some $a \in A$, then $a = aa^\delta \in A \cap B$, so that $\operatorname{Ker} d \subseteq A \cap B$. On the other hand, if $a \in A \cap B$, then $a(a^{-1}(a^{-1})^\delta) \in B$ and so $(a^{-1})^\delta \in B \cap M = 1$. Therefore $a^\delta = 1$ and hence $A \cap B \subseteq \operatorname{Ker} d$. This proves 2).

Finally, let δ be a surjective derivation, $a \in A$ and $m \in M$. Then $m = b^\delta$ for some $b \in A$ and so $am = ab^\delta = (ab^{-1})(bb^\delta)$ belongs to the set AB. Therefore $G = AB$. Conversely, if this equality holds, then $m = bcc^\delta$ for some elements b, c of A and so $bc \in A \cap M = 1$. Hence $m = c^\delta$ and this implies 3). $\boxed{QED}$

Examples. **1.** (J. Lawrence [19].) Let D be a division ring and D^* its multiplicative group acting on the additive group of D by the right multiplication. Then every derivation from D^* into D is inner. In other words, each function $\delta : D^* \to D$ such that $(xy)^\delta = (x^\delta)y + y^\delta$ must be of the form $x^\delta = c(x-1)$ for a fixed element $c \in D$.

2. Let M be a group whose automorphism group $\operatorname{Aut}(M)$ contains a non-abelian free subgroup F freely generated by a set S. If the cardinality of M is not exceeded that of S, then there exists a surjective derivation $\delta : F \to M$ from F onto M.

Indeed, using the functional equation $(xy)^\delta = (x^\delta)^y y^\delta$ for $x, y \in F$, one can extend every surjective mapping $\delta : S \to M$ to a surjective derivation δ from F onto M. $\boxed{QED}$

Although two complements A and B to M in $G = M \rtimes A = M \rtimes B$ need not be conjugate in general, they are isomorphic and so conjugate in an HNN-extension of G. The following assertion describes this situation in detail.

19 Proposition. *Let A and B be two complements to M in $G = M \rtimes A$ and let $<u>$ be an infinite cyclic group. Denote by $M\star<u>$ the free product of M and $<u>$. Then the action of A on M can be extended to that of A on $M\star<u>$ so that the subgroups A and B are conjugate in the semidirect product $(M\star<u>) \rtimes A$ by the element u, that is $A^u = B$.*

Proof. Clearly for each element $a \in A$ there exists a unique element $m \in M$ such that $am \in B$. The mapping $\delta : A \to M$ defined by the rule $a^\delta = m$ is a derivation from A into M because $(a_1a)^\delta = (a_1^\delta)^a a^\delta$ for all $a, a_1 \in A$. Therefore $B = \{aa^\delta \mid a \in A\}$. Put $u^a = u(a^\delta)^{-1}$ for each $a \in A$. As it is easily verified, this allows to extend the action of A on M to that of A on $M\star\!<\!u\!>$ and so to consider the semidirect product $(M\star\!<\!u\!>) \rtimes A$. Since $a^u = aa^\delta$ for each $a \in A$, this implies that $A^u = B$, as desired. $\boxed{QED}$

In particular, if the subgroup M is abelian, then the commutator subgroup $[M, <u>]$ coincides with the derived subgroup of the free product $M\star <u>$ and so is normal in the semidirect product $(M\star <u>) \rtimes A$. Since the factor group $M\star\!<\!u\!>/[M, <\!u\!>]$ is isomorphic to the direct product $M\times <\!u\!>$, the following statement is an immediate consequence of Proposition 19.

20 Corollary. *If in the semidirect product $G = M \rtimes A$ the normal subgroup M is abelian and B is a complement to M in G, then there exists an automorphism u of G such that $G\rtimes <\!u\!>= (M\times <\!u\!>) \rtimes A$ and $B = A^u$.*

7 Bijective derivations

In this section A is a group acting on a group M and $\delta : A \to M$ is a derivation from A into M. The following assertion which is an immediate consequence of Theorem 18 characterizes bijective derivations in terms of triply factorized groups.

21 Proposition. *A derivation $\delta : A \to M$ is bijective if and only if in the semidirect product $G = M \rtimes A$ there exists a complement B to M in G such that $G = M \rtimes A = M \rtimes B = AB$ and $A \cap B = 1$.*

22 Example. Let R be a radical ring, i.e. an associative ring whose set of all elements forms a group under the *adjoint multiplication* $r \circ s = r + s + rs$ with $r, s \in R$ which is called the adjoint group of R and denoted by R°. Clearly R° acts on R by the rule $r^s = r + rs$ for all $r, s \in R$ and the identity mapping ι on R determines a bijective derivation from R° onto R. Thus the additive group of every radical ring is a bijective derivation image of the adjoint group of this ring. $\boxed{QED}$

Clearly if M is a bijective derivation image of A, then its structure is increasingly influenced by the structure of A. Below we consider some simple cases when the structure of M can completely be determined by A. A description of groups factorized by two infinite cyclic subgroups with trivial intersection given in [31] leads to the following result.

23 Proposition. *If the group A is infinite cyclic and the derivation $\delta : A \to M$ is bijective, then the group M is either infinite cyclic or infinite dihedral. Moreover, if $A =<\!a\!>$ and $a^\delta = x \in M$, then the group $G = M \rtimes A$ is one of the following:*

a) $G =<\!x\!> \times <\!a\!>$ with $M =<\!x\!>$;

b) $G = (<b> \rtimes <x>) \rtimes <a>$ *with* $M = <b, x \mid (bx)^2 = x^2 = 1>$, $b^a = b^{-1}$ *and* $x^a = bx$.

If the group A is finite cyclic, then the structure of its bijective derivation image M is in general more complicated. For the case when A is a cyclic p-group, it can easily be derived from [31], Lemma 6, where a complete description of triply factorized groups $G = M \rtimes A = M \rtimes B = AB$ with $A \cap B = 1$ is contained.

24 Lemma. *Suppose the group A is cyclic of order p^n and the derivation $\delta : A \rightarrow M$ is bijective. Then the group M is cyclic for $p > 2$ and either cyclic or dihedral or generalized quaternion for $p = 2$. Moreover, if $A =< a >$ and $a^\delta = x \in M$, then the semidirect product $G = M \rtimes A$ is one of the following:*

a) $G =< x > \rtimes < a >$ *with* $M =< x \mid x^{p^n} = 1 >$ *and* $x^a = x^{1+p^m}$, *where* $1 \leq m \leq n$ *except for the case* $p = 2$ *,*$n \geq 2$ *in which* $2 \leq m \leq n$;

b) $G = (<b> \rtimes <x>) \rtimes <a>$ *with* $M =<b, x \mid b^{2^{n-1}} = x^2 = (bx)^2 = 1>$, $b^a = b^{1+2^m}$ *and* $x^a = bx$, *where* $2 \leq m \leq n$;

d) $G = (< b >< x >) \rtimes < a >$ *with* $M =< b, x \mid b^{2^{n-1}} = 1, b^{2^{n-2}} = x^2 = (bx)^2 >$, $b^a = b^{1+2^m}$ *and* $x^a = bx^{-1}$, *where* $2 \leq m \leq n - 1$.

Finally, the following assertion describes bijective derivation images of dihedral and generalized quaternion 2-groups. It is derived from [2], Lemma 5.6, and [34], Lemma 8.

25 Lemma. *Let $\delta : A \rightarrow M$ be a bijective derivation from the group A of order $2^n \geq 4$ onto M. If A is dihedral or generalized quaternion and $< a >$ is the Frattini subgroup of A, then $< a >^\delta =< a^\delta >$ except for the case $n = 4$ in which $< a >^\delta$ can also be an elementary abelian subgroup of M. In particular, the group M either contains a cyclic subgroup of index 4 or is a group of order 16.*

8 Nearrings

A *(left) nearring* $(R, +, \cdot)$ is a set R with two binary operations $+$ and $\cdot$ such that $(R, +)$ is a not necessarily abelian group, $(R, \cdot)$ is a semigroup and $\cdot$ satisfies the left distributive law with respect to $+$, i.e. $r \cdot (s + t) = r \cdot s + r \cdot t$ for all elements r, s, t of R.

As usual, the group $(R, +)$ is called the *additive group* of $(R, +, \cdot)$ and denoted by R^+. Its neutral element is denoted by 0. Furthermore, if $r \in R$ and n is a positive integer, then $r \cdot n$ or rn means $\underbrace{r + \cdots + r}_{n}$. It is easy to verify that

$r \cdot 0 = 0$ and $r \cdot (-s) = -(r \cdot s)$, so that $r(sn) = (rs)n$ for all r, s of R and all $n \in \mathbb{Z}$.

Note that from the definition of $(R, +, \cdot)$ it does not follow that $0 \cdot r = 0$ for each $r \in R$. A nearring $(R, +, \cdot)$ in which $0 \cdot r = 0 = r \cdot 0$ for every $r \in R$ is called a *zero-symmetric* nearring. If $(R, \cdot)$ is a semigroup with an identity element $\mathbf{1}$, i.e. $r \cdot \mathbf{1} = \mathbf{1} \cdot r = r$ for every $r \in R$, then $(R, +, \cdot)$ is called a *nearring with identity element* $\mathbf{1}$. In this case the set of all invertible elements of $(R, \cdot)$ is a group which will be called the multiplicative group of R and denoted by R^*.

The concepts of a *subnearring* and a *nearring homomorphism* are defined by the same way as for rings. In particular, if λ is a nearring homomorphism of $(R, +, \cdot)$, then its kernel $\operatorname{Ker} \lambda$ is a subnearring of $(R, +, \cdot)$ whose additive subgroup is normal in R^+.

A subnearring I of $(R, +, \cdot)$ is an *ideal* of $(R, +, \cdot)$ if $I = \operatorname{Ker} \lambda$ for some λ. It can simply be verified that

I is an ideal of R if and only if its additive group I^+ is a normal subgroup of R^+ and for any elements $r, s \in R$ and $a \in I$ the inclusions $ra \in I$ and $(r + a)s - rs \in I$ hold.

For each ideal I of $(R, +, \cdot)$, the *factor nearring* $(R/I, +, \cdot)$ is the factor group R^+/I^+ with multiplication $(r + I) \cdot (s + I) = rs + I$ for all $r, s \in R$ and the mapping $r \mapsto r + I$ determines a natural nearring homomorphism from $(R, +, \cdot)$ onto $(R/I, +, \cdot)$ whose kernel is I.

In ring theory, left or right ideals of a ring are introduced as subgroups of its additive group which are invariant under the left or right multiplication by any element of this ring. For a nearring $(R, +, \cdot)$, the same definition leads to notions of *left* or *right R-subgroups* of R. For instance, for every $r \in R$ the set $rR = \{rs \mid s \in R\}$ is a right R-subgroup of R. Furthermore, a subgroup M of R^+ is called an *(R, R)-subgroup* of R, if M is both a right and a left R-subgroup. Note that in general there is no direct connection between (R, R)-subgroups and ideals of R.

Obviously every right or left R-subgroup of R is even a subnearring of R. It is easy to see that for every non-empty subset X of R the (right) *annihilator*

$$\operatorname{Ann}_R(X) = \{r \in R \mid xr = 0 \quad \text{for all} \quad x \in X\}$$

of X in R is a normal subgroup of the group R^+. Moreover, if R is zero-symmetric, then $\operatorname{Ann}_R(X)$ is a right R-subgroup of R^+. Furthermore, it follows from the left distributive law that for each $x \in R$ the mapping $r \mapsto xr$, $r \in R$, determines an endomorphism of R^+ whose kernel coincides with $\operatorname{Ann}_R(x)$ and its image with xR. If in particular $x = 0$, then $\operatorname{Ann}_R(0)$ and $0 \cdot R$ form subnearrings of R which are called the *zero-symmetric part* and the *constant part* of R and denoted by $R_{\mathfrak{o}}$ and $R_{\mathfrak{c}}$, respectively. Clearly if R is a nearring with identity element $\mathbf{1}$, then $\mathbf{1} \in R_{\mathfrak{o}}$ and $R_{\mathfrak{o}}^* = R_{\mathfrak{o}} \cap R^*$ because for each $r \in R^*$ the equality $0 \cdot r = 0$ implies $0 \cdot r^{-1} = 0$. Furthermore, $R_{\mathfrak{o}} \cap R_{\mathfrak{c}} = 0$ and $R = R_{\mathfrak{o}} + R_{\mathfrak{c}}$ because $r = (r - 0 \cdot r) + (0 \cdot r)$ for each $r \in R$.

26 Lemma. *Let R be a nearring with unity $\boldsymbol{1}$. Then the set $\boldsymbol{1} + R_{\mathfrak{c}}$ is a subgroup of R^* isomorphic to the additive group $R_{\mathfrak{c}}^+$ and $R^* = R_{\mathfrak{o}}^*(\boldsymbol{1} + R_{\mathfrak{c}})$ with $R_{\mathfrak{o}}^* \cap (\boldsymbol{1} + R_{\mathfrak{c}}) = \boldsymbol{1}$.*

Proof. If $s, t \in R_{\mathfrak{c}}$, then $(\mathbf{1} + s)(\mathbf{1} + t) = \mathbf{1} + s + t$ and so $(\mathbf{1} + s)(\mathbf{1} - s) = (\mathbf{1} - s)(\mathbf{1} + s) = \mathbf{1}$. Therefore $\mathbf{1} + R_{\mathfrak{c}}$ is a subgroup of R^* and the mapping $\mathbf{1} + s \mapsto s$ determines an isomorphism from this subgroup onto $R_{\mathfrak{c}}^+$.

Since every element $u \in R^*$ can uniquely be written in the form $u = r + s = r(\mathbf{1} + s)$ with $r \in R_{\mathfrak{o}}$ and $s \in R_{\mathfrak{c}}$, this implies that $r = u(\mathbf{1} - s) \in R^* \cap R_{\mathfrak{o}} = R_{\mathfrak{o}}^*$ and hence R^* has the required factorization. $\boxed{QED}$

The following lemma is concerned with conditions under which $\mathrm{Ann}_R(X)$ is an ideal of R. As usual, for any two subsets X and Y of R we put $XY = \{xy \mid x \in X,\ y \in Y\}$.

27 Lemma. *Let R be a nearring and X a non-empty subset of R. If $XR \subseteq X$, then $\mathrm{Ann}_R(X)$ is an ideal of R.*

Proof. If $r, s \in R$, $a \in \mathrm{Ann}_R(X)$ and $x \in X$, then $x((r + a)s - rs) = (xr + xa)s - xrs = xrs - xrs = 0$ and so $(r + a)s - rs \in \mathrm{Ann}_R(X)$. Next, if $XR \subseteq X$, then $xr \in X$ and $x(ra) = (xr)a = 0$, so that $ra \in \mathrm{Ann}_R(X)$. As $\mathrm{Ann}_R(X)$ is normal in R^+, it is an ideal of R. $\boxed{QED}$

Examples. **1** . Every additive (not necessarily abelian) group A with multiplication $a \cdot b = b$ for all $a, b \in A$ forms a nearring $(A, +, \cdot)$ which will be called a *constant nearring*. Obviously every subgroup of the group A is a left A-subgroup and so a subnearring of $(A, +, \cdot)$ and every normal subgroup of A is an ideal of $(A, +, \cdot)$. On the other hand, A itself is the only right A-subgroup of A because $aA = A$ for each $a \in A$.

2 . Let A be an additive group and $\mathrm{Map}(A)$ the set of all mappings from the group A into itself. For each $\alpha \in \mathrm{Map}(A)$ and every $a \in A$, let a^α denote the image of a under α. Define the sum $\alpha + \beta$ and the product $\alpha \cdot \beta$ of two mappings α and β of $\mathrm{Map}(A)$ by the rules $a^{\alpha+\beta} = a^\alpha + a^\beta$ and $a^{\alpha\cdot\beta} = (a^\alpha)^\beta$ for every $a \in A$. Then it is easily verified that $(\mathrm{Map}(A), +, \cdot)$ is a nearring with identity element ι which is the identity mapping on A.

Clearly the multiplicative group $\mathrm{Map}(A)^*$ of $(\mathrm{Map}(A), +, \cdot)$ consists of all bijective mappings of $\mathrm{Map}(A)$.

If A has at least two elements, then the nearring $(\mathrm{Map}(A), +, \cdot)$ is not zero-symmetric and the subsets

$$\mathrm{Map}_{\mathfrak{o}}(A) = \{\alpha \in \mathrm{Map}(A) \mid 0^\alpha = 0\}$$

and

$$\mathrm{Map}_{\mathfrak{c}}(A) = \{\alpha \in \mathrm{Map}(A) \mid a^{\alpha} = 0^{\alpha} \quad \text{for all} \quad a \in A\}$$

form the zero-symmetric and constant parts of $(\mathrm{Map}(A), +, \cdot)$. $\boxed{\mathit{QED}}$

9 Embeddings

Let R be a nearring, regarded as a subgroup of an additive group A. For each $r \in R$ and every $a \in A$, we define a mapping $\hat{r} \in \mathrm{Map}(A)$ by the rule

$$a^{\hat{r}} = \begin{cases} ar & \text{if} \quad a \in R \\ r & \text{if} \quad a \notin R. \end{cases}$$

It is easy to see that $\widehat{r+s} = \hat{r} + \hat{s}$ and $\widehat{rs} = \hat{r}\hat{s}$ for any $r, s \in R$, so that the mapping $r \mapsto \hat{r}$, $r \in R$, determines a nearring homomorphism from R into $(\mathrm{Map}(A), +, \cdot)$. Thus the kernel $\mathrm{Ker}\,\hat{}\; = \{r \mid \hat{r} = 0,\, r \in R\}$ is an ideal of R and the image $\widehat{R}$ is a subnearring of $(\mathrm{Map}(A), +, \cdot)$. This homomorphism can be viewed as a *natural representation* of R in $\mathrm{Map}(A)$ leaving invariant the zero-symmetric and constant parts of R. Indeed, the following equalities are immediately verified.

28 Lemma. *It holds $\widehat{R} \cap \mathrm{Map}_{\mathfrak{0}}(A) = \widehat{R_{\mathfrak{0}}}$ and $\widehat{R} \cap \mathrm{Map}_{\mathfrak{c}}(A) = \widehat{R_{\mathfrak{c}}}$.*

If $\mathrm{Ker}\,\hat{}\; = 0$, the natural representation of R in $\mathrm{Map}(A)$ is faithful and so R can be identified with $\widehat{R}$. Clearly this is the case when A properly contains R. If $A = R$, then $\mathrm{Ker}\,\hat{}\; = \mathrm{Ann}_R(R)$ and so the natural representation of R in $\mathrm{Map}(R)$ is faithful if and only if $\mathrm{Ann}_R(R) = 0$.

This leads to the following result which is well-known (see [27], Theorem 1.86 or [6], Theorem 1.3.27).

29 Proposition. *Every (zero-symmetric) nearring can be embedded into a (zero-symmetric) nearring with an identity element*

Proof. Indeed, if $R \neq 0$ is a nearring and A is the direct sum of two copies of R, then Lemma 28 shows that the natural representation of R in $\mathrm{Map}(A)$ gives a desirable embedding. $\boxed{\mathit{QED}}$

It is well-known that any ring can be viewed as an ideal in a ring with identity element. Unfortunately, this is not always possible for nearrings.

As for constant nearrings, the following holds.

30 Lemma. *Let R be a constant nearring. Then $\widehat{R} = \mathrm{Map}_{\mathfrak{c}}(R)$ and so R can be regarded as the constant part of* $\mathrm{Map}(R)$.

Proof. Indeed, if $r, s \in R$, then $r^{\hat{s}} = rs = s = 0 \cdot s = 0^{\hat{s}}$. Therefore $\hat{s} \in \mathrm{Map}_{\mathfrak{c}}(R)$. Conversely, if $\alpha \in \mathrm{Map}_{\mathfrak{c}}(R)$ and $0^{\alpha} = s$, then $r^{\alpha} = 0^{\alpha} = s = r^{\hat{s}}$ for each $r \in R$. Hence $\alpha = \hat{s} \in \widehat{R}$, as desired. $\boxed{\mathit{QED}}$

A subnearring S of R is *generated by a subset* X of S if S is the smallest subnearring of R containing X. In what follows let $< X >_{ad}$ and $< X >_{mul}$ denote the subgroup of R^+ and the subsemigroup of $(R, \cdot)$ generated by X, respectively.

31 Lemma. *Let R be a nearring, X a subset of R and $Y =< X >_{mul}$. For each integer $n \geq 1$, we put $X_1 =< Y >_{ad}$ and $X_{n+1} =< X_n, X_nY >_{ad}$. If S is the subnearring of R generated by X, then $S = \bigcup_{n=1}^{\infty} X_n$.*

Proof. It is easy to see that $X_n \subseteq S$ for every $n \geq 1$ and the union $\bigcup_{n=1}^{\infty} X_n$ is a subgroup of R^+. Show that this union is also a subsemigroup of $(R, \cdot)$ and so a subnearring of R which must coincide with S. Clearly it suffices to verify that $X_nX_n \subseteq X_{2n}$ for each $n \geq 1$.

Indeed, let $r, s \in X_n$. If $s \in X_1$, then $s = y_1 + \cdots + y_m$ for some elements $y_1, \ldots, y_m$ of Y and so $rs = ry_1 + \cdots + ry_m \in< X_nY >_{ad} \subseteq X_{n+1}$. Arguing by induction on n, we may assume that for all $t \in X_{n-1}$ the inclusion $rt \in X_{2n-1}$ holds true. Since $X_n =< X_{n-1}, X_{n-1}Y >_{ad}$, it follows that $s = t_1 + u_1y_1 + \cdots + t_m + u_my_m$ for some elements $t_1, u_1, \ldots, t_m, u_m$ of X_{n-1} and $y_1, \ldots, y_m$ of Y. Therefore $rs = rt_1 + (ru_1)y_1 + \cdots + rt_m + (ru_m)y_m \in < X_{2n-1}, X_{2n-1}Y >_{ad} = X_{2n}$, as desired. $\boxed{QED}$

32 Lemma. *Let N be a nearring with identity element $\mathbf{1}$, R its subnearring and S the subnearring of N generated by the union $R \cup \{\mathbf{1}\}$. Then $RS = R$ and the right annihilator $\mathrm{Ann}_S(R)$ of R in S is an ideal of S.*

Proof. Put $S_1 =< R, \mathbf{1} >_{ad}$ and $S_{n+1} =< S_n, S_nR >_{ad}$ for each integer $n \geq 1$. Then $S = \cup_{n=1}^{\infty} S_n$ by Lemma 31. Furthermore, $RS_1 = R$ and so $R(S_1R) \subseteq R$. By induction on n, this implies that $RS_n = R$ for each $n \geq 1$ and thus $RS = R$. Now it follows from Lemma 27 that $\mathrm{Ann}_S(R)$ is an ideal of S. $\boxed{QED}$

10 Construction subgroups

Let R be a nearring with identity element $\mathbf{1}$ and V its additive subgroup. Following P. Hubert [15], V will be called a *construction subgroup* of R if the set $\mathbf{1} + V$ is a subgroup of the multiplicative group R^* of R. Since in this case $\mathbf{1} + V = (\mathbf{1} + V)^2 = \mathbf{1} + V + (\mathbf{1} + V)V$, it follows that $(\mathbf{1} + V)V \subseteq V$. In particular, if R is a ring, then $(\mathbf{1} + V)V = V + V^2$ and so $V^2 \subseteq V$. Thus in the ring case V is a subring of R. However in the general case the construction subgroup V need not be a subnearring of the nearring R.

Examples. 1 . Let R be a ring with identity element $\mathbf{1}$ and S a subring of R. Then S is a construction subgroup of R if and only if S is a radical subring of R. Indeed, $S = S^\circ$ if and only if the set $A = \mathbf{1} + S$ is a subgroup of R^*.

2 . Let R be a constant nearring, identified with the constant part of the nearring $\mathrm{Map}(R)$ by Lemma 30. Then R is a construction subgroup of $\mathrm{Map}(R)$. Indeed, if ι is the identity mapping on R, then $A = \iota + \mathrm{Map}_{\mathfrak{c}}(R)$ is the set of all translations on R and so A is an isomorphic to R multiplicative subgroup of $\mathrm{Map}(R)^*$. $\boxed{QED}$

Construction. If R is a nearring with identity element $\mathbf{1}$ and R^* is its multiplicative group, then for each $s \in R^*$ the mapping $r \mapsto s^{-1}r$ with $r \in R$ determines an automorphism of the additive group R^+. Therefore R^* becomes a group of automorphisms of R^+ if its action on R^+ is defined by the rule $r^s = s^{-1}r$ for every $r \in R$ and $s \in R^*$.

Let A be a subgroup of R^* and let M and N be A-invariant subgroups of R^+ such that N is normal in M. Then the action of A on the factor group M/N is induced by that of R^* on R^+, so that $(m+N)^a = a^{-1}m + N$ for every $m \in M$ and $a \in A$. Hence one can construct the semidirect product $G(M,N,A)$ of M/N by A. To avoid a confusion, we shall look at $G(M,N,A)$ as a group of all pairs $(a, m+N)$ with $a \in A$ and $m \in M$ which are multiplied by the rule

$$(b, l+N)(a, m+N) = (ba, a^{-1}l + m + N) \quad \text{for all} \quad a, b \in A \quad \text{and} \quad l, m \in M.$$

Then the pair $(\mathbf{1}, N)$ is the identity element of $G(M,N,A)$ denoted by 1 and the groups A and M/N are identified with the subgroups $\{(a,N) \mid a \in A\}$ and $\{(\mathbf{1}, m+N) \mid m \in M\}$ of $G(M,N,A)$, respectively.

Suppose now that M is a construction subgroup of R and $A = \mathbf{1} + M$. Then the mapping $\delta : a = (\mathbf{1}+m)^{-1} \mapsto -m + N$ with $m \in M$ determines a surjective derivation from A onto M/N. Indeed, if $l \in M$ and $b = (\mathbf{1}+l)^{-1}$, then $b^{-1}a^{-1} = (\mathbf{1}+l)(\mathbf{1}+m) = \mathbf{1} + l + (\mathbf{1}+l)m$ and $ab = (\mathbf{1} + l + (\mathbf{1}+l)m)^{-1}$, so that $(ab)^\delta = -(\mathbf{1}+l)m - l + N = b^{-1}(-m+N) + (-l+N) = (a^\delta)^b + b^\delta$. Hence it follows from Theorem 18 that

$$B = \{((\mathbf{1}+m)^{-1}, -m+N) \mid m \in M\}$$

is a subgroup of $G(M,N,A)$ such that $B \cap M = 1$, $A \cap B = \{(\mathbf{1}+m, N) \mid m \in N\}$ and

$$G(M,N,A) = (M/N) \rtimes A = (M/N) \rtimes B = AB$$

is a triply factorized group.

If in particular $N = 0$, then the group $G(M,0,A) = M \rtimes A = M \rtimes B = AB$ is a triply factorized group with $A \cap B = 1$. Clearly $G(M,0,A)$ is the subgroup of $G(R^+, 0, R^*)$ consisting of all pairs (a,m) with $a \in A$ and $m \in M$. In what follows, $G(R)$ will be written instead $G(R^+,0,R^*)$ and called the *group associated with the nearring* R. Similarly, $G(M) = G(M,0,A)$ if M is a construction subgroup of R and $A = \mathbf{1} + M$.

Conversely, as it was shown by P. Hubert in [15], every triply factorized group $G = M \rtimes A = M \rtimes B = AB$ with $A \cap B = 1$ can be identified with a group $G(V)$ for some construction subgroup V of $\mathrm{Map}(M)$.

Indeed, using Proposition 19, the group G can be extended to a group $<G, u>=<M, u> \rtimes A$ such that $u^A = uM$ and $A^u = B$. Then $C_A(u) = 1$ because $A^u \cap A = 1$. For convenience, in the following we apply for A and $<G, u>$ the multiplicative notation and for $<M, u>$ additive. In these notations $u^A = u+M$ and $<G, u>$ consists of the elements ax with $a \in A$ and $x \in <M, u>$ which are multiplied by the rule $(ax)(by) = (ab)(x^b + y)$ for all $b \in A$ and $y \in <M, u>$. Thus for each $m \in M$ there exists a unique $a \in A$ such that $u^a = u - m$ and hence $M = \{-u + u^b \mid b \in A\}$.

Define now a mapping $\gamma : A \to \mathrm{Map}(M)$ by the rule

$$(-u + u^b)^{\gamma(a)} = -u + u^{a^{-1}b} \quad \text{for all} \quad a, b \in A.$$

Then γ is a group monomorphism from A into the multiplicative group $\mathrm{Map}(M)^*$ because $\gamma(1) = \iota$ is the identity mapping on M, $\mathrm{Ker}\,\gamma = 1$ and $\gamma(ac) = \gamma(a)\gamma(c)$ for all $a, c \in A$.

33 Lemma. *Let $U = \mathrm{Im}(\gamma)$ and $V = -\iota + U$. Then V is a group with respect to addition and so a construction subgroup of* $\mathrm{Map}(M)$*. Furthermore, the mapping $\beta : M \to V$ given by*

$$-u + u^b \mapsto -\iota + \gamma(b^{-1}) \quad \textit{for each} \quad b \in A$$

is a group isomorphism.

Proof. Clearly for every $a, c \in A$ there exists $d \in A$ such that

$$(-u + u^{a^{-1}}) - (-u + u^{c^{-1}}) = -u + u^{d^{-1}}.$$

Thus it suffices to check that $(-\iota + \gamma(a)) - (-\iota + \gamma(c)) = -\iota + \gamma(d)$. Indeed,

$$\begin{gathered}(-u + u^b)^{(-\iota+\gamma(a))-(-\iota+\gamma(c))} = (-u^b + u) + (-u + u^{a^{-1}b})+ \\ +(-u^{c^{-1}b} + u) + (-u + u^b) = -u^b + u^{a^{-1}b} - u^{c^{-1}b} + u^b = \\ (-u + u^{d^{-1}})^b = -u^b + u - u + u^{d^{-1}b} = (-u + u^b)^{-\iota+\gamma(d)},\end{gathered}$$

as desired. $\boxed{QED}$

It is similarly verified that the mapping

$$am \mapsto (\gamma(a), \beta(m))$$

with $a \in A$ and $m \in M$ determines a group isomorphism from G onto $G(V)$. As a summary, we obtain the above-mentioned result of P. Hubert.

34 Theorem. *If $G = M \rtimes A = M \rtimes B = AB$ is a triply factorized group with $A \cap B = 1$, then the nearring* $\mathrm{Map}(M)$ *contains a construction subgroup V isomorphic to M such that A is isomorphic to $\iota + V \subseteq \mathrm{Map}(M)^*$ and G is isomorphic to the group $G(V)$.*

11 Local nearrings

Let R be a nearring with identity element $\mathbf{1} \neq 0$, and let L_R be the set of all elements of R which are not right invertible in R, i.e. $L_R = \{r \in R \mid rR \neq R\}$. If $L_R = 0$, then R is a *nearfield*, i.e. every non-zero element of R is right invertible an so invertible. In particular, every division ring can be regarded as a special case of a nearfield.

Following C. Maxson [21], the nearring R will be called *local*, if L_R forms a subgroup of the additive group of R.

It should be noted that this definition is slightly distinct from the original definition given by Maxson who supposed that R is zero-symmetric. This means that the subgroup L_R always contains the constant part $R_{\mathfrak{c}}$ of R, so that in particular every nearfield is zero-symmetric.

The following properties of L_R were in fact established by C. Maxson in [21] for the zero-symmetric case. The general case was considered in [2], Lemma 3.2.

35 Lemma. *Let R be a local nearring. Then the following statements hold:*

1) the elements of L_R do not have left inverses in R and $R = L_R \cup R^*$;

2) $RL_RR = R$, i.e. L_R is an (R, R)-subgroup of R;

3) every proper left or right R-subgroup of R is contained in L_R;

4) the set $\mathbf{1} + L_R$ is a subgroup of R^*, i.e. L_R is a construction subgroup of R.

Examples. **1** . Every local ring R is a zero-symmetric local nearring whose subgroup L_R coincides with the Jacobson radical of R.

2 . For a group A, the nearring $\mathrm{Map}(A)$ is local if and only if A is of order 2. In this case the subgroup of all non-invertible elements of $\mathrm{Map}(A)$ coincides with its constant part $\mathrm{Map}_{\mathfrak{c}}(A)$.

3 . The set $xF[[x]]$ of all power series without constant terms over a field F under the usual operations of componentwise addition of power series and their composition given by

$$(\sum_{i=1}^{\infty} a_i x^i) \circ (\sum_{j=1}^{\infty} b_j x^j) = \sum_{i=1}^{\infty} b_i (\sum_{j=1}^{\infty} a_j x^j)^i$$

is a nearring $P = (xF[[x]], +, \circ)$ with identity element x. It can be verified that the element $\sum_{i=1}^{\infty} a_i x^i$ is invertible in P if and only if $a_1 \neq 0$. Hence the additive subgroup $x^2F[[x]]$ is the set of all non-invertible elements of P, so that P is a local nearring with $L_P = x^2F[[x]]$.

4 . (C. Lyons and G. Peterson [20].) If G is a finite p-group and A is a p-group of automorphisms of G containing the group $\mathrm{Inn}(G)$ of inner automorphisms of G, then the subnearring of $\mathrm{Map}(G)$ generated by A is local.

5 . Let R be a local nearring whose additive group R^+ is abelian. Then the collection

$$A_{aff}(R) = \{\alpha \in \mathrm{Map}(R) \mid x^\alpha = ax + b,\ a, b \in R\}$$

of all affine transformations of R under the operations of pointwise addition and function composition forms a nearring $A = A_{aff}(R)$ with identity element ι where $x^\iota = x$. Clearly $A_{\mathfrak{o}} = \{\alpha \in A \mid x^\alpha = ax,\ a \in R\}$ and $A_{\mathfrak{c}} = \{\alpha \in A \mid x^\alpha = b,\ b \in R\}$. In particular, both the zero-symmetric and constant parts of A, regarded as subnearrings of A, are isomorphic to R. Furthermore, an element $\alpha \in A$ is invertible in A if and only if $x^\alpha = ax+b$ for some $a \in R^*$ and $b \in R$. On the other hand, if L_R is the subgroup of all non-invertible elements of R, then

$$L_A = \{\alpha \in A \mid x^\alpha = ax + b,\ a \in L_R,\ b \in R\}$$

is the subgroup of all non-invertible elements of A. As $R = R^* \cup L_R$, it follows that $A = A^* \cup L_A$ and so the nearring A of the affine transformations of R is local. $\boxed{QED}$

It is clear that if L_R is an ideal of R, then the factor nearring R/L_R is a nearfield. However, it is unknown at present *whether for every local nearring R the subgroup L_R is an ideal of R.* The following proposition shows that in solving this problem it suffices to restrict oneself to the case of zero-symmetric local nearrings.

36 Proposition. *A nearring R with an identity element is local if and only if its zero-symmetric part $R_{\mathfrak{o}}$, regarded as a subnearring of R, is local. Moreover, in this case the subgroup L_R is an ideal of R if and only if the intersection $L_R \cap R_{\mathfrak{o}}$ is an ideal of $R_{\mathfrak{o}}$.*

Proof. If R is local, then $R = L_R \cup R^*$ by Lemma 35.1) and so $R_{\mathfrak{o}} = (R_{\mathfrak{o}} \cap L_R) \cup (R_{\mathfrak{o}} \cap R^*)$. Since $R_{\mathfrak{o}} \cap R^* = R_{\mathfrak{o}}^*$, the subnearring $R_{\mathfrak{o}}$ is also local. It is also obvious that if L_R is an ideal of R, then the intersection $L_R \cap R_{\mathfrak{o}}$ is an ideal of $R_{\mathfrak{o}}$.

Conversely, let $R_{\mathfrak{o}}$ be a local subnearring of R and $R_{\mathfrak{o}}^*$ its multiplicative group. If $L_{\mathfrak{o}}$ is the subgroup of all non-invertible elements of $R_{\mathfrak{o}}$, then $R_{\mathfrak{o}} = L_{\mathfrak{o}} \cup R_{\mathfrak{o}}^*$ and so $R = R_{\mathfrak{o}} + R_{\mathfrak{c}} = (L_{\mathfrak{o}} + R_{\mathfrak{c}}) \cup (R_{\mathfrak{o}}^* + R_{\mathfrak{c}})$. Clearly $L_{\mathfrak{o}} + R_{\mathfrak{c}}$ is an additive subgroup of R^+ because $0 \cdot (-c + x + c) = -c + 0 \cdot x + c = 0$ for each $c \in R_{\mathfrak{c}}$ and $x \in L_{\mathfrak{o}}$. Furthermore, $R^* = R_{\mathfrak{o}}^*(\mathbf{1} + R_{\mathfrak{c}}) = R_{\mathfrak{o}}^* + R_{\mathfrak{c}}$ by Lemma 26. Therefore R is a local nearring with $L_R = L_{\mathfrak{o}} + R_{\mathfrak{c}}$. Furthermore, if $L_{\mathfrak{o}}$ is an ideal of $R_{\mathfrak{o}}$, then L_R is an ideal of R by [2], Lemma 3.3. $\boxed{QED}$

Each local nearring can also be characterized as a nearring R with identity element whose multiplicative group R^* additively generates R and acts transitively by left multiplication on the set of all elements outside a proper subgroup of R^+. Recall that a group G acting on a set X is called transitive if for every two elements $x, y \in X$ there exists an element $g \in G$ such that $x^g = y$.

37 Proposition. *Let R be a nearring with identity element and $G(R) = R^+ \rtimes R^*$ the group associated with R. Then R is local if and only if R is additively generated by R^* and there exists a proper subgroup L of R^+ such that in the group $G(R)$ the set $R \setminus L$ is R^*-invariant and the action of R^* on $R \setminus L$ is transitive.*

Proof. Indeed, if R is a local nearring with the subgroup L_R of all non-invertible elements of R, then $R = L_R \cup R^*$ by Lemma 35.1), so that R is generated by R^* and the set $R \setminus L_R$ in $G(R)$ has desired properties.

Conversely, let R be a nearring with identity element $\mathbf{1}$ which is additively generated by R^*, and let L be a proper subgroup of R^+ such that in the group $G(R)$ the set $R \setminus L$ is R^*-invariant and the action of R^* on $R \setminus L$ is transitive. Then there exists an element $x \in R$ such that $R^*x = R \setminus L$. If x is non-invertible in R, then every element of R^*x is so. Therefore in this case $R^* \subseteq L$ and hence $R = L$, contrary to the assumption. Thus $x \in R^*$ and so $R^* = R^*x = R \setminus L$ which means that the nearring R is local. $\boxed{QED}$

12 Nearfields

According to the above definition, if F is a nearfield, then $F = F^* \cup \{0\}$ and so for every two non-zero elements $x, y \in F$ there exists exactly one element $a \in F^*$ such that $a^{-1}x = y$, namely $a = xy^{-1}$. In other words, the action of F^* on F^+ by left multiplication is *sharply transitive*. It turns out that a nearfield is essentially the same as a group with an automorphism group acting sharply transitive on its non-trivial elements.

38 Proposition. *Let G be a group and A a group of automorphisms of G. If A acts sharply transitive on the non-trivial elements of G, then up to* *isomorphism there exists only one nearfield F whose group $G(F) = F^+ \rtimes F^*$ associated with F is isomorphic to the semidirect product of G by A.*

Proof. Clearly two nearfields E and F are isomorphic if and only if their associated groups $G(E)$ and $G(F)$ are so. Therefore it suffices to show that such a nearfield exists. Let G be written additively with neutral element 0 and let i be a non-zero element of G. Since A is sharply transitive on G, it follows that $G = i^A \cup \{0\}$ and for every $a, b \in A$ the equality $i^a = i^b$ holds if and only if $a = b$. Define an operation "$\cdot$" on G by the rule $0 \cdot i^a = i^a \cdot 0 = 0$ and $i^a \cdot i^b = i^{ba}$ for all $a, b \in A$. It is easy to see that this operation is associative and so $(G, \cdot)$ is a semigroup with identity element i. Show next that the operation "$\cdot$" satisfies a left distributive law with respect to addition.

Indeed, for each $c \in A$ either $i^b + i^c = i^d$ for some $d \in A$ or $i^b + i^c = 0$ and then $i^c = -i^b$. Therefore in the first case $i^a \cdot (i^b + i^c) = i^a \cdot i^d = i^{da} = (i^d)^a = (i^b + i^c)^a = i^{ba} + i^{ca} = i^a \cdot i^b + i^a \cdot i^c$ and in the second one $i^a \cdot (i^b + i^c) = i^a \cdot 0 = 0 = i^{ba} - i^{ba} = i^{ba} + (-i^b)^a = i^{ba} + i^{ca} = i^a \cdot i^b + i^a \cdot i^c$, as desired.

Thus the group G forms a nearring under addition and the multiplication given by the operation "$\cdot$". Since $i^a \cdot i^{a^{-1}} = i^{a^{-1}a} = i$, this implies that every non-zero element of the nearring $(G, +, \cdot)$ is invertible and so $F = (G, +, \cdot)$ is a required nearfield. $\boxed{QED}$

It turns out that the additive structure of nearfields and usual fields are identical. This follows from the following result obtained by B.H. Neumann [25], J. Zemmer [41], et al.

39 Theorem. *The additive group of every nearfield is abelian and so it is either an elementary abelian p-group for some prime p or a torsion-free divisible group.*

A detailed account of results concerning nearfields can be found in the book of H. Waehling [35]. Some of them are contained in the following theorem. Recall that an element d of a nearring R is said to be *distributive* if $(r + s)d = rd + sd$ for all $r, s \in R$.

40 Theorem. *Let F be a nearfield with identity element $\mathbf{1}$ and $x, y \in F$. Then*

1) if $x^2 = \mathbf{1}$, then either $x = \mathbf{1}$ or $x = -\mathbf{1}$;

2) $(-\mathbf{1})x = x(-\mathbf{1})$;

3) $(-x)y = -xy = x(-y)$;

4) the set D of all distributive elements of F is a division subring of F;

5) if the multiplicative group F^* of F has an abelian subgroup of finite index, then the additive group of D is a subgroup of finite index in F^+.

First examples of non-commutative nearfields were given by L. Dickson (1905). The smallest of them is a non-commutative Dickson nearfield coupled to the Galois field F_9 of order 9.

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

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

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

The finite nearfields were classified by H. Zassenhaus [40]. His proof provides one of the first deep group theoretical classifications which can for instance be found in the books of M. Hall [11], Chapter 20, or H. Waehling [35], Chapter 4. We state these results here as a theorem. As usual, $SL(2,p)$ and C_n denote special linear groups of degree 2 over fields with p elements and cyclic groups of order n.

42 Theorem. *Let F be a finite nearfield. Then F is of order p^n for some prime p and $n \geq 1$ and its multiplicative group F^* is either metacyclic or isomorphic to one of the following seven groups:*

1) $SL(2,3)$*,*

2) $SL(2,3) \times C_5$*,*

3) a subgroup $O(2,7)$ *of order* 48 *of the group* $SL(2,7)$*,*

4) $O(2,7) \times C_{11}$*,*

5) $SL(2,5)$*,*

6) $SL(2,5) \times C_7$*,*

7) $SL(2,5) \times C_{29}$*.*

Actually, Zassenhaus proved more than it is necessary to characterize the finite nearfields. He essentially characterized the groups of fixed-point-free automorphisms of finite groups. Furthermore, he shown that for each finite sharply 2-transitive permutation group G there exists a finite nearfield F such that G is isomorphic to the group $G(F)$ associated with F. Recall that a permutation group G acting on a set X is called *sharply 2-transitive*, provided that for every two pairs (x_1, x_2) and (y_1, y_2) of elements of X with $x_1 \neq x_2$ and $y_1 \neq y_2$ there exists exactly one $g \in G$ such that $x_i^g = y_i$ for $i = 1, 2$. The question *whether every sharply* 2*-transitive permutation group can be realized as a group associated with a nearfield* is still open.

The following important result was obtained by M. Pettet [26].

43 Theorem. *An infinite nearfield whose multiplicative group is a finite extension of an FC-group is a commutative field.*

13 Local nearrings: the general properties

Almost all results of this section can be found in [2], Section 3, and concern the further properties of the subgroup L_R of a local nearring R. The most part of them pertains to the question *under which conditions L_R is an ideal of R.* Clearly in this case the subgroups L_R and $\mathbf{1}+L_R$ must be normal in the additive group R^+ and the multiplicative group R^*, respectively.

On the other hand, it turns out that if the subgroup $\mathbf{1} + L_R$ is normal in R^*, then the converse is valid.

44 Lemma. *Let R be a local nearring. Then L_R is an ideal of R if and only if $\mathbf{1} + L_R$ is a normal subgroup of the multiplicative group R^* of R.*

Unfortunately, it is unknown at present *whether L_R is a normal subgroup of* R^+. It is easy to see that in the other case L_R must coincide with its normalizer $N_{R^+}(L_R)$ in R^+. Indeed, if $L_R \neq N_{R^+}(L_R)$, then there exists some $r \in R^*$ such that $L_R + r = r + L_R$. Multiplying this equality from the left on the element sr^{-1} for each $s \in R$, we have $L_R + s = s + L_R$ which means that L_R is normal in R^+.

In contrast to Lemma 44, it is also unclear *whether L_R is an ideal of R provided that L_R is a normal subgroup of R^+.* Nevertheless, the case under consideration is much better than general. Indeed, the following assertion shows that in this case there exists a local subnearring N of R containing L_R as an ideal.

45 Proposition. *Let R be a local nearring and let L_R be a normal subgroup of the additive group R^+ of R. Then the union $N = L_R \cup N_{R^*}(\mathbf{1}+L_R)$ is a local subnearing of R and L_R is an ideal of N.*

Recall that an element r of a nearring R is said to be *nilpotent* if there exists a positive integer n such that $r^n = 0$. Clearly in this case $0 \cdot r = r \cdot 0 = 0$, so that every nilpotent element is zero-symmetric. If S is a subset of R and $S^m = (S^{m-1})S$ for each integer $m \geq 2$, then S is called *nilpotent*, provided that $S^m = 0$ for some $m \geq 2$, and S is *nil* if every element of S is nilpotent.

46 Lemma. *Let R be a local nearring whose subgroup L_R is nil. Then L_R is an ideal of R.*

Proof. It suffices to prove that for every $r, s \in R$ and each $a \in L_R$ the element $t = (r + a)s - rs$ belongs to L_R.

Suppose the contrary and let n be the least positive integer such that $a^n = 0$. Then $t \in R^*$ and $n > 1$, so that $a^{n-1} \neq 0$. Since $a^{n-1}t = a^{n-1}(r+a)s - a^{n-1}rs = (a^{n-1}r + a^n)s - a^{n-1}rs = a^{n-1}rs - a^{n-1}rs = 0$, this implies $a^{n-1} = 0 \cdot t^{-1} = a \cdot (0 \cdot t^{-1}) = a^n = 0$, contrary to the choice of n. $\boxed{QED}$

Note that the subgroup L_R can be nil only if the local nearring R is zero-symmetric. The following special case of [22], Theorem 5.38, gives some conditions under which this subgroup is a nilpotent subset of R (but not necessarily a nilpotent subgroup of R^+ !).

47 Proposition. *Let R be a zero-symmetric local nearring satisfying the minimal condition on right R-subgroups. Then the subgroup L_R is a nilpotent subset of R.*

As a consequence of the above results, a wide class of local nearrings whose subgroups of non-invertible elements are always ideals can be determined. It turns out that every finite local nearring has this property.

48 Corollary. *If R is a local nearring satisfying the minimal condition on right R-subgroups, then L_R is an ideal of R.*

Proof. If R is zero-symmetric, then the subgroup L_R is a nilpotent subset of R by Proposition 47 and so L_R is an ideal of R by Lemma 46. The general case follows now from Lemma 36. $\boxed{QED}$

Turn now to the additive structure of local nearrings. An additive not necessarily abelian group A will said to be π-*divisible* for some set of primes π if for every element $a \in A$ and each prime $p \in \pi$ the equation $px = a$ has a solution in A. If π coincides with the set of all primes, then A is called *divisible* which means that the equation $nx = a$ has a solution for every non-zero integer n. As usual, p' denotes the set of all primes distinct from the prime p.

49 Lemma. *Let R be a local nearring. Then the subgroup L_R contains a left R-subgroup M such that M is normal in R^+ and the factor group R^+/M is either a p-group of prime exponent p or a divisible torsion-free group. Moreover, both R^+ and L_R are either p'-divisible groups whose elements of finite order are p-elements or divisible torsion-free groups, respectively.*

In particular, the periodic case of this lemma we state here as a corollary.

50 Corollary. *Let R be a local nearring with identity element $\mathbf{1}$ satisfying one of the following statements:*

1) the additive group R^+ is periodic, or

2) the subgroup L_R is periodic and non-trivial.

Then R^+ is a p-group of finite exponent for some prime p.

Proof. Indeed, if statement 1) holds, then R^+ is a p-group for some p by Lemma 49 and so $\mathbf{1} \cdot p^n = 0$ for some n. Therefore $Rp^n = 0$, as desired.

Now let statement 2) hold and $0 \neq x \in L_R$. Then the right annihilator $\operatorname{Ann}_R(x) = \{r \in R \mid xr = 0\}$ is a normal subgroup of R^+ and the factor group $R^+/\operatorname{Ann}_R(x)$ is isomorphic to the subgroup xR of R^+. Since both $\operatorname{Ann}_R(x)$ and xR are contained in L_R by Lemma 35, the group R^+ is periodic and so it is a p-group of finite exponent by 1). $\boxed{QED}$

On the other hand, it was proved by P. Hubert [13] that *every p-group of finite exponent can be embedded in the additive group of a local nearring.*

As another application of Lemma 49, we have also the following assertion.

51 Corollary. *Let R be a local nearring whose subgroup L_R has finite index in the additive group R^+ of R. Then L_R is a normal subgroup of R^+.*

Proof. Indeed, the subgroup L_R contains a normal subgroup M of R^+ such that the factor group R^+/M is either a p-group for some prime p or a divisible torsion-free group by Lemma 49. Since L_R/M is a subgroup of finite index in R^+/M, it is subnormal in R^+/M and hence L_R is subnormal in R^+. Thus L_R is normal in R^+ by the remarks made after Lemma 44. $\boxed{QED}$

In connection with the above results the following conjecture seems to be valid.

52 Conjecture. *If R is a local nearring whose subgroup L_R is of finite index in the additive group of R, then L_R is an ideal of R.*

In particular, it follows from Proposition 45 that this conjecture is true if L_R has a prime index in R^+.

It turns out that for every infinite local nearring R which is not a nearfield the subgroup L_R must be infinite.

53 Lemma. *Let R be a local nearring whose subgroup L_R is finite and non-zero. Then R is finite.*

Proof. The right annihilator $\operatorname{Ann}_R(L_R) = \bigcap_{a \in L_R} \operatorname{Ann}_R(a)$ of L_R in R has finite index in R^+ because L_R is finite and $aR \subseteq L_R$ for every $a \in L_R$ by Lemma 35. Hence, if R is infinite, the intersection $R^* \cap \operatorname{Ann}_R(L_R)$ is non-empty and so $L_R \cdot r = 0$ for some $r \in R^*$. But then $L_R = \{0 \cdot r^{-1}\}$ and thus $L_R = 0$, contrary to the hypothesis of the lemma. Therefore R must be finite, as desired. $\boxed{QED}$

The final result of this section concerns the structure of the subgroup L_R of a finite local nearring R. Recall that R^+ is a p-group for some prime p by Corollary 50 and so R is of order p^n for some positive integer n As above, if G is a group, then $\Phi(G)$ denotes the Frattini subgroup of G.

54 Theorem. *Let R be a finite local nearring of order p^n with identity element $\mathbf{1}$ and let $G(R) = R^+ \rtimes R^*$ be the group associated with R. Then $H = R^+ \rtimes (\mathbf{1} + L_R)$ is the normal Sylow p-subgroup of $G(R)$ and $L_R = R^+ \cap \Phi(H)$. In particular, if the subgroup L_R is non-abelian, then its center is non-cyclic.*

Proof. Note first that L_R is an ideal of R by Corollary 48 and so $\mathbf{1}+L_R$ is a normal p-subgroup of R^* by Lemma 44. Therefore H is a normal p-subgroup of $G(R)$ and the factor groups $G(R)/H$ and $R^*/(\mathbf{1}+L_R)$ are isomorphic. Since the factor nearring R/L_R is a nearfield of order p^m for some positive integer $m \le n$, its multiplicative group is of order $p^m - 1$ and isomorphic to $R^*/(\mathbf{1}+L_R)$. Thus $G(R)/H$ is of order $p^m - 1$ and so H is the Sylow p-subgroup of $G(R)$. Show next that $L_R = R^+ \cap \Phi(H)$.

For convenience, we shall look at $G(R)$ as a group of all pairs (t, r) with $t \in R^*$ and $r \in R$ which are multiplied by the rule $(u, s)(t, r) = (ut, t^{-1}s + r)$ for all $t, u \in R^*$ and $r, s \in R$. Then the pair $(\mathbf{1}, 0)$ is the identity element of $G(R)$ denoted by 1 and the groups R^+, R^*, L_R and $\mathbf{1} + L_R$ are identified with the subgroups $M = \{(\mathbf{1}, r) \mid r \in R\}$, $A = \{(t, 0) \mid t \in R^*\}$, $L = \{(\mathbf{1}, s) \mid s \in L_R\}$ and $U = \{(u, 0) \mid u \in \mathbf{1} + L_R\}$ of $G(R)$, respectively. In this notation we have to prove that $L = M \cap \Phi(H)$.

As $H = M \rtimes U$ is a p-group, its Frattini subgroup $\Phi(H)$ contains the derived subgroup H'. Put $e = (\mathbf{1}, \mathbf{1})$. Then $e \in M$, $e^U = eL$ and $M = e^A \cup L$ because $R = R^* \cup L_R$ by Lemma 35. This implies $L = e^{-1}e^U = [e, U] \subseteq H'$ and hence $L \subseteq M \cap \Phi(H)$.

Conversely, the additive group of the nearfield R/L_R and so the factor group M/L is abelian by Theorem 39. Furthermore, the subgroup A acts transitively on M/L and hence M/L is a minimal normal subgroup of the factor group $G(R)/L$. As H/L is a normal p-subgroup of $G(R)/L$, its Frattini subgroup $\Phi(H/L) = \Phi(H)/L$ intersects trivially the subgroup M/L. Therefore $M \cap \Phi(H) \subseteq L$ and so $M \cap \Phi(H) = L$.

Finally, as it has been proved by B. King [18], every non-abelian normal subgroup of a finite p-group contained in its Frattini subgroup has a non-cyclic center. This implies in particular that if the subgroup L_R is non-abelian, then its center is non-cyclic. $\boxed{\mathit{QED}}$

14 Local nearrings with cyclic-by-finite multiplicative group

In this final part the results about triply factorized groups are applied for studying local nearrings whose multiplicative groups are close to cyclic groups.

55 Lemma. *If R is a local nearring whose multiplicative group R^* is polycyclic-by-finite, then the additive group of R is a p-group for some prime p.*

Proof. Let P be a subnearring of R generated by its identity element $\mathbf{1}$, so that P is a homomorphic image of the ring $\mathbb{Z}$ of integers. Then P is a commutative subring of R and the intersection $L_R \cap P$ is an ideal of P such that the factor ring $P/L_R \cap P$ is a field. If $S = \mathbf{1} + (L_R \cap P)$, then S is a subsemigroup of R^* and therefore the ring of quotients $P_S = PS^{-1}$ is a local subring of R.

If P is isomorphic to $\mathbb{Z}$, then P_S is a local subring of the field $\mathbb{Q}$ of rational numbers and so the multiplicative group P_S^* must contain a free abelian subgroup of infinite rank. However $P_S^* \subseteq R^*$ and this implies a contradiction. Hence P is finite and so isomorphic to the residue ring $\mathbb{Z}/p^n\mathbb{Z}$ for some $n \geq 1$. Thus $\mathbf{1} \cdot p^n = 0$ and so R^+ is a group of exponent p^n. $\boxed{QED}$

56 Theorem. *Let R be a local nearring whose multiplicative group R^* has a cyclic subgroup of finite index. Then R is finite of order p^n for some prime p and a positive integer n.*

Proof. Since the group L_R of all non-invertible elements of R is a construction subgroup of R by Lemma 35.3), the group $G(L_R) = L_R \rtimes (\mathbf{1} + L_R)$ associated with L_R is a triply factorized group $G = M \rtimes A = M \rtimes B = AB$ with subgroups A and B isomorphic to $\mathbf{1} + L_R$ and a normal subgroup M isomorphic to L_R. As $\mathbf{1} + L_R$ is a subgroup of R^*, the subgroups A and B are cyclic-by-finite and the subgroup M is a p-group of finite exponent by Lemma 55. Therefore M is finite by Theorem 13 and so either $L_R = 0$ or the nearring R is also finite by Lemma 53. Thus R is infinite only if it is a nearfield. Since an infinite nearfild with cyclic-by-finite multiplicative group is a commutative field by Theorem 43, it is a field of prime characteristic which is finitely generated as a ring and so must be finite by Hilbert' Nullstellensatz. This contradiction shows that R is finite, as desired. $\boxed{QED}$

In conclusion some classification results about finite local nearrings with multiplicative groups close to cyclic will be given. Finite rings with cyclic multiplicative groups were classified by R. Gilmer in [9]. An analogous result for local nearrings was obtained by A. Gorodnik [10].

57 Theorem. *Let R be a local nearring whose multiplicative group R^* is cyclic. If R is not a local ring, then its additive group R^+ is abelian of order 8 and one of the following statements holds.*

1) *$R^+ = <\mathbf{1}> \oplus <r>$ with $\mathbf{1} \cdot 4 = r \cdot 2 = 0$, $L_R = <\mathbf{1} \cdot 2> \oplus <r>$ and the semigroup $(R, \cdot)$ satisfies the relations:*

$$(\mathbf{1} + r)r = r + \mathbf{1} \cdot 2 \qquad \textit{and} \qquad r^2 = r \cdot 2 = (\mathbf{1} \cdot 2 + r)r = 0.$$

2) $R^+ = <\mathbf{1}> \oplus <r_1> \oplus <r_2>$ *with* $\mathbf{1} \cdot 2 = r_1 \cdot 2 = r_2 \cdot 2 = 0$, $L_R = <r_1> \oplus <r_2>$ *and the semigroup* $(R, \cdot)$ *satisfies the relations:*

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

and

$$r_ir_j = (r_1 + r_2)r_i = 0 \qquad \textit{for all} \qquad 1 \leq i, j \leq 2.$$

In particular, the subgroup L_R *has a zero multiplication and* $R^* = \mathbf{1} + L_R$*.*

A description of local nearings with dihedral multiplicative groups was begun by B. Amberg, P. Hubert and the author in [2] and completed by P. Hubert in his dissertation [14].

58 Theorem. *Let* R *be a local nearring whose multiplicative group* R^* *is dihedral. Then the additive group of* R *is either a* 3*-group of order at most* 9 *or a* 2*-group of order at most* 16 *and the subgroup* L_R *is abelian.*

It was shown by J. Clay and C. Maxson [7] that a generalized quaternion group cannot be the additive group of any nearring with identity element. On the other hand, the local nearrings whose multiplicative group is generalized quaternion were recently described by S. Di Termini and the author in [34]. Recall that an abelian p-group is said to be of type $(p^{n_1}, \dots, p^{n_k})$ with positive integers $n_1, \dots, n_k$ if it is the direct product of k cyclic groups of orders $p^{n_1}, \dots, p^{n_k}$, respectively.

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

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

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

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

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

Using some calculations made by means of a GAP-program based on the package “SONATA, version 2.3” of computer algebra system GAP 4.4, it can be shown that the number of non-isomorphic local nearrings R of order 16 with quaternion group R^* is divided in two halves: there exist 24 such nearrings with R^+ of type $(2, 2, 2, 2)$ and as many with R^+ of type $(2, 2, 4)$.

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

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

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

Then the subgroup L of R^+ generated by the elements r_1, r_2, r_3 consists of non-invertible elements of R and the multiplicative subgroup of R^* generated by the elements a, b is quaternion of order 8 and so must coincide with R^* because $L \cap R^* = \emptyset$ and L has the same order. Hence R^* is the quaternion group and $R = L \cup R^*$ is a local nearring with $L_R = L$.

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

$$\begin{array}{cccccc}
(\mathbf{1}+r_1)r_1 & = & \mathbf{1}\cdot 2+r_1, & (\mathbf{1}+r_2)r_1 & = & r_1, \\
(\mathbf{1}+r_1)r_2 & = & \mathbf{1}\cdot 2+r_2, & (\mathbf{1}+r_2)r_2 & = & \mathbf{1}\cdot 2+r_2, \\
r_1r_2 & = & 0, & r_1^2=r_2^2=r_2r_1 & = & \mathbf{1}\cdot 2, \\
(r_1+r_2)r_1 & = & 0, & (r_1+r_2)r_2 & = & \mathbf{1}\cdot 2, \\
(\mathbf{1}\cdot 2)\cdot r_1 & = & (\mathbf{1}\cdot 2)\cdot r_2 & = & 0. &
\end{array}$$

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

The final two examples of local nearrings of order 32 arose from studying generalized quaternion groups of automorphisms of the abelian groups of type $(2, 2, 2, 2, 2)$ and $(2, 2, 2, 4)$. Most calculations were also made with computer algebra system GAP 4.4.

3 . Let R be the nearring with identity $\mathbf{1}$ whose additive group R^+ is abelian of type $(2, 2, 2, 2, 2)$ with generators $\mathbf{1}, r_1, r_2, r_3, r_4$ and whose semigroup

$(R, \cdot)$ satisfies the relations:

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

Then the group R^* is generalized quaternion of order 16 and $R = L \cup R^*$, so that R is a local nearring with $L_R = L$.

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

$$\begin{array}{rcl rcl}
(\mathbf{1}+r_1)r_1 & = & \mathbf{1}\cdot 2+r_1+r_3, & (\mathbf{1}+r_2)r_1 & = & \mathbf{1}\cdot 2+r_1, \\
(\mathbf{1}+r_1)r_2 & = & r_2+r_3, & (\mathbf{1}+r_2)r_2 & = & \mathbf{1}\cdot 2+r_2, \\
(\mathbf{1}+r_1)r_3 & = & r_1+r_2+r_3, & (\mathbf{1}+r_2)r_3 & = & \mathbf{1}\cdot 2+r_1+r_2+r_3 \\
\text{and} & & (r_i+r_j)r_k & = \quad (r_i+r_j+r_k)r_l & = & 0 \qquad \text{for all} \\
1 \leq \ i,j,k,l & \leq & 4. & & &
\end{array}$$

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

References

[1] Amberg B., Franciosi S., de Giovanni F.: Products of Groups. Clarendon Press, Oxford, (1992).

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

[3] Amberg B., Sysak Ya. P.: Radical rings and products of groups, In: Groups St. Andrews (1997) in Bath, Vol. I, 1–19, London Math. Soc. Lecture Note Ser., 260, Cambridge Univ. Press, Cambridge, (1999).

[4] Amberg B., Sysak Ya. P.: *Products of two groups containing cyclic subgroups of index at most* 2, Arch. Math. (Basel), **90** (2008), 101–111.

[5] Chernikov N. S.: *On the product of almost Abelian groups*, Ukr. Mat. Zh., **33** (1981), 136–138.

[6] Clay J. R.: Nearrings. Geneses and applications. Clarendon Press, New York, (1992).

[7] Clay J. R., Maxson C. J.: *The near-rings with identities on generalized quaternion groups*, Ist. Lombardo Accad. Sci. Lett. Rend. A, **104** (1970), 525–530.

[8] Cohn P. M.: *A remark on the general product of two infinite cyclic groups*, Arch. Math. (Basel), **7** (1956), 94–99.

[9] Gilmer R. W.: *Finite rings having a cyclic group of units*, Amer. Math. J., **85** (1963), 447–452.

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

[11] Hall M. Jr.: The theory of groups. Macmillan, New York, (1959).

[12] Jabara E.: *A note on some factorized groups*, J. Algebra **279** (2004), 308–314.

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

[14] Hubert P.: *Nearrings and a construction of triply factorized groups*, Dissertation zur Erlangung des Grades "Doktor der Naturwissenschaften", Johannes-Gutenberg- Universität Mainz, (2005).

[15] Hubert P.: Triply factorised groups and nearrings, In: Groups St. Andrews (2005), Vol. II, 496–503, London Mathematical Society Lecture Note Ser., 340, Cambridge Univ. Press, Cambridge, (2007).

[16] Huppert B.: *Über die Auflösbarkeit faktorisierbarer Gruppen*, Math. Z., **59** (1953), 1–7.

[17] Itô N.: *Über das Product von zwei abelschen Gruppen*, Math. Z., **62** (1955), 400–401.

[18] King B. W.: *Normal subgroups of groups of prime-power order*, In: Proc. Second Intern. Conf. on the Theory of Groups (Australian Nat. Univ., Canberra, 1973), 401–408. Lecture Notes in Math., Vol. **372**, Springer, Berlin, (1974).

[19] Lawrence J.: *The cocycle equation in division rings*, Aeq. Math., **22** (1981), 70–72.

[20] Lyons C.: *Peterson, G., Local endomorphism near-rings*, Proc. Edinburg Math. Soc., **31** (1988), 409–414.

[21] Maxson C. J.: *On local near-rings*, Math. Z. **106** (1968), 197–205.

[22] Meldrum J. D. P.: Near-rings and their links with groups. Pitman, London, (1985).

[23] Monakhov V. S.: *The product of two groups, one of which contains a cyclic subgroup of index* ≤ 2, Mat. Zametki, **16** (1974), 285–295.

[24] Monakhov V. S.: *On the product of two groups with cyclic subgroups of index* 2, (Russian) Vesti Akad. Navuk. Belarusi, Ser. Fiz-Mat. Navuk, no. 3 (1996), 21–24.

[25] Neumann B. H.: *On the commutativity of addition*, J. London Math. Soc. **15** (1940), 203–208.

[26] Pettet M. R.: *Free actions on virtually FC-groups*, Arch. Math. (Basel), **86** (2006), 26–30.

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

[28] Robinson D. J. S.: A course in the theory of groups. Springer-Verlag, Berlin, (1982).

[29] Scott W. R.: *Solvable factorizable groups*, Illinois J. Math., **1** (1957), 389–394.

[30] Shunkov V. P.: *Periodic groups with an almost regular involution*, Algebra i Logika **11** (1972), 470–493.

[31] Sysak Ya. P.: *Products of locally cyclic torsion-free groups*, Algebra i Logika, **25** (1986), 672–686.

[32] Sysak Ya. P.: *Products of almost abelian groups, In: Investigations of groups with restrictions for subgroups*, (Russian), Akkad. Nauk Ukrain. SSR, Inst. Mat., Kiev, (1988), 81–85.

[33] Sysak Ya. P.: Some examples of factorized groups and their relation to ring theory, In: Infinite Groups (1994) (Ravello), W. de Gruyter, Berlin (1996), 257–269.

[34] Sysak Ya. P., Di Termini S.: *Local nearrings with generalized quaternion multiplicative group*, Ricerche Mat., **56** (2007), 61–72.

[35] Wähling H.: Theorie der Fastkörper. Thales Verlag, Essen, (1987).

[36] Wehrfritz B. A. F.: Infinite Linear Groups. Springer-Verlag, Berlin, (1973).

[37] Wilson J. S.: *On products of soluble groups of finite rank*, Comment. Math. Helv., **60** (1985), 337–353.

[38] Wilson J. S.: *A note on products of abelian-by-finite groups*, Arch. Math. (Basel), **54** (1990), 117–118.

[39] Zaitsev D. I.: *Itô's theorem and products of groups*, Mat. Zametki, **33** (1983), 807–818.

[40] Zassenhaus H.: *Über endliche Fastkörper*, Ab. Math. Sem. Univ. Hamburg, **11** (1935/36), 187–220.

[41] Zemmer J. L.: *The additive group of an infinite near-field is abelian*, J. London Math. Soc. **44** (1969), 65–67.