Czechoslovak Mathematical Journal

Wen-Fong Ke; Johannes H. Meyer; Günter F. Pilz; Gerhard Wendt
On zero-symmetric nearrings with identity whose additive groups are simple

Czechoslovak Mathematical Journal, Vol. 74 (2024), No. 3, 869–880

Persistent URL: http://dml.cz/dmlcz/152585

Terms of use:

© Institute of Mathematics AS CR, 2024

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

Czechoslovak Mathematical Journal, 74 (149) (2024), 869–880

ON ZERO-SYMMETRIC NEARRINGS WITH IDENTITY WHOSE ADDITIVE GROUPS ARE SIMPLE

Wen-Fong Ke, Tainan, Johannes H. Meyer, Bloemfontein,
Günter F. Pilz, Gerhard Wendt, Linz

Received March 2, 2024. Published online July 24, 2024.

Abstract. We investigate conditions on an infinite simple group in order to construct a zero-symmetric nearring with identity on it. Using the Higman-Neumann-Neumann extensions and Clay's characterization, we obtain zero-symmetric nearrings with identity with the additive groups infinite simple groups. We also show that no zero-symmetric nearring with identity can have the symmetric group $\mathrm{Sym}(\mathbb{N})$ as its additive group.

Keywords: infinite simple group; HNN extension; nearring with identity

MSC 2020: 20E06, 16Y30, 20E32, 20B30

1. Introduction

The Higman-Neumann-Neumann (HNN) extensions, introduced in [7], can be used to construct simple groups. Utilizing the HNN extensions, we present in this paper for the first time, infinite simple groups that are the additive groups of zero-symmetric nearrings with identity, see Section 4.

Here, a *nearring* refers to a *right nearring,* which is a triple $(N, +, \cdot)$, where $(N, +)$ is a group (with neutral element 0 and not necessarily abelian), $(N, \cdot)$ is a semigroup, and the right distributive law holds, i.e.,

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall\, a, b, c \in N.$$

A left nearring is defined in an analogous way, where the left distributive law is required to hold. Whenever it is clear from the context, the multiplication operator will usually be suppressed, and $a \cdot b$ will be written simply as ab.

DOI: 10.21136/CMJ.2024.0086-24

© Institute of Mathematics, Czech Academy of Sciences 2024.

A nearring N is said to be *zero-symmetric* if $n0 = 0n = 0$ for every $n \in N$, and is a *nearring with identity* if there is an element $1 \in N$ satisfying $n1 = 1n = n$ for all $n \in N$. The reader is referred to [12] for general definitions and results with respect to the theory of nearrings. Henceforth, all the nearrings in this paper will be assumed to be zero-symmetric.

Nearrings occur naturally. For example, given a group $(G, +)$, the set $M_0(G)$ of all functions $f\colon G \to G$ with $f(0) = 0$ is a nearring with pointwise addition as the additive operation and the function composition as the multiplicative operation. In fact, every nearring can be embedded in $M_0(G)$ as a subnearring for a group G.

On the other hand, given an additive group $(G, +)$, one may construct a nearring N such that the additive group $(N, +)$ is $(G, +)$. In this case, we say that G *supports* the nearring N. Clay in [2] has characterized necessary and sufficient conditions for a group G to support a nearring N. We shall recall the characterization in the next section.

Every group can support nearrings. However, it is a rare phenomenon for a simple group to support a nearring with identity. As a matter of fact, the only finite simple groups that support nearrings with identity are the cyclic groups $(\mathbb{Z}_p, +)$, where p is a prime. In this case, for each prime p, one obtains the field $(\mathbb{Z}_p, +, \cdot)$ as the nearring with identity, see [3]. Up to now, no infinite simple group that supports a nearring with identity was known, and the purpose of this paper is to exhibit such groups.

Now, for an infinite simple group G to support a nearring with identity, it has to be either torsion-free or of a prime exponent, see Theorem 3.1. Thus, most of the known infinite simple groups are ruled out. Furthermore, G must have nonabelian proper subgroups (see Theorem 3.3), which destroyed our hope on using the Tarski monster groups (as in [10] and [11]) for the task. In fact, as a result of Theorem 3.2, G has to have a lot of proper subgroups which are isomorphic to G itself. Using the HNN extensions, we are able to construct simple groups with the required property, and show that they support nearrings with identity.

It was shown by Clay and Malone (see [3], Theorem 4) that no symmetric group S_n, $n \geqslant 3$, can support a nearring with identity. We show, in the final section, that this is also the case for the symmetric group $\mathrm{Sym}\,(\mathbb{N})$ on the set of all positive integers.

We note that an infinite simple group can be the additive group of a nearring with *right* identities as Kaarli shows in [8]. The only requirement is the existence of an isomorphism from the group to a proper subgroup.

Next, we recall the procedure of finding all nearrings with a given additive group.

2. Nearrings with a given additive group

Let $(N, +, \cdot)$ be a nearring. For every element $a \in N$, the mapping $n \mapsto na$ for all $n \in N$ is an endomorphism of the additive group $(N, +)$ as $\cdot$ is right distributive over $+$. Based on this, Clay demonstrated in [2] how one can construct a nearring N such that the additive group $(N, +)$ of N is a given additive group $(G, +)$. The notation $\mathrm{End}\,(G)$ denotes the set of all endomorphisms of the group G.

Theorem 2.1 ([2]). *For a group $(G, +)$, let $\varphi\colon\ G \to \mathrm{End}\,(G)$; $a \mapsto \varphi_a$ be a map that satisfies $\varphi_a \circ \varphi_{a'} = \varphi_{\varphi_a(a')}$ for all $a, a' \in G$, and $\varphi_0(b) = 0$ for all $b \in G$. Then $(N, +, \cdot_\varphi)$ is a zero-symmetric nearring, where $(N, +) = (G, +)$, and $n \cdot_\varphi n' = \varphi_{n'}(n)$ for all $n, n' \in N$. Moreover, all possible multiplications to turn $(G, +)$ into a zero-symmetric nearring can be obtained in this way.*

Note that different φ's can provide isomorphic nearrings. See also [12], 9.90–9.116. Of course, to obtain a zero-symmetric nearring $(N, +, \cdot_\varphi)$ with identity, the mapping φ must satisfy some additional conditions.

Theorem 2.2 ([2]). *Let $(G, +)$ be a group and φ a map satisfying the conditions of Theorem 2.1 so that $(N, +, \cdot_\varphi)$ is a zero-symmetric nearring. Then an element $e \in N$ is an identity element for the nearring N if and only if φ_e is the identity map in $\mathrm{End}\,(N)$ and for all $n \in N$, $\varphi_n(e) = n$.*

3. Nearrings with an additive infinite simple group

In this section, we investigate nearrings with identity having an infinite simple group as the additive group. Recall that an additive group $(G, +)$ *supports* a zero-symmetric nearring with identity if there is a zero-symmetric nearring N with identity and such that $(N, +) = (G, +)$. Now, we have the following general result.

Theorem 3.1. *Let $G = (G, +)$ be a simple group. If G supports a zero-symmetric nearring N with identity, then either G is torsion-free, or every nonzero element of G is of a fixed prime order.*

P r o o f. Suppose that G supports a zero-symmetric nearring $(N, +, \cdot)$ with identity. By Theorem 2.2, the multiplication $\cdot$ is the same as the binary operation $\cdot_\varphi$ on G given by a mapping $\varphi\colon\ G \to \mathrm{End}\,(G)$; $a \mapsto \varphi_a$ with a specific element $e \in G$ such that $\varphi_a(e) = a$ for all $a \in G$. For any nonzero $a \in G$, we have $\varphi_a(e) = a \neq 0$. Thus, $\ker \varphi_a \neq G$. By the simplicity of G, we have $\ker \varphi_a = \{0\}$, and so φ_a is a monomorphism on G. Hence, the order of $a = \varphi_a(e)$ is the same (finite or infinite) as that of e.

Suppose that the order of e is finite, say $o(e) = k$, and that $k = st$, $s > 1$ and $t > 1$. Then $(se) \cdot (te) = (st)e = 0$. So, se is contained in the kernel of φ_{te} which is $\{0\}$. But then $se = 0$, which implies $s \geqslant k = st > s$, a contradiction. Therefore, k has to be a prime. □

This theorem rules out most known infinite simple groups for supporting zero-symmetric nearrings with identity. For example, the finitary alternating group $A(\kappa)$, κ an infinite cardinal, does not support a zero-symmetric nearring with identity. This is because $A(\kappa)$ has elements of various orders. For the same reason, the simple groups $\mathrm{PSL}_m(K)$, $m \geqslant 2$, where K is an infinite field (see [4]), the infinite series $G^+_{n,r}$ $(n, r \in \mathbb{N},\ n \geqslant 2)$ of infinite simple groups, as well as the derived subgroup $S'_{n,r}$ of $S_{n,r}$, and those $S_{n,r}$ with $\gcd(r, n-1) = 1$ (cf. [16]), cannot support zero-symmetric nearrings with identity. There are well-known finitely generated infinite simple groups, called the *Tarski monster groups*, first constructed by Ol'shanskii (see [11]), the nontrivial proper subgroups of which are all of a prime order. There is another finitely generated infinite simple group constructed by Ol'shanskii (see [10]), the nontrivial proper subgroups of which are all infinitely cyclic. So they fit the requirements of Theorem 3.1. However, they cannot support zero-symmetric nearrings with identity as we are going to see next.

Theorem 3.2. *Let N be an infinite zero-symmetric nearring with identity* 1. *Suppose that $(N, +)$ is a simple group. For every nonzero element $a \in N$, $(Na, +)$ is an isomorphic copy of $(N, +)$.*

P r o o f. Let $a \in N \setminus \{0\}$. Then the endomorphism $\varphi_a \colon N \to N$ of $(N, +)$, given by $\varphi_a(n) = na$ for all $n \in N$, is nontrivial as $\varphi_a(1) = a$. By the simplicity of $(N, +)$, the kernel of φ_a is $\{0\}$, and so $(N, +)$ is isomorphic to the additive subgroup $\operatorname{Im}\varphi_a = Na$ of $(N, +)$. □

Theorem 3.3. *Let $G = (G, +)$ be an infinite simple group. If all of the proper subgroups of G are abelian, then G cannot support a zero-symmetric nearring with identity.*

P r o o f. Assume on the contrary that all of the proper subgroups of G are abelian and that G supports a zero-symmetric nearring $(N, +, \cdot)$ with identity. Let $a \in N$ be a nonzero element. Then, as an additive group, $Na = \operatorname{Im}\varphi_a$ is isomorphic to G, which is not abelian. This implies that $Na = N$. Let $x \in N$ such that $xa = 1$. Then $x \neq 0$, and so $Nx = N$. We can find some $y \in N$ such that $yx = 1$, which gives $y = yxa = a$. This shows that a is invertible. With every nonzero element of N being invertible, N is a nearfield. But then $(N, +)$ is an abelian group (cf. [12], Theorem 8.11), i.e., G is abelian, a contradiction. This proves the theorem. □

If G is one of the infinite simple groups constructed by Ol'shanskii, then every proper subgroup of G is cyclic, and hence abelian. Therefore, G cannot support a zero-symmetric nearring with identity by Theorem 3.3.

4. An infinite simple group supporting a nearring with identity

We have learned from above that for an infinite simple group G to support a zero-symmetric nearring with identity, G has to be either torsion-free (of exponent 0) or of a fixed prime exponent p, and needs to have many proper subgroups which are all isomorphic to G. To find such a group, we use the Higman-Neumann-Neumann (HNN) extensions, see [7] and also [1], [9], [13].

4.1. First construction. Let us start with $G = \mathbb{Z}$ or $\mathbb{Z}_p$ (p an odd prime), and construct a sequence of groups

$$G = G_0 \subseteq G_1 \subseteq G_2 \subseteq \dots$$

inductively, as described in the next paragraph. It is convenient to put $G_{-1} = \{0\}$.

Suppose that we have already obtained G_i for some $i \geqslant 0$, which has the same exponent as G. Thus, any two nontrivial cyclic subgroups of G_i are isomorphic, and so the HNN construction is applicable for G_i. To get G_{i+1}, we designate free generators $t_{\alpha,\beta}$ such that

$$-t_{\alpha,\beta} + \alpha + t_{\alpha,\beta} = \beta$$

for every pair of distinct elements $\alpha, \beta \in G_i \setminus \{0\}$ with either $\alpha \notin G_{i-1}$ or $\beta \notin G_{i-1}$. Then we collect all of these $t_{\alpha,\beta}$'s into the set $\mathcal{T}(G_i)$. If G_i is torsion-free, we put $G_{i+1} = \langle G_i \cup \mathcal{T}(G_i)\rangle$, which is torsion-free. If G_i is of exponent p, we let $\widetilde{G}_{i+1} = \langle G_i \cup \mathcal{T}(G_i)\rangle$, take $N = N(p\widetilde{G}_{i+1})$ the normal subgroup of $\widetilde{G}_{i+1}$ generated by $p\widetilde{G}_{i+1} = \{pg\colon\ g \in \widetilde{G}_{i+1}\}$ and put $G_{i+1} = \widetilde{G}_{i+1}/N$, which is of exponent p. Notice that $G_i \cap N = \{0\}$. Thus, for $g_1, g_2 \in G_i$, $g_1 + N = g_2 + N$ if and only if $g_1 = g_2$, and so G_i can be embedded in $\widetilde{G}_{i+1}/N$ as a subgroup. By abusing the notation, in the latter case, we use G_i for $\{g + N\colon\ g \in \widetilde{G}_i\}$ and $\mathcal{T}(G_i)$ for $\{t + N\colon\ t \in \mathcal{T}(G_i)\}$. In this way, with G_i torsion-free or of exponent p, we have the group

$$G_{i+1} = \langle G_i \cup \mathcal{T}(G_i)\rangle,$$

which is of the same exponent as that of G, and all nonzero elements in G_i are conjugate in G_{i+1}. Let $G^* = \bigcup_{i=0}^{\infty} G_i$. Then G^* is a simple group.

Next, let us show how to associate with every nonzero element of G^* a proper subgroup of G^* which is isomorphic to G^*, and that we can construct a zero-symmetric nearring with identity on it.

Let $\gamma \in G^* \setminus \{0\}$. Then $\gamma \in G_i \setminus G_{i-1}$ for some $i \geqslant 0$. Set $H_0 = \langle \gamma \rangle \leqslant G_i$. Then H_0 and G_0 are isomorphic groups, and there is a group isomorphism $f_\gamma^{(0)}\colon G_0 \to H_0$ such that $f_\gamma^{(0)}(1) = \gamma$.

Now, within the group G_{i+1}, we take the subset $\widetilde{\mathcal{T}}_0(\gamma)$ of $\mathcal{T}(G_i)$:

$$\widetilde{\mathcal{T}}_0(\gamma) = \{t_{\mu,\nu} \in \mathcal{T}(G_i)\colon\ \mu, \nu \in H_0 \setminus \{0\},\, \mu \neq \nu\}.$$

Note that

$$t_{\alpha,\beta} \leftrightarrow t_{f_\gamma^{(0)}(\alpha), f_\gamma^{(0)}(\beta)}\ (\alpha, \beta \in G_0 \setminus \{0\},\, \alpha \neq \beta)$$

is a bijection between $\mathcal{T}(G_0)$ and $\widetilde{\mathcal{T}}_0(\gamma)$. Set

$$H_1 = \langle H_0 \cup \widetilde{\mathcal{T}}_0(\gamma) \rangle \leqslant G_{i+1}.$$

It is clear that H_1 is isomorphic to

$$G_1 = \langle G_0 \cup \mathcal{T}(G_0) \rangle$$

with an isomorphism $f_\gamma^{(1)}\colon G_1 \to H_1$ such that $f_\gamma^{(1)}(\lambda) = f_\gamma^{(0)}(\lambda)$ for all $\lambda \in G_0$, and $f_\gamma^{(1)}(t_{\alpha,\beta}) = t_{f_\gamma^{(0)}(\alpha), f_\gamma^{(0)}(\beta)}$ for $\alpha, \beta \in G_0 \setminus \{0\}$ with $\alpha \neq \beta$.

Next, within the group G_{i+2}, we take the subset $\widetilde{\mathcal{T}}_1(\gamma)$ of $\mathcal{T}(G_{i+1})$:

$$\widetilde{\mathcal{T}}_1(\gamma) = \{t_{\mu,\nu} \in \mathcal{T}(G_{i+1})\colon\ \mu, \nu \in H_1 \setminus \{0\},\, \mu \neq \nu \text{ with } \mu \notin H_0 \text{ or } \nu \notin H_0\}.$$

Note that

$$t_{\alpha,\beta} \leftrightarrow t_{f_\gamma^{(1)}(\alpha), f_\gamma^{(1)}(\beta)}\ (\alpha, \beta \in G_1 \setminus \{0\},\, \alpha \neq \beta \text{ with } \alpha \notin G_0 \text{ or } \beta \notin G_0)$$

is a bijection between $\mathcal{T}(G_1)$ and $\widetilde{\mathcal{T}}_1(\gamma)$. Set $H_2 = \langle H_1 \cup \widetilde{\mathcal{T}}_1(\gamma) \rangle \leqslant G_{i+2}$. Now, H_2 and G_2 are isomorphic with an isomorphism $f_\gamma^{(2)}\colon G_2 \to H_2$ determined by $f_\gamma^{(2)}(\lambda) = f_\gamma^{(1)}(\lambda)$ for all $\lambda \in G_1$, and $f_\gamma^{(2)}(t_{\alpha,\beta}) = t_{f_\gamma^{(1)}(\alpha), f_\gamma^{(1)}(\beta)}$ for distinct $\alpha, \beta \in G_1 \setminus \{0\}$ with either $\alpha \notin G_0$ or $\beta \notin G_0$.

Continuing in this manner, we obtain a sequence of subgroups H_j of G^* and isomorphisms $f_\gamma^{(j)}\colon G_j \to H_j$, $j = 0, 1, 2, \ldots$ Then we set $H_\gamma^* = \bigcup\limits_{j=0}^{\infty} H_j$, which is a subgroup of G^* isomorphic to G^* itself with an isomorphism $f_\gamma\colon G^* \to H_\gamma^*$ such that $f_\gamma|_{G_j} = f_\gamma^{(j)}$ for all $j \geqslant 0$. From the construction, we see that $f_\gamma^{(0)}$ determines $f_\gamma^{(1)}$, $f_\gamma^{(1)}$ determines $f_\gamma^{(2)}$, etc., i.e., f_γ is uniquely determined by $f_\gamma^{(0)}$.

Recall that $G_0 = \mathbb{Z}$ or $\mathbb{Z}_p$. Let $\lambda, \tau \in G^*$. From $f_\tau(1) = \tau$ we get

$$(f_\lambda \circ f_\tau)(m) = f_\lambda(f_\tau(m)) = f_\lambda(m f_\tau(1)) = m f_\lambda(\tau) = m f_{f_\lambda(\tau)}(1) = f_{f_\lambda(\tau)}(m)$$

for all $m \in G_0$. Therefore, $f_\lambda \circ f_\tau = f_{f_\lambda(\tau)}$. It follows from Theorems 2.1 and 2.2 that we can use f to define a zero-symmetric simple nearring N on G^* with 1 as the identity of N.

4.2. Second construction. In the previous construction, we start from the groups $G = \mathbb{Z}$ or $\mathbb{Z}_p$, and obtain a simple group G^*, which is countable. To get uncountable simple groups that support zero-symmetric nearrings with identity, we have to start with uncountable groups.

Let G be a free group of infinite rank with a basis B, and again, set $G_{-1} = \{0\}$ and $G_0 = G$. Suppose that we have already obtained G_i for some $i \geqslant 0$. For each distinct pair $\alpha, \beta \in G_i \setminus \{0\}$ such that either $\alpha \notin G_{i-1}$ or $\beta \notin G_{i-1}$, we add a free generator $t_{\alpha,\beta}$ to G_i with the relation $-t_{\alpha,\beta} + \alpha + t_{\alpha,\beta} = \beta$. Denote by $\mathcal{T}(G_i)$ the set of all such $t_{\alpha,\beta}$. Put $G_{i+1} = \langle G_i \cup \mathcal{T}(G_i)\rangle$. Then G_{i+1} is a torsion-free group, where all nonzero elements in G_i are conjugate in G_{i+1}. This way, we get a sequence of groups $G = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots$ with $G^* = \bigcup\limits_{i=0}^{\infty} G_i$ a simple group.

Certainly, when the free rank of G is uncountable, G^* is uncountable. The question is whether we can get G^* to support a zero-symmetric nearring with identity. To do this, we need to associate with every nonzero element of G^* a subgroup which is isomorphic to G^*, and that the isomorphisms interact correctly. While the idea is the same as we have done in the countable case before, there are great details needed to be taken care of, especially the step of setting up the first subgroup of G^* which is isomorphic to G_0.

First of all, let X be the smallest ordinal number with $|X| = |B|$. We denote the well ordering relation in X by $\prec$, the least element of X by 0, and the successor of an $\iota \in X$ by $\iota + 1$. Also, we may write $s' \succ s$ if $s, s' \in X$ and $s \prec s'$. Then, we index B by X, so that $B = \{\pi_\iota \colon \iota \in X\}$.

Lemma 4.1. *For every $\zeta \in G^* \setminus \{0\}$, there is a finite subset $\Delta_\zeta \subseteq X$, uniquely determined by ζ, such that $\{\zeta\} \cup \{\pi_\iota \colon \iota \notin \Delta_\zeta\}$ is independent.*

P r o o f. Let $\zeta \in G^* \setminus \{0\}$. If $\zeta \in G_0$, then, in its freely reduced form, ζ is expressed uniquely as a finite sum $\sum\limits_{i=1}^{k} s_{\nu_i}\pi_{\nu_i}$ for some $k \geqslant 1$, where $s_{\nu_i} \in \mathbb{Z} \setminus \{0\}$ and $\pi_{\nu_i} \in B$ for $1 \leqslant i \leqslant k$. Those π_{ν_i}'s which appear in this sum are said to be involved in ζ, and they are uniquely determined by ζ. Now, $\{\zeta\} \cup (B \setminus \{\pi_{\nu_i} \colon 1 \leqslant i \leqslant k\})$ is independent, and we see that $\Delta_\zeta = \{\nu_i \colon 1 \leqslant i \leqslant k\} = \{\iota \in X \colon \pi_\iota \text{ is involved in } \gamma\}$ is the required subset of X.

Assume that $\zeta \in G_{i+1} \setminus G_i$, where $i \geqslant 0$. Then ζ can be written uniquely in the normal form

$$\zeta = \zeta_0 + \varepsilon_1 t_1 + \zeta_1 + \ldots + \varepsilon_k t_k + \zeta_k, \tag{4.1}$$

where $\zeta_0, \zeta_j \in G_i$, $t_j \in \mathcal{T}(G_i)$ and $\varepsilon_j = \pm 1$, $j = 1, 2, \ldots k$ for some $k \geqslant 1$ such that if $j \in \{1, 2, \ldots, k-1\}$ and $\varepsilon_j + \varepsilon_{j+1} = 0$, then $\varepsilon_j t_j + \zeta_j + \varepsilon_{j+1}\zeta_{j+1} \notin G_i$,

see e.g. [13], Theorem 11.83. For each $j \in \{1, 2, \ldots, k\}$ we have $t_j = t_{\alpha_j, \beta_j}$ for some $\alpha_j, \beta_j \in G_i \setminus \{0\}$. In this case, we say that ζ_0, α_1, β_1, ζ_1, …, α_k, β_k and ζ_k are involved in ζ. If, say, τ is one of these which are involved in ζ, and τ is in $G_i \setminus G_{i-1}$, then those $\tau_0, \tau_1, \ldots, \tau_m \in G_{i-1}$ that are involved in τ are said to be involved in ζ as well. Working the way down to G_0, we find finitely many elements in G_0 that are involved in ζ (which are uniquely determined by ζ). Let ω_1, ω_2, …, ω_l be all of the elements in G_0 which are involved in γ. Each ω_j $(1 \leqslant j \leqslant l)$ determines a unique finite subset $\Gamma_{\omega_j} = \{\iota \in X\colon \pi_\iota \text{ is involved in } \omega_j\}$ of X, and the set $\Delta_\zeta = \bigcup_{j=1}^{l} \Gamma_{\omega_l}$ is the one with the required property. □

Now, let $\gamma \in G^* \setminus \{0\}$. To start, we need a subgroup H_γ of G^* containing γ and isomorphic to G_0.

Let $\Delta_\gamma = \{\widetilde{m}_0 \prec \widetilde{m}_1 \prec \ldots \prec \widetilde{m}_k\}$. Since the initial segment $\{\iota \in X\colon 0 \preceq \iota \prec \widetilde{m}_k\}$ cannot be order isomorphic to X by [6], Theorem 6.3 (iv), and X is the smallest ordinal number with the cardinality $|X|$, we have $|\widetilde{m}_k| < |X|$. It follows that the cardinality of $\{\iota \in X\colon \widetilde{m}_k \preceq \iota\}$ is equal to $|X|$. Set $\mu_\gamma = \widetilde{m}_k$, and we have that $\iota \mapsto \mu_\gamma + \iota$ is an order isomorphism from X onto $\{\iota \in X\colon \widetilde{m}_k \preceq \iota\}$.

Let $B_\gamma = \{\gamma\} \cup \{\pi_{\mu_\gamma + \iota}\colon \iota \in X, \iota \succ 0\}$, which is independent, and $|B_\gamma| = |B|$. Then the subgroup $H_\gamma = \langle B_\gamma \rangle$ of G^* is isomorphic to G_0 with an isomorphism $f_\gamma^{(0)}\colon G_0 \to H_\gamma$ such that $f_\gamma^{(0)}(\pi_0) = \gamma$ and $f_\gamma^{(0)}(\pi_\iota) = \pi_{\mu_\gamma + \iota}$ for all $\iota \succ 0$.

Now, put $H_{-1} = \{0\}$ and $H_0 = H_\gamma$. Inductively for $j \geqslant 0$, we define the subgroup H_{j+1} of G_{j+1} as $\langle H_j \cup \widetilde{\mathcal{T}}_j(\gamma) \rangle$, where $\widetilde{\mathcal{T}}_j(\gamma)$ is the subset of $\mathcal{T}(G_j)$ consisting of the elements $t_{\mu,\nu}$, where μ and ν are distinct nonzero elements from H_j such that either $\mu \notin H_{j-1}$ or $\nu \notin H_{j-1}$. Then H_{j+1} is isomorphic to $G_{j+1} = \langle G_j \cup \mathcal{T}(G_j) \rangle$ with an isomorphism $f_\gamma^{(j+1)}\colon G_{j+1} \to H_{j+1}$ such that

$$f_\gamma^{(j+1)}(\lambda) = f_\gamma^{(j)}(\lambda) \quad \text{for } \lambda \in G_j,$$

$$f_\gamma^{(j+1)}(t_{\alpha,\beta}) = t_{f_\gamma^{(j)}(\alpha), f_\gamma^{(j)}(\beta)} \text{ for } \alpha \neq \beta \text{ in } G_j \setminus \{0\} \text{ with either } \alpha \notin G_{j-1} \text{ or } \beta \notin G_{j-1}.$$

The subgroup $H_\gamma^* = \bigcup_{j=0}^{\infty} H_j$ of G^* is isomorphic to G^* with an isomorphism $f_\gamma\colon G^* \to H_\gamma^*$ such that $f_\gamma|_{G_j} = f_\gamma^{(j)}$ for all $j \geqslant 0$. Moreover, from the construction, we see that f_γ is completely determined by $f_\gamma^{(0)}$.

Now, let $\zeta, \tau \in G^*$ be arbitrary. We have to check that $f_\zeta \circ f_\tau = f_{f_\zeta(\tau)}$. It is easy to see that this is true if $\zeta = 0$ or $\tau = 0$. Thus, we assume that both ζ and τ are nonzero.

Recall that $\Delta_{f_\zeta(\tau)}$ consists of those $\iota \in X$ such that π_ι is involved in $f_\zeta(\tau)$.

Lemma 4.2. $\Delta_{f_\zeta(\tau)} = \{\mu_\zeta + \iota\colon \iota \in \Delta_\tau\}$.

P r o o f. Suppose that $\tau \in G_0$ and $\sum_{j=1}^{k} s_{\nu_j}\pi_{\nu_j}$ is the freely reduced form of τ, where $s_{\nu_j} \in \mathbb{Z} \setminus \{0\}$ and $\pi_{\nu_j} \in B$, $1 \leqslant j \leqslant k$. Then $f_\zeta\Big(\sum_{j=1}^{k} s_{\nu_j}\pi_{\nu_j}\Big) = \sum_{j=1}^{k} s_{\nu_j}\pi_{\mu_\zeta+\nu_j}$, which is also freely reduced. If $\iota \in \Delta_\tau$, i.e., π_ι is involved in τ, then $\pi_\iota = \pi_{\nu_j}$ for some $j \in \{1, 2, \dots, k\}$, and so $\pi_{\mu_\zeta+\iota} = \pi_{\mu_\zeta+\nu_j}$ is involved in $f_\zeta(\tau)$. That is, $\mu_\zeta+\iota \in \Delta_{f_\zeta(\tau)}$, and we have $\{\mu_\zeta + \iota\colon\ \iota \in \Delta_\tau\} \subseteq \Delta_{f_\zeta(\tau)}$. On the other hand, if $\iota' \in \Delta_{f_\zeta(\tau)}$, then $\pi_{\iota'}$ appears in $\sum_{j=1}^{k} s_{\nu_j}\pi_{\mu_\zeta+\nu_j}$. That is, $\pi_{\iota'} = \pi_{\mu_\zeta+\nu_j}$ for some $j \in \{1, 2, \dots, k\}$, and so $\iota' = \mu_\zeta + \nu_j$. As $\nu_j \in \Delta_\tau$, we have $\Delta_{f_\zeta(\tau)} \subseteq \{\mu_\zeta + \iota\colon\ \iota \in \Delta_\tau\}$.

Assume that $\tau \in G_{i+1} \setminus G_i$, where $i \geqslant 0$, and that we have $\Delta_{f_\zeta(\lambda)} = \{\mu_\zeta + \iota\colon\ \iota \in \Delta_\lambda\}$ for all $\lambda \in G_i \setminus \{0\}$. As we have seen in (4.1), ζ can be written uniquely in the normal form

$$\zeta = \zeta_0 + \varepsilon_1 t_1 + \zeta_1 + \ldots + \varepsilon_k t_k + \zeta_k,$$

where $\zeta_0, \zeta_j \in G_i$, $t_j \in \mathcal{T}(G_i)$ and $\varepsilon_j = \pm 1$, $j = 1, 2, \dots k$ for some $k \geqslant 1$, and for each $j \in \{1, 2, \dots, k\}$, $t_j = t_{\alpha_j,\beta_j}$ for some $\alpha_j, \beta_j \in G_i \setminus \{0\}$. Then we have

$$\Delta_\tau = \Big(\bigcup_{j=0}^{k} \Delta_{\zeta_j}\Big) \cup \Big(\bigcup_{j=1}^{k} \Delta_{\alpha_j}\Big) \cup \Big(\bigcup_{j=1}^{k} \Delta_{\beta_j}\Big)$$

and

$$\Delta_{f_\zeta(\tau)} = \Big(\bigcup_{j=0}^{k} \Delta_{f_\zeta(\zeta_j)}\Big) \cup \Big(\bigcup_{j=1}^{k} \Delta_{f_\zeta(\alpha_j)}\Big) \cup \Big(\bigcup_{j=1}^{k} \Delta_{f_\zeta(\beta_j)}\Big).$$

Since $\Delta_{f_\zeta(\lambda)} = \{\mu_\zeta + \iota\colon\ \iota \in \Delta_\lambda\}$ for $\lambda \in \{\zeta_0, \dots, \zeta_k\} \cup \{\alpha_1, \dots, \alpha_k\} \cup \{\beta_1, \dots, \beta_k\}$ by the induction hypothesis, we see that $\Delta_{f_\zeta(\tau)} = \{\mu_\zeta + \iota\colon\ \iota \in \Delta_\tau\}$ as stated. □

Thus, if $\Delta_\tau = \{\widetilde{m}_0 \prec \widetilde{m}_1 \prec \ldots \prec \widetilde{m}_l\}$, then

$$\Delta_{f_\zeta(\tau)} = \{\mu_\zeta + \widetilde{m}_0 \prec \mu_\zeta + \widetilde{m}_1 \prec \ldots \prec \mu_\zeta + \widetilde{m}_l\}.$$

From this, it is clear that $\mu_{f_\zeta(\tau)} = \mu_\zeta + \widetilde{m}_l = \mu_\zeta + \mu_\tau$. Now, for $\iota \succ 0$ we have

$$(f_\zeta \circ f_\tau)(\pi_\iota) = f_\zeta(f_\tau(\pi_\iota)) = f_\zeta(\pi_{\mu_\tau+\iota}) = \pi_{\mu_\zeta+\mu_\tau+\iota} = \pi_{\mu_{f_\zeta(\tau)}+\iota} = f_{f_\zeta(\tau)}(\pi_\iota).$$

Also, we have

$$(f_\zeta \circ f_\tau)(\pi_0) = f_\zeta(f_\tau(\pi_0)) = f_\zeta(\tau) = f_{f_\zeta(\tau)}(\pi_0).$$

Hence, $f_\zeta \circ f_\tau = f_{f_\zeta(\tau)}$. It follows from Theorem 2.1 that we can use f to define a zero-symmetric nearring N on G^*. Moreover, with $f_\gamma(\pi_0) = \gamma$ for all $\gamma \in G^*$, N is a nearring with π_0 as its identity by Theorem 2.2.

Remark 4.3. Note that we can obtain a simple group G^* which is of prime exponent $p > 2$ (and a zero-symmetric nearring with identity) if we start with $G_0 = F/N(pF)$, where F is a free group of infinite rank and $N(pF)$ is the normal subgroup of F generated by pF, and for each i, take $G_i = \widetilde{G}_i/N(p\widetilde{G}_i)$ just like we have done in the first construction.

5. The symmetry group on the natural numbers

It is known that the symmetry group S_n on n symbols, $n \geqslant 3$, does not support a zero-symmetric nearring with identity, see [3], Theorem 4. We consider now the group $G = \mathrm{Sym}\,(\mathbb{N})$, the symmetry group on the set of natural numbers, and we will show that there cannot be any nearring with identity having G as the additive group. Again, Clay's construction will be used, and so we need some information on the endomorphisms of G.

It was shown by Schreier and Ulam (see [14]) that there are only two nontrivial proper normal subgroups in G, namely, the subgroup S of the finitary permutations (permutations which move only finitely many elements), and the subgroup A of the even finitary permutations. Also, they showed in [15] that all automorphisms of G are inner, cf. [17], 11.4.6.

There are many monomorphisms on G which are not automorphisms. We give some examples here.

(1) Let Σ be an infinite proper subset of $\mathbb{N}$ and $\sigma\colon \Sigma \to \mathbb{N}$ a bijection. Then $H = \mathrm{Sym}\,(\Sigma)$ and G are isomorphic groups. But H is also a subgroup of G. Thus, an isomorphism $f\colon G \to H \subsetneqq G$ gives a monomorphism on G which is not surjective.

(2) Let $\{p_1, p_2, \ldots\}$ be the set of all prime numbers. For each $n \in \mathbb{N}$, define $f(\sigma)(n)$, where $\sigma \in G$, to be 1 when $n = 1$, and $p_{\sigma(i_1)}^{\varepsilon_1} p_{\sigma(i_2)}^{\varepsilon_2} \ldots p_{\sigma(i_k)}^{\varepsilon_k}$ if $n = p_{i_1}^{\varepsilon_1} p_{i_2}^{\varepsilon_2} \ldots p_{i_k}^{\varepsilon_k}$ (with each $\varepsilon_i > 0$) is the unique prime factorization of n if $n > 1$. One sees that $f(\sigma\delta) = f(\sigma)f(\delta)$ for all $\sigma, \delta \in G$, i.e., f is an endomorphism on G. It is in fact a monomorphism: $f(\sigma)(n) = n$ if and only if $p_{\sigma(i)} = f(\sigma)(p_i) = p_i$ for all $i \in \mathbb{N}$; i.e., $\sigma = (1)$, the identity permutation on $\mathbb{N}$; since $f(\sigma)(1) = 1$ for all $\sigma \in G$, the transposition $(1, 2)$ is not in $\mathrm{Im}\,(f)$, and so f is not surjective.

Next let us show that there are no endomorphisms on G having S or A as their kernel. We will use the following result by Dixon, Neumann and Thomas.

Theorem 5.1 ([5], Theorem 1)**.** *If H is a subgroup of G with $[G : H] < 2^\omega$, then there is a finite subset $\Delta \subseteq \mathbb{N}$ such that $G_{(\Delta)} \leqslant H \leqslant G_{\{\Delta\}}$.*

Here

$$G_{(\Delta)} = \{f \in G\colon\ f(n) = n\ \forall\, n \in \Delta\} \quad \text{and} \quad G_{\{\Delta\}} = \{f \in G\colon\ f(\Delta) = \Delta\}.$$

Also, we have

$$G_{\{\Delta\}} = G_{(\Delta)} \cdot \mathrm{Sym}\,(\Delta),$$

where $\mathrm{Sym}\,(\Delta)$ is the permutation group on Δ. Note that the elements in $G_{(\Delta)}$ commute with the elements in $\mathrm{Sym}\,(\Delta)$. Hence, every element $\sigma \in G_{\{\Delta\}}$ can be written uniquely as a product $\sigma_1\sigma_2$ with $\sigma_1 \in G_{(\Delta)}$ and $\sigma_2 \in \mathrm{Sym}\,(\Delta)$.

Lemma 5.2. *If $f\colon\ G \to G$ is an endomorphism with nontrivial kernel, then f is the trivial endomorphism.*

P r o o f. Assume that $f\colon\ G \to G$ is a nontrivial endomorphism with $\ker(f) \in \{S, A\}$. Then the image $\mathrm{Im}\,(f)$ is a subgroup of G and is isomorphic to G/S or G/A. Since G is uncountable and both S and A are countable, it follows that $\mathrm{Im}\,(f)$ is an uncountable subgroup of G with index $[G\colon\ \mathrm{Im}\,(f)] = \omega < 2^{\omega}$. By Theorem 5.1, we have that $G_{(\Delta)} \subseteq \mathrm{Im}\,(f) \subseteq G_{\{\Delta\}}$ for a finite subset Δ of $\mathbb{N}$. We will derive a contradiction.

Notice that $\mathrm{Im}\,(f) \neq G_{(\Delta)}$. Otherwise, from the fact that Δ is finite, $G_{(\Delta)}$ is isomorphic to G. Then there is an isomorphism $h\colon\ G_{(\Delta)} \to G$, and so $h \circ f$ is an automorphism of G. Consequently, f is a one-one map. But this is not the case as $\ker(f) = S$ or A by our assumption.

Define $g\colon\ G_{\{\Delta\}} \to \mathrm{Sym}\,(\Delta)$ by $g(\sigma) = \sigma_2$ if $\sigma \in G_{\{\Delta\}}$ is expressed as the product $\sigma_1\sigma_2$, where $\sigma_1 \in G_{(\Delta)}$ and $\sigma_2 \in \mathrm{Sym}\,(\Delta)$. This map is clearly an epimorphism. Thus, we have a group homomorphism $g \circ f\colon\ G \to G$ with $\mathrm{Im}\,(g \circ f)$ contained in $\mathrm{Sym}\,(\Delta)$. Since $\mathrm{Im}\,(f) \neq G_{(\Delta)}$, we have that $g \circ f$ is nontrivial. With $\ker f \subseteq \ker(g \circ f)$, we see that $\ker(g \circ f) = A$ or S. But then $\mathrm{Im}\,(g \circ f)$ is uncountable and is contained in $\mathrm{Sym}\,(\Delta)$. This is a contradiction. □

We are ready to state and prove the following theorem.

Theorem 5.3. *The group* $\mathrm{Sym}\,(\mathbb{N})$ *does not support a zero-symmetric nearring with identity.*

P r o o f. For the group $G = \mathrm{Sym}\,(\mathbb{N})$ to support a zero-symmetric nearring with identity, it is required that there is a map $\varphi\colon\ G \to \mathrm{End}\,(G); a \mapsto \varphi_a$ with a specific element $e \in G$ such that $\varphi_a(e) = a$ for all $a \in G$. Since G has no nontrivial endomorphism which is not a monomorphism, we have that $a = \varphi_a(e)$ and e are of the same order as long as a is not the zero element of G (i.e., $a \neq (1)$). This is certainly not the case. Hence, G cannot support a zero-symmetric nearring with identity. □

Acknowledgement. We thank the reviewer for taking the time to review our manuscript, carefully reading it, pointing out errors in the original version, and providing insightful comments and suggestions that have improved the quality of the manuscript.

References

[1] *G. Baumslag*: Topics in Combinatorial Group Theory. Lectures in Mathematics, ETH Zürich. Birkhäuser, Basel, 1993. zbl MR doi
[2] *J. R. Clay*: The near-rings on groups of low order. Math. Z. *104* (1968), 364–371. zbl MR doi
[3] *J. R. Clay, J. J. Malone, Jr.*: The near-rings with identities on certain finite groups. Math. Scand. *19* (1966), 146–150. zbl MR doi
[4] *L. E. Dickson*: Theory of linear groups in an arbitrary field. Trans. Am. Math. Soc. *2* (1901), 363–394. zbl MR doi
[5] *J. D. Dixon, P. M. Neumann, S. Thomas*: Subgroups of small index in infinite symmetric groups. Bull. Lond. Math. Soc. *18* (1986), 580–586. zbl MR doi
[6] *A. G. Hamilton*: Numbers, Sets and Axioms: The Apparatus of Mathematics. Cambridge University Press, Cambridge, 1982. zbl MR doi
[7] *G. Higman, B. H. Neumann, H. Neumann*: Embedding theorems for groups. J. Lond. Math. Soc. *24* (1949), 247–254. zbl MR doi
[8] *K. Kaarli*: On ideal transitivity in near-rings. Contributions to General Algebra 8. Höder-Pichler-Tempsky, Vienna, 1992, pp. 81–89. zbl MR
[9] *R. C. Lyndon, P. E. Shupp*: Combinatorial Group Theory. Ergebnisse der Mathematik und ihrer Grenzgebiete 89. Springer, Berlin, 1977. zbl MR doi
[10] *A. Y. Ol'shanskii*: An infinite simple Noetherian group without torsion. Math. USSR, Izv. *15* (1980), 531–588; Translation from Izv. Akad. Nauk SSSR, Ser. Mat. *43* (1979), 1328–1393. zbl MR doi
[11] *A. Y. Ol'shanskii*: Groups of bounded period with subgroups of prime order. Algebra Logic *21* (1983), 369–418; Translation from Algebra Logika *21* (1982), 553–618. zbl MR doi
[12] *G. Pilz*: Near-Rings: The Theory and Its Applications. North-Holland Mathematics Studies 23. North-Holland, Amsterdam, 1977. zbl MR doi
[13] *J. J. Rotman*: An Introduction to the Theory of Groups. Graduate Texts in Mathematics 148. Springer, Berlin, 1995. zbl MR doi
[14] *J. Schreier, S. Ulam*: Über die Permutationsgruppe der natürlichen Zahlenfolge. Stud. Math. *4* (1933), 134–141. (In German.) zbl doi
[15] *J. Schreier, S. Ulam*: Über die Automorphismen der Permutationsgruppe der natürlichen Zahlenfolge. Fundam. Math. *28* (1937), 258–260. (In German.) zbl doi
[16] *E. A. Scott*: A tour around finitely presented infinite simple groups. Algorithms and Classification in Combinatorial Group Theory. Springer, New York, 1992, pp. 83–119. zbl MR doi
[17] *W. R. Scott*: Group Theory. Dover, New York 1987. zbl MR

Authors' addresses: Wen-Fong Ke (correspponding author), Department of Mathematics, National Cheng Kung University, 1st, Dasyue Rd, East District, Tainan 701, Taiwan, e-mail: wfke@mail.ncku.edu.tw; Johannes H. Meyer, Department of Mathematics and Applied Mathematics, University of the Free State, PO Box 339, Bloemfontein, 9300, South Africa, e-mail: meyerjh@ufs.ac.za; Günter F. Pilz, Gerhard Wendt, Department of Algebra, Johannes Kepler Universität Linz, Altenberger Strasse 69, 4040 Linz, Austria, e-mail: guenter.pilz@jku.at, gerhard.wendt@gmx.at.