Article Accepted by Journal of Symbolic Computation

Algorithms for Finite Near-rings and their N-Groups*

Franz Binder† and Peter Mayr‡

Department of Algebra, Johannes Kepler University, A-4040 Linz, Austria

Abstract

In this note, we present algorithms to deal with finite near-rings, the appropriate algebraic structure to study non-linear functions on finite groups. Just as rings (of matrices) operate on vector spaces, near-rings operate on groups. In our approach, we have developed efficient algorithms for a variety of problems that involve the structure of the operation of a near-ring on a group. From this, we retrieve information about the near-ring itself.

1. Introduction

Convention 1.1: *All algebraic structures in this paper are finite.*

Important examples of *rings* are matrix-rings; these arise as linear mappings on vector spaces. In the present note, we compute with algebraic structures appropriate for dealing with non-linear mappings, namely *near-rings* [Pilz, 1983, Meldrum, 1985, Clay, 1992].

Definition 1.1: A set N together with two binary operations $+$ and $\cdot$ is called a *(right) near-ring* if

1. $(N, +)$ is a (not necessarily abelian) group.
2. $(N, \cdot)$ is a semigroup.
3. $\cdot$ is right distributive over $+$, i.e.,
   $\forall\, a, b, c \in N\colon (a + b) \cdot c = a \cdot c + b \cdot c.$

*This work has been supported by the Austrian National Science Foundation (Fonds zur Förderung der wissenschaftlichen Forschung) under Grant P12911-INF. More details are available at `www.algebra.uni-linz.ac.at/sonata/`.

†`mailto:Franz.Binder@algebra.uni-linz.ac.at`

‡`mailto:Peter.Mayr@algebra.uni-linz.ac.at`

The equality $f0 = 0$ for $f \in N$ is not implied by these axioms.

DEFINITION 1.2: The *zero-symmetric part* of a near-ring N is usually denoted by N_0 and defined by $N_0 := \{f \in N \mid f0 = 0\}$. Also, both the elements of N_0 and any near-ring that fulfills $N = N_0$ are called *zero-symmetric*. A near-ring with commutative addition is called *abelian*.

Note that the missing left distributive law, $a(b + c) = ab + ac$, has to do with linearity if a is considered as a function. In fact, functions on groups are the typical examples of near-rings. Let Γ be a group, and let $\mathrm{M}(\Gamma)$ be the set of all mappings from Γ into Γ (we will call them *transformations*). We define $+$ and $\cdot$ on $\mathrm{M}(\Gamma)$ by $(f + g)(\gamma) := f(\gamma) + g(\gamma)$ and $(f \cdot g)(\gamma) := f(g(\gamma))$. Then $(\mathrm{M}(\Gamma), +, \cdot)$ is a near-ring, the *full transformation near-ring.* For the appropriate algebraic sub-structures, the *sub-near-rings,* we then write $N \leq \mathrm{M}(\Gamma)$ and call them *transformation near-rings.* In fact, every near-ring can be represented as a transformation near-ring on some group Γ. But we are interested mainly in the natural case, where Γ is small, and N is (very) big, but generated by a small number of generators. If *small* means 100, then N can have up to 100^{100} elements, which is almost infinite ([Scott, 1979] contains many impressive examples). In particular, *big* means that the elements of N cannot be enumerated in practice, whereas *small* means that it is no problem to loop over all elements of Γ, or over all generators. So our main concern is to compute as much as we can with generators only. We note that a corresponding problem in group theory is solved via Sim's stabilizing chains [Sims, 1970]. Though we could not develop such a powerful tool for near-ring theory, we can give solutions for many important special cases as well as completely satisfactory solutions to a variety of related problems.

In contrast to ring theory, no systematic attempt of an algorithmic treatment of near-ring theory seems to have been done so far, apart from Binder et al. [2000] and a project funded by the Austrian Science Fonds, which resulted in the development of the package SONATA based on GAP 4 [Aichinger et al., 2000]. This article contains some of the theory behind the development of that package and extends Binder et al. [2000] by a more complete and better structured set of algorithms for N-groups, including the efficient computation of commutators. All these methods now also work for N_0-subgroups, where N (not N_0) is given by generators. We consider centralizer near-rings, in particular those with a group of fixed-point-free automorphisms. A straightforward, but very effective method to compute N-endomorphisms allows us to significantly generalize the previous solution to the realizability problem, using a more general interpolation algorithm together with more precise density results.

2. N-Groups

Just in the same way as R-modules or vector spaces are used in ring theory, N-groups are used in near-ring theory.

Definition 2.1: Let N be a near-ring. An *N-group* is an additive group Γ together with an *operation of N on* Γ (i.e., a mapping $N \times \Gamma \to \Gamma$), denoted by juxtaposition, such that for all $n, m \in N$ and $\gamma \in \Gamma$,

$$(n+m)\gamma = n\gamma + m\gamma,$$
$$(nm)\gamma = n(m\gamma).$$

We say that N operates *faithfully on* Γ (or that Γ is a *faithful* N-group) if $n\gamma = 0$ for all $\gamma \in \Gamma$ is true only if $n = 0$.

Remark 2.1: Equivalently, an N-group can be described by a homomorphism from the near-ring N into $\mathrm{M}(\Gamma)$, which is an embedding iff the operation is faithful.

As for R-modules, the actual operation is always to be understood from the context.

N-groups are always written additively, even if they are not abelian.

For each fixed near-ring N, the N-groups form a variety (just as the near-rings themselves). General definitions are obtained from the corresponding ones from group theory by prefixing them with the near-ring involved. In particular:

Definition 2.2: Let N be a near-ring.

1. A group-homomorphism α between two N-groups Γ_1 and Γ_2 is called an *N-homomorphism* if for all $n \in N$ and for all $\gamma \in \Gamma_1$,

$$\alpha(n\gamma) = n(\alpha\gamma).$$

2. A subgroup H of an N-group Γ (we write $H \leq \Gamma$ for this) is called an *N-subgroup* (written as $H \leq_N \Gamma$) if it is closed under the operation of N, i.e., if $n\gamma \in H$ for all $n \in N$, $\gamma \in H$.
3. If H is the kernel of an N-homomorphism, then it is called an *N-normal subgroup* and we write $H \trianglelefteq_N \Gamma$.

Using the term "N-normal" for the kernels of homomorphisms (as we do here) seems to be quite natural but is not standard in near-ring theory. The notions "N-ideal" or sometimes "N-module" are used instead by most authors.

Example 2.1:

1. If $N \leq \mathrm{M}(\Gamma)$, then Γ is a faithful N-group via function application as operation (or via the identity as the homomorphism into $\mathrm{M}(\Gamma)$).
2. The additive group $(N, +)$ of a near-ring $(N, +, \cdot)$ is an N-group via the near-ring multiplication.

3. N-Subgroups

For the following, we introduce some useful notations:

DEFINITION 3.1: Let Γ be an N-group, $H \leq \Gamma$, $E \subseteq N$, and $F \subseteq \Gamma$. Then

1. $\langle E \rangle$ denotes the sub-near-ring generated by E;
2. $\langle F \rangle$ denotes the subgroup generated by F;
3. $\langle E^+ \rangle$ denotes the (additive) subgroup generated by E additively;
4. $EF := \{ a\gamma \mid a \in E, \gamma \in F \}$.
5. H is called *E-invariant* if $EH \subseteq H$;
6. $\langle F \rangle_E$ denotes the smallest E-invariant subgroup of Γ containing F; in particular, $\langle F \rangle_N$ denotes the N-subgroup generated by F;

Note that these definitions apply e.g. when Γ is $(N, +)$. We also use the usual simplifications for singleton sets, e.g., $E\gamma := E\{\gamma\}$.

The following is immediate:

PROPOSITION 3.1: *Let E be a subset of a near-ring N. Then $\langle E \rangle = \langle E^+ \rangle_E$.*

This means that we can use induction proofs over N: to prove a statement for all $f \in N$, we just show that it is true for all generators and that it is closed under subtraction and under multiplications by generators from the left. This technique is demonstrated by the (easy) proof below.

PROPOSITION 3.2: *Let Γ be an N-group, $N = \langle E \rangle$, $F \subseteq \Gamma$, and $\gamma \in \Gamma$. Then:*

1. $\langle F \rangle_N = \langle F \rangle_E$;
2. $N\gamma = \langle E\gamma \rangle_E$;
3. $NF = \bigcup_{\eta \in F} N\eta$.

Proof: For the first part, we have to show that $\langle F \rangle_E$ is N-invariant, i.e., that $f(\langle F \rangle_E) \subseteq \langle F \rangle_E$ for all $f \in N$. We use induction on f.

Base case: For $f \in E$, the statement is true by definition.

Subtraction case: Assume that it is true for f and g in E, and let $\eta \in \langle F \rangle_E$. Then, $(-f+g)\eta = -f\eta + g\eta \in \langle F \rangle_E$, by induction and because $\langle F \rangle_E$ is a group.

Multiplication case: Finally, assume that the statement is true for $f \in N$ and take $e \in E$, $\eta \in \langle F \rangle_E$. Then,

$$(ef)\eta = e(\underbrace{f\eta}_{\in \langle F \rangle_E}) \in \langle F \rangle_E,$$

by induction and because $\langle F \rangle_E$ is E-invariant.

The other parts are immediate. □

Algorithm 1 Computing Orbits

Let Γ be an N-group.
Require: $N = \langle E \rangle$, $F \subseteq \Gamma$.
Ensure: $H = \langle F \rangle_E$

```
H := ⟨F⟩
while EH ⊈ H do
  H := ⟨H ∪ EH⟩
end while
```

These results lead to easy, but essential, algorithms.

Corollary 3.1: *Under the same hypotheses, $\langle F \rangle_N$, $N\gamma$, $\{N\eta \mid \eta \in \Gamma\}$, and NF can be computed within $\mathrm{O}(|E|\,|\Gamma|)$ operations.*

Proof: From the proposition, the method to compute $\langle F \rangle_E$ is obvious and made explicit in Algorithm 1. The computation of $N\gamma$ is just a special case of this. And NF is just the union of the $N\eta$'s. To obtain the complexity bound, note first that all of the necessary group-oriented operations (i.e., generating subgroups) can be done within the bound and need not be counted. What essentially remains to be done is to compute all products $e\eta$ for $e \in E$ and for each η in the result, which is at most Γ. Thus, with appropriate storage of the intermediate results, we still do not exceed the bound. □

Remark 3.1: If N is a near-ring with identity, then $NF = \langle F \rangle_N$.

Remark 3.2: If we add some obvious book-keeping to Algorithm 1, we can compute more information. For example, for each $\eta \in N\gamma$, we then can determine an appropriate $f \in N$ such that $\eta = f\gamma$. We could even store how f is constructed from the generators in E.

4. Difference Operator

Computations in spaces of continuous functions are usually performed using linearization via the differential operator. In the discrete case, we can do something similar with a difference operator. We define it in the following way.

Definition 4.1: Let N be a near-ring and Γ an N-group. For $f \in N$ and $x, a \in \Gamma$, we define

$$\Delta f x a := -fx + f(x + a),$$

and call it the *difference of f at x in direction a.*

Thus the operator Δ is understood to map an element of N into a function that maps elements of Γ into elements of $\mathrm{M}(\Gamma)$. In particular, $\Delta f x \in \mathrm{M}(\Gamma)$. This operator is also useful in the case $\Gamma = N$.

PROPOSITION 4.1: *With the notation of the definition we have*

$$\Delta fx(a+b) = \Delta fxa + \Delta f(x+a)b, \qquad \textit{(quasi-linearity)} \tag{1}$$
$$\Delta f(x+a)b = -\Delta fxa + \Delta fx(a+b). \qquad \textit{(translation rule)} \tag{2}$$

Proof: Of course, both equations are equivalent. We show (2):

$$\begin{aligned} -\Delta fxa + \Delta fx(a+b) &= -f(x+a) + fx - fx + f(x+a+b) \\ &= \Delta f(x+a)b. \end{aligned}$$ □

PROPOSITION 4.2: *Continuing the above notation and with $g \in N$, we have*

$$\begin{aligned} \Delta(f+g)xa &= -gx + \Delta fxa + gx + \Delta gxa, \\ \Delta(-f)xa &= -(fx + \Delta fxa - fx). \end{aligned}$$

Proof: We show the second equation: $\Delta(-f)xa = -(-f)x + (-f)(x+a) = fx - f(x+a) = -(f(x+a) - fx) = -(fx - fx + f(x+a) - fx) = -(fx + \Delta fxa - fx)$. □

Thus, in general, Δ is not linear in the first argument unless Γ is abelian. When considering normal subgroups, these annoying conjugations are absorbed.

Of course, the definition of the difference operator should mirror that of the differential operator for functions on linear spaces. In contrast to the latter, the difference at a point, Δfx, need not be a linear function. Equation (1), however, suggests that it is not too far away. In particular, if we know the difference in directions generating Γ (as a group), then we know it in any direction. This is similar to partial derivatives. On the other hand, the equivalent equation (2) shows that the difference at 0, $\Delta f0$, already determines the difference at any point Δfx. This is far away from the idea that the difference at a point should describe a function locally.

PROPOSITION 4.3: *The operator Δ fulfills the following chain rule:*

$$\Delta(fg)xa = \Delta f(gx)\Delta gxa. \tag{3}$$

Proof: $\Delta(fg)xa = -fgx + fg(x+a) = -fgx + f(gx + \Delta gxa) = \Delta f(gx)\Delta gxa$. □

The difference operator can be iterated in the following way. The definition is motivated by the formalism $\Delta^{n+1}f = \Delta(\Delta^n f)$.

DEFINITION 4.2: Let Γ be an N-group, $f \in N$, $x, a, b \in \Gamma$, $\mathbf{a} \in \Gamma^n$. Then we define the higher order difference operators as

$$\Delta^{n+1}fxb\mathbf{a} := -\Delta^n fx\mathbf{a} + \Delta^n f(x+b)\mathbf{a}.$$

In particular,

$$\begin{aligned}\Delta^2 fxba &= \Delta(\Delta f)xba \\ &= -\Delta fxa + \Delta f(x+b)a \\ &= -f(x+a) + fx - f(x+b) + f(x+b+a).\end{aligned}$$

Remark 4.1: If Γ is abelian, then Δ^n is symmetric in the last n arguments.

Proposition 4.4: *Δ^2 fulfills the following chain rule:*

$$\Delta^2(fg)xba = \Delta^2 f(gx)(\Delta gxa)(\Delta gxb) + \Delta f\,(g(x+b) + \Delta gxa)\,\Delta^2 gxab.$$

Proof: We compute

$$\begin{aligned}\Delta^2(fg)xba &= -\Delta(fg)xa + \Delta(fg)(x+b)a \\ &= -\Delta f(gx)\,(\Delta gxa) + \Delta f\,(g(x+b))\,(\Delta gxa) \\ &\qquad - \Delta f\,(g(x+b))\,(\Delta gxa) + \Delta f\,(g(x+b))\,(\Delta g(x+b)a) \\ &= \Delta^2 f(gx)(\Delta gxb)(\Delta gxa) + \Delta f\,(g(x+b) + \Delta gxa)\,(\Delta^2 gxba).\end{aligned}$$

The last stage has used the translation rule (2) with $x \mapsto g(x+b)$ and $a \mapsto \Delta gxa$.
□

Definition 4.3: Let $E \subseteq N$ and $A, F \subseteq \Gamma$.

1. By $\Delta EAF := \{\, \Delta ea\gamma \mid e \in E, a \in A, \gamma \in F \,\}$, the Δ-operator can be applied to sets, and we use the obvious modifications for singleton sets.
2. We say that F is *ΔEA-invariant* iff $\Delta EAF \subseteq F$;
3. $(F)_{\Delta EA}$ denotes the smallest ΔEA-invariant normal subgroup containing F.

5. N-Normal Subgroups

N-normal subgroups, are usually characterized as follows.

Proposition 5.1: *Let Γ be an N-group and H a subgroup of Γ. Then $H \trianglelefteq_N \Gamma$ iff $H \trianglelefteq \Gamma$ and*

$$-f\gamma + f(\gamma+\eta) \in H \quad \textit{for all } \eta \in H,\ f \in N, \textit{ and } \gamma \in \Gamma.$$

Note that $-f\gamma + f(\gamma+\eta) = \Delta f\gamma\eta$. In fact, we can express this as

Corollary 5.1: *A normal subgroup of Γ is N-normal iff it is $\Delta N\Gamma$-invariant.*

N-normal subgroups of N^+ (i.e., N considered as an N-group) are called *left ideals.*

Corollary 5.2: *A left ideal of a near-ring N is a ΔNN-invariant normal subgroup.*

An efficient method to compute N-normal subgroups is provided by a stronger result.

PROPOSITION 5.2: *Let Γ be an N-group with $N = \langle E \rangle$. A normal subgroup is N-normal iff it is $\Delta E\Gamma$-invariant.*

Proof: Let H be a $\Delta E\Gamma$-invariant normal subgroup. To show that $\Delta f\Gamma H \subseteq H$ for all $f \in N$, we use induction on f. The base case holds. For the subtraction case, consider $\Delta(-f+g)x\gamma = -gx - (fx + \Delta fx\gamma - fx) + gx + \Delta gx\gamma \in H$, using Proposition 4.2 and by normality. And for the multiplication case, consider $e \in E$ and $f \in N$ fulfilling the statement. Then, using the chain rule (3), we have $\Delta(ef)x\gamma = \Delta e(fx)\Delta fx\gamma \in H$, because $\Delta fx\gamma \in H$. □

COROLLARY 5.3: *The N-normal subgroup generated by a set I can be computed within $\mathrm{O}(|E|\,|\Gamma|\,k)$ operations, where k is a bound for the number of generators necessary to generate any normal subgroup of Γ.*

Proof: By Proposition 5.2, we need to compute $(I)_{\Delta E\Gamma}$. The straightforward algorithm is similar to Algorithm 1. This leads to the complexity bound $\mathrm{O}(|E|\,|\Gamma|^2)$. To improve it, note that we can use quasi-linearity (1). □

6. Commutators

In the previous sections, we have developed efficient algorithms to compute the lattice of N-subgroups as well as the lattice of N-normal subgroups, i.e., the congruence lattice of an N group. In addition to this, we would like to be able to compute the commutator operation on the congruences, in the sense of Universal Algebra. We will use the notation $[X,Y]_N$ to distinguish the N-commutator (i.e., that with respect to the variety of N-groups) from the usual group commutator $[X,Y]$. Using the definition of Gumm [1980], we obtain the following adaptation for N-groups.

DEFINITION 6.1: Let Γ be an N-group of a near-ring N and $X \trianglelefteq_N \Gamma$, $Y \trianglelefteq_N \Gamma$. With $\xi := \{(a,\, a+x) \mid a \in \Gamma, x \in X\}$, we define

$$\delta_X^Y := (\{\,(y,y) \mid y \in Y\,\})_{\Delta N\xi};$$
$$[X,Y]_N := \{\,z \mid (0,z) \in \delta_X^Y\,\}.$$

Then $[X,Y]_N \trianglelefteq_N \Gamma$, and it is called the *$N$-commutator of X and Y.*

Remember that the congruence associated with a normal subgroup X is given as ξ above and that any N-congruence is an N-subgroup of $\Gamma \times \Gamma$.

THEOREM 6.1: *Let N be a transformation near-ring generated by E, and let X and Y be N-normal subgroups of the N-group Γ, generated additively by I and J, respectively. Then the N-commutator of X and Y is the N-normal subgroup of Γ generated by $[X,Y]$ and $\Delta^2 E\Gamma IJ$.*

Proof: Let ξ be as in Definition 6.1 and $Z := ([X,Y] \cup \Delta^2 E\Gamma XY)_{\Delta N\xi}$.

At first, we show that the commutator $[X,Y]_N$ indeed contains all the generators of Z. Note that $\{z \mid (0,z) \in \delta_X^Y\} = \{z \mid (y,\, y+z) \in \delta_X^Y\}$, for any $y \in Y$, as δ_X^Y contains all pairs of the form (y,y). Because $-(0,x)+(y,y)+(0,x) \in \delta_X^Y$, we have $-y-x+y+x \in [X,Y]_N$ for all $x \in X$, $y \in Y$. Similarly, by $\Delta e(a,\, a+x)(y,y) = (\Delta eay, \Delta e(a+x)y) \in \delta_X^Y$, we have $-\Delta eay + \Delta e(a+x)y = \Delta^2 eaxy \in [X,Y]_N$ for all $e \in N$, $a \in \Gamma$, $x \in X$, $y \in Y$. Thus $Z \subseteq [X,Y]_N$.

Conversely, to prove $Z \supseteq [X,Y]_N$, define $\delta := \{\, (y,\, y+z) \mid y \in Y,\, z \in Z \,\}$. Below we show that δ is N-normal in ξ. Because δ contains the generators of δ_X^Y, this means that $\delta \supseteq \delta_X^Y$ and, consequently, that $Z = \{z \mid (0,z) \in \delta\} \supseteq \{z \mid (0,z) \in \delta_X^Y\} = [X,Y]_N$.

For the following, let $y_1, y_2, y \in Y$, $z_1, z_2, z \in Z$, $x \in X$, and $a \in \Gamma$.

δ is a subgroup: $(y_1,\, y_1+z_1) - (y_2,\, y_2+z_2) = (y_1-y_2,\; y_1+z_1-z_2-y_2)$. Clearly, $y_1 - y_2 \in Y$, and $y_2 - y_1 + y_1 + z_1 - z_2 - y_2 = y_2 + (z_1 - z_2) - y_2 \in Z$, as Z is normal.

δ is normal: $(a,\, a+x) + (y,\, y+z) - (a,\, a+x) = (a+y-a,\; a+x+y+z-x-a)$ should be in δ. Clearly, $a+y-a \in Y$, and, since Z is normal $-(a+y-a) + (a+x+y+z-x-a) = a \underbrace{-y+x+y-x}_{\in Z} + \underbrace{x+z-x}_{\in Z} - a \in Z$.

δ is $\Delta E\xi$-invariant: $\Delta e(a,\, a+x)(y,\, y+z) = (\,\Delta eay,\; \Delta e(a+x)(y+z)\,)$ should be in δ. Clearly, $\Delta eay \in Y$, and

$$\begin{aligned} -\Delta eay + \Delta e(a+x)(y+z) &= -\Delta eay + \Delta e(a+x)y + \Delta e(a+x+y)z \\ &= \underbrace{\Delta^2 eaxy}_{\in Z} + \underbrace{\Delta e(a+x+y)z}_{\in Z} \in Z. \end{aligned}$$

The validity of the restriction to the additive generators of the ideals again follows from quasilinearity. □

Corollary 6.1: *N-commutators of N-normal subgroups of N-groups can be computed within* $\mathrm{O}(|E|\,|\Gamma|\,k^2)$ *operations, with k as in Corollary 5.3.*

7. Left Ideals and N_0-Subgroups

Our algorithms for computing with an N-group Γ (N given by a small set E of generators) depend on the efficient computation of orbits (e.g. $N\gamma$). We show that essentially the same methods work if, instead of N, we encounter a left ideal given by (left ideal) generators.

Proposition 7.1: *Let N be a near-ring, Γ an N-group, and L a left ideal of N. If $\gamma \in \Gamma$ and I is a set of (left ideal) generators of L, then*

$$L\gamma = (I\gamma)_{\Delta E(N\gamma)}.$$

Proof: Let $H := (I\gamma)_{\Delta E(N\gamma)}$. For all $f \in L$ and $h \in H$, we have to show that $f\gamma \in H$. We do this by induction on f using $L = (I)_{\Delta EN}$. The base case is trivial, so are the difference case and the conjugation case. For the Δ-case, consider $e \in E$, $n \in N$, and $f \in L$ for which the statement is true. Then

$$(\Delta enf)\gamma = \Delta e(\underbrace{n\gamma}_{\in N\gamma})(\underbrace{f\gamma}_{\in H}) \in H.$$

□

Corollary 7.1: *$L\gamma$ can be computed within $\mathrm{O}(|E|\,|\Gamma|\,k)$ operations, with k as in Corollary 5.3.*

For an arbitrary subset E of N, we define

$$E_0 = \{-f0 + f \mid f \in E\}.$$

It is immediate that this notation just extends that for the zero-symmetric part of a near-ring. Unfortunately, $N = \langle E\rangle$ does not imply $N_0 = \langle E_0\rangle$. In fact, we are not aware of any general efficient method to compute near-ring generators of N_0 from those of N.

Nevertheless, N_0 is a left ideal of N and E_0 generates N_0 as a left ideal.

Proposition 7.2: *Let N be a near-ring generated by a set $\langle E\rangle$. Then*

$$N_0 = (E_0)_{\Delta NN} = (E_0)_{\Delta EN} = (E_0)_{\Delta E(N0)}.$$

Proof: That N_0 is a left ideal is well known and immediately checked. Let $M := (E_0)_{\Delta EN0}$. It remains to prove $N_0 \subseteq M$. Note that $N_0 = \{-f0 + f \mid f \in N\}$. Thus, we have to show that $-f0 + f \in M$, for all $f \in N$, which we prove by induction on f. The base case, $f \in E$, is trivial. For the difference case, let $f, g \in N$ such that $-f0 + f \in M$ and $-g0 + g \in M$. We have to show that $-(f-g)0 + (f-g) \in M$. Using normality,

$$\begin{aligned}
-(f-g)0 + (f-g) &= g0 - f0 + f - g \\
&= g0 - f0 + f - g0 + g0 - g + g0 - g0 \\
&= \underbrace{g0 \underbrace{-f0 + f}_{\in M} - g0}_{\in M} + \underbrace{g0 - (\underbrace{-g0 + g}_{\in M}) - g0}_{\in M} \in M.
\end{aligned}$$

For the multiplication case, we need to show that $-ef0 + ef \in M$ for $e \in E$ under the assumption that $-f0 + f \in M$. We apply the $\Delta E(N0)$-invariance:

$$\begin{aligned}
-ef0 + ef &= -ef0 + e(f0 - f0 + f) \\
&= \Delta e(f0)\underbrace{(-f0 + f)}_{\in M} \in M.
\end{aligned}$$

□

Corollary 7.2: *Let Γ be an N-group and $\gamma \in \Gamma$. If N is generated by E, then $N_0\gamma = (E_0\gamma)_{\Delta E(N\gamma)}$.*

Proof: Just combine the previous results. □

8. Centralizer Near-rings

DEFINITION 8.1: Let Γ be a group and S be a semigroup of endomorphisms of Γ. Then the sub-near-ring of $\mathrm{M}(\Gamma)$

$$\mathrm{M}_S(\Gamma) := \{f \in \mathrm{M}(\Gamma) \mid fs = sf \text{ for all } s \in S\}$$

is called a *centralizer near-ring.*

Particular examples are $\mathrm{M}(\Gamma)$ (for $S = \varnothing$) and $\mathrm{M}_0(\Gamma)$ (for $S = \{0\}$). In this context, we use $S^0 := S \cup \{0\}$.

For a centralizer near-ring, it is easy to decide whether it contains a given $f \in \mathrm{M}(\Gamma)$. This is in contrast to the case of transformation near-rings. Dually, it is hard to compute non-trivial elements of an arbitrary centralizer near-ring (easy for a transformation near-ring).

An automorphism α of Γ is called *fixed-point-free* if for all $\gamma \in \Gamma, \gamma \neq 0$, the equation $\alpha(\gamma) = \gamma$ implies $\alpha = \mathrm{id}$. If $\alpha \neq \mathrm{id}$ is fixed-point-free on Γ, then $\alpha f = f\alpha$ for $f \in \mathrm{M}(\Gamma)$ implies that $f(0) = 0$ since $\alpha f(0) = f\alpha(0) = f(0)$. For D a group of fixed-point-free automorphisms and $|D| > 1$, we have that $\mathrm{M}_D(\Gamma) = \mathrm{M}_{D^0}(\Gamma)$. These centralizer near-rings are essential for the structure theory of near-rings This is a consequence of the well-known density theorems. As an example, we cite a simplified version of Theorem 4.52 in Pilz [1983].

THEOREM 8.1: *Let N be a zero-symmetric near-ring with identity and Γ a faithful N-group without proper N-subgroups. Let D be the set of all non-zero N-endomorphisms of Γ. Then D is a group of fixed-point-free automorphisms, N is a simple near-ring, and*

- *either N is a full matrix ring (if N is a ring)*
- *or $N = \mathrm{M}_{D^0}(\Gamma)$ (if N is not a ring).*

This shows that the near-rings $\mathrm{M}_{D^0}(\Gamma)$ (D fixed-point-free) can be regarded as a non-linear version of matrix rings. In fact, there is even more analogy, because the elements of these near-rings can be described explicitly, very similar to the construction of matrices (or linear mappings) using a basis.

The following is Theorem 3.31 in Meldrum [1985].

THEOREM 8.2: *Let Γ be a group, D be a group of fixed-point-free automorphisms of Γ, and A be a set of non-zero orbit representatives, i.e., $\Gamma \setminus \{0\} = \biguplus_{\gamma \in A} D\gamma$. Then each function h from A into Γ can be extended to exactly one element $f \in \mathrm{M}_{D^0}(\Gamma)$ by $f(0) := 0$ and*

$$f(\alpha\gamma) := \alpha h(\gamma),$$

for each $\alpha \in D$ and $\gamma \in A$. In particular,

$$|\mathrm{M}_{D^0}(\Gamma)| = |\Gamma|^{|A|}.$$

Thus, A is used instead of a vector basis here.

For transformation near-rings, note that the assumptions of Theorem 8.1 can be checked easily by the methods developed so far and those in section 10.

Variants of these results in Pilz [1983] also work for non-zero-symmetric near-rings.

9. N-Endomorphisms

The previous section shows that in order to represent a transformation near-ring $N \leq \mathrm{M}(\Gamma)$ as a centralizer near-ring, it is important to have an effective method to determine the N-endomorphisms of Γ.

PROPOSITION 9.1: *Let $\langle E\rangle = N \leq \mathrm{M}(\Gamma)$. Then the endomorphism $\alpha \in \mathrm{End}(\Gamma)$ is an N-endomorphism iff*

$$\alpha e = e\alpha, \quad \textit{for all } e \in E.$$

Proof: The necessarity is trivial. For the sufficiency, we have to prove $\alpha f = f\alpha$, for all $f \in N$. This is done by induction on f. Let α commute with $e \in E$ and $f, g \in N$. Then

$$\begin{aligned} (ef)\alpha &= e\alpha f = \alpha(ef); \\ (-f+g)\alpha &= -f\alpha + g\alpha = -\alpha f + \alpha g = \alpha(-f+g). \end{aligned}$$

The second computation has used that α is a group-homomorphism. □

An N-homomorphism on Γ is uniquely determined by its restriction to any set G with $\langle G\rangle_N = \Gamma$. The total number of N-endomorphisms of Γ is bounded by $|\Gamma|^{|G|}$, where G is a minimal N-generating set. This is particularly nice if Γ can be generated by a single element γ. For all possible images $i \in \Gamma$, we test whether the homomorphism from Γ to Γ induced by $\gamma \mapsto i$ commutes with all generators of N. If it does, it is indeed an N-homomorphism.

If $\Gamma = \langle \gamma_1, \ldots, \gamma_l\rangle_N$ needs l N-generators, $l > 1$, we can still use an inductive approach, determining the partial N-homomorphisms from $H = \langle \gamma_1, \ldots, \gamma_k\rangle_N$ to Γ, and then extending each of them to N-homomorphisms from $\langle H, \gamma_{k+1}\rangle_N$ to Γ by finding a feasible image for γ_{k+1}, if possible.

Algorithm 2 shows how to extend a partial N-homomorphism α from $H \leq_N \Gamma$ into Γ to an N-homomorphism β defined on $\langle H, g\rangle_N$.

The condition that $|\langle \{\, (h, \alpha(h)) \mid h \in H \,\} \cup \{\, (g, i) \,\}\rangle_N| = |\langle H, g\rangle_N|$ is necessary and sufficient for β determined by $\beta|_H = \alpha$ and $\beta(g) = i$ to be a group homomorphism on $\langle H, g\rangle_N$. If β commutes with all generators of N, then it is an N-homomorphism by Proposition 9.1.

REMARK 9.1: Of course, not every element i of Γ is a feasible image of a particular g under a group homomorphism, let alone an N-homomorphism. We can

Algorithm 2 Extending N-homomorphism

Let N be a near-ring of transformations on the group Γ.

Require: $N = \langle E \rangle$, $H <_N \Gamma$, $\alpha \in \mathrm{Hom}_N(H, \Gamma)$ and $g \in \Gamma \setminus H$.
Ensure: $Nhomos = \{ \beta \in \mathrm{Hom}_N(\langle H, \gamma \rangle_N, \Gamma) \mid \beta|_H = \alpha \}$

```
Nhomos = ∅
for i ∈ Γ do
  if |⟨{ (h, α(h)) | h ∈ H } ∪ { (g, i) }⟩_N| = |⟨H, g⟩_N| then
    Define β on ⟨H, g⟩_N such that β|_H = α and β(g) = i.
    if for all e ∈ E : eβ = βe then
      Add β to Nhomos
    end if
  end if
end for
```

restrict the search space to elements fulfilling a number of criteria that are easy to check by using only near-ring generators. Thus we avoid using the costlier computation of the size of the N-groups by the closure algorithm for a choice of i which is obviously not feasible.

The order of i divides the order of g, and it is equal to the order of g if Algorithm 2 is used for the computation of N-*auto*morphisms.

If g is an element of $e\Gamma$ for some $e \in E$, then the image of g under an N-endomorphism is again an element of $e\Gamma$. For any N-automorphism we also have that if $g \notin e\Gamma$ for some $e \in E$, then the image of g is not in $e\Gamma$.

Moreover, if we already know a group S of N-automorphisms (e.g., the inner automorphisms), we may compute the stabilizer $S' := \{s \in S \mid s\alpha = \alpha\}$ of the partial N-endomorphism α in S. Let i be a feasible image for g to extend α on $\langle H, g \rangle_N$ to an N-endomorphism β. Then si, for $s \in S'$, also gives an N-endomorphism, namely, $s\beta$. Thus, because we are satisfied with (semi)group generators for the N-(endo)automorphisms, it is sufficient to search for images i to extend α on g under the representatives of the orbits of Γ under S'.

Then S and the list of N-endomorphisms that are computed by using Algorithm 2 iteratively generate all N-endomorphisms.

For those cases, where we have to expect that there are particularly many N-homomorphisms, namely, if Γ is a direct product of N-groups, we can find a representation of the N-homomorphisms in terms of the N-homomorphisms of smaller N-groups.

PROPOSITION 9.2: *Let N be zero-symmetric and $\Gamma = H_1 \times H_2$ be the direct product of the N-groups H_1 and H_2.*

Then α is an N-endomorphism of Γ iff there exist $\alpha_{ij} \in \mathrm{Hom}_N(H_j, H_i)$ such that $\alpha(x_1, x_2) = (\alpha_{11}(x_1) + \alpha_{12}(x_2), \alpha_{21}(x_1) + \alpha_{22}(x_2))$ with $x_i \in H_i$.

Proof: Straightforward generalization of the corresponding result for groups. □

10. Transformation Near-rings

Let Γ be a group, $N \leq \mathrm{M}(\Gamma)$, and $N = \langle E \rangle$. If Γ is small (note that N still can be very big), then, by the methods discussed so far, we have no problems computing anything we want to know about the N-group Γ.

Now we turn to the problem of getting information about N itself. The trick is to transfer near-ring problems to N-group problems.

An element f of a near-ring N is called *distributive on* N iff $f(g+h) = fg+fh$ for all $f, h \in N$. A near-ring is *distributive* iff all of its elements are distributive on N. Obviously, a near-ring is a ring iff it is abelian and distributive.

Of course, if f is an endomorphism of Γ, then it is distributive on N. But this condition is not necessary. We need a weaker one. Call f an *N-piecewise endomorphism* iff all restrictions of f to $N\gamma$, $\gamma \in \Gamma$, are endomorphisms. Note that this notion, like distributivity, depends on the near-ring N involved.

PROPOSITION 10.1: *Let $f \in N \leq \mathrm{M}(\Gamma)$. Then $f \in N$ is distributive iff it is a piecewise endomorphism on N.*

Proof: Let f be distributive and $g\gamma, h\gamma \in N\gamma$. Then $f(g\gamma + h\gamma) = f(g+h)\gamma = (fg+fh)\gamma = f(g\gamma) + f(h\gamma)$. So the restriction of f to $N\gamma$ is a homomorphism. Clearly $f(g\gamma) = (fg)\gamma \in N\gamma$. Conversely, if $f(g+h)\gamma = (fg+fh)\gamma$ for all $\gamma \in \Gamma$, then, using faithfulness, $f(g+h) = fg+fh$. Hence f is distributive. □

Note that the $N\gamma$ can be computed efficiently by Algorithm 1.

REMARK 10.1: To test whether a mapping f is a homomorphism on a group Γ generated (as a group) by a set F, it is enough to test whether $f(\gamma + \varphi) = f(\gamma) + f(\varphi)$ for all $\gamma \in \Gamma$, $\varphi \in F$. Thus the test has complexity $\mathrm{O}(|\Gamma|\,|F|)$.

PROPOSITION 10.2: *$N \leq M(\Gamma)$ is an abelian near-ring iff for each $\gamma \in \Gamma$ the group $N\gamma$ is abelian.*

Proof: Let $f\gamma, g\gamma \in N$. Then $f\gamma + g\gamma = (f+g)\gamma = (g+f)\gamma = g\gamma + f\gamma$ if N is abelian. Conversely, for $f, g \in N$ we have to show that $(f+g)\gamma = (g+f)\gamma$, for any γ, which again follows directly from $N\gamma$ being abelian. □

PROPOSITION 10.3: *An abelian near-ring N is distributive iff all its generators are distributive.*

Proof: Let $f, g \in N$ be distributive and $a, b \in N$. Then $(fg)(a+b) = f(ga+gb) = (fg)a + (fg)b$. Similarly, using that N is abelian, $(f+g)(a+b) = f(a+b) + g(a+b) = fa+fb+ga+gb = fa+ga+fb+gb = (f+g)a + (f+g)b$. □

COROLLARY 10.1: *Within $\mathrm{O}(|\Gamma|\,|E|^2)$ operations, we can test whether N is a ring.*

Many more properties can be tested efficiently by a reduction to the computation of some $N\gamma$ as before, e.g.:

PROPOSITION 10.4: *$f \in N$ is in the center of N (i.e., commutes with all $g \in N$) iff f is distributive and commutes with all generators.*

The algorithms in this section do not depend on having generators of N. It is enough to be able to compute orbits. We have seen that this works nicely for N_0, too, where only N is given by generators.

COROLLARY 10.2: *We can test efficiently whether N_0 is a ring.*

DEFINITION 10.1: Let Γ be a group, and let $N \leq M \leq \mathrm{M}(\Gamma)$. We say that N has the *k-interpolation property with respect to M* iff for all finite subsets A of Γ with $|A| \leq k$ and for all $m \in M$ there exists an element $n \in N$ such that $n|_A = m|_A$.

REMARK 10.2: N has the 1-interpolation property with respect to $\mathrm{M}(\Gamma)$ iff $N\gamma = \Gamma$ for all $\gamma \in \Gamma$.

Thus, it is easy to test the 1-interpolation property. We observe that $\Gamma \times \Gamma$ is an N-group, too, by componentwise operation: $n(\gamma_1, \gamma_2) = (n\gamma_1, n\gamma_2)$.

PROPOSITION 10.5: *$N \leq \mathrm{M}(\Gamma)$ has the 2-interpolation property with respect to $\mathrm{M}(\Gamma)$ iff $N(a, b) = \Gamma \times \Gamma$ for all $a, b \in \Gamma, a \neq b$.*

Proof: The condition just means that, for an arbitrary pair (c, d) of values, there is some $f \in N$ such that $f(a) = c$ and $f(b) = d$. □

COROLLARY 10.3: *Let $\langle E \rangle = N \leq \mathrm{M}(\Gamma)$. Then we can test the 2-interpolation property of N with respect to $\mathrm{M}(\Gamma)$ within $\mathrm{O}(|E|\,|\Gamma|^2)$ operations.*

In fact, we can generalize these results to interpolation with respect to $\mathrm{M}_{D^0}(\Gamma)$, D a group of fixed-point-free automorphisms.

THEOREM 10.1: *Let D be a group of fixed-point-free automorphisms of Γ. Take a set A of orbit representatives according to the operation of D on Γ. Then, for $k \leq |A|$, $N \leq \mathrm{M}_{D^0}(\Gamma)$ has the k-interpolation property with respect to $\mathrm{M}_D(\Gamma)$ iff $N(\gamma_1, \ldots, \gamma_k) = \Gamma^k$ for each tuple $(\gamma_1, \ldots, \gamma_k) \in A^k$ (with all γ_i distinct).*

Proof: By Theorem 8.2, each element of the centralizer near-ring is the unique extension of a function from A into Γ. Therefore, it is enough to interpolate the latter ones. □

COROLLARY 10.4: *One can determine whether $N = \langle E \rangle$ has the k-interpolation property with respect to $\mathrm{M}_D(\Gamma)$, D fixed-point-free, within $\mathrm{O}(|E|\,|A|^k)$ operations, where A is a set of orbit representatives.*

11. Realizability

Our solution of the k-interpolation problem (we use the notation as in Corollary 10.4) is useful only for really small k because $|A| > 1$ for all non-trivial cases. Note that for $k \geq |A|$, the k-interpolation property just means $N = \mathrm{M}_D(\Gamma)$, which we would like to be able to decide. Therefore, we need a better method to do k-interpolation for $k > 2$. A different form of density result helps us.

THEOREM 11.1: *Let N be a sub-near-ring of $\mathrm{M}_{D^0}(\Gamma)$, (D a group of fixed-point-free automorphisms), that has the 2-interpolation property with respect to $\mathrm{M}_{D^0}(\Gamma)$. If N is not a ring, then $N = \mathrm{M}_{D^0}(\Gamma)$.*

Proof: This follows from Theorem 4.21 in Aichinger [1994] or from Algorithm 3. □

Note that the 2-interpolation property can be tested efficiently and that we can find out whether N_0 is a ring.

Often we are not satisfied with the information that some $f \in \mathrm{M}_D(\Gamma)$ happens to be in N, but rather want to know how f can be realized, i.e., how it can be obtained from the generators using addition and composition.

PROBLEM 11.1: [Completeness and Realizability] Let $\langle E \rangle = N \leq \mathrm{M}_D(\Gamma)$. Determine whether $N = \mathrm{M}_D(\Gamma)$ and, in the affirmative case, show how each $f \in \mathrm{M}_D(\Gamma)$ can be constructed from the generators, i.e., compute a term t in the free near-ring over E that realizes f.

DEFINITION 11.1: A *Kaiser multiplication for $N \leq \mathrm{M}(\Gamma)$* is a bivariate function $K\colon \Gamma \times \Gamma \to \Gamma$ such that

- $K(\gamma, 0) = K(0, \gamma) = 0$ for all $\gamma \in \Gamma$;
- $K(\alpha, \beta) \neq 0$ for some $\alpha, \beta \in \Gamma$;
- $K(f, g) \in N$, for $f, g \in N$, where $K(f, g)(\gamma) := K(f(\gamma), g(\gamma))$ for all $\gamma \in \Gamma$.

In Algorithm 3, we need a Kaiser-multiplication for the case that N is not a ring. In fact, there is a very natural choice, the one that has has been constructed in Aichinger [1994]:

PROPOSITION 11.1: *If N is not a ring, then we can define a Kaiser multiplication K as follows:*

- *If $(\Gamma, +)$ is not abelian, then we can find α and β in Γ with $\alpha + \beta \neq \beta + \alpha$, and define $K(\gamma_1, \gamma_2) := -\gamma_1 - \gamma_2 + \gamma_1 + \gamma_2$.*
- *If N is not distributive, then we can find $f \in N$, such that there are $\alpha, \beta \in \Gamma$ with $f(\alpha + \beta) \neq f(\alpha) + f(\beta)$. Then we define $K(\gamma_1, \gamma_2) := f(\gamma_1) + f(\gamma_2) - f(\gamma_1 + \gamma_2)$.*

COROLLARY 11.1: *Algorithm 3, which uses $\mathrm{O}(k^2)$ interpolations, together with appropriate book-keeping and our solution of the 2-interpolation problem, gives an efficient solution to the realizability problem for any fixed-point-free automorphism group D.*

Algorithm 3 Interpolation

Let $\langle E\rangle = N \leq M_D(\Gamma)$, D a group of fixed-point free automorphisms, A a set of orbit representatives with respect to D, and K a Kaiser-multiplication for N.

Require: A set $S \subset A$, $\gamma \in A \setminus S$, $m \in M_D(\Gamma)$.
Ensure: A term f satisfying $f|_{S\cup\{\gamma\}} = m|_{S\cup\{\gamma\}}$ for all $i = 1, \ldots, n$, $\gamma \in A$.
  if $|S| \leq 2$ **then**
    Find f using 2-interpolation as in Proposition 10.5
  else
    Recursively find f_1 such that $f_1|_S = m|_S$
    Use the algorithm ***LagrangePoly*** below to find a term f_2 such that
      $f_2(S) = 0$ and $f_2(\gamma) = m(\gamma) - f_1(\gamma)$.
    $f := f_2 + f_1$
  end if

The following algorithm ***LagrangePoly*** solves a specific interpolation problem by a divide and conquer strategy.

Require: A set $S \subset A$, $\gamma \in A \setminus S$, $m \in \mathrm{M}_D(\Gamma)$ with $m(A) = 0$.
Ensure: A function $f \in N$ satisfying $f(S) = 0$ and $f(\gamma) = m(\gamma)$.
  if $|S| \leq 2$ **then**
    Find f using 2-interpolation as in Proposition 10.5
  else
    Partition S into two smaller subsets S_1, S_2
    Let α, β be such that $K(\alpha, \beta) \neq 0$
    Recursively determine
      f_1 such that $f_1(S_1) = 0$ and $f_1(\gamma) = \alpha$
      f_2 such that $f_2(S_2) = 0$ and $f_2(\gamma) = \beta$
    $h := K(f_1, f_2)$
    Find $g \in N$ such that $g(0) = 0$ and $g(K(\alpha, \beta)) = m(\gamma)$
      (using 2-interpolation again)
    $f := g \circ h$
  end if

12. Conclusion

Our emphasis has been the study of sub-near-rings N of $\mathrm{M}(\Gamma)$, Γ small, that are given by a small number of generators but are potentially very big. Various efficient algorithms for problems in this area have been developed. Based on these, some interesting properties of N can be determined via its natural operation on Γ. As this topic is still rather new, the results in this article should be considered as a solid basis for further investigations.

The following problems have been solved only partially and seem to be really challenging.

PROBLEM 12.1: Let Γ be a group and $\langle E\rangle = N \leq \mathrm{M}(\Gamma)$.

1. *N-endomorphisms:* Determine a (nearly) minimal set of semigroup generators for the set of all N-endomorphisms of Γ.
2. *Membership:* For any given $f \in \mathrm{M}(\Gamma)$, decide whether $f \in N$.
3. *Size:* Compute the Size of N.

This article contains a solution for problem 1 that is quite useful. For bigger groups that are not N-direct products but still have many N-endomorphisms, better methods are needed.

For the problems 2 and 3, we have presented a solution that is nice whenever Theorem 8.2 can be applied. Another partial solution is contained in Binder et al. [2000].

References

E. Aichinger. Interpolation with near-rings of polynomial functions. Master's thesis, Johannes Kepler University Linz, Austria, 1994. Also available at http://www.algebra.uni-linz.ac.at/~erhard/.

E. Aichinger, F. Binder, J. Ecker, R. Eggetsberger, P. Mayr, and C. Nöbauer. *SONATA: Systems Of Nearrings And Their Applications, Package for the group theory system GAP4.* Johannes Kepler University Linz, Austria, 2000. Available from http://www.algebra.uni-linz.ac.at/sonata/.

F. Binder, E. Aichinger, J. Ecker, C. Nöbauer, and P. Mayr. Algorithms for near-rings of non-linear transformations. In C. Traverso, editor, *Proceedings of ISSAC 2000, St. Andrews, Scotland*, pages 23–29. ACM, 2000. Also available at http://www.algebra.uni-linz.ac.at/sonata/papers/.

James R. Clay. *Nearrings: Geneses and applications.* The Clarendon Press Oxford University Press, New York, 1992.

H.-Peter Gumm. An easy way to the commutator in modular varieties. *Arch. Math. (Basel)*, 34(3):220–228, 1980.

J. D. P. Meldrum. *Near-rings and their links with groups.* Pitman (Advanced Publishing Program), Boston, MA, 1985.

Günter Pilz. *Near-rings.* North-Holland Publishing Co., Amsterdam, second edition, 1983.

S. D. Scott. Involution near-rings. *Proc. Edinburgh Math. Soc. (2)*, 22(3):241–245, 1979.

Charles C. Sims. Computational methods in the study of permutation groups. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 169–183. Pergamon, Oxford, 1970.