Congruence preserving functions and polynomial functions on expanded groups

Erhard Aichinger

Department of Algebra
Johannes Kepler University Linz

20$^{\text{th}}$ International Conference on Near-rings and Near-fields
Linz 2007

Outline

Expanded Groups

Definition of expanded groups

An algebra $\langle V, +, -, 0, f_1, f_2, \ldots \rangle$ is an *expanded group* if $\langle V, +, -, 0 \rangle$ is a (not necessarily abelian) group.

Examples of expanded groups

- Every group (ring, near-ring, vector-space) is an expanded group.
- Every ring-module is an expanded group.
- For a near-ring N, every N-group Γ is an expanded group.

Expanded Groups

Definition of expanded groups

An algebra $\langle V, +, -, 0, f_1, f_2, \ldots \rangle$ is an *expanded group* if $\langle V, +, -, 0\rangle$ is a (not necessarily abelian) group.

Examples of expanded groups

- Every group (ring, near-ring, vector-space) is an expanded group.
- Every ring-module is an expanded group.
- For a near-ring N, every N-group Γ is an expanded group.

Expanded Groups

Definition of expanded groups

An algebra $\langle V, +, -, 0, f_1, f_2, \ldots \rangle$ is an *expanded group* if $\langle V, +, -, 0 \rangle$ is a (not necessarily abelian) group.

Examples of expanded groups

- Every group (ring, near-ring, vector-space) is an expanded group.
- Every ring-module is an expanded group.
- For a near-ring N, every N-group Γ is an expanded group.

Expanded Groups

Definition of expanded groups

An algebra $\langle V, +, -, 0, f_1, f_2, \ldots \rangle$ is an *expanded group* if $\langle V, +, -, 0 \rangle$ is a (not necessarily abelian) group.

Examples of expanded groups

- Every group (ring, near-ring, vector-space) is an expanded group.
- Every ring-module is an expanded group.
- For a near-ring N, every N-group Γ is an expanded group.

Expanded Groups

Definition of expanded groups

An algebra $\langle V, +, -, 0, f_1, f_2, \ldots \rangle$ is an *expanded group* if $\langle V, +, -, 0 \rangle$ is a (not necessarily abelian) group.

Examples of expanded groups

- Every group (ring, near-ring, vector-space) is an expanded group.
- Every ring-module is an expanded group.
- For a near-ring N, every N-group Γ is an expanded group.

Congruences and Ideals

Ideals

Let $\mathbf{V} = \langle V, +, -, 0, f_1, f_2, \ldots \rangle$ be an expanded group. Then a normal subgroup I of $\langle V, +, -, 0 \rangle$ is an *ideal* of $\mathbf{V}$ if

$$f_j(v_1 + i_1, \ldots, v_n + i_n) - f_j(v_1, \ldots, v_n) \in I$$

for all fundamental operations f_j of $\mathbf{V}$.

Theorem

Let $\mathbf{V}$ be an expanded group. Then the ideals are in bijective correspondence with the congruence relations of $\mathbf{V}$.

Congruences and Ideals

Ideals

Let $\mathbf{V} = \langle V, +, -, 0, f_1, f_2, \ldots \rangle$ be an expanded group. Then a normal subgroup I of $\langle V, +, -, 0 \rangle$ is an *ideal* of $\mathbf{V}$ if

$$f_j(v_1 + i_1, \ldots, v_n + i_n) - f_j(v_1, \ldots, v_n) \in I$$

for all fundamental operations f_j of $\mathbf{V}$.

Theorem

Let $\mathbf{V}$ be an expanded group. Then the ideals are in bijective correspondence with the congruence relations of $\mathbf{V}$.

Congruence preserving functions

Congruence preserving functions

Let $\mathbf{V}$ be and expanded group, and let $f : V \to V$. Then f is a *congruence preserving function* if for all ideals I of $\mathbf{V}$ and for all $x, y \in V$ with $x - y \in I$, we have $f(x) - f(y) \in I$.

Near-rings of congruence preserving functions

Let $\mathbf{V}$ be an expanded group. We define

$$\begin{aligned} C(\mathbf{V}) &:= \{f : V \to V \mid f \text{ is congruence preserving on } V\} \\ C_0(\mathbf{V}) &:= \{f \in C(\mathbf{V}) \mid f(0) = 0\}. \end{aligned}$$

Then $\langle C_0(\mathbf{V}), +, \circ \rangle$ is a zero-symmetric near-ring that contains id_V.

Congruence preserving functions

Congruence preserving functions

Let $\mathbf{V}$ be and expanded group, and let $f : V \to V$. Then f is a *congruence preserving function* if for all ideals I of $\mathbf{V}$ and for all $x, y \in V$ with $x - y \in I$, we have $f(x) - f(y) \in I$.

Near-rings of congruence preserving functions

Let $\mathbf{V}$ be an expanded group. We define

$$\begin{aligned} C(\mathbf{V}) &:= \{f : V \to V \mid f \text{ is congruence preserving on } V\} \\ C_0(\mathbf{V}) &:= \{f \in C(\mathbf{V}) \mid f(0) = 0\}. \end{aligned}$$

Then $\langle C_0(\mathbf{V}), +, \circ \rangle$ is a zero-symmetric near-ring that contains id_V.

Ideals of $C_0(\mathbf{V})$

Theorem (Cannon, Kabza, Q.M. 2001)

Let $\mathbf{V}$ be an expanded group such that the ideal lattice of $\mathbf{V}$ is a three element chain $\{0, A, V\}$. We assume $|A| \geq 2$. Then the ideals of $C_0(\mathbf{V})$ are $C_0(\mathbf{V})$, $(A : V)$, $(0 : A)$, $(A : V) \cap (0 : A)$, and 0.

Ideals of $C_0(\mathbf{V})$

Theorem (E.A., Cannon, Ecker, Kabza, Neuerburg)

Let $\mathbf{V}$ be a finite expanded group. If $\mathbf{Id}\,\mathbf{V}$ is a chain $0 = A_1 < A_2 < \cdots < A_n = V$ with $|A_i/A_{i-1}| \geq 3$ for all $i \in \{2, \ldots, n\}$, then we have:

1. Every ideal of $C_0(\mathbf{V})$ is an intersection of Noetherian Quotients $(A_i : A_j)_{C_0(\mathbf{V})}$.
2. The near-ring $C_0(\mathbf{V})$ has $\frac{1}{n+1}\binom{2n}{n}$ ideals.
3. The near-ring $C_0(\mathbf{V})$ is subdirectly irreducible, and its unique minimal ideal is $(0 : A_{n-1})_{C_0(\mathbf{V})} \cap (A_2 : G)_{C_0(\mathbf{V})}$.
4. $C_0(\mathbf{V})$ has $n-1$ maximal ideals.

Ideals of $C_0(\mathbf{V})$

Theorem (E.A., Cannon, Ecker, Kabza, Neuerburg)

Let $\mathbf{V}$ be a finite expanded group. If $\mathbf{Id}\,\mathbf{V}$ is a chain $0 = A_1 < A_2 < \cdots < A_n = V$ with $|A_i/A_{i-1}| \geq 3$ for all $i \in \{2, \ldots, n\}$, then we have:

1. Every ideal of $C_0(\mathbf{V})$ is an intersection of Noetherian Quotients $(A_i : A_j)_{C_0(\mathbf{V})}$.
2. The near-ring $C_0(\mathbf{V})$ has $\frac{1}{n+1}\binom{2n}{n}$ ideals.
3. The near-ring $C_0(\mathbf{V})$ is subdirectly irreducible, and its unique minimal ideal is $(0 : A_{n-1})_{C_0(\mathbf{V})} \cap (A_2 : G)_{C_0(\mathbf{V})}$.
4. $C_0(\mathbf{V})$ has $n-1$ maximal ideals.

Ideals of $C_0(\mathbf{V})$

Theorem (E.A., Cannon, Ecker, Kabza, Neuerburg)

Let $\mathbf{V}$ be a finite expanded group. If $\mathbf{Id}\,\mathbf{V}$ is a chain $0 = A_1 < A_2 < \cdots < A_n = V$ with $|A_i/A_{i-1}| \geq 3$ for all $i \in \{2, \ldots, n\}$, then we have:

1. Every ideal of $C_0(\mathbf{V})$ is an intersection of Noetherian Quotients $(A_i : A_j)_{C_0(\mathbf{V})}$.
2. The near-ring $C_0(\mathbf{V})$ has $\frac{1}{n+1}\binom{2n}{n}$ ideals.
3. The near-ring $C_0(\mathbf{V})$ is subdirectly irreducible, and its unique minimal ideal is $(0 : A_{n-1})_{C_0(\mathbf{V})} \cap (A_2 : G)_{C_0(\mathbf{V})}$.
4. $C_0(\mathbf{V})$ has $n-1$ maximal ideals.

Ideals of $C_0(\mathbf{V})$

Theorem (E.A., Cannon, Ecker, Kabza, Neuerburg)

Let $\mathbf{V}$ be a finite expanded group. If $\mathbf{Id}\,\mathbf{V}$ is a chain $0 = A_1 < A_2 < \cdots < A_n = V$ with $|A_i/A_{i-1}| \geq 3$ for all $i \in \{2, \ldots, n\}$, then we have:

1. Every ideal of $C_0(\mathbf{V})$ is an intersection of Noetherian Quotients $(A_i : A_j)_{C_0(\mathbf{V})}$.
2. The near-ring $C_0(\mathbf{V})$ has $\frac{1}{n+1}\binom{2n}{n}$ ideals.
3. The near-ring $C_0(\mathbf{V})$ is subdirectly irreducible, and its unique minimal ideal is $(0 : A_{n-1})_{C_0(\mathbf{V})} \cap (A_2 : G)_{C_0(\mathbf{V})}$.
4. $C_0(\mathbf{V})$ has $n-1$ maximal ideals.

Ideals of $C_0(\mathbf{V})$

Theorem (E.A., Cannon, Ecker, Kabza, Neuerburg)

Let $\mathbf{V}$ be a finite expanded group. If $\mathbf{Id}\,\mathbf{V}$ is a chain $0 = A_1 < A_2 < \cdots < A_n = V$ with $|A_i/A_{i-1}| \geq 3$ for all $i \in \{2, \ldots, n\}$, then we have:

1. Every ideal of $C_0(\mathbf{V})$ is an intersection of Noetherian Quotients $(A_i : A_j)_{C_0(\mathbf{V})}$.
2. The near-ring $C_0(\mathbf{V})$ has $\frac{1}{n+1}\begin{pmatrix} 2n \\ n \end{pmatrix}$ ideals.
3. The near-ring $C_0(\mathbf{V})$ is subdirectly irreducible, and its unique minimal ideal is $(0 : A_{n-1})_{C_0(\mathbf{V})} \cap (A_2 : G)_{C_0(\mathbf{V})}$.
4. $C_0(\mathbf{V})$ has $n-1$ maximal ideals.

Maximal ideals of $C_0(\mathbf{V})$

Lemma

Let $\mathbf{V}$ be a finite expanded group. Then every maximal ideal of $C_0(\mathbf{V})$ is of the form $(A : B)_{C_0(\mathbf{V})}$ with $A \prec B$ in $\mathbf{Id}\,(\mathbf{V})$.

Theorem (E.A., JPAA 2006)

Let $\mathbf{V}$ be a finite expanded group, and let $A \prec B$ and $C \prec D$ be ideals of $\mathbf{V}$. Then the following are equivalent:

1. $(A : B)_{C_0(\mathbf{V})} = (C : D)_{C_0(\mathbf{V})}$.
2. The intervals $I[A, B]$ and $I[C, D]$ are projective intervals in $\mathbf{Id}\,(\mathbf{V})$.

Maximal ideals of $C_0(\mathbf{V})$

Lemma

Let $\mathbf{V}$ be a finite expanded group. Then every maximal ideal of $C_0(\mathbf{V})$ is of the form $(A : B)_{C_0(\mathbf{V})}$ with $A \prec B$ in $\mathbf{Id}\,(\mathbf{V})$.

Theorem (E.A., JPAA 2006)

Let $\mathbf{V}$ be a finite expanded group, and let $A \prec B$ and $C \prec D$ be ideals of $\mathbf{V}$. Then the following are equivalent:

1. $(A : B)_{C_0(\mathbf{V})} = (C : D)_{C_0(\mathbf{V})}$.
2. The intervals $I[A, B]$ and $I[C, D]$ are projective intervals in $\mathbf{Id}\,(\mathbf{V})$.

Maximal ideals of $C_0(\mathbf{V})$

Lemma

Let $\mathbf{V}$ be a finite expanded group. Then every maximal ideal of $C_0(\mathbf{V})$ is of the form $(A : B)_{C_0(\mathbf{V})}$ with $A \prec B$ in $\mathbf{Id}\,(\mathbf{V})$.

Theorem (E.A., JPAA 2006)

Let $\mathbf{V}$ be a finite expanded group, and let $A \prec B$ and $C \prec D$ be ideals of $\mathbf{V}$. Then the following are equivalent:

1. $(A : B)_{C_0(\mathbf{V})} = (C : D)_{C_0(\mathbf{V})}$.
2. The intervals $I[A, B]$ and $I[C, D]$ are projective intervals in $\mathbf{Id}\,(\mathbf{V})$.

Maximal ideals of $C_0(\mathbf{V})$

Lemma

Let $\mathbf{V}$ be a finite expanded group. Then every maximal ideal of $C_0(\mathbf{V})$ is of the form $(A : B)_{C_0(\mathbf{V})}$ with $A \prec B$ in $\mathbf{Id}\,(\mathbf{V})$.

Theorem (E.A., JPAA 2006)

Let $\mathbf{V}$ be a finite expanded group, and let $A \prec B$ and $C \prec D$ be ideals of $\mathbf{V}$. Then the following are equivalent:

1. $(A : B)_{C_0(\mathbf{V})} = (C : D)_{C_0(\mathbf{V})}$.
2. The intervals $I[A, B]$ and $I[C, D]$ are projective intervals in $\mathbf{Id}\,(\mathbf{V})$.

Quotients modulo the maximal ideals

Quotients modulo the maximal ideals

Let $\mathbf{V}$ be a finite expanded group. Let $A_0 \prec B_0$ be ideals of $\mathbf{V}$, and let $\{(A_0, B_0), (A_1, B_1), \ldots, (A_n, B_n)\}$ be the class of prime intervals projective to $I[A_0, B_0]$. Then:

1. If exactly one of the A_i is a join irreducible element in $\mathbf{Id}(\mathbf{V})$, then $C_0(\mathbf{V})/(A_0 : B_0)_{C_0(\mathbf{V})}$ is isomorphic to $M_0(B_0/A_0)$.
2. If more than one of the A_i are join irreducible, $C_0(\mathbf{V})/(A_0 : B_0)_{C_0(\mathbf{V})}$ is isomorphic to a full matrix ring over a finite field.

Quotients modulo the maximal ideals

Quotients modulo the maximal ideals

Let $\mathbf{V}$ be a finite expanded group. Let $A_0 \prec B_0$ be ideals of $\mathbf{V}$, and let $\{(A_0, B_0), (A_1, B_1), \ldots, (A_n, B_n)\}$ be the class of prime intervals projective to $I[A_0, B_0]$. Then:

1. If exactly one of the A_i is a join irreducible element in $\mathbf{Id}(\mathbf{V})$, then $C_0(\mathbf{V})/(A_0 : B_0)_{C_0(\mathbf{V})}$ is isomorphic to $M_0(B_0/A_0)$.
2. If more than one of the A_i are join irreducible, $C_0(\mathbf{V})/(A_0 : B_0)_{C_0(\mathbf{V})}$ is isomorphic to a full matrix ring over a finite field.

Quotients modulo the maximal ideals

Quotients modulo the maximal ideals

Let $\mathbf{V}$ be a finite expanded group. Let $A_0 \prec B_0$ be ideals of $\mathbf{V}$, and let $\{(A_0, B_0), (A_1, B_1), \ldots, (A_n, B_n)\}$ be the class of prime intervals projective to $I[A_0, B_0]$. Then:

1. If exactly one of the A_i is a join irreducible element in $\mathbf{Id}\,(\mathbf{V})$, then $C_0(\mathbf{V})/(A_0 : B_0)_{C_0(\mathbf{V})}$ is isomorphic to $M_0(B_0/A_0)$.
2. If more than one of the A_i are join irreducible, $C_0(\mathbf{V})/(A_0 : B_0)_{C_0(\mathbf{V})}$ is isomorphic to a full matrix ring over a finite field.

Theorem (E.A., JPAA 2006)

Let $\mathbf{V}$ be a finite expanded group, and let A be an ideal of $\mathbf{V}$. Then there exists a function $e \in C_0(\mathbf{V})$ such that $e(V) \subseteq A$ and $e(a) = a$ for all $a \in A$ iff A is a distributive element of the lattice $\mathbf{Id}\,\mathbf{V}$.

Polynomial functions

Polynomial functions

Let $\mathbf{V}$ be an expanded group. Then $P(\mathbf{V})$ is the set of all polynomial functions on $\mathbf{V}$.

Lemma

$P(\mathbf{V}) \subseteq C(\mathbf{V})$.

Polynomial functions

Polynomial functions

Let $\mathbf{V}$ be an expanded group. Then $P(\mathbf{V})$ is the set of all polynomial functions on $\mathbf{V}$.

Lemma

$P(\mathbf{V}) \subseteq C(\mathbf{V})$.

Possible sets of polynomial functions

Theorem (E.A., P. Mayr, Acta Math. Hung. 2007)

Let p, q be odd primes with $p \neq q$. Then there are exactly 17 subnear-rings of $M(\mathbb{Z}_{pq})$ that contain $M_{\mathrm{aff}}(\mathbb{Z}_{pq})$.