On solvable polynomial equations over $\mathbb{Z}_n$ and some remarks on zero-preserving polynomials over a ring R with $J(R)^2 = 0$

Joerg Forstner
Department of Algebra, Johannes Kepler University
Linz, Austria
chesshero@algebra.uni-linz.ac.at

Basics

Proposition 1. *Every finite ring R can be uniquely represented (up to order) as a direct product of rings R_i with cardinality of a prime power.*

Proposition 2. *Let R be a finite ring and let $R_1 \oplus \ldots \oplus R_k$ be the decomposition as in Proposition 1. Then*

$$R[x] \cong R_1[x] \oplus \ldots \oplus R_k[x]$$

Theorem 1. *Let $n \in \mathbb{N}$, let $p_1, \ldots, p_k$ be pairwise different primes, $t_1, \ldots, t_k \in \mathbb{N}$ with $n = \prod_{i=1}^{k} p_i^{t_i}$. Then*

$$(\mathbb{Z}_n[x], +, \cdot) \cong (\mathbb{Z}_{p_1^{t_1}}[x], +, \cdot) \times \ldots \times (\mathbb{Z}_{p_k^{t_k}}[x], +, \cdot)$$

Concepts of universal algebra

Definition 1. Let A be an algebra of the variety V with Ω as its set of operations and let $X = \{x_i \mid i \in I\}$ be a set of indeterminates. The set $A(X, V)$ as constructed in LN is called the ***V-polynomial algebra over A in the set of indeterminates X***. Its elements will be called ***polynomials in X over A***.

Definition 2. Let A be an algebra of the variety V. An algebra B of V containing A as a subalgebra is called a ***V-extension of A***.

Definition 3. Let V be any variety, A an algebra of V and $X = \{x_1, \ldots, x_k\}$ be a finite set of indeterminates. An ***algebraic equation over (A, V) in the indeterminates*** $x_1, \ldots, x_k$ is a pair (f, g) or shortly written

$$f = g$$

where $f, g \in A(X, V)$.

Hence we can talk of a congruence Θ_P generated by the equation $P : f = g$.

Solvable polynomial equations

Definition 4. Let B be an arbitrary V-extension of A. An element $(b_1, \ldots, b_k) \in B^k$ is called ***solution*** of the equation $f = g$ if $f(b_1, \ldots, b_k) = g(b_1, \ldots, b_k)$.

Definition 5. The equation $f = g$ is ***solvable*** if there exists a V-extension B of A such that the system has a solution in B.

Definition 6. A congruence Θ on $A(X, V)$ is called ***separating***, if $a\Theta b$ implies $a = b$ for all $a, b \in A$.

Theorem 2. *The algebraic equation $P : f = g$ over (A, V) in $X = \{x\}$ is solvable if and only if the congruence Θ_P is separating.*

Theorem 3. *Let* $f \in \mathbb{Z}_n[x]$,V *the variety of commutative rings with identity and consider the equation* $f = 0$. *Let* (f) *denote the ideal generated by* f. *TFAE:*

1. $f = 0$ *is solvable.*

2. $\nexists c \in \mathbb{Z}_n : c \neq 0$ *and* $c \in (f)$.

Definition 7. Let R be a commutative ring with identity. An element $x \in R$ is called ***unit*** if it is invertible, i.e. there exists $y \in R$ such that $x \cdot y = y \cdot x = 1$.

Theorem 4. *Let* p *be a prime,* $\alpha \in \mathbb{N}$ *and let* $f \in \mathbb{Z}_{p^\alpha}[x]$, $f \neq 0$. *Then we have*

$$f = 0 \text{ is not solvable} \Leftrightarrow f \text{ is of the form } f = k \cdot u,$$

where k *is a constant,* $k \neq 0$, *and* u *is a unit in* $\mathbb{Z}_{p^\alpha}[x]$.

Lemma 1. *Let p be a prime, $\alpha \in \mathbb{N}$ and let $a = a_0 + a_1 x + \ldots + a_n x^n$,
$b = b_0 + b_1 x + \ldots + b_m x^m \in \mathbb{Z}_{p^\alpha}[x]$. Moreover, let $c \neq 0$ be constant in $\mathbb{Z}_{p^\alpha}[x]$. Then we have*

$$a \cdot b = c \Rightarrow (a = c_1 \cdot u_1 \wedge b = c_2 \cdot u_2),$$

where c_1, c_2 are constant, $c_1 \neq 0, c_2 \neq 0$, and u_1, u_2 are units in $\mathbb{Z}_{p^\alpha}[x]$.

Remarks on zero-preserving polynomials over a ring R with $J(R)^2 = 0$

Definition 8. We denote the set of all univariate polynomial functions over R by $P(R)$ and the set $\{p \in P(R) \mid p(0) = 0\}$ of zero-preserving polynomial functions over R by $P_0(R)$.

The set of all endomorphisms on $J(R)$ will be denoted by $End(J(R))$.

Proposition 3. $\forall a, b \in I : (a - b \in I \Rightarrow p(a) - p(b) \in I)$

Lemma 2. *Let R be a ring and let $J(R)$ be its Jacobson radical. Then for all $a \in J(R)$ and for all $p \in P_0(R)$ we have: $p(a) \in J(R)$.*

Lemma 3. *Let A and B be ideals of a ring R and let AB denote the ideal product of A and B. Further, let $p \in P_0(R)$. Then for all $a \in A, b \in B$ we have:*

$$p(a) + p(b) \equiv p(a + b) \; mod \; AB$$

Proposition 4. *Let R be a ring with $J(R)^2 = 0$. Then $P_0(R)_{|_{J(R)}} \subseteq End(J(R))$.*

We define an operation $* : \mathbb{N}_0 \times R \to R$, $(m, r) \mapsto m * r := \underbrace{r + \ldots + r}_{m\,times}$.

Lemma 4. *If for all $f \in End(J(R))$ there exists a $k \in \mathbb{N}_0$ such that for all $j \in J(R)$ we have $f(j) = k*j$, then $End(J(R)) \subseteq \{\phi_k : x \mapsto k*x \mid k \in \mathbb{N}_0, x \in J(R)\} \subseteq P_0(R)_{|_{J(R)}}$.*

Proposition 5. *Let R be a ring with $J(R)^2 = 0$. If the group $(J(R), +)$ is cyclic (let's say generated by c), then $End(J(R)) \subseteq \{\phi_k : x \mapsto k * x \mid k \in \mathbb{N}_0, x \in J(R)\} \subseteq P_0(R)_{|_{J(R)}}$.*