Journal of Comprehensive Pure and Applied Mathematics

On algebraic congruence varieties over semirings

Derong Qiu

School of Mathematical Sciences, Capital Normal University, Beijing 100048, P.R.China

Article Details

Article Type: Research Article

Received date: 11^{th} September, 2024

Accepted date: 09^{th} December, 2024

Published date: 11^{th} December, 2024

***Corresponding Author**: Derong Qiu, School of Mathematical Sciences, Capital Normal University, Beijing 100048, P.R.China.

Citation:Derong, Qiu., (2024). On algebraic congruence varieties over semirings. J Compr Pure Appl Math, 2(1): 112. doi: https://doi.org/10.33790/cmap1100112.

Abstract In this paper, we develop some foundations for a theory of algebraic varieties of congruences on commutative semirings. By studying the structure of congruences, firstly, we show that the spectrum $\mathrm{Spec}^c(A)$ consisting of prime congruences on a semirings A has a Zariski topological structure; Then, for two semirings $A \subset B$, we consider the polynomial semiring $S = A[x_1, \cdots, x_n]$ and the affine $n-$space B^n. For any congruence σ on S and congruence ρ on B, we introduce the $\rho-$algebraic varieties $Z_\rho(\sigma)(B)$ in B^n, which are the set of zeros in B^n of the system of polynomial $\rho-$congruence equations given by σ. When ρ is a prime congruence, we find these varieties satisfying the axiom of closed sets, and forming a (Zariski) topology on B^n. Some results about their structures including a version of Nullstellensatz of congruences are obtained.

Keywords: Congruence of Semiring, algebraic variety, Nullstellensatz of congruences, universal algebraic geometry.

2010 Mathematics Subject Classification: (primary) 14A10, 16Y60, 08A30 (Secondary) 14A05, 14A25, 14T05, 12E12.

1. Introduction

As known, ideals are very important in studying ring structure and the polynomial equations over rings, and, in a commutative ring, the ideal and the congruence corresponds to each other equivalently. Yet, in a commutative semiring, this changes, and congruences seem to behave more natural than ideals.

Our motivation here is to consider the problem of solving polynomial equations over semirings, like the same important problem in algebraic geometry on rings. We focus on congruences, and try to develop some foundations for a theory of algebraic varieties of congruences on commutative semirings. Firstly, we study prime congruence, maximal congruence, congruence generated by a subset and a few other types congruence, and obtain some results about their structures (see Prop.2.6, 2.10, 2.12, 2.13, 2.16, 2.19, 2.21, 2.23). In particular, we show that the spectrum $\mathrm{Spec}^c(A)$ consisting of prime congruences on a semirings A has a Zariski topological structure (see Theorem 2.25). Then, for two semirings $A \subset B$, we consider the polynomial semiring $S = A[x_1, \cdots, x_n]$ and the affine $n-$space B^n. For any congruence σ on S and congruence ρ on B, we introduce the $\rho-$algebraic varieties $Z_\rho(\sigma)(B)$ in B^n, which are the set of zeros in B^n of the system of polynomial $\rho-$congruence equations given by σ (see Def.3.1). When ρ is a prime congruence, we find these varieties satisfying the axiom of closed sets, and forming a (Zariski) topology on B^n (see Theorem 3.4). Some results about their structures including a version of Nullstellensatz of congruences are obtained (see Prop.3.9, Theorems 3.7, 3.10, 3.11, 3.12).

These facts show one possible way among others to consider the problem of solving polynomial (congruence) equations in semirings, they seem to be well corresponded to the ones of classical algebraic geometry of ideals on commutative rings, yet in a different background. Also, the results of (Zariski) topology for congruences and varieties established here, might be useful in further study on some more deep questions about such as Sheaf theory, scheme on semirings.

Another possible application of this work, is about some questions in tropical geometry. One of the key connection might be the Nullstellensatz question. Recently, in the tropical setting, an analogue of Hilbert's Nullstellensatz has been extensively studied and many interesting results about it have been obtained (see, e.g., [1-7] etc.). In this paper, we provide a version of Nullstellensatz of $\rho-$algebraic varieties on semirings. For an possible application in tropical geometry, it seems that the radical of congruence used in this paper need to be improved, and we wish to consider it in a future work.

There are more general version of algebraic equations than our congruence ones considered here. When we do some work on arithmetic problems in number theory, we usually only need to consider the solution of positive integers even prime numbers. So I ask myself a question that how to work on algebraic equations if there is no subtraction? and I come to realize that the usual polynomial equations can be viewed as a special class of the general algebraic relations, which led to my consideration of the present work. In fact, I learn that this is related to the context of universal algebraic geometry and logical geometry (see, e.g., [8-12]).

Lastly, we need to give an explanation about the use of prime congruences here. Unlike working with prime ideals on rings, when we study congruences on semirings, we confront with several versions of prime congruences in the literature, and they are usually used for different purposes. The prime congruences of Def.2.1(1) below we use in this work based on our trying to find a suitable topology to do some geometry about the set of (congruence) zeros, i.e., the varieties, as shown in Theorem 3.4 below. It seems to us that not all the other version of prime congruences can satisfy our demand here.

Notation. The sign $\subset$ is used for inclusion of a subset, including the possibility of equality. When we say that A is a proper subset of $B, A \subsetneqq B$ is intended.

2. The structure of congruences

Let $(A, +, \cdot)$ be a semiring, that is, A is a non-empty set on which we have defined operations of addition and multiplication satisfying the following four conditions (see [14, p.1]): (1) $(A, +)$ is a commutative monoid with identity element 0; (2) $(A, \cdot)$ is a monoid with identity element $1 \neq 0$; (3) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ $(\forall a, b, c \in A)$; (4) $0a = 0 = a0$ $(\forall a \in A)$.

The semiring A is commutative if the monoid $(A, \cdot)$ is commutative. In the following, unless otherwise stated, the semiring always means a commutative semiring.

Now for a commutative semiring A, recall that a (binary) relation on A is a subset of $A \times A$ (see [15, p.14]), and a relation ρ of A is a congruence if it is an equivalence relation satisfying the following condition (see [14, p.4]):

$(a, b), (c, d) \in \rho \Longrightarrow (a + c, b + d) \in \rho$ and $(ac, bd) \in \rho$ $(a, b, c, d \in A)$.

So an equivalence relation ρ is a congruence on A if and only if ρ is a subsemiring of $A \times A$. The identity congruence on A is denoted by $\mathrm{id}_A = \{(a, a) : a \in A\}$. Let ρ be a congruence on A, if $\rho \neq A \times A$ then it is called a proper congruence. Obviously, ρ is not proper if and only if $(1, 0) \in \rho$. The quotient semiring of A by ρ is denoted by $\overline{A} = A/\rho$. For $c \in A$, we denote $\overline{c} = c \bmod \rho \in \overline{A}$. Moreover, for any positive integer n and subset C of A^n, where $A^n = \{(a_1, \cdots, a_n) : a_1, \cdots, a_n \in A\}$, we denote $C/\rho = \{(\overline{c_1}, \cdots, \overline{c_n}) : (c_1, \cdots, c_n) \in C\} \subset (A/\rho)^n$. For $0 \neq a \in A$, if there exists an element $0 \neq b \in A$ such that $a \cdot b = 0$, then a is called a zero divisor of A. If A contains no zero divisors, then A is called a semidomain. If A is a semidomain, and $(A \setminus \{0\}, \cdot)$ is a multiplicative group, then A is called a semifield. For example, $(\mathbb{Z}_{\geq 0}, +, \cdot)$ is a semidomain, and $(\mathbb{Q}_{\geq 0}, +, \cdot)$ is a semifield, where $\mathbb{Z}_{\geq 0}$ (resp. $\mathbb{Q}_{\geq 0}$) is the set of non-negative integers (resp. rational numbers).

Definition 2.1. Let A be a commutative semiring, and ρ be a congruence of

A such that $\rho \neq A \times A$.

(1) If ρ satisfies the following condition:

for $(a, b), (c, d) \in A \times A,\ (ac + bd, ad + bc) \in \rho \Rightarrow (a, b) \in \rho$ or $(c, d) \in \rho$.

Then ρ is called a prime congruence.

(2) If ρ satisfies the following condition:

$(ab, 0) \in \rho \Rightarrow (a, 0) \in \rho$ or $(b, 0) \in \rho \quad (a, b \in A)$.

Then ρ is called a semi-prime congruence.

(3) If ρ satisfies the following condition:

for a congruence $\tau :\ \rho \subset \tau \subset A \times A \Rightarrow \tau = \rho$ or $\tau = A \times A$.

Then ρ is called a maximal congruence.

(4) If ρ satisfies the following condition:

for $a \in A,\ (a, 0) \notin \rho \Rightarrow (ab, 1) \in \rho$ for some $b \in A$.

Then ρ is called a semi-maximal congruence.

Note that there are several other definitions for prime congruences (yet their meaning are not always the same) in the literature on semirings. The above Def.2.1(1) of prime congruences is the same as in [2, 13]. We denote

$$\mathrm{Spec}^c(A) = \{\rho :\ \rho \text{ is a prime congruence of } A\},$$

$$\mathrm{Spec}^{c'}(A) = \{\rho :\ \rho \text{ is a semi-prime congruence of } A\},$$

$$\mathrm{Max}^c(A) = \{\rho :\ \rho \text{ is a maximal congruence of } A\},$$

$$\mathrm{Max}^{c'}(A) = \{\rho :\ \rho \text{ is a semi-maximal congruence of } A\}.$$

And call $\mathrm{Spec}^c(A)$ (resp. $\mathrm{Spec}^{c'}(A), \mathrm{Max}^c(A)$ or $\mathrm{Max}^{c'}(A)$) the spectrum of prime (resp. semi-prime, maximal or semi-maximal) congruences of A. Obviously, $\mathrm{Spec}^c(A) \subset$

$\mathrm{Spec}^{c'}(A)$.

Recall that an ideal I of a commutative semiring A is a non-empty subset I of A which is closed under addition and satisfies the condition that if $a \in A$ and $b \in I$ then $ab \in I$. A prime ideal P of A is an ideal P which satisfies the condition that if $a \cdot b \in P$ then $a \in P$ or $b \in P$ $(a, b \in A)$. We denote $\mathcal{I}(A) = \{\text{all ideals of } A\}$, $\mathcal{E}(A) = \{\text{all equivalences of } A\}$ and $\mathcal{C}(A) = \{\text{all congruences of } A\}$. For any non-empty subsets S and T of A, we denote $S + T = \{s + t : \ s \in S, \ t \in T\}$, $S \cdot T = \{st : \ s \in S, \ t \in T\}$, and for $a \in A, a + S = \{a + s : \ s \in S\}$, $a \cdot S = \{as : \ s \in S\}$. For $J \in \mathcal{I}(A)$ and $\sigma \in \mathcal{C}(A)$, we denote $\rho_J = \{(a, b) \in A \times A : \ a + J = b + J\}$ and $I_\sigma = \{a \in A : \ (a, 0) \in \sigma\}$.

Lemma 2.2. Let A be a commutative semiring. We have

(1) $\rho_J \in \mathcal{C}(A)$ $(\forall J \in \mathcal{I}(A))$; (2) $I_\sigma \in \mathcal{I}(A)$ $(\forall \sigma \in \mathcal{C}(A))$;

(3) $I_{\rho_J} \subset J$ $(\forall J \in \mathcal{I}(A))$; (4) $\rho_{I_\sigma} \subset \sigma$ $(\forall \sigma \in \mathcal{C}(A))$;

(5) $J \subset J' \Rightarrow \rho_J \subset \rho_{J'}$ $(J, J' \in \mathcal{I}(A))$; (6) $\sigma \subset \tau \Rightarrow I_\sigma \subset I_\tau$ $(\sigma, \tau \in \mathcal{C}(A))$.

Proof. Follow directly from the definitions. $\square$

Note that if A is a commutative ring (obviously it is also a commutative semiring), then it is easy to see that $I_{\rho_J} = J$ and $\rho_{I_\sigma} = \sigma$ for all $J \in \mathcal{I}(A)$ and $\sigma \in \mathcal{C}(A)$. But this property changes for a commutative semiring, i.e., the inclusions in the above Lemma 2.2(3-4) may be strict in general for a commutative semiring A. For example, let $A = (\mathbb{Z}_{\geq 0}, +, \cdot)$ be the semidomain as above. Take the ideal $J = 2 \cdot \mathbb{Z}_{\geq 0} = \{2n : n \in \mathbb{Z}_{\geq 0}\}$. Then it is easy to see that $\rho_J = \mathrm{id}_A$. Hence $I_{\rho_J} = \{0\} \subsetneqq J$, i.e., $I_{\rho_J} \subsetneqq J$. Now take the congruence $\sigma = \{(a, b) \in A \times A : \ a \equiv b \pmod 2\} \neq \mathrm{id}_A$. Then by definition, $I_\sigma = \{a \in A : \ a \equiv 0 \pmod 2\} = J$. So $\rho_{I_\sigma} = \rho_J = \mathrm{id}_A \subsetneqq \sigma$, i.e., $\rho_{I_\sigma} \subsetneqq \sigma$.

From now on, we mainly study the congruences on commutative semirings.

For a congruence $\rho \neq A \times A$ on a commutative semiring A, it is easy to see that,

ρ is a semi-prime congruence $\Leftrightarrow A/\rho$ is a semidomain;

ρ is a semi-maximal congruence $\Leftrightarrow A/\rho$ is a semifield;

ρ is contained in a maximal congruence of A. In particular, A contains a maximal congruence. Obviously, a semi-maximal congruence is also a semi-prime congruence. Moreover, it is easy to see that the intersection of a family of congruences of A is also a congruence. So, for any relation R on A, there exists a unique smallest congruence of A containing R, which is the intersection of all congruences of A containing R. We denote it by R^c, and call it the congruence generated by R.

Definition 2.3. Let A be a commutative semiring. We use the operation $*$ to denote the twisted product on $A \times A$ as follows (see e.g.,[1, 2, 13]):

$$(a, b) * (c, d) = (ac + bd, ad + bc) \quad (\forall (a, b), (c, d) \in A \times A).$$

Then for every positive integer n, we define $(a, b)^{*n}$ inductively as follows:

$(a, b)^{*1} = (a, b),\ (a, b)^{*2} = (a, b) * (a, b),\ \cdots, (a, b)^{*n} = (a, b)^{*(n-1)} * (a, b)$.

We also define $(a, b)^{*0} = (1, 0)$.

Using this operation, the condition for a congruence ρ of A to be a prime congruence is as follows: $(a, b) * (c, d) \in \rho \Rightarrow (a, b) \in \rho$ or $(c, d) \in \rho$ $(a, b, c, d \in A)$.

In the following, for two non-empty subsets S and T of $A \times A$, we shall write $S * T = \{\alpha \in A \times A :\ \alpha = (a, b) * (c, d) \text{ with } (a, b) \in S, (c, d) \in T\}$.

Lemma 2.4. Let A be a commutative semiring.

(1) $*$ is associative: $((a, b) * (c, d)) * (e, f) = (a, b) * ((c, d) * (e, f))$;

(2) $*$ is commutative: $(a,b)*(c,d) = (c,d)*(a,b)$;

(3) $*$ is distributive: $((a,b)+(c,d))*(e,f) = (a,b)*(e,f)+(c,d)*(e,f)$;

(4) $(a,b)*(c,c) \in \mathrm{id}_A$;

(5) $(a,b)*(1,0) = (a,b),\ (a,b)*(0,1) = (b,a),\ (a,b)*(0,0) = (0,0)$.

(6) for positive integers n, we have

$(b,a)^{*n} = \begin{cases} (a,b)^{*n} & \text{if } 2 \mid n \\ (a,b)^{*n}*(0,1) & \text{if } 2 \nmid n. \end{cases}$ In particular, $(0,1)^{*n} = \begin{cases} (1,0) & \text{if } 2 \mid n \\ (0,1) & \text{if } 2 \nmid n. \end{cases}$

$(a,b,c,d,e,f \in A)$.

Proof. (1)$\sim$ (5) follow directly from the definitions, and (6) is proved by induction. □

Remark 2.5. Let A be a commutative semiring. Then $(A \times A, +, *)$ is a commutative semiring with additive zero $(0,0)$ and multiplicative unity $(1,0)$, and the congruences on A may connect with the ideals of $(A \times A, +, *)$.

Proposition 2.6. Let A be a commutative semiring, and n be a positive integer. Then for $(a,b),(c,d) \in A \times A$, we have

$$(a,b)^{*n} = (\sum_{2|i,\ i=0}^{n} \binom{n}{i} a^{n-i}b^i,\ \sum_{2\nmid i,\ i=1}^{n} \binom{n}{i} a^{n-i}b^i),$$

$$((a,b)+(c,d))^{*n} = (a+c,b+d)^{*n} = \sum_{i=0}^{n} \binom{n}{i} (a,b)^{*i}*(c,d)^{*(n-i)}.$$

Proof. We use induction on n. The case for $n=1$ is obvious. For the first equality, assume it holds for n, then

$$
\begin{aligned}
(a,b)^{*(n+1)} &= (a,b)*(a,b)^{*n} = (a,b)*(\sum_{2|i,\ i=0}^{n}\binom{n}{i}a^{n-i}b^{i},\ \sum_{2\nmid i,\ i=1}^{n}\binom{n}{i}a^{n-i}b^{i}) \\
&= (\sum_{2|i,\ i=0}^{n}\binom{n}{i}a^{n+1-i}b^{i}+\sum_{2\nmid i,\ i=1}^{n}\binom{n}{i}a^{n-i}b^{i+1},\ \sum_{2|i,\ i=0}^{n}\binom{n}{i}a^{n-i}b^{i+1} \\
&\qquad +\sum_{2\nmid i,\ i=1}^{n}\binom{n}{i}a^{n+1-i}b^{i}) \\
&= (\sum_{2|i,\ i=0}^{n}\binom{n+1}{i}a^{n+1-i}b^{i}+\frac{1+(-1)^{n+1}}{2}b^{n+1},\ \sum_{2\nmid i,\ i=1}^{n}\binom{n+1}{i}a^{n+1-i}b^{i} \\
&\qquad +\frac{1-(-1)^{n+1}}{2}b^{n+1}) \\
&= (\sum_{2|i,\ i=0}^{n+1}\binom{n+1}{i}a^{n+1-i}b^{i},\ \sum_{2\nmid i,\ i=1}^{n+1}\binom{n+1}{i}a^{n+1-i}b^{i}).
\end{aligned}
$$

So via the induction, the first equality holds for all positive integers n.

For the second equality, assume it holds for n, then

$$
\begin{aligned}
((a,b)+(c,d))^{*(n+1)} &= ((a,b)+(c,d))*\sum_{i=0}^{n}\binom{n}{i}(a,b)^{*i}*(c,d)^{*(n-i)} \\
&= \sum_{i=0}^{n}\binom{n}{i}(a,b)^{*(i+1)}*(c,d)^{*(n-i)}+\sum_{i=0}^{n}\binom{n}{i}(a,b)^{*i}*(c,d)^{*(n+1-i)} \\
&= \sum_{i=1}^{n+1}\binom{n}{i-1}(a,b)^{*i}*(c,d)^{*(n+1-i)}+\sum_{i=0}^{n}\binom{n}{i}(a,b)^{*i}*(c,d)^{*(n+1-i)} \\
&= \sum_{i=1}^{n}\binom{n+1}{i}(a,b)^{*i}*(c,d)^{*(n+1-i)}+\binom{n+1}{n+1}(a,b)^{*(n+1)}*(c,d)^{*0} \\
&\quad +\binom{n+1}{0}(a,b)^{*0}*(c,d)^{*(n+1)} \\
&= \sum_{i=0}^{n+1}\binom{n+1}{i}(a,b)^{*i}*(c,d)^{*(n+1-i)}.
\end{aligned}
$$

So via the induction, the second equality holds for all positive integers n. □

Definition 2.7. Let A be a commutative semiring and R be a relation of A.

We define $R_+ = \{(a,b)\in A\times A:\ (a+c,b+c)\in R \text{ for some } c\in A\}$.

Lemma 2.8. Let ρ be a congruence on a commutative semiring A. Then ρ_+ is also a congruence of A, and $\rho_+ \supset \rho$. Moreover, $(\rho_+)_+ = \rho_+$.

Proof. Follows easily from the definition. $\square$

Definition 2.9. Let ρ be a congruence on a commutative semiring A. We define a radical of ρ by

$$\sqrt{\rho} = \{(a,b) \in A \times A : (a+c, b+c)^{*n} \in \rho \text{ for some } c \in A \text{ and some positive integer } n\}.$$

This can also be defined as follows, as pointed out by an anonymous expert:

$$\sqrt{\rho} = \{(a,b) \in A \times A : (a,b)^{*n} + (c,c) \in \rho \text{ for some } c \in A \text{ and some positive integer } n\},$$

which follows from the fact that $(a+c+1, b+c+1)^{*n} = (a,b)^{*n} + (c,c) + (d,d)$ for some $d \in A$ by the binomial expansion in Prop.2.6 above (note that $(c+1, c+1)^{*n} = (c,c) + ((2^{n-1}n-1)c, (2^{n-1}n-1)c) + (e,e)$ for some $e \in A$). Obviously, $\rho \subset \sqrt{\rho}$.

Proposition 2.10. Let ρ be a congruence on a commutative semiring A. Then $\sqrt{\rho}$ is also a congruence on A. Moreover, $(\sqrt{\rho})_+ = \sqrt{\rho}$.

Proof. Firstly, $(a,b) \in \sqrt{\rho} \Leftrightarrow (b,a) \in \sqrt{\rho}$. In fact, if $(a,b) \in \sqrt{\rho}$, then $(a+c, b+c)^{*n} \in \rho$ for some $c \in A$ and some positive integer n. So $(a+c, b+c)^{*n} * (0,1) \in \rho$. Thus by Lemma 2.4 above, $(b+c, a+c)^{*n} \in \rho$, so $(b,a) \in \sqrt{\rho}$. and vice versa. Next, if $(a,b), (b,c) \in \sqrt{\rho}$, then $(a+e, b+e)^{*m} \in \rho$ and $(b+f, c+f)^{*n} \in \rho$ for some $e, f \in A$ and some positive integers m, n. Then by Lemma 2.4 and Prop.2.6

above,

$$
\begin{aligned}
&(a+e+f,b+e+f)^{*m} = ((a+e,b+e)+(f,f))^{*m}\\
&= \sum_{i=0}^{m}\binom{m}{i}(a+e,b+e)^{*i} * (f,f)^{*(m-i)}\\
&= (a+e,b+e)^{*m} + \sum_{i=0}^{m-1}\binom{m}{i}(a+e,b+e)^{*i} * (f,f)^{*(m-i)} \in \rho.
\end{aligned}
$$

Similarly, $(b+e+f,c+e+f)^{*n} \in \rho$. Write $t = e+f$, then $(a+t,b+t)^{*m},\ (b+t,c+t)^{*n} \in \rho$. Write $s = b+2t \in A$ and $k = m+n$. For $i = 0,1,\cdots,k$, if $i \geq m$, then $(a+t,b+t)^{*i} = (a+t,b+t)^{*m} * (a+t,b+t)^{*(i-m)} \in \rho$. If $i < m$, then $k-i > k-m = n$, so $(b+t,c+t)^{*(k-i)} = (b+t,c+t)^{*n} * (b+t,c+t)^{*(k-i-n)} \in \rho$. Then

$$
\begin{aligned}
&(a+s,c+s)^{*k} = ((a+t,b+t)+(b+t,c+t))^{*k}\\
&= \sum_{i=0}^{k}\binom{k}{i}(a+t,b+t)^{*i} * (b+t,c+t)^{*(k-i)} \in \rho.
\end{aligned}
$$

So $(a,c) \in \sqrt{\rho}$. Also $\mathrm{id}_A \subset \rho \subset \sqrt{\rho}$. Therefore, $\sqrt{\rho}$ is an equivalence relation of A. Next, let $(a,b),(c,d) \in \sqrt{\rho}$. Then by definition, $(a+e,b+e)^{*m} \in \rho$ and $(c+f,d+f)^{*n} \in \rho$ for some $e,f \in A$ and some positive integers m,n. Write $k = m+n$. By Prop.2.6 above, $((a+e,b+e)+(c+f,d+f))^{*k} = \sum_{i=0}^{k}\binom{k}{i}(a+e,b+e)^{*i} * (c+f,d+f)^{*(k-i)}$. For $i = 0,1,\cdots,k$, if $i \geq m$, then $(a+e,b+e)^{*i} = (a+e,b+e)^{*m} * (a+e,b+e)^{*(i-m)} \in \rho$; if $i < m$, then $k-i > k-m = n$, so $(c+f,d+f)^{*(k-i)} = (c+f,d+f)^{*n} * (c+f,d+f)^{*(k-i-n)} \in \rho$, which implies that $((a+e,b+e)+(c+f,d+f))^{*k} \in \rho$, i.e., $((a+c+e+f,b+d+e+f))^{*k} \in \rho$. So $(a+c,b+d) \in \sqrt{\rho}$, i.e., $(a,b)+(c,d) \in \sqrt{\rho}$. The remainder is to show that $(a,b) \in \sqrt{\rho} \Rightarrow (ac,bc) \in \sqrt{\rho}$ $(\forall c \in A)$. Indeed, $(a,b) \in \sqrt{\rho} \Rightarrow (a+e,b+e)^{*n} \in \rho$ for some $e \in A$ and some positive integer n. Then by Prop.2.6 above,

$$\begin{aligned}
&((a+e)c,(b+e)c)^{*n} \\
&= (\sum_{2|i,\ i=0}^{n} \binom{n}{i} ((a+e)c)^{n-i} \cdot ((b+e)c)^{i},\ \sum_{2\nmid i,\ i=1}^{n} \binom{n}{i} ((a+e)c)^{n-i} \cdot ((b+e)c)^{i}) \\
&= c^n \cdot (\sum_{2|i,\ i=0}^{n} \binom{n}{i} (a+e)^{n-i} \cdot (b+e)^{i},\ \sum_{2\nmid i,\ i=1}^{n} \binom{n}{i} (a+e)^{n-i} \cdot (b+e)^{i}) \\
&= c^n \cdot (a+e,b+e)^{*n} \in \rho \text{ (here we write } x \cdot (y,z) = (xy,xz)\ (\forall x,y,z \in A)),
\end{aligned}$$

so $(ac+ec, bc+ec)^{*n} \in \rho$, hence $(ac,bc) \in \sqrt{\rho}$. Therefore, $\sqrt{\rho}$ is a congruence. To show that $(\sqrt{\rho})_+ = \sqrt{\rho}$, firstly, by Lemma 2.8 above, $\sqrt{\rho} \subset (\sqrt{\rho})_+$. Conversely, if $(a,b) \in (\sqrt{\rho})_+$, then $(a+c,b+c) \in \sqrt{\rho}$ for some $c \in A$. So $(a+c+d,b+c+d)^{*n} \in \rho$ for some $d \in A$ and some positive integer n, i.e., $(a+e,b+e)^{*n} \in \rho$ with $e = c+d \in A$, so $(a,b) \in \sqrt{\rho}$, and so $(\sqrt{\rho})_+ \subset \sqrt{\rho}$. Therefore $(\sqrt{\rho})_+ = \sqrt{\rho}$, and the proof is completed. $\square$

Definition 2.11. Let A and ρ be as in Def.2.9 above.

(1) If $\sqrt{\rho} = \rho$, then ρ is called to be a radical congruence on A.

(2) If $\sqrt{\rho} = \rho_+$, then ρ is called to be a quasi-radical congruence on A.

(3) Denote $R_{\text{nil}}(A) = \{(a,b) \in A \times A :\ (a,b)^{*n} \in \text{id}_A \text{ for some positive integer } n\}$ and $\rho_{\text{nil}}(A) = R_{\text{nil}}(A)_+$, then $\rho_{\text{nil}}(A) = \sqrt{\text{id}_A}$, and $\rho_{\text{nil}}(A)$ is called to be the nilpotent congruence of A.

Proposition 2.12. Let A be a commutative semiring. Let ρ, ρ_1 and ρ_2 be congruences on A.

(1) $\rho_1 \subset \rho_2 \Rightarrow \sqrt{\rho_1} \subset \sqrt{\rho_2}$ and $(\rho_1)_+ \subset (\rho_2)_+$. (2) $\rho_+ \subset \sqrt{\rho}$.

(3) $\sqrt{\sqrt{\rho}} = \sqrt{\rho} = \sqrt{\rho_+}$. Particularly, $\sqrt{\rho}$ is a radical congruence on A.

(4) $(a,b),\ (b,c) \in R_{\text{nil}}(A) \Rightarrow (a,c)^{*k} + (e,e) \in \text{id}_A$ for some $e \in A$ and some

positive integer k.

(5) If ρ is a prime congruence, then $\sqrt{\rho} = \rho_+$, i.e., ρ is a quasi-radical congruence. If the prime congruence ρ satisfies $\rho = \rho_+$, then ρ is a radical congruence.

Proof. (1) and (2) follow directly from the definitions.

(3) Since $\rho \subset \sqrt{\rho}$, we only need to show that $\sqrt{\sqrt{\rho}} \subset \sqrt{\rho}$. Let $(a,b) \in \sqrt{\sqrt{\rho}}$, then $(a,b)^{*n} + (c,c) \in \sqrt{\rho}$ for some $c \in A$ and some $n \in \mathbb{Z}_{>0}$. So $((a,b)^{*n} + (c,c))^{*m} + (d,d) \in \rho$ for some $d \in A$ and some $m \in \mathbb{Z}_{>0}$. By the binomial expansion in Prop.2.6 above, we get $((a,b)^{*n} + (c,c))^{*m} = (a,b)^{*(mn)} + (e,e)$ with $e \in A$, which implies $(a,b) \in \sqrt{\rho}$, so $\sqrt{\sqrt{\rho}} = \sqrt{\rho}$. Also $\rho \subset \rho_+ \subset \sqrt{\rho}$, so $\sqrt{\rho} \subset \sqrt{\rho_+} \subset \sqrt{\sqrt{\rho}}$, and so $\sqrt{\rho_+} = \sqrt{\rho}$.

(4) Follows from the above Prop.2.6 and Lemma 2.4.

(5) Follows from the definition. The proof is completed. $\square$

Recall that the semiring A satisfies the additive annihilation law if $a + c = b + c \Rightarrow a = b$ $(a, b, c \in A)$. For example, $(\mathbb{Z}_{\geq 0}, +, \cdot)$ satisfies the additive annihilation law.

Proposition 2.13. Let A be a commutative semiring satisfying the additive annihilation law. Then $\rho_{\text{nil}}(A) = R_{\text{nil}}(A)$, and $\rho_{\text{nil}}(A/\rho_{\text{nil}}(A)) = \text{id}$.

Proof. Follows from the above Prop.2.6 and Prop.2.10. $\square$

For a commutative semiring A, if $R_{\text{nil}}(A) = \text{id}_A$, then A is called to be reduced. If $\rho_{\text{nil}}(A) = \text{id}_A$, then A is called to be strongly reduced. obviously, strongly reduced $\Rightarrow$ reduced. We denote $\mathfrak{N}_c(A) = R_{\text{nil}}(A)^c$, which is the congruence of A generated by the relation $R_{\text{nil}}(A)$, and call $\mathfrak{N}_c(A)$ the quasi-nilpotent congruence of A. Obviously, $\rho_{\text{nil}}(A) \supset \mathfrak{N}_c(A)$, also, A is reduced if and only if $\mathfrak{N}_c(A) = \text{id}_A$.

Now for two relations R and R' on a non-empty set S, recall that their product

$$R \circ R' = \{(a, c) \in S \times S :\ \exists\ b \in S \text{ such that } (a, b) \in R \text{ and } (b, c) \in R'\},$$

and the inverse $R^{-1} = \{(a, b) \in S \times S :\ (b, a) \in R\}$ (see [15, pp.14, 15]). Obviously, for relations $R, R_1, \cdots, R_n, R', R''$ on S, one has $(R^{-1})^{-1} = R$; $(R_1 \circ \cdots \circ R_n)^{-1} = R_n^{-1} \circ \cdots \circ R_1^{-1}$; $R \subset R' \Rightarrow R^{-1} \subset R'^{-1}$, $R \circ R'' \subset R' \circ R''$ and $R'' \circ R \subset R'' \circ R'$. As in [15], for any relation R on S, we denote its transitive closure by R^∞, which is defined by $R^\infty = \cup_{n=1}^\infty R^n$, where $R^n = \underbrace{R \circ \cdots \circ R}_{n}$. It is well known that R^∞ is the smallest transitive relation on S containing R (see [15, p.20]). Also, we denote by R^e the equivalence on S generated by R, i.e., the smallest equivalence on S containing R. Then $R^e = (R \cup R^{-1} \cup \mathrm{id}_S)^\infty$ (see [15, p.20]). Moreover, $(x, y) \in R^e \Leftrightarrow x = y$ or for some positive integer n there exists a sequence $x = z_1 \to z_2 \to \cdots \to z_n = y$ in which for each $i \in \{1, 2, \cdots, n-1\}$ either $(z_i, z_{i+1}) \in R$ or $(z_{i+1}, z_i) \in R$ (see [15, p.21]).

Definition 2.14. Let A be a commutative semiring, R be a relation on A, and E be an equivalence relation on A. We define the relations

$$R^L = \{(ax + y, bx + y) :\ (a, b) \in R, x, y \in A\}, \text{ and}$$

$$E^\flat = \{(a, b) \in A \times A :\ (ax + y, bx + y) \in E \text{ for all } x, y \in A\}.$$

Since $0, 1 \in A$, we have $R \subset R^L$. Also, $\rho^L = \rho$ for any congruence ρ of A.

Lemma 2.15. Let A be a commutative semiring, R_1 and R_2 be two relations on A, and E be an equivalence relation on A. We have

(1) $R_1 \subset R_1^L$; (2) $(R_1^L)^{-1} = (R_1^{-1})^L$; (3) $R_1 \subset R_2 \Rightarrow R_1^L \subset R_2^L$;

(4) $(R_1^L)^L = R_1^L$; (5) $(R_1 \cup R_2)^L = R_1^L \cup R_2^L$;

(6) $R_1 = R_1^L$ if and only if R_1 satisfies the following condition:

$(a, b) \in R_1 \Rightarrow (ax, bx), (a + y, b + y) \in R_1$ $(\forall x, y \in A)$.

(7) $R_1 = R_1^L \Rightarrow R_1^n = (R_1^n)^L$ for all positive integer n.

(8) $E^\flat$ is the largest congruence on A contained in E.

Proof. Follow easily from the definitions. $\square$

Proposition 2.16. Let R be a relation on a commutative semiring A. Then $R^c = (R^L)^e$, where R^c is the congruence of A generated by R as before.

Proof. By definition, $(R^L)^e$ is the equivalence on A generated by R^L. Denote $S = R^L \cup (R^L)^{-1} \cup \mathrm{id}_A$, then $(R^L)^e = S^\infty$ (see [15, p.20]). By Lemma 2.15 above, $S = (R \cup R^{-1} \cup \mathrm{id}_A)^L$, so $S^L = S$, and so $S^n = (S^n)^L$ for all positive integers n. Now for any $(a, b) \in (R^L)^e$, by the above discussion, $(a, b) \in S^n$ for some positive integer n. Since $S^n = (S^n)^L$, by Lemma 2.15 above, $(ax, bx) \in S^n$ and $(a + y, b + y) \in S^n$, hence $(ax, bx), (a+y, b+y) \in (R^L)^e$ $(\forall x, y \in A)$. In particular, if $(a, b), (c, d) \in (R^L)^e$, then $(a + c, b + c) \in (R^L)^e$ and $(b + c, b + d) \in (R^L)^e$, so $(a + c, b + d) \in (R^L)^e$. Hence $(R^L)^e$ is a congruence of A containing R. Now let ρ be a congruence of A containing R. Then by Lemma 2.15 above, $R^L \subset \rho^L = \rho$. So $(R^L)^e \subset \rho^e = \rho$, which shows that $R^c = (R^L)^e$, and the proof is completed. $\square$

Corollary 2.17. Let R be a relation on a commutative semiring A. Then for $a, b \in A, (a, b) \in R^c$ if and only if $a = b$ or for some positive integer n there exists a sequence $a = z_1 \to z_2 \to \cdots \to z_n = b$ in which for each $i \in \{1, 2, \cdots, n-1\}$ either $(z_i, z_{i+1}) \in R^L$ or $(z_{i+1}, z_i) \in R^L$.

Proof. Follows from the above Prop.2.16 (see [15, p.21]). $\square$

Let R and ρ be a relation and a congruence on a commutative semiring A, respectively. Recall that $R/\rho = \{(a\rho, b\rho) : (a,b) \in R\} = \{(\overline{a}, \overline{b}) \in A/\rho \times A/\rho : (a,b) \in R\}$ is a relation on the quotient semiring $\overline{A} = A/\rho$. If $\mathrm{id}_A \subset R \subset \rho$, then $R/\rho = \mathrm{id}_{\overline{A}}$.

Corollary 2.18. Let R and ρ be a relation and a congruence on a commutative semiring A, respectively. Then $R^c/\rho = (R/\rho)^c$ on $\overline{A} = A/\rho$.

Proof. Follows from the above Cor.2.17. $\square$

For a commutative semiring A, recall that $\mathcal{E}(A)$ and $\mathcal{C}(A)$ denote the set of all equivalences and the set of all congruences on A, respectively. It is known that both $(\mathcal{E}(A), \subset, \wedge, \vee)$ and $(\mathcal{C}(A), \subset, \wedge, \vee)$ are complete lattices (for lattice, see e.g.,[15, p.12]): if $\rho, \sigma \in \mathcal{E}(A)$, then $\rho \wedge \sigma = \rho \cap \sigma$ is their intersection, while $\rho \vee \sigma = (\rho \cup \sigma)^e$. Similarly, for $\rho, \sigma \in \mathcal{C}(A), \rho \wedge \sigma = \rho \cap \sigma$ and $\rho \vee \sigma = (\rho \cup \sigma)^c = ((\rho \cup \sigma)^L)^e = (\rho \cup \sigma)^e$ follows by Lemma 2.15 and Prop.2.16 above. So the join of ρ and σ in $\mathcal{C}(A)$ coincides with their join in $\mathcal{E}(A)$. Both $\mathcal{E}(A)$ and $\mathcal{C}(A)$ have the maximum element $A \times A$ and minimum element id_A.

Proposition 2.19. Let ρ and σ be two congruences on a commutative semiring A. Then $\rho \vee \sigma = (\rho \circ \sigma)^\infty$. In other words, for $a, b \in A$, $(a,b) \in \rho \vee \sigma$ if and only if for some positive integer n there exist elements $x_1, x_2, \cdots, x_{2n-1} \in A$ such that $(a, x_1) \in \rho, (x_1, x_2) \in \sigma, (x_2, x_3) \in \rho, \cdots, (x_{2n-2}, x_{2n-1}) \in \rho, (x_{2n-1}, b) \in \sigma$.

Proof. Follows from Prop.2.16 above. $\square$

Corollary 2.20. If ρ and σ are two congruences on a commutative semiring A satisfying $\rho \circ \sigma = \sigma \circ \rho$. Then $\rho \vee \sigma = \rho \circ \sigma$.

Proof. Follows from Prop.2.19 above. $\square$

For example, if A is a semifield and $\rho, \sigma \in \mathcal{C}(A)$, then $\rho \circ \sigma = \sigma \circ \rho$, so $\rho \vee \sigma = \rho \circ \sigma$.

Proposition 2.21. Let A be a commutative semiring. For $a, b \in A$, denote $R(a,b) = \{(ax+by+z, bx+ay+z) : x, y, z \in A\} = (a,b) * (A \times A) + \mathrm{id}_A$. Then $R(a,b)_+$ (as defined in Def.2.7 above) is a congruence on A, and $R(a,b) \subset \rho \subset R(a,b)_+ \subset \rho_+$ with $\rho = \{(a,b)\}^c$.

Proof. Obviously, $\mathrm{id}_A \subset R(a,b)_+$. Also, if $(u,v) \in R(a,b)_+$, then $(u+s, v+s) \in R(a,b)$ for some $s \in A$, so $(u+s, v+s) = (ax+by+z, bx+ay+z)$ for some $x, y, z \in A$, so $(v+s, u+s) = (ay+bx+z, by+ax+z) \in R(a,b)$, so $(v,u) \in R(a,b)_+$. Now let $(u,v), (v,w) \in R(a,b)_+$. Then $(u+s, v+s), (v+t, w+t) \in R(a,b)$ for some $s, t \in A$, so $(u+s, v+s) = (ax+by+z, bx+ay+z)$ and $(v+t, w+t) = (ax'+by'+z', bx'+ay'+z')$ for some $x, y, z, x', y', z' \in A$. Then $(u+s+t, v+s+t) = (ax+by+z+t, bx+ay+z+t)$, and $(v+s+t, w+s+t) = (ax'+by'+z'+s, bx'+ay'+z'+s)$. Write $d = v+s+t = bx+ay+z+t = ax'+by'+z'+s$, then $u+s+t+d = a(x+x')+b(y+y')+z+z'+s+t$, and $w+s+t+d = b(x+x')+a(y+y')+z+z'+s+t$. So $(u+s+t+d, w+s+t+d) \in R(a,b)$, and so $(u,w) \in R(a,b)_+$. Therefore, $R(a,b)_+$ is an equivalence on A. Next, let $(u,v), (u',v') \in R(a,b)_+$, then $(u+s, v+s), (u'+s', v'+s') \in R(a,b)$ for some $s, s' \in A$. So $(u+s, v+s) = (ax+by+z, bx+ay+z)$ and $(u'+s', v'+s') = (ax'+by'+z', bx'+ay'+z')$ for some $x, y, z, x', y', z' \in A$. Hence $(u+u'+s+s', v+v'+s+s') = (a(x+x')+b(y+y')+z+z', b(x+x')+a(y+y')+z+z') \in R(a,b)$, so $(u,v)+(u',v') = (u+u', v+v') \in R(a,b)_+$. Moreover, for $(u,v), s, x, y, z$ above, let $t \in A$, then $(ut+st, vt+st) = (a(tx)+b(ty)+tz, b(tx)+a(ty)+tz) \in R(a,b)$, so $(ut, vt) \in R(a,b)_+$. Therefore, $R(a,b)_+$ is a congruence on A. The inclusion $R(a,b) \subset \rho$ follows from Cor.2.5 above. The remainder can be verified directly, and the proof is completed. $\square$

Lemma 2.22. Let A be a commutative semiring and ρ be a congruence on A. let $(a,b),(c,d) \in A \times A$ and $c = z_1 \to z_2 \to \cdots \to z_n = d$ $(n \geq 2)$ be a sequence in A. If $(a,b) * (z_i, z_{i+1}) \in \rho_+$ for all $i \in \{1,2,\cdots,n-1\}$, then $(a,b)*(c,d) \in \rho_+$.

Proof. By Lemma 2.8 above, ρ_+ is a congruence on A, and $(\rho_+)_+ = \rho_+$. Write $t = az_2 + bz_2$, then from $(a,b)*(z_1,z_2) \in \rho_+$ and $(a,b)*(z_2,z_3) \in \rho_+$, we have $(az_1 + bz_3 + t, az_3 + bz_1 + t) = (a,b)*(z_1,z_2) + (a,b)*(z_2,z_3) \in \rho_+$, so $(az_1 + bz_3, az_3 + bz_1) \in (\rho_+)_+ = \rho_+$, i.e., $(a,b)*(z_1,z_3) \in \rho_+$. Then, from $(a,b)*(z_1,z_3) \in \rho_+$ and $(a,b)*(z_3,z_4) \in \rho_+$, we also have $(a,b)*(z_1,z_4) \in \rho_+$, and so on. After finite steps, we get $(a,b)*(z_1,z_n) \in \rho_+$, i.e., $(a,b)*(c,d) \in \rho_+$. The proof is completed. $\square$

Proposition 2.23. Let A be a commutative semiring and ρ be a maximal congruence on A. If $\rho = \rho_+$, then ρ is also a prime congruence.

Proof. Let $(a,b),(c,d) \in A \times A$ be such that $(a,b)*(c,d) \in \rho$. If $(c,d) \notin \rho$, then we need to show that $(a,b) \in \rho$. To see this, let $R = \{(c,d)\} \cup \rho$, then R is a relation on A and $R \supsetneqq \rho$. So $R^c \supsetneqq \rho$, and so $R^c = A \times A$ because ρ is maximal. In particular, $(1,0) \in R^c$. By Cor.2.17 above, there exists a sequence $1 = z_1 \to z_2 \to \cdots \to z_n = 0$ in which for each $i \in \{1,2,\cdots,n-1\}$ either $(z_i, z_{i+1}) \in R^L$ or $(z_{i+1}, z_i) \in R^L$. By Lemma 2.15 above, $R^L = (\{(c,d)\} \cup \rho)^L = \{(c,d)\}^L \cup \rho^L = \{(c,d)\}^L \cup \rho$ because $\rho^L = \rho$. By definition, $\{(c,d)\}^L = \{(cx + y, dx + y) : x, y \in A\}$. So $R^L = \{(cx + y, dx + y) : x, y \in A\} \cup \rho$. As above, for each $i \in \{1,2,\cdots,n-1\}$ either $(z_i, z_{i+1}) \in R^L$ or $(z_{i+1}, z_i) \in R^L$. If $(z_i, z_{i+1}) \in R^L$, then $(z_i, z_{i+1}) \in \rho$ or $(z_i, z_{i+1}) = (cx_i + y_i, dx_i + y_i)$ for some $x_i, y_i \in A$. If $(z_i, z_{i+1}) \in \rho$, then $(a,b)*(z_i,z_{i+1})\in\rho$. If $(z_i,z_{i+1})=(cx_i+y_i,dx_i+y_i)$, write $t=ay_i+by_i\in A$, then $(a,b)*(z_i,z_{i+1})=(a,b)*(cx_i+y_i,dx_i+y_i)=(acx_i+bdx_i+t,adx_i+bcx_i+t)=((a,b)*(c,d))\cdot(x_i,x_i)+(t,t)\in\rho$. So $(z_i,z_{i+1})\in R^L\Rightarrow(a,b)*(z_i,z_{i+1})\in\rho$.

Similarly, $(z_{i+1},z_i)\in R^L\Rightarrow(a,b)*(z_{i+1},z_i)\in\rho$.

Note that $(a,b)*(z_{i+1},z_i)=((a,b)*(z_i,z_{i+1}))*(0,1)$. So the above discussion shows that $(a,b)*(z_i,z_{i+1})\in\rho$ for all $i\in\{1,2,\cdots,n-1\}$. By our assumption, $\rho=\rho_+$. Hence by Lemma 2.22 above, we get $(a,b)*(1,0)=(a,b)*(z_1,z_n)\in\rho$, i.e., $(a,b)\in\rho$. Therefore, ρ is a prime congruence on A, and the proof is completed. □

A question. Is a maximal congruence in a commutative semiring always prime?

As known, in [2] it is shown that maximal congruences are always prime in an additively idempotent semiring.

Definition 2.24. Let A be a commutative semiring and σ be a congruence on A. We define $V^{\mathrm{co}}(\sigma)=\{\rho\in\mathrm{Spec}^c(A):\ \rho\supset\sigma\}$.

Theorem 2.25. Let A be a commutative semiring.

(1) If σ_1 and σ_2 are two congruences on A, then $V^{\mathrm{co}}(\sigma_1)\cup V^{\mathrm{co}}(\sigma_2)=V^{\mathrm{co}}(\sigma_1\cap\sigma_2)$.

(2) If $\{\sigma_\alpha\}_{\alpha\in\Lambda}$ is a family of congruences on A, then $\cap_{\alpha\in\Lambda}V^{\mathrm{co}}(\sigma_\alpha)=V^{\mathrm{co}}(\sigma)$, where $\sigma=(\cup_{\alpha\in\Lambda}\sigma_\alpha)^c$ is the congruence on A generated by the set $\cup_{\alpha\in\Lambda}\sigma_\alpha$.

(3) $V^{\mathrm{co}}(\mathrm{id}_A)=\mathrm{Spec}^c(A)$ and $V^{\mathrm{co}}(A\times A)=\emptyset$.

Proof. (1) Since $\sigma_1\cap\sigma_2\subset\sigma_i$ $(i=1,2)$, $V^{\mathrm{co}}(\sigma_1\cap\sigma_2)\supset V^{\mathrm{co}}(\sigma_i)$ $(i=1,2)$, so $V^{\mathrm{co}}(\sigma_1\cap\sigma_2)\supset V^{\mathrm{co}}(\sigma_1)\cup V^{\mathrm{co}}(\sigma_2)$. Conversely, if $\rho\in V^{\mathrm{co}}(\sigma_1\cap\sigma_2)$, then $\rho\supset\sigma_1\cap\sigma_2$. If $\rho\not\supset\sigma_1$, equivalently, $\rho\notin V^{\mathrm{co}}(\sigma_1)$, then there exists an element $(a,b)\in\sigma_1$, but $(a,b) \notin \rho$. Now for any $(c,d) \in \sigma_2$, we have $(ac,ad) \in \sigma_2$. Also $(d,c) \in \sigma_2$, so $(bd,bc) \in \sigma_2$, and then $(ac+bd, ad+bc) \in \sigma_2$, i.e., $(a,b)*(c,d) \in \sigma_2$, also $(a,b)*(c,d) \in \sigma_1$, so $(a,b)*(c,d) \in \sigma_1 \cap \sigma_2 \subset \rho$, which implies that $(c,d) \in \rho$ because ρ is prime. So $\sigma_2 \subset \rho$, i.e., $\rho \in V^{\mathrm{co}}(\sigma_2)$. This shows that $V^{\mathrm{co}}(\sigma_1 \cap \sigma_2) \subset V^{\mathrm{co}}(\sigma_1) \cup V^{\mathrm{co}}(\sigma_2)$, and the equality holds.

(2) $\rho \in \cap_{\alpha\in\Lambda} V^{\mathrm{co}}(\sigma_\alpha) \Leftrightarrow \rho \in V^{\mathrm{co}}(\sigma_\alpha)$ $(\forall \alpha \in \Lambda) \Leftrightarrow \rho \supset \sigma_\alpha$ $(\forall \alpha \in \Lambda) \Leftrightarrow \rho \supset \cup_{\alpha\in\Lambda}\sigma_\alpha \Leftrightarrow \rho \in V^{\mathrm{co}}(\sigma)$ with $\sigma = (\cup_{\alpha\in\Lambda}\sigma_\alpha)^c$.

(3) Obvious. The proof is completed. □

From Theorem 2.25 above, the set of $V^{\mathrm{co}}(\sigma)$ for all congruences σ on A satisfies the axiom of closed subsets, and give a topology on $\mathrm{Spec}^c(A)$, which is called the Zariski topology on $\mathrm{Spec}^c(A)$. A subset of $\mathrm{Spec}^c(A)$ is equipped with the subspace topology induced from the Zariski topology on $\mathrm{Spec}^c(A)$. In the following section, a (Zariski) topology will also be constructed for the congruence algebraic varieties.

3. Zeros of polynomial congruence equations

Let A and B be two commutative semirings with $A \subset B$. Let $A[x_1, \cdots, x_n]$ be the commutative semiring of polynomials in n variables over A (see [14, p.3]). Let $B^n = \{(b_1, \cdots, b_n) : \; b_1, \cdots, b_n \in B\}$ be the affine $n-$space over B. An element $P \in B^n$ will be called a point, and if $P = (b_1, \cdots, b_n)$ with $b_i \in B$, then the b_i will be called the coordinates of P.

Definition 3.1. For the commutative semirings $A \subset B$ as above, write $S = A[x_1, \cdots, x_n]$. let $T \subset S \times S$ be a non-empty subset, and let ρ be a congruence on B. Then we define

$$Z_\rho(T)(B) = \{P \in B^n : \ (f(P), g(P)) \in \rho \text{ for all } (f, g) \in T\},$$

and call $Z_\rho(T)(B)$ the $\rho-$zero set of T in B^n. In particular, if $\rho = \mathrm{id}_B$ is the identity congruence on B, then $Z_\rho(T)(B)$ is the set of solutions (i.e. common zeros) of the system of polynomial equations $\{f = g \ (\forall \ (f, g) \in T)\}$ in B^n. In the following, we will call $\{(f, g) \in \rho \ (\forall \ (f, g) \in T)\}$ a system of polynomial $\rho-$equations. A subset Y of B^n will be called an $\rho-$algebraic variety over A if there exists a non-empty subset $T \subset S \times S$ such that $Y = Z_\rho(T)(B)$.

Remark 3.2. The motivation here comes from algebraic varieties (see [16, Chapter 1]). As we know, one of the main problem of algebraic geometry is to solve polynomial equations in rings. Let A and B be two commutative rings with $A \subset B$, $\{f_\alpha\}_{\alpha \in \Lambda} \subset A[x_1, \cdots, x_n]$, the solutions in B^n of the system of polynomial equations $f_\alpha = 0$ $(\alpha \in \Lambda)$ is then the set $Z(f_\alpha)_{\alpha \in \Lambda}(B) = \{P \in B^n : \ f_\alpha(P) = 0 \ (\forall \alpha \in \Lambda)\}$ (see [16, p.2, 17, p.10]). By using the identity congruence id_B on B, this set can be rewritten as $Z(f_\alpha)_{\alpha \in \Lambda}(B) = \{P \in B^n : \ (f_\alpha(P), 0) \in \mathrm{id}_B \ (\forall \alpha \in \Lambda)\}$. So it is natural to consider the polynomial questions in semirings, in a sense of congruence, generalizing the identity congruence (i.e. equality), as stated in the above Def.3.1. Note that, in a ring, the equation $f = g$ can be always changed to be $f - g = 0$, i.e., the form $h = 0$. The case for the system of polynomial equations $(f_\alpha = g_\alpha)_{\alpha \in \Lambda}$ is similar. But, this is not true in a semiring, because usually there is no subtraction in a semiring. One can also consider the polynomial congruence equations or other related congruence equations in non-commutative semirings, yet it may be more complicated. Here we only consider the case of commutative semirings.

Lemma 3.3. Let A, B, ρ and $S = A[x_1, \cdots, x_n]$ be as in Def.3.1 above. Assume $\rho \neq B \times B$. Then we have

(1) $Z_\rho((0,1))(B) = \emptyset$, and $Z_\rho((f,f))(B) = B^n$ $(\forall f \in S)$.

(2) Let T_1 and T_2 be two non-empty subsets of $S \times S$, then

$Z_\rho(T_1)(B) \cup Z_\rho(T_2)(B) \subset Z_\rho(T_1 * T_2)(B)$, where $T_1 * T_2$ is defined as Def.2.3 above.

(3) The intersection of any family of $\rho-$algebraic varieties is an $\rho-$algebraic variety.

Proof. (1) Obvious.

(2) Let $P \in Z_\rho(T_1)(B)$, then $(f_1(P), g_1(P)) \in \rho$, also $(g_1(P), f_1(P)) \in \rho$ $(\forall (f_1, g_1) \in T_1)$. Now for any $\alpha \in T_1 * T_2$, by definition, $\alpha = (f_1, g_1) * (f_2, g_2)$ for some $(f_1, g_1) \in T_1$ and $(f_2, g_2) \in T_2$. So $\alpha(P) = (f_1(P), g_1(P)) * (f_2(P), g_2(P)) = (f_1(P)f_2(P) + g_1(P)g_2(P), f_1(P)g_2(P) + f_2(P)g_1(P)) = f_2(P)(f_1(P), g_1(P)) + g_2(P)(g_1(P), f_1(P)) \in \rho$, and so $P \in Z_\rho(T_1 * T_2)(B)$, which shows that $Z_\rho(T_1)(B) \subset Z_\rho(T_1 * T_2)(B)$. Similarly $Z_\rho(T_2)(B) \subset Z_\rho(T_1 * T_2)(B)$.

(3) If $Y_\alpha = Z_\rho(T_\alpha)(B)$ is any family of $\rho-$algebraic varieties, then $\cap Y_\alpha = Z_\rho(\cup T_\alpha)(B)$, so $\cap Y_\alpha$ is also an $\rho-$algebraic variety, and the proof is completed. $\square$

Theorem 3.4. Let A, B and $S = A[x_1, \cdots, x_n]$ be as in Def.3.1 above. If $\rho \in \mathrm{Spec}^c(B)$ is a prime congruence on B, then for the $\rho-$algebraic varieties in B^n over A, we have

(1) The union of two $\rho-$algebraic varieties is an $\rho-$algebraic variety;

(2) The intersection of any family of $\rho-$algebraic varieties is an $\rho-$algebraic variety;

(3) The empty set $\emptyset$ and B^n are $\rho-$algebraic varieties.

Proof. (1) If $Y_1 = Z_\rho(T_1)(B)$ and $Y_2 = Z_\rho(T_2)(B)$ for some $T_1, T_2 \subset S \times S$, then by Lemma 3.3 above, $Y_1 \cup Y_2 \subset Z_\rho(T_1 * T_2)(B)$. Conversely, if $P \in Z_\rho(T_1 * T_2)(B)$, and $P \notin Y_1$, then there is an element $(f_1, g_1) \in T_1$ such that $(f_1(P), g_1(P)) \notin \rho$. On the other hand, for any $(f_2, g_2) \in T_2$, we have $(f_1, g_1) * (f_2, g_2) \in T_1 * T_2$, so $((f_1, g_1) * (f_2, g_2))(P) \in \rho$, i.e., $(f_1(P), g_1(P)) * (f_2(P), g_2(P)) \in \rho$, which implies that $(f_2(P), g_2(P)) \in \rho$ since ρ is a prime congruence, so that $P \in Y_2$. Therefore $Y_1 \cup Y_2 = Z_\rho(T_1 * T_2)(B)$ is an $\rho-$algebraic variety.

(2) and (3) follow from Lemma 3.3 above, and the proof is completed. □

Definition 3.5. Let A, B and $S = A[x_1, \cdots, x_n]$ be as in Def.3.1 above. If $\rho \in \text{Spec}^c(B)$ is a prime congruence on B, then by Theorem 3.4 above, the set of all $\rho-$algebraic varieties in B^n over A satisfies the axiom of closed subsets, and give a topology $\tau_{\rho,A}$ on B^n, i.e., a subset X of B^n is open in $\tau_{\rho,A}$ if and only if its complement $B^n \setminus X$ is an $\rho-$algebraic variety. $\tau_{\rho,A}$ will be called the Zariski $\rho-$topology on B^n. For such ρ, a subset of B^n is equipped with the subspace topology induced from $\tau_{\rho,A}$. An $\rho-$algebraic variety X of B^n is irreducible if it can not be expressed as the union $X = X_1 \cup X_2$ of two proper subsets, each one of which is closed in X.

Definition 3.6. Let A, B, ρ and S be as in Def.3.1 above. For any subset $Y \subset B^n$, we define

$$\rho_B(Y) = \{(f, g) \in S \times S : \ (f(P), g(P)) \in \rho \text{ for all } P \in Y\}.$$

Obviously, $\rho_B(Y)$ is a congruence on S.

Theorem 3.7. Let A, B, ρ and $S = A[x_1, \cdots, x_n]$ be as in Def.3.1 above.

(1) If $T_1 \subset T_2$ are subsets of $S \times S$, then $Z_\rho(T_1)(B) \supset Z_\rho(T_2)(B)$.

(2) If $T \subset S \times S$, then $Z_\rho(T)(B) = Z_\rho(T^c)(B)$ and $T \subset \rho_B(Z_\rho(T)(B))$.

(3) If $Y_1 \subset Y_2$ are subsets of B^n, then $\rho_B(Y_1) \supset \rho_B(Y_2)$.

(4) For any two subsets Y_1, Y_2 of B^n, we have $\rho_B(Y_1 \cup Y_2) = \rho_B(Y_1) \cap \rho_B(Y_2)$.

Proof. (1) and (3) follow easily from the definitions.

(2) $T \subset \rho_B(Z_\rho(T)(B))$ follows directly from the definition. For the equality, Since $T \subset T^c$, by (1), $Z_\rho(T^c)(B) \subset Z_\rho(T)(B)$. Conversely, let $P \in Z_\rho(T)(B)$, then $(h_1(P), h_2(P)) \in \rho$ for all $(h_1, h_2) \in T$. For any $(f, g) \in T^c$, by Cor.2.17 above, $f = g$ or for some positive integer n there exists a sequence $f = f_1 \to f_2 \to \cdots \to f_n = g$ in which for each $i \in \{1, 2, \cdots, n-1\}$ either $(f_i, f_{i+1}) \in T^L$ or $(f_{i+1}, f_i) \in T^L$. If $f = g$, then obviously $(f(P), g(P)) \in \rho$. If $(f_i, f_{i+1}) \in T^L$, then $(f_i, f_{i+1}) = (a_i g_i + h_i, b_i g_i + h_i)$ for some $(a_i, b_i) \in T$ and some $g_i, h_i \in S$. By the choice of P, $(a_i(P), b_i(P)) \in \rho$, so

$$(f_i(P), f_{i+1}(P)) = (a_i(P)g_i(P) + h_i(P), b_i(P)g_i(P) + h_i(P))$$

$$= (a_i(P), b_i(P)) \cdot (g_i(P), g_i(P)) + (h_i(P), h_i(P)) \in \rho.$$

Similarly, if $(f_{i+1}, f_i) \in T^L$, then $(f_{i+1}(P), f_i(P)) \in \rho$, which also implies that $(f_i(P), f_{i+1}(P)) \in \rho$ because ρ is a congruence. So for the above sequence, we always have $(f_i(P), f_{i+1}(P)) \in \rho$ for all $i \in \{1, 2, \cdots, n-1\}$, that is,

$(f_1(P), f_2(P)), (f_2(P), f_3(P)), \cdots, (f_{n-1}(P), f_n(P)) \in \rho,$

so $(f_1(P), f_n(P))$, i.e., $(f(P), g(P)) \in \rho$. This shows that $(f(P), g(P)) \in \rho$ for all $(f, g) \in T^c$, hence $P \in Z_\rho(T^c)(B)$, which implies that $Z_\rho(T)(B) \subset Z_\rho(T^c)(B)$. Therefore, $Z_\rho(T)(B) = Z_\rho(T^c)(B)$.

(4) By (3), $\rho_B(Y_1 \cup Y_2) \subset \rho_B(Y_i)$ $(i = 1, 2)$, so $\rho_B(Y_1 \cup Y_2) \subset \rho_B(Y_1) \cap \rho_B(Y_2)$. Conversely, if $(f, g) \in \rho_B(Y_1) \cap \rho_B(Y_2)$, then $(f(P), g(P)) \in \rho$ for all $P \in Y_i$ $(i = 1, 2)$, i.e., $(f(P), g(P)) \in \rho$ for all $P \in Y_1 \cup Y_2$, so $(f, g) \in \rho_B(Y_1 \cup Y_2)$, which implies that $\rho_B(Y_1) \cap \rho_B(Y_2) \subset \rho_B(Y_1 \cup Y_2)$. Therefore, $\rho_B(Y_1 \cup Y_2) = \rho_B(Y_1) \cap \rho_B(Y_2)$. The proof

is completed. $\square$

Lemma 3.8. Let A, B, ρ and $S = A[x_1, \cdots, x_n]$ be as in Def.3.1 above. For $f, g \in S, P \in B^n$ and positive integer m, we have

$(f, g)^{*m}(P) = (f(P), g(P))^{*m} \in B \times B$ (here we write $(f, g)(P) = (f(P), g(P))$).

Proof. By Prop.2.6 above,

$$(f,g)^{*m} = (\sum_{2|i,\ i=0}^{m} \binom{m}{i} f^{m-i}g^i,\ \sum_{2\nmid i,\ i=1}^{m} \binom{m}{i} f^{m-i}g^i),\ \text{so}$$
$$(f,g)^{*m}(P) = (\sum_{2|i,\ i=0}^{m} \binom{m}{i} f(P)^{m-i}g(P)^i,\ \sum_{2\nmid i,\ i=1}^{m} \binom{m}{i} f(P)^{m-i}g(P)^i)$$
$$= (f(P), g(P))^{*m}.$$

The proof is completed. $\square$

Next, we will state a version of Nullstellensatz for congruences. For this, we need write some notations. Let A be a commutative semiring and θ be a congruence on A. Let $S = A[x_1, \cdots, x_n]$ be the commutative semiring of polynomials in n variables over A. For two monomials $ax_1^{i_1} \cdots x_n^{i_n}$ and $bx_1^{i_1} \cdots x_n^{i_n}$ $(a, b \in A, i_1, \cdots, i_n \in \mathbb{Z}_{\geq 0})$, we denote

$$ax_1^{i_1} \cdots x_n^{i_n} \equiv bx_1^{i_1} \cdots x_n^{i_n} \pmod{\theta} \quad \text{if } (a, b) \in \theta.$$

In general, for two polynomials $f = \Sigma a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ and $g = \Sigma b_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ in S, we denote $f \equiv g \pmod{\theta}$ if all the corresponding coefficients $a_{i_1 \cdots i_n}$ and $b_{i_1 \cdots i_n}$ satisfy $(a_{i_1 \cdots i_n},\ b_{i_1 \cdots i_n}) \in \theta$. If $f \equiv g \pmod{\theta}$, then obviously $(f(P), g(P)) \in \theta$ for all $P \in A^n$, where A^n is the affine $n-$space over A as before.

Now for the semirings $A, B, S = A[x_1, \cdots, x_n]$ and the congruence ρ of B in

Def.3.1 above, let σ be a congruence on S, we define

$$\sqrt{\sigma/\rho} = \{(f_1, f_2) \in S \times S : f_i \equiv g_i (\text{mod} \sqrt{\rho})\ (i = 1, 2) \text{ for some } (g_1, g_2) \in \sqrt{\sigma}\}.$$

By definition, obviously $\sqrt{\sigma} \subset \sqrt{\sigma/\rho}$, and if $\sqrt{\rho} = \text{id}$ is the identity congruence, then $\sqrt{\sigma/\rho} = \sqrt{\sigma}$. In general, it is easy to see that the relation $\sqrt{\sigma/\rho}$ on S satisfies almost all the properties of a congruence except the transitivity, that is, it might not be transitively closed, so it might not be a congruence. Recall that $(\sqrt{\sigma/\rho})^c$ is the congruence on S generated by the relation $\sqrt{\sigma/\rho}$.

Proposition 3.9. Let A, B, ρ and $S = A[x_1, \cdots, x_n]$ be as in Def.3.1 above. Then for any congruence σ on S, we have $(\sqrt{\sigma/\rho})^c \subset (\sqrt{\rho})_B(Z_\rho(\sigma)(B))$.

Proof. Since the right-hand side of the inclusion is a congruence, we only need to show that $\sqrt{\sigma/\rho} \subset (\sqrt{\rho})_B(Z_\rho(\sigma)(B))$. let $(f, g) \in \sqrt{\sigma/\rho}$, then there is an element $(f_1, g_1) \in \sqrt{\sigma}$ such that $f \equiv f_1(\text{mod}\sqrt{\rho})$ and $g \equiv g_1(\text{mod}\sqrt{\rho})$. By definition, $(f_1 + h, g_1 + h)^{*m} \in \sigma$ for some $h \in S$ and some positive integer m. For any $P \in Z_\rho(\sigma)(B)$, $(f_0(P), g_0(P)) \in \rho$ for all $(f_0, g_0) \in \sigma$, so in particular, $(f_1 + h, g_1 + h)^{*m}(P) \in \rho$. Then by Lemma 3.8 above, $(f_1(P) + h(P), g_1(P) + h(P))^{*m} = (f_1 + h, g_1 + h)^{*m}(P) \in \rho$, so $(f_1(P), g_1(P)) \in \sqrt{\rho}$. which implies that $(f(P), g(P)) \in \sqrt{\rho}$ because $(f(P), f_1(P)) \in \sqrt{\rho}$ and $(g(P), g_1(P)) \in \sqrt{\rho}$. Hence $(f, g) \in (\sqrt{\rho})_B(Z_\rho(\sigma)(B))$, and the proof is completed. □

The Example 3.13 below gives some indication that the equality in the above Prop.3.9 might hold. So we have the following question

A question about Nullstellensatz of congruences Under what conditions can the equality $(\sqrt{\sigma/\rho})^c = (\sqrt{\rho})_B(Z_\rho(\sigma)(B))$ hold ?

As pointed out by an anonymous expert, recently, motivated by tropical geometry, several versions of the Nullstellensatz question have been raised and answered for the tropical polynomials focusing on the case of additively idempotent semirings (see, e.g.,[1, 2]). There are other approaches were taken on this question in the literature (see, e.g. [3-7]).

Theorem 3.10. Let A, B, ρ and $S = A[x_1, \cdots, x_n]$ be as in Def.3.1 above. If $\rho \in \mathrm{Spec}^c(B)$ is a prime congruence on B. Then for any subset $Y \subset B^n$, we have $Z_\rho(\rho_B(Y))(B) = \overline{Y}$, the closure of Y in B^n with the Zariski $\rho-$topology $\tau_{\rho,A}$.

Proof. Let $P \in Y$, then $(f(P), g(P)) \in \rho$ for all $(f, g) \in \rho_B(Y)$, so $P \in Z_\rho(\rho_B(Y))(B)$. Thus $Y \subset Z_\rho(\rho_B(Y))(B)$. Since $Z_\rho(\rho_B(Y))(B)$ is closed, we get $\overline{Y} \subset Z_\rho(\rho_B(Y))(B)$. On the other hand, let W be any closed subset containing Y. Then $W = Z_\rho(\sigma)(B)$ for some congruence σ on S. So $Z_\rho(\sigma)(B) \supset Y$. By Theorem 3.7 above, $\sigma \subset \rho_B(Z_\rho(\sigma)(B)) \subset \rho_B(Y)$. So $W = Z_\rho(\sigma)(B) \supset Z_\rho(\rho_B(Y))(B)$. Therefore, $Z_\rho(\rho_B(Y))(B) = \overline{Y}$, and the proof is completed. $\square$

Theorem 3.11. Let A, B, ρ and $S = A[x_1, \cdots, x_n]$ be as in Theorem 3.10 above. Let $Y \subset B^n$ be an $\rho-$algebraic variety. If Y is irreducible, then $\rho_B(Y)$ is a prime congruence on S.

Proof. Let $(f_1, g_1), (f_2, g_2) \in S \times S$. If $(f_1, g_1) * (f_2, g_2) \in \rho_B(Y)$, then by Theorems 3.7 and 3.10 above, $Z_\rho((f_1, g_1) * (f_2, g_2))(B) \supset Z_\rho(\rho_B(Y))(B) = \overline{Y} = Y$. From the proof of Theorem 3.4(1) above, we have $Z_\rho((f_1, g_1) * (f_2, g_2))(B) = Z_\rho((f_1, g_1))(B) \cup Z_\rho((f_2, g_2))(B)$, so $Y \subset Z_\rho((f_1, g_1))(B) \cup Z_\rho((f_2, g_2))(B)$. Thus $Y = (Y \cap Z_\rho((f_1, g_1))(B)) \cup (Y \cap Z_\rho((f_2, g_2))(B))$, both being closed subsets of

Y. Since Y is irreducible, we have either $Y = Y \cap Z_\rho((f_1, g_1))(B)$, in which case $Y \subset Z_\rho((f_1, g_1))(B)$, or $Y \subset Z_\rho((f_2, g_2))(B)$. So by Theorem 3.7 above, $(f_1, g_1) \in \rho_B(Z_\rho((f_1, g_1))(B)) \subset \rho_B(Y)$, i.e., $(f_1, g_1) \in \rho_B(Y)$, or $(f_2, g_2) \in \rho_B(Y)$, and so $\rho_B(Y)$ is a prime congruence. The proof is completed. $\square$

Let A, B be two commutative semirings, and ϕ be a homomorphism from A to B, i.e., $\phi : A \to B$ is a map such that $\phi(0) = 0, \phi(1) = 1$, and for all $a, b \in A, \phi(a+b) = \phi(a)+\phi(b)$ and $\phi(ab) = \phi(a) \cdot \phi(b)$. Then the kernel $\ker\phi = \{(a_1, a_2) \in A \times A : \phi(a_1) = \phi(a_2)\}$ is a congruence on A, and ϕ induces a unique injective homomorphism, say $\overline{\phi} : A/\ker\phi \to B$ such that $\phi = \overline{\phi} \circ \eta$, where $\eta : A \to A/\ker\phi$ is the natural surjective homomorphism. Moreover, via such ϕ, B is an $A-$semimodule, hence an $A-$semialgebra. In general, for a commutative semiring A, a set B is an $A-$semialgebra if B is both a commutative semiring and an $A-$semimodule such that $a(bc) = (ab)c = b(ac)$ $(\forall a \in A, b, c \in B)$. For two $A-$semialgebras B and C, a map $\phi : B \to C$ is an $A-$semialgebra homomorphism if ϕ is both a semiring homomorphism and an $A-$semimodule homomorphism. We let $\mathrm{Hom}_{A-\mathrm{alg}}(B, C)$ to denote the set of all $A-$semialgebra homomorphisms from B to C.

Now come back to our semirings $A \subset B$ and $S = A[x_1, \cdots, x_n]$ as in Def.3.1 above. Let ρ be a congruence on B, and $T \subset S \times S$ be a non-empty subset. Recall that T^c is the congruence on S generated by T. Then it is easy to see that both the quotient semirings S/T^c and B/ρ are $A-$semialgebras. Recall that for a subset Y of B^n, $Y/\rho = \{(\overline{c_1}, \cdots, \overline{c_n}) : (c_1, \cdots, c_n) \in Y\} \subset B^n/\rho$ with $\overline{c_i} = c_i \bmod \rho \in B/\rho$.

Theorem 3.12. Let A, B and $S = A[x_1, \cdots, x_n]$ be as in Def.3.1 above. Let ρ be a congruence on B, and $T \subset S \times S$ be a non-empty subset. Then there exists an one-to-one map of $Z_\rho(T)(B)/\rho$ onto $\mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho)$, so the cardinals $\sharp Z_\rho(T)(B)/\rho = \sharp\mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho)$. In particular, if $\rho = \mathrm{id}_B$, then $\sharp Z_{\mathrm{id}_B}(T)(B) = \sharp\mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B)$.

Proof. By the composition of homomorphisms $A \hookrightarrow B \to B/\rho$ (resp. $A \hookrightarrow S \to S/T^c$), B/ρ (resp. S/T^c) becomes a natural $A-$semialgebra. Define a map

$\phi_0 : \ Z_\rho(T)(B) \longrightarrow \mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho), \ P \mapsto \phi_0(P)$,

where $\phi_0(P) : \ S/T^c \longrightarrow B/\rho$ is defined as follows:

Write $P = (b_1, \cdots, b_n)$ with $b_i \in B$ $(i = 1, \cdots, n)$, we have a homomorphism of semirings

$\gamma_P : \ S \longrightarrow B/\rho, \ h(x_1, \cdots, x_n) \mapsto \overline{h(b_1, \cdots, b_n)} = \overline{h(P)}$ $(\forall h \in S)$.

For any $(f, g) \in T, (f(P), g(P)) \in \rho$ since $P \in Z_\rho(T)(B)$. So $\gamma_P(f) = \overline{f(P)} = \overline{g(P)} = \gamma_P(g)$, i.e., $(f, g) \in \ker\gamma_P$, so $T \subset \ker\gamma_P$, and so $T^c \subset \ker\gamma_P$. Therefore, there is a unique homomorphism of semirings, say $\phi_0(P) : \ S/T^c \longrightarrow B/\rho$ such that $\phi_0(P) \circ \eta = \gamma_P$, where $\eta : S \longrightarrow S/T^c$ is the natural surjective homomorphism. Moreover, for any $a \in A$ and $f \in S$, $\phi_0(P)(a \cdot \overline{f}) = \phi_0(P)(\overline{af}) = \gamma_P(af) = \overline{(af)(P)} = \overline{a \cdot f(P)} = \overline{a} \cdot \overline{f(P)} = a \cdot \gamma_P(f) = a \cdot \phi_0(P)(\overline{f})$, so $\phi_0(P)$ is also an $A-$semimodule homomorphism, hence $\phi_0(P) \in \mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho)$. By this way, the map ϕ_0 is given. Now let $P, Q \in Z_\rho(T)(B)$ be two points such that $\phi_0(P) = \phi_0(Q)$, then for any $f \in S, \gamma_P(f) = \phi_0(P)(\eta(f)) = \phi_0(P)(\overline{f}) = \phi_0(Q)(\overline{f}) = \gamma_Q(f)$. So $\gamma_P = \gamma_Q$. If we write $P = (b_1, \cdots, b_n)$ and $Q = (c_1, \cdots, c_n)$, then coordinates $b_i = x_i(P)$ and $c_i = x_i(Q)$. So $\overline{b_i} = \overline{x_i(P)} = \gamma_P(x_i) = \gamma_Q(x_i) = \overline{x_i(Q)} = \overline{c_i}$, and so $\overline{P} = (\overline{b_1}, \cdots, \overline{b_n}) = (\overline{c_1}, \cdots, \overline{c_n}) = \overline{Q}$, i.e., $\overline{P} = \overline{Q} \in Z_\rho(T)(B)/\rho$. Conversely, if $P, Q \in Z_\rho(T)(B)$ satisfy $\overline{P} = \overline{Q} \in Z_\rho(T)(B)/\rho$, then obviously, $\gamma_P = \gamma_Q$, and so

$\phi_0(P) = \phi_0(Q)$. Therefore, $\phi_0(P) = \phi_0(Q) \Leftrightarrow \overline{P} = \overline{Q}$, and so ϕ_0 induces an injective map

$\phi: \ Z_\rho(T)(B)/\rho \longrightarrow \mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho), \ \overline{P} \mapsto \phi_0(P) \ (\forall \ P \in Z_\rho(T)(B))$.

Next, we define a map

$\psi: \ \mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho) \longrightarrow Z_\rho(T)(B)/\rho, \ \gamma \mapsto \psi(\gamma)$,

where the point $\psi(\gamma) \in Z_\rho(T)(B)/\rho$ is defined as follows:

By composing γ with the natural $A-$semialgebra homomorphism $\eta : S \longrightarrow S/T^c$, we get an $A-$semialgebra homomorphism $\beta = \gamma \circ \eta : \ S \longrightarrow B/\rho$. For each $i = 1, \cdots, n$ write $u_i = \beta(x_i) = \gamma(\eta(x_i)) \in B/\rho$, so $u_i = \overline{b_i}$ for some $b_i \in B$. Then we define $\psi(\gamma) = (\overline{b_1}, \cdots, \overline{b_n}) \in B^n/\rho$. We need to show that $(b_1, \cdots, b_n) \in Z_\rho(T)(B)/\rho$. For this, write $P = (b_1, \cdots, b_n) \in B^n$. For any $(f, g) \in T(\subset T^c), \overline{f} = \overline{g} \in S/T^c$, so $\beta(f) = \gamma(\eta(f)) = \gamma(\overline{f}) = \gamma(\overline{g}) = \gamma(\eta(g)) = \beta(g)$. Note that $f = f(x_1, \cdots, x_n), g = g(x_1, \cdots, x_n)$ and β is an $A-$semialgebra homomorphism, we have

$$f(\beta(x_1), \cdots, \beta(x_n)) = \beta(f(x_1, \cdots, x_n)) = \beta(f)$$

$$= \beta(g) = \beta(g(x_1, \cdots, x_n)) = g(\beta(x_1), \cdots, \beta(x_n)),$$

i.e., $f(\overline{b_1}, \cdots, \overline{b_n}) = g(\overline{b_1}, \cdots, \overline{b_n}) \in B/\rho$, which means $\overline{f(P)} = \overline{g(P)}$, so $(f(P), g(P)) \in \rho$, which implies that $P \in Z_\rho(T)(B)$. So the above $\psi(\gamma) = \overline{P} \in Z_\rho(T)(B)/\rho$. By this way, the map ψ is given.

Now we consider the composition map

$\psi \circ \phi: \ Z_\rho(T)(B)/\rho \longrightarrow \mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho) \longrightarrow Z_\rho(T)(B)/\rho$.

For any $P \in Z_\rho(T)(B)$, by definition,

$$(\psi \circ \phi)(\overline{P}) = \psi(\phi(\overline{P})) = \psi(\phi_0(P)) = (\phi_0(P)(\overline{x_1}), \cdots, \phi_0(P)(\overline{x_n}))$$

$$= (\gamma_P(x_1), \cdots, \gamma_P(x_n)) = (\overline{x_1(P)}, \cdots, \overline{x_n(P)}) = \overline{P}.$$

So $\psi \circ \phi = \mathrm{id}$ is the identity map.

Also for the composition map

$\phi \circ \psi : \ \mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho) \longrightarrow Z_\rho(T)(B)/\rho \longrightarrow \mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho)$.

For any $\gamma \in \mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho)$, write $\psi(\gamma) = \overline{P}$ for some $P = (b_1, \cdots, b_n) \in Z_\rho(T)(B)$. Then by definition, $\psi(\gamma) = (\gamma(\overline{x_1}), \cdots, \gamma(\overline{x_n}))$, so $\gamma(\overline{x_i}) = \overline{b_i}$ $(i = 1, \cdots, n)$. On the other hand, by definition, $\phi_0(P)(\overline{x_i}) = \gamma_P(x_i) = \overline{x_i(P)} = \overline{b_i}$ $(i = 1, \cdots, n)$. So $\phi_0(P)(\overline{x_i}) = \gamma(\overline{x_i})$, and hence $\phi_0(P) = \gamma$, i.e., $(\phi \circ \psi)(\gamma) = \phi(\overline{P}) = \phi_0(P) = \gamma$, which implies that $\phi \circ \psi = \mathrm{id}$ is the identity map. Therefore, both ϕ and ψ are bijective, so $\sharp Z_\rho(T)(B)/\rho = \sharp \mathrm{Hom}_{A-\mathrm{alg}}(S/T^c, B/\rho)$, and the proof is completed. $\square$

Example 3.13. (1) Let $A = (\mathbb{Z}_{\geq 0}, +, \cdot)$ be the semidomain as before, p be a prime number, and $\rho = \mathrm{mod}\ p$ be the modulo p congruence, i.e., $\rho = \{(a, b) : a, b \in A, a \equiv b \pmod p\}$. Let $S = A[t]$ be the commutative semiring of polynomials in one variable over A. Take $T = \{(t, 0)\} \subset S \times S$, and let $\sigma = T^c$ be the congruence on S generated by T. By definition, we have easily that

$$Z_\rho(\sigma)(A) = Z_\rho(T)(A) = \{mp : \ m \in \mathbb{Z}_{\geq 0}\}, \quad \text{and}$$

$$(\sqrt{\rho})_A(Z_\rho(\sigma)(A)) = \{(f, g) \in S \times S : f(0) \equiv g(0) \pmod p\}.$$

So for $(f, g) \in (\sqrt{\rho})_A(Z_\rho(\sigma)(A))$, we have $f(0) \equiv g(0) \pmod p$. We may as well assume that $g(0) = f(0) + mp$ for some $m \in \mathbb{Z}_{\geq 0}$. Then $(f, g) = (tf_1 + f(0), tg_1 +$

$f(0)+mp)$ for some $f_1, g_1 \in S$. By Prop.2.21 above, we have $(tf_1+f(0), tg_1+f(0)) \in R(t,0) \subset \sigma \subset \sqrt{\sigma}$. Note that $f = tf_1 + f(0)$ and $g \equiv tg_1 + f(0) (\text{mod } p)$, in other words, $f \equiv tf_1 + f(0) (\text{mod} \rho)$ and $g \equiv tg_1 + f(0) (\text{mod } \rho)$, so by definition, $(f, g) \in (\sqrt{\sigma/\rho})^c$, and so $(\sqrt{\rho})_A(Z_\rho(\sigma)(A)) \subset (\sqrt{\sigma/\rho})^c$. Therefore, by Prop.3.9 above, the equality holds, i.e., $(\sqrt{\sigma/\rho})^c = (\sqrt{\rho})_A(Z_\rho(\sigma)(A))$.

(2) As discussed in (1) above, $Z_\rho(T)(A) = \{mp : \ m \in \mathbb{Z}_{\geq 0}\}$, so $Z_\rho(T)(A)/\rho = \{\overline{0}\}$. On the other hand, $S/T^c = S/\sigma = A = \mathbb{Z}_{\geq 0}$ because $(t, 0) \in \sigma$. Note that $A/\rho = \{\overline{0}, \cdots, \overline{p-1}\}$, so $\text{Hom}_{A-\text{alg}}(S/T^c, A/\rho) = \text{Hom}_{A-\text{alg}}(A, A/\rho) = \{\phi\}$, where $\phi : A \to A/\rho, 1 \mapsto \overline{1}$. Hence $\sharp Z_\rho(T)(A)/\rho = 1 = \sharp\text{Hom}_{A-\text{alg}}(S/T^c, A/\rho)$, the same as shown in Theorem 3.12 above. $\square$

Remark 3.14. This paper is a revised version of the early one [18]. I thank the anonymous experts for pointing out another useful equivalent form of the radical of congruence in Definition 2.9 above, which help me to simplify the early version [18, Prop.2.12, 2.13] of the results and proofs about radical and nilpotent congruences. I also thank the anonymous experts for their useful list of many related papers on tropical geometry and universal algebraic geometry, that might stimulate me in further study concerning with this work.

Acknowledgments I would like to thank the referee for helpful suggestions and comments.

Conflicts of interest. The author declares no competing interests.

References

[1] Bertram, A. and Easton, R. (2017). The Tropical Nullstellensatz for congruences, Advances in Mathematics, 308, 36-82.

[2] Jo´o, D. and Mincheva, K. Prime congruences of idempotent semirings and a Nullstellensatz for tropical polynomials, arXiv: 1408.3817.

[3] Izhakian, Z. (2008). Tropical algebraic sets, ideals and an algebraic Nullstellensatz, Internat.J. Algebra Comput., 18, 1067-1098.

[4] Izhakian, Z. and Shustin, E. (2007). A tropical Nullstellensatz, Proc. Amer. Math. Soc., 135, no.12, 3815-3821.

[5] Giansiracusa, J. and Giansiracusa, N. (2016). Equations of Tropical varieties, Duke Math.J., Vol.165, 18, 3379-3433.

[6] Grigoriev, D. On a tropical dull Nullstellensatz, arXiv: 1108.0519.

[7] Maclagan, D. and Rinc´on, F. Tropical Ideals, arXiv: 1609.03838.

[8] Plotkin, B. (1997). Some notions of algebraic geometry in universal algebra, Algebra and Analysis 9(4), 224-248, St.Petersburg Math.j. 9(4)(1998), 859-879.

[9] Plotkin, B. (2004). algebraic geometry in first order logic, Sovremennaja Matematika and Applications 22, 16-62, J. Math. Sci. 137(5) 2006, 5049-5097.

[10] Plotkin, B. and Plotkin, E. (2015). Multi-sorted logic and logical geometry: some problems. Demonstratio Mathematica, Vol.XLVIII no.4, 578-616.

[11] Daniyarova, E.Yu., Myasnikov, A.G., Remeslennikov, V.N. (2012). Algebraic geometry over algebraic systems. II. Foundations. J. Math.Sci., 185, no.3, 389-416.

[12] Daniyarova, E.Yu., Myasnikov, A.G., Remeslennikov, V.N. (2012). Algebraic geometry over algebraic systems. V. The case of arbitrary signature, Algebra Logic, 51, no.1, 28-40.

[13] Jo´o, D. and Mincheva, K. On the dimension of polynomial semirings, arXiv:1501.02493.

[14] Golan, J.S. (2003). Semirings and Affine Equations over Them: Theory and Applications. Boston.

[15] Howie, J.M. (1976). An Introduction to Semigroup Theory. New York: Academic Press.

[16] Hartshorne, R. (1977). Algebraic Geometry. New York: Springer-Verlag.

[17] Kemper, G. (2011). A Course in Commutative Algebra. Berlin: Springer-Verlag.

[18] Derong Qiu, On algebraic congruences, first version, arXiv: 1512.08088 v1, 26 Dec., 2015; second version, arXiv: 1512.08088 v2, 24 Jan., 2017.