TROPICAL SCHEME THEORY

5. Commutative algebra over idempotent semirings II

Quotients of semirings

When we work with rings, a quotient object is specified by an ideal. When dealing with semirings (and lattices), however, quotient objects are instead specified by *congruences*.

Definition 5.1. *A congruence on a semiring is an equivalence relation $\sim$ that preserves the operations. That is, if $r \sim r'$ and $s \sim s'$ then*

$$r + s \sim r' + s'$$

and

$$rs \sim r's'.$$

Example 5.2. The trivial congruence, in which $r \sim r'$ if and only if $r = r'$.

Example 5.3 (Bourne relations—the congruence associated to an ideal)**.** Let R be a semiring and let $I \subset R$ be an ideal. Then define a congruence $\sim_I$ by setting $r \sim_I r'$ if there are elements a and a' in I such that $r + a = r' + a'$.

Note that if $r \sim_I r'$ and $s \sim_I s'$ then $r + s \sim_I r' + s'$ and $rs \sim_I r's'$.

Lemma 5.4. *If R is additively idempotent and $I \subset R$ is an ideal then $r \sim_I r'$ if and only if there is some $b \in I$ such that $r + b = r' + b$.*

Proof. ($\Leftarrow$) This is immediate from the definition.
($\Rightarrow$) Say $r \sim_I r'$ so there exist $a, a' \in I$ with $r + a = r' + a'$. Then we have

$$r + a + a' = r' + a' + a' = r' + a' = r + a = r + a + a = r' + a' + a.$$

So setting $b = a + a'$ we have $r + b = r' + b$. $\square$

Remark 5.5. Let R be an additively cancellative semiring. Define a new semiring $S = (R \times R, +, *)$, with $+$ being the obvious addition and multiplication given by $(a, b) * (c, d) = (ac + bd, ad + bc)$. The set $\Delta = \{(a, a) \mid a \in R\}$ is an ideal of S and S/Δ is a ring.

Comment 5.6 (Sam)**.** This construction seems to be introducing subtractionm i.e. we might think of the equivalence class of (a, b) in S/Δ as corresponding to "$a - b$". As an example, if we start with $R = (\mathbb{N}, +, *)$ then the quotient S/Δ is canonically isomorphic to $\mathbb{Z}$.

Remark 5.7 (Relation to the ring case)**.** If R is a ring and $I \subset R$ is an ideal then R/I is canonically isomorphic to $R/{\sim_I}$.

Date: September 21/26, 2017, *Speaker*: Kalina Mincheva, *Scribe*: Netanel Friedenberg.

Remark 5.8. If $\sim$ is a congruence on R then $J = \{x \in R \,|\, x \sim 0\}$ is an ideal of R.

Relation between ideals and congruences in additively idempotent semirings

If R is a ring then there is a natural bijection between ideals in R and congruences on R, given by Remarks 5.7 and 5.8. We now explore the relationship between ideals and congruences in additively idempotent semirings.

Let R be an additively idempotent semiring and let J be an ideal of R.

Proposition 5.9. *The congruence $\sim_J$ is generated by $\{(x, 0) \,|\, x \in J\}$.*

Proof. Let $\equiv$ be the equivalence relation generated by $\{(x, 0) \,|\, x \in J\}$.

Suppose $x \in J$. Since R is additively idempotent, $0+x = x+x$, and hence $x \sim_J 0$. This shows that $\equiv$ is contained in $\sim_J$.

We now prove that $\sim_J$ is contained in $\equiv$. Suppose $x \sim_J y$. By definition, this means that there is some $z \in J$ such that $x + z = y + z$. Then $z \equiv 0$ and hence $x \equiv x + z$. Since $x + z = y + z$ and $y + z \equiv y$, it follows that $x \equiv y$, as required. □

Definition 5.10. *The saturation of the ideal $J \subset R$ is*

$$\bar{J} = \{x \in R \,|\, x + z = z \text{ for some } z \in J\}.$$

Equivalently, $\bar{J} = \{x \in R \,|\, x \sim_J 0\}$.

Proposition 5.11. *Saturation is a closure operation on ideals in R. In other words, the saturation $\bar{J}$ is an ideal, $J \subset \bar{J}$, $\bar{J} = \bar{\bar{J}}$, and if $I \subset J$ then $\bar{I} \subset \bar{J}$.*

Proof. That $\bar{J}$ is an ideal is immediate from Remark 5.8. The containment $J \subset \bar{J}$ is an immediate consequence of additive idempotence. If $I \subset J$ then the containment $\bar{I} \subset \bar{J}$ is also obvious. It remains to show that $\bar{J} = \bar{\bar{J}}$.

Suppose $x \in \bar{\bar{J}}$. Then there is some $z \in \bar{J}$ such that $x + z = z$. And since $z \in \bar{J}$ there is some $z' \in J$ such that $z + z' = z'$. Then

$$x + z' = x + z + z' = z + z' = z',$$

and hence $x \in \bar{J}$. □

Example 5.12. The saturation of an ideal J in the polynomial ring $\mathbb{T}[x_1, ..., x_n]$ is the smallest monomial ideal that contains J. In other words, if J is generated by $\{f_1, \ldots, f_m\}$ then $\bar{J}$ is generated by the monomials $x_1^{a_1} \cdots x_n^{a_n}$ that appear with nonzero coefficient in one of the generators f_i. In particular, if J contains a polynomial with nonzero constant term then $\bar{J} = \mathbb{T}[x_1, \ldots, x_n]$.

The analogous statement holds in $\mathbb{B}[x_1, \ldots, x_n]$. In particular, the ideal $(x, x+1)$ in $\mathbb{B}[x]$ considered in Lecture 2 is not saturated, and its saturation is $\mathbb{B}[x]$.

Definition 5.13. *A congruence $\sim$ is cancellative if $ab \sim ac$ implies that either $b \sim c$ or $a \sim 0$.*

Theorem 5.14. *If J is saturated and cancellative, then J is prime.*

Proof. Suppose J is saturated and cancellative, and $ab \in J$. Then $a \cdot b \sim_J a \cdot 0$, so either $a \sim_J 0$ or $b \sim_J 0$. Since J is saturated, this implies $a \in J$ or $b \in J$. □

Remark 5.15. The converse to Theorem 5.14 is false. For examples of prime ideals J that are not saturated and for which $\sim_J$ is not cancellative, see [Les11, Remark 3.14].

Kernels of homomorphisms

Definition 5.16. *Let $\varphi : R \to S$ be a morphism of semirings. The kernel of φ is*

$$\ker \varphi = \{(a, b) \in R \times R \,|\, \varphi(a) = \varphi(b)\}$$

Similarly, if $\mathcal{C} \subset S \times S$ is any congruence on S then we can consider the preimage congruence $\varphi^{-1}(\mathcal{C}) = \{(a, b) \in R \times R \,|\, (\varphi(a), \varphi(b)) \in \mathcal{C}\}$. Then $\ker(\varphi) = \varphi^{-1}(\Delta)$ where $\Delta \subset S \times S$ is the trivial congruence. Equivalently, $\phi^{-1}(\mathcal{C})$ is the kernel of the induced map $R \to S/\mathcal{C}$.

Remark 5.17 ("Ideal-theoretic kernels" versus "congruence-theoretic kernels")**.** The ideal-theoretic kernel of a morphism $\varphi : R \to S$ is $\varphi^{-1}(0)$. Consider surjective morphisms $\mathbb{T}[x] \to \mathbb{T}$. The only such morphism that has non-trivial ideal-theoretic kernel is the one which sends $x \mapsto 0_{\mathbb{T}} = \infty$. On the other hand there are many congruences that can be realized as $\ker \varphi$. For example, for each $t \in \mathbb{T}$ we have the evaluation morphism $\varphi_t : \mathbb{T}[x] \to \mathbb{T}$ $f(x) \mapsto f(t)$. If we let $\sim$ be the intersection of the kernels of all such φ_t, then $\mathbb{T}[x]/\sim$ is $\mathrm{CPL}_{\mathbb{Z}}(\mathbb{R})$.

Proposition 5.18. *The only additively idempotent semiring with no nontrivial proper congruences is the Boolean semiring $\mathbb{B}$.*

Proof. Let R be an additively idempotent semiring. Suppose R has zero-divisors, i.e. there are $x, y \in R\backslash\{0\}$ such that $xy = 0$. Consider

$$\mathcal{C} = \{(a, b) \,|\, xa = xb\}.$$

Then $\mathcal{C}$ is a congruence on R. It is nontrivial because $(y, 0) \in \mathcal{C}$ and proper because $(1, 0) \notin C$.

Now suppose R has no zero-divisors. Then we can define a morphism $\varphi : R \to \mathbb{B}$ by

$$\varphi(x) = \begin{cases} 0_{\mathbb{B}} & \text{if } x = 0_R \\ 1_{\mathbb{B}} & \text{if } x \neq 0_R \end{cases}.$$

This is a morphism because, in an additively idempotent semiring, if $a + b = 0$ then both a and b are 0. Then $\ker \varphi$ is a proper subset of $R \times R$, and so either $\ker \varphi$ is nontrivial or φ is an isomorphism onto $\mathbb{B}$. (Since $\mathbb{B}$ has no nontrivial automorphisms, this isomorphism is unique.) □

Remark 5.19. Even more is true: if R is an arbitrary commutative semiring (not necessarily additively idempotent) with no nontrivial proper congruences then either $R = \mathbb{B}$ or R is a field. See [Go99, Proposition 8.11].

Remark 5.20. The Boolean semifield $\mathbb{B}$ does not have any nontrivial proper ideals either. More generally, semifields do not have any nontrivial proper ideals. On the other hand, by Proposition 5.18 we know that semifields other than $\mathbb{B}$ will have nontrivial proper congruences.

Example 5.21. The tropical semiring $\mathbb{T}$ has a unique nontrivial proper congruence and the quotient of $\mathbb{T}$ by this congruence is $\mathbb{B}$.

To see this, suppose $\sim$ is a nontrivial congruence on $\mathbb{T}$. Then $a \sim b$ for two distinct elements a and b in $\mathbb{T}$, with $a \neq 0_{\mathbb{T}}$. Multiplying the relation $a \sim b$ by a^{-1}, we may assume $a = 1_{\mathbb{T}}$. If $b = 0_{\mathbb{T}}$, then $\sim$ is not proper (i.e. it identifies everything with $0_{\mathbb{T}}$).

It remains to consider the case where b is nonzero and there is a nontrivial relation $1_{\mathbb{T}} \sim b$. Taking inverses on both sides, we also have $1_{\mathbb{T}} = b^{-1}$. Since inverse in $\mathbb{T}$ is negation in $\mathbb{R}$, we may therefore assume that b is positive in $\mathbb{R}$. For any c in the interval $(0, b)$ we then have $1_{\mathbb{T}} = 1_{\mathbb{T}} + c \sim b + c = c$. Repeating the argument with b replaced by b^n in $\mathbb{T}$ (which is nb in $\mathbb{R}$), for all positive integers n, we see that $1_{\mathbb{T}}$ is identified with every positive element of $\mathbb{R}$. Taking inverses then shows that $1_{\mathbb{T}}$ is identified with every element of $\mathbb{T} \smallsetminus 0_{\mathbb{R}}$, and hence $\mathbb{T}/\sim = \mathbb{B}$, as claimed.

Goal: We want to show one of the pieces of information that congruences can capture is a suitable notion of Krull dimension (of a semiring/algebra). We will see later that this can also be related to the dimension of geometric objects. In order to do this, we will define prime congruences and semifields of fractions and show that we can "extract" the dimension from the semiring of fractions.

Semifield of fractions:

Every (multiplicatively) cancellative semiring R embeds into its semifield of fractions, denoted $\mathrm{Frac}(R)$.

: If R is a ring then R is cancellative if and only if R has no zero-divisors. This fails for semirings. While we still have that a cancellative semiring has no zero-divisors, the converse is false. For example, $\mathbb{T}[x]$ has no zero divisors but $(x^2+1)(x^2+x+1) = (x^2+x+1)^2$.

The elements of $\mathrm{Frac}(R)$ are equivalence classes in $R \times (R \backslash \{0\})$ under the equivalence relation $(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1$. The operations on $\mathrm{Frac}(R)$ are given by

$$(r_1, s_1) + (r_2, s_2) = (r_1 s_2 + r_2 s_1, s_1 s_2)$$

and

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2).$$

We can also "localize" by certain smaller subsets of R, that is, construct $S^{-1}R$ for $S \subseteq R$. See [Go99, Chapter 11].

Prime congruences

Let R be a semiring, and let $\mathcal{C} \subset R \times R$ be a congruence.

Definition 5.22 (Twisted product)**.** *The twisted product of* $\alpha = (\alpha_1, \alpha_2)$ *and* $\beta = (\beta_1, \beta_2)$ *in* $R \times R$ *is*

$$\alpha * \beta = (\alpha_1\beta_1 + \alpha_2\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1).$$

Congruences are always closed under twisted product. Even more is true, if $\mathcal{C}$ contains $\alpha = (\alpha_1, \alpha_2)$ and if $\beta = (\beta_1, \beta_2)$ is an arbitrary element of $R \times R$, then $\alpha * \beta$ is in $\mathcal{C}$.

Remark 5.23. Suppose $\mathcal{C}$ is the congruence induced by an ideal I in a ring. Then I is prime if and only if $\alpha * \beta \in \mathcal{C}$ implies that $\alpha \in \mathcal{C}$ or $\beta \in \mathcal{C}$.

To see this, note that α is in $\mathcal{C}$ if and only if $\alpha_1 - \alpha_2$ is in I. So we are simply saying that I is prime if and only if $(\alpha_1-\alpha_2)(\beta_1-\beta_2) \in I$ implies either $(\alpha_1-\alpha_2) \in I$ or $(\beta_1 - \beta_2) \in I$.

Definition 5.24. *The congruence $\mathcal{C}$ is prime if it is a proper subset of $R \times R$ and $\alpha * \beta \in \mathcal{C}$ implies $\alpha \in \mathcal{C}$ or $\beta \in \mathcal{C}$.*

Definition 5.25. *The congruence $\mathcal{C}$ is irreducible if it has no nontrivial expression as an intersection of congruences.*

In other words, $\mathcal{C}$ is irreducible if whenever $\mathcal{C}$ is an intersection of two congruences $\mathcal{C}_1 \cap \mathcal{C}_2$ then $\mathcal{C} = \mathcal{C}_1$ or $\mathcal{C} = \mathcal{C}_2$. The following results on prime ideals appear in [JM17]. See the original paper for the proofs that are omitted.

Theorem 5.26 ([JM17] Theorem 2.12)**.** *If R is additively idempotent then a congruence $\mathcal{C} \subset R \times R$ is prime if and only if it is cancellative and irreducible.*

Recall from Definition 5.13 that if $\mathcal{C}$ is a cancellative congruence then $R/\mathcal{C}$ is a cancellative semiring, in other words, $(a, b) \in \mathcal{C}$ implies $(a, c) \in \mathcal{C}$ or $(b, 0) \in \mathcal{C}$.

Remark 5.27. While the definition of prime congruence makes sense in any semiring, the conclusion of Theorem 5.26 fails for semirings that are not additively idempotent.

An additively idempotent semiring carries a natural partial order, in which $a \leq b$ if and only if $a + b = b$. Semirings which are totally ordered play a special role in the theory.

Proposition 5.28. *If $\mathcal{C}$ is a prime congruence on an additively idempotent semiring R then $R/\mathcal{C}$ is totally ordered.*

Proof. Assume without loss of generality that $\mathcal{C} = \Delta$ and this is prime. Note that the twisted product $(a, a + b) * (b, a + b) = (a^2 + ab + b^2, a^2 + ab + b^2)$, which is in Δ. Therefore $(a, a + b) \in \Delta$ or $(b, b + a) \in \Delta$. This shows that $a \leq b$ or $b \leq a$, so R is totally ordered. $\square$

Remark 5.29. Note that if $R/\mathcal{C}$ is totally ordered it does not mean that $\mathcal{C}$ is prime. However, if $R/\mathcal{C}$ is also cancellative then $\mathcal{C}$ is prime. In other words, a congruence $\mathcal{C}$ is prime if and only if the quotient $R/\mathcal{C}$ is cancellative and totally ordered. See [JM17, Proposition 2.10].

Example 5.30. By the preceding remark, it is sensible to try to classify prime congruences on a semiring but considering the possible total orderings on the quotient. We now carry this through for the Laurent polynomial semiring over the Boolean semifield $\mathbb{B}[x^{\pm}]$.

Let $\mathcal{C}$ be a prime congruence on $\mathbb{B}[x^{\pm}]$. We consider the various possibilities for the order relation between $[x]$ and 1 in $\mathbb{B}[x^{\pm}]/\mathcal{C}$.

- If $[x] = 1$, then $\mathcal{C}$ contains the congruence generated by $(x, 1)$. Note that $\mathbb{B}[x^{\pm}]/\langle(x,1)\rangle = \mathbb{B}$, which has no nontrivial prime congruences. It follows that $\mathcal{C} = \langle(x,1)\rangle$.
- If $[x] > 1$, then $[x^i] > [x^j]$ for $i > j$. Therefore, every Laurent polynomial will be congruent to its monomial with highest exponent. For example, $x^2+x+1 \sim x^2$. So we see that $\mathbb{B}[x^{\pm}]/\mathcal{C} \cong (\mathbb{Z} \cup \{-\infty\}, \max, +)$.
- If $[x] < 1$ then $\mathbb{B}[x^{\pm}]/\mathcal{C} \cong (\mathbb{Z} \cup \{\infty\}, \min, +)$, by a similar argument.

A computation similar to that in the preceding example shows that there are no infinite chains of prime congruences on $\mathbb{B}[x]$. Note, however, that there are infinite chains of prime ideals in $\mathbb{B}[x]$ (as we saw in Lecture 2, Example 2.7), and $\mathbb{B}[x, y]$ has infinite chains of (non-prime) cancellative congruences. See [JM15, Proposition 2.12].

Definition 5.31. *Let R be an additively idempotent semiring. The Krull dimension $\dim R$ is the number of strict inclusions in the longest chain of prime congruences.*

Note: There may be maximal chains of prime congruences of different lengths, but there is a unique longest chain.

Theorem 5.32 ([JM15] Theorem 3.16)**.** *Let A be any (additively idempotent) semiring. Then $\dim A[x_1, \ldots, x_n] = \dim A + n$.*

In particular:

- $\dim \mathbb{B}[x] = 1$
- $\dim \mathbb{B}[x_1, \ldots, x_n] = n$
- $\dim \mathbb{T}[x_1, \ldots, x_n] = n + 1$

: This behavior is better than that of Krull dimension for arbitrary commutative rings R. If R is a ring then we only have $\dim R + 1 \leq \dim R[x] \leq 2 \dim R + 1$. For an example where $\dim R > 0$ and $\dim R[x] = 2 \dim R + 1$, see [Se54].

Definition 5.33. *The ideal-theoretic kernel of a congruence $\mathcal{C}$ on a semiring R is $\{x \in R \mid (x, 0) \in \mathcal{C}\}$. In other words, $\ker \mathcal{C}$ is the ideal-theoretic kernel of the quotient map $R \to R/\mathcal{C}$.*

Theorem 5.34 ([JM15] Proposition 3.15)**.** *Let R be (multiplicatively) cancellative and totally ordered. Then $\dim R = \dim \mathrm{Frac}(R)$. Moreover, the prime congruences $\mathcal{C}$ of R with $\ker \mathcal{C} = 0$ form a chain of maximum length.*

To show the above statement we need to relate the congruences of R and $\mathrm{Frac}(R)$. If C is a congruence on R we denote by $\langle C \rangle_{\mathrm{Frac}(R)}$ the congruence generated by C in $\mathrm{Frac}(R)$. On the other hand, if $\mathcal{C}$ is a congruence on $\mathrm{Frac}(R)$ we can restrict $\mathcal{C}$ to R and consider the congruence $\mathcal{C}|_R = \langle (a, b) \in \mathcal{C} \mid a, b \in R \rangle$.

Proposition 5.35 ([JM15] Proposition 3.8 (ii))**.** *Let R be a cancellative semiring and let C be a congruence of R such that R/C is cancellative and C has trivial kernel. Then $\langle C \rangle_{\mathrm{Frac}(R)} |_R = C$. Conversely, if $\mathcal{C}$ is a congruence in $\mathrm{Frac}(R)$ then $\langle \mathcal{C}|_R \rangle_{\mathrm{Frac}(R)} = \mathcal{C}$.*

This proposition gives us the dimension equality once we know that the claimed prime congruences form a chain of maximum length.

When R is not cancellative, let $P_0 \subset P_1 \subset \cdots \subset P_k$ be a chain of maximum length. Then consider R/P_0, and look at $\Delta \subset P_1' \subset \cdots \subset P_k'$.

Question 5.36 (Daping)**.** *Is is true that* $\dim A = \dim S^{-1}A$*, for some* $S \subsetneq A$*?*

References

[Go99] J. Golan, *Semirings and Their Applications*, Kluwer, Dordrecht, 1999

[JM17] D. Joó and K. Mincheva, *Prime congruences of idempotent semirings and a Nullstellensatz for tropical polynomials*, Selecta Mathematica (2017), doi:10.1007/s00029-017-0322-x

[JM15] D. Joó and K. Mincheva, *On the dimension of the polynomial and the Laurent polynomial semiring*, arXiv:1510.02493

[Les11] P. Lescot *Absolute Algebra II-Ideals and Spectra*, Journal of Pure and Applied Algebra 215(7), 2011, 1782-1790.

[Se54] A. Seidenberg, *On the dimension theory of rings II*, Pacific J. Math. 4 (1954) 603-614.