Algebraic geometry over the residue field of the infinite place

Márton Hablicsek
Mathematics Department, University of Pennsylvania
mhabli@math.upenn.edu

Máté L. Juhász
Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
juhasz.mate.lehel@renyi.mta.hu

January 10, 2017

Abstract

Nikolai Durov introduced the theory of generalized rings and schemes to study Arakelov geometry in an alternative algebraic framework, and introduced the residue field at the infinite place, $\mathbb{F}_\infty$. We show an elementary algebraic approach to modules and algebras over this object, define prime congruences, show that the polynomial ring of n variables is of Krull dimension n, and derive a prime decomposition theorem for these primes.

1 Introduction

In the category of schemes, the initial object is $\mathsf{Spec}\,\mathbb{Z}$, which is not a complete variety. Suren Yurevich Arakelov introduced the concept of Arakelov geometry in [1] and [2], by introducing Hermitian metrics on holomorphic vector bundles over the complex points of an arithmetic surface. Arakelov geometry can be used to study diophantine equations from a geometric point of view. For instance, it can be used to prove certain results over number fields which are known over function fields (see [4] and [7] for examples). In Nikolai Durov's doctoral dissertation ([3]), Durov introduces a new approach to Arakelov geometry, the theory of generalized rings and fields, and uses them, among others, to construct a completion of $\mathsf{Spec}\,\mathbb{Z}$.

To understand the completion, consider that the divisor of a rational function on a complete curve is always of degree zero. Put differently, the sum of all valuations of a rational function at all points of the curve gives zero. The analoguous formulation for $\mathsf{Spec}\,\mathbb{Z}$ states that the product of all valuations on $\mathbb{Q}$ of a rational number is always one. Recall that the valuations on $\mathbb{Q}$ are of two kinds: an Archimedean valuation $|.|$ and for all primes p a non-Archimedean valuation $|.|_p$. Just like the valuations of a complete curve, each non-Archimedean valuation on $\mathbb{Q}$ corresponds to a closed point of $\mathsf{Spec}\,\mathbb{Z}$, however, the Archimedean valuation, called for analogical reasons the *valuation at the infinite place or infinity*, is missing from $\mathsf{Spec}\,\mathbb{Z}$.

Durov uses this idea to complete $\mathsf{Spec}\,\mathbb{Z}$, and, among others, he defines the residue field corresponding to the valuation at infinity. In general, for a prime p, we introduce $\mathbb{Z}_{(p)} = \{q \in \mathbb{Q} \mid |q|_p \leq 1\}$ and the open unit ball $U_p := \{q \in \mathbb{Z}_{(p)} \mid |q|_p < 1\}$, and define the residue field as the quotient $\mathbb{F}_p = \mathbb{Z}_{(p)}/U_p$. For the Archimedean valuation, $\mathbb{Z}_{(\infty)} = [-1,1] \cap \mathbb{Q}$ and $U_\infty = (-1,1) \cap \mathbb{Q}$, and $\mathbb{F}_\infty$ is, intuitively, the closed interval $[-1,1]$ with its interior identified as a single element, 0. This is in fact the underlying set of the object that Nikolai Durov refers to as $\mathbb{F}_\infty$. In this paper we investigate algebras over this generalized ring.

The paper consists of two parts. First, instead of using Nikolai Durov's full machinery, we give a gentle introduction to the theory of algebras and modules over $\mathbb{F}_\infty$. In Section 2, we introduce semifields, including finite extensions, modules and algebras, and motivate using polynomial rings as the ring of functions. By looking at modules as semilattices, with the addition functioning as a meet-operation, in Section 3 we show how these can be extended into lattices (3.4, 3.17), and use this to understand dual modules (3.7, 3.17) and Hom-modules (3.26), at first for finite modules, then using topology, to infinite modules. In fact, any module can be embedded into one where infinite sums and joins exist. In Section 4, we examine the theory of congruences and kernels. In particular, it turns out that for any ideal there is always a maximal congruence whose kernel is the ideal, which can be identified by a separability condition (4.7 and 4.9). Then we turn to congruences in semifields, where the congruence is characterized completely by the equivalence class of 1, neatly mirroring classical ring theory with the equivalence class of 0.

Second, we take the first steps towards algebraic geometry over $\mathbb{F}_\infty$. Our theory is mainly motivated by a novel approach by Dániel Joó and Kalina Mincheva ([5], [6]). One of the key ideas in these papers is that congruences are more natural objects to study than ideals. The authors define prime congruences, and study tropical geometry using prime congruences instead of prime ideals. We follow this key idea and we define prime congruences in algebras over $\mathbb{F}_\infty$ and, among others, we show that the polynomial ring of n variables has Krull dimension n (see Corollary 6.3), and we derive a prime decomposition theorem (see Theorem 7.10). As a consequence, we bring in line the theory of modules and algebras over $\mathbb{F}_\infty$ with the theory of classical finite fields.

Acknowledgement: We thank Kalina Mincheva and Dániel Joó for patiently explaning their work to us. Most of the techniques we use in the second part of the paper appear in some form in their work.

2 Modules and algebras over $\mathbb{F}_\infty$

Intuitively, a module over the field at infinity, $\mathbb{F}_\infty$, correspond to the faces of a symmetric polyhedron, where the binary operation is *the smallest face containing both.* Then the field $\mathbb{F}_\infty$ itself is the digon $[-1, 1]$ with three elements: 1, -1 and 0, and the binary operation is *the element between.* Although there are modules that can not be realized as actual symmetric polyhedra, this can be a useful visualization.

Definition 2.1. *An $\mathbb{F}_\infty$-**module** is a structure $(V, 0_0, -_1, +_2)$ such that:*

- $(a + b) + c = a + (b + c)$, $a + b = b + a$;
- $a + a = a$, $a + (-a) = 0$;
- $-(a + b) = (-a) + (-b)$; $-(-a) = a$.

*A **submodule**, **congruence**, **quotient module** and **module homomorphism** are defined as usual.*

In particular, 0 is an absorbing element in an $\mathbb{F}_\infty$-module.

Example. *The set $\mathbb{F}_\infty = \{-1, 0, 1\}$ is a $\mathbb{F}_\infty$-module, defined uniquely by the module axioms.*

Proposition 2.2. *An $\mathbb{F}_\infty$-module has a natural partial order defined by $a \leq b$ if $a + b = a$, with 0 being the smallest element, i.e. $0 + x = 0$.*

Proof. Reflexivity arises from idempotence, symmetry from commutativity. If $a \leq b \leq c$, then $a + b = a$ and $b + c = b$, hence $a + c = (a + b) + c = a + b = a$, therefore $a \leq c$. □

Definition 2.3. *A **maximal element** x is such that there is no such y that $x < y$, i.e. $x + y = x$ if and only if $x = y$. A **minimal element** x is such that $y < x$ only for $y = 0$, i.e. $x + y = y$ if and only if $x = y$ or $y = 0$.*

We will also need rings over $\mathbb{F}_\infty$:

Definition 2.4. *An $\mathbb{F}_\infty$-**algebra** or **ring** is a $\mathbb{F}_\infty$-module A with a semigroup structure $(A, \cdot_2)$ such that*

- $a \cdot 0 = 0 \cdot a = 0$;
- $-a \cdot b = a \cdot -b = -(a \cdot b)$;
- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

*A **unital commutative algebra** is a commutative monoid structure $(V, 1_0, \cdot_2)$ such that $a \cdot 1 = 1 \cdot a = a$. An **invertible element** a is such that there is an a^{-1} such that $a \cdot a^{-1}$, and the group of invertible elements is denoted by $A^\times$. The unital algebra is a **division algebra** or **(semi)field** if $(V \setminus \{0\}, 1, \cdot)$ is a group.*

Proposition 2.5. *In a finite unital algebra, all invertible elements are unordered.*

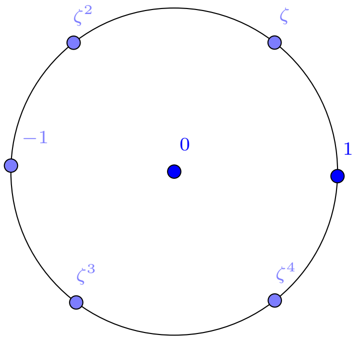
Proof. First, 1 is not less than any invertible element, since if $1 < a$ for a invertible, then a^i gives an infinite increasing sequence. Similarly 1 is not greater than any invertible element. Then, if a and b are invertible, and $a < b$, we may multiply both sides by a^{-1}, which preserves the inequality by the distributivity of multiplication. Hence $1 < a^{-1}b$, which is a contradiction. □

Corollary 2.6. *In a finite division algebra, all non-zero elements are minimal and maximal. Hence for any a, $b \in A$, $a + b = 0$ unless $a = b$.*

Example.

- *The field $\mathbb{F}_\infty$ is the commutative division algebra generated by 1. Its underlying set is $\{-1, 0, 1\}$ with $a + b = 0$ unless $a = b \neq 0$.*

- *The field $\mathbb{F}_{\infty^k}$ is a commutative division algebra generated by ζ_k such that $\zeta_k^k = -1$. Its elements are $\{\zeta_k^i \mid i \in \{0, 1, \dots, 2k-1\}\}$. These fields can be embedded as subsets of $\mathbb{C}$, and the diagram below shows the $k = 3$ case.*



- *Given $k|\ell$, there is a natural embedding of $\mathbb{F}_{\infty^k}$ into $\mathbb{F}_{\infty^\ell}$, given by $\zeta_k = \zeta_\ell^{\ell/k}$. The field $\mathbb{F}_{\infty^\infty} := \varinjlim \mathbb{F}_{\infty^k}$ can be embedded as a subset of $\mathbb{C}$. Its elements are the roots of unity and 0.*

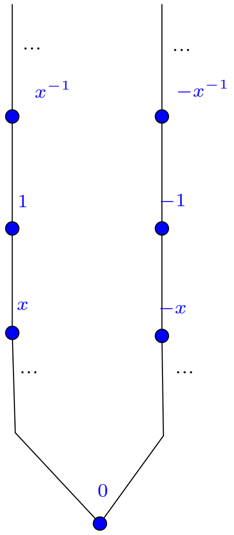
- *The underlying sets of all these finite fields can be embedded into $\mathbb{C}$ as the kth roots of unity. The Euclidean closure of $\mathbb{F}_{\infty^\infty}$ in $\mathbb{C}$ is given as $\overline{\mathbb{F}_{\infty^\infty}} := \mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\} \cup \{0\}$. Using the multiplication on $\mathbb{C}$ and defining addition as $a + b = 0$ unless $a = b$, this gives a field structure to the set $\overline{\mathbb{F}_{\infty^\infty}}$.*

- *We may also consider the extension with $\zeta^k = 1$. In this case, its elements are $\pm\zeta^i$ for $i \in \{0, \dots, k\}$. These and $\mathbb{F}_{\infty^k}$ will appear later as quotients of the polynomial ring $\mathbb{F}_\infty[x]$ in 5.9.*

- *More generally, given a group G and a field $\mathbb{F}$, the* ***group algebra*** $\mathbb{F}[G]$ *consists of elements 0 and λg with $\lambda \in \mathbb{F}^\times$ and $g \in G$, with the law of addition that $\lambda g + \lambda' g' = (\lambda + \lambda')g$ if $g = g'$, otherwise 0, and $\lambda g \cdot \lambda' g' = (\lambda\lambda')(gg')$. The previous example is in fact $\mathbb{F}_\infty[\mathbb{Z}/k\mathbb{Z}]$.*

- *There is a more general way to construct fields. Consider a commutative group G with an injective map $f\colon \mathbb{F}_\infty^\times \to G$. Then the set $G \cup \{0\}$ has a natural $\mathbb{F}_\infty$-algebra structure that is a division algebra, defined via the group operation as multiplication, $a + b = 0$ unless $a = b$, and $-a = f(-1)a$. This generalizes group algebras, with $G = \mathbb{F}^\times \times H$ for $\mathbb{F}[H]$.*

- *For an example of a division algebra where the order is non-trivial, consider the set $\{\pm x^i \mid i \in \mathbb{Z}\} \cup \{0\}$ with the addition $x^i + x^j = x^i$ if $i \geq j$, and $x^i \cdot x^j = x^{i+j}$.*



Modules and algebras can also be considered over other fields.

Definition 2.7. *Assume $\mathbb{A}$ is an $\mathbb{F}_\infty$-algebra. An $\mathbb{A}$-module M is an $\mathbb{F}_\infty$-module with a binary operation $\mathbb{A} \times M \to M$, such that*

- $a \cdot (b \cdot m) = (a \cdot b) \cdot m$ *for* $a, b \in \mathbb{A}$, $m \in M$;

- $a \cdot (m + n) = a \cdot m + a \cdot n$ *and* $(a + b) \cdot m = a \cdot m + b \cdot m$ *for* $a, b \in \mathbb{A}$, $m, n \in M$;

- $(-a) \cdot m = -(a \cdot m) = a \cdot (-m)$ *for* $a \in \mathbb{A}$, $m \in M$;

- $0 \cdot m = a \cdot 0 = 0$ *for* $a \in \mathbb{A}$, $m \in M$;

- *If $\mathbb{A}$ is unital, we further postulate $1 \cdot m = m$ for $m \in M$.*

An $\mathbb{A}$-algebra M is an $\mathbb{A}$-module that is also an $\mathbb{F}_\infty$-algebra, such that

- *$a \cdot (m \cdot n) = (a \cdot m) \cdot n = m \cdot (a \cdot n)$ for $a \in \mathbb{A}$, m, $n \in M$.*

Henceforth we will consider only unital algebras.

Let $\mathbb{F}$ denote an $\mathbb{F}_\infty$-division algebra. Recall that $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.

Definition 2.8. *The **dimension** of an $\mathbb{F}$-module M, denoted by $\mathsf{dim}\, M$, is the maximal length of a chain of decreasing elements.*

Example. *Fix an integer $n \geq 2$, and let us denote the vertices of a regular $2n$-gon P by v_i for $i \in \{0, \ldots, 2n-1\}$ and the edges connecting v_i to v_{i+1} by e_i. The lattice of all faces $\{P, v_i, e_i \mid i \in \{0, \ldots, 2n-1\}\}$ has a natural $\mathbb{F}_\infty$-module structure with $P = 0$, $-v_i = v_{i\pm n}$ and $v_i + v_{i+1} = e_i$, otherwise $x + y = 0$. It has dimension 2, since the sum of pairwise uncomparable elements is non-zero if and only if there is a single term, or two adjecent vertices.*

Example. *Given a convex, symmetric polyhedron P in $\mathbb{R}^n$ such that it has a non-empty interior, the set of faces has a natural $\mathbb{F}_\infty$-module structure with $P = 0$ and $f + f'$ is the smallest face that contains f and f'. This has dimension n, as the longest chain of faces contains one of each dimension, including P.*

Definition 2.9. *For two modules M_1 and M_2, $M_1 + M_2$ is the **coproduct**, whose elements are of the form $m_1 \in M_1$, $m_2 \in M_2$ and $m_1 \oplus m_2$, with $0_{M_1} = 0_{M_2} = 0_{M_1} + 0_{M_2}$ identified.*
*$M_1 \times M_2$ is the **Cartesian product**. The **free module** generated by n elements is given by $\mathbb{F} + \cdots + \mathbb{F}$.*
The set of module-homomorphisms is denoted by $\mathsf{Hom}(M_1, M_2)$.

Proposition 2.10. *The coproduct and Cartesian product are the category theoretical coproduct and product. Also, the free module $\mathcal{F}(S)$ generated by a set S is isomorphic to the infinite coproduct $\sum_{s \in S} \mathbb{F}$.*

Proof. These are all trivial consequences of theorems in universal algebra. □

Proposition 2.11. *$\mathsf{Hom}(M_1, M_2)$ has a natural $\mathbb{F}$-structure.*

Proof. The pointwise sum and scalar multiple of two homomorphisms is a homomorphism. □

Definition 2.12. *Given two $\mathbb{F}$-modules M_1 and M_2, the **tensor product** $M_1 \otimes M_2$ is a module with a natural bilinear map $M_1 \times M_2 \to M_1 \otimes M_2$ where $M_1 \times M_2$ is the set of pairs, such that for any bilinear map $M_1 \times M_2 \to N$ for some other module N, there is exactly one map $M_1 \otimes M_2 \to N$ that makes the diagram $M_1 \times M_2 \to M_1 \otimes M_2 \to N$ commute.*

Proposition 2.13. *Given two $\mathbb{F}$-modules M_1 and M_2, $M_1 \otimes M_2$ exists and is unique. It is generated by elements of the form $m_1 \otimes m_2$ with $m_1 \in M_1$ and $m_2 \in M_2$. Furthermore $\cdot \otimes M$ is a covariant functor.*

Proof. This is a classical theorem from universal algebra, and the proof is identical to the case of vector spaces. Uniqueness can be checked via diagram chasing. We can prove the existence by constructing $M_1 \otimes M_2$ explicitly. Let us consider the free module generated by pairs $m_1 \otimes m_2$ with $m_1 \in M_1$ and $m_2 \in M_2$, and quotienting by the congruence generated by $(m_1+m_1')\otimes m_2 \sim m_1\otimes m_2+m_1'\otimes m_2$, $\lambda(m_1 \otimes m_2) \sim (\lambda m_1) \otimes m_2 \sim m_1 \otimes (\lambda m_2)$. Naturally, any bilinear map $M_1 \times M_2 \to N$ extends uniquely into a map $M_1 \otimes M_2 \to N$.

Finally, for the functoriality, given a map $f\colon A \to B$, we need to construct $A \otimes M \to B \otimes M$. We may define the bilinear map $A \times M \to B \otimes M$ defined by $(a, m) \to f(a) \otimes m$, and this extends into the desired map. Identity and composition can be checked as usual. □

Proposition 2.14. *$\mathsf{Hom}(M_1, \mathsf{Hom}(M_2, M_3)) \cong \mathsf{Hom}(M_1 \otimes M_2, M_3)$, $A \otimes \mathbb{F} \cong A$, $(A + B) \otimes C \cong (A \otimes C) + (B \otimes C)$.*

Proof. Since elements of $\mathsf{Hom}(M_1, \mathsf{Hom}(M_2, M_3))$ correspond naturally to bilinear maps $M_1 \times M_2 \to M_3$, there is a natural embedding to $\mathsf{Hom}(M_1 \otimes M_2, M_3)$. On the other hand, a map $\varphi\colon M_1 \otimes M_2 \to M_3$ restricts to a map $\varphi'\colon M_1 \times M_2 \to M_3$ that is bilinear. Therefore $\varphi'(m)$ for $m \in M_1$ is a homomorphism, and φ' is a homomorphism from M_1.

The second one is trivial, since an element $a \otimes \lambda \in A \otimes \mathbb{F}$ is equal to $(\lambda a) \otimes 1$.

For the third one, there is a natural bilinear map from $(A + B) \times C$ to $A \otimes C + B \otimes C$, defined as $(a \oplus b, c) \to (a \otimes c) \oplus (b \otimes c)$, which extends to a unique map $(A + B) \otimes C \to A \otimes C + B \otimes C$. On the other hand, since $A \otimes C + B \otimes C$ is the coproduct, and there are maps from $A \otimes C$ and $B \otimes C$ to $(A + B) \otimes C$, these define a unique map $A \otimes C + B \otimes C \to (A + B) \otimes C$. It can be shown that the composition in either direction is the identity using the universality of the tensor product and the corpoduct. □

To do algebraic geometry, we need to construct the coordinate ring of an affine space.

Definition 2.15. *The* ***free ring*** *or* ***polynomial ring*** *in n variables x_1, …, x_n over $\mathbb{F}$, denoted by $\mathbb{F}[x_1, \dots, x_n]$, is the free coproduct*

$$\sum_{\mu \in \mathbb{N}^n_{\geq 0}} (x_1^{\mu_1} \cdot \dots \cdot x_n^{\mu_n})\mathbb{F}$$

with multiplication defined on monomials and extended to the ring.

Unfortunately, contrary to the theory of classical fields, the n-dimensional module is not unique, hence we should not expect a single coordinate ring for each dimension. In fact, each module gives rise to an affine space, with identical underlying set, and they will correspond to different coordinate rings. To motivate the definition, we will first consider homogeneous functions over projective spaces.

Definition 2.16. *Let A be an $\mathbb{F}$-algebra. Then $\bigotimes^n A$ or $A^{\otimes n}$ denotes the tensor product $A \otimes \cdots \otimes A$. The congruence generated by $\mathbf{a}_1 \otimes a_2 \otimes a_3 \otimes \mathbf{a}_4 \sim \mathbf{a}_1 \otimes a_3 \otimes a_2 \otimes \mathbf{a}_4$ for $\mathbf{a}_1 \in A^{\otimes n_1}$, $\mathbf{a}_4 \in A^{\otimes n_2}$ for $n_1 + n_2 + 2 = n$ and a_2, $a_3 \in A$ is the kernel of the surjective map $A^{\otimes n} \to \mathsf{Sym}^n A$ that defines the* ***symmetric power*** *of A. Furthermore, there are natural maps $\bigotimes^{n_1} A \otimes \bigotimes^{n_2} A \to \bigotimes^{n_1+n_2} A$ and $\mathsf{Sym}^{n_1} A \otimes \mathsf{Sym}^{n_2} A \to \mathsf{Sym}^{n_1+n_2} A$.*

Note that $\mathbb{F}[x_1, \ldots, x_n]$ is isomorphic as a module to $\sum_{i=0}^{\infty} \mathsf{Sym}^i \mathcal{F}(\{x_1, \ldots, x_n\})$.

Definition 2.17. *Given an $\mathbb{F}$-module M, its* ***projectivization*** *$\mathbb{P}M$ is the set of equivalence classes of $\{m \in M \mid m \neq 0\}$ identified by $m \sim \lambda m$ for some $\lambda \in \mathbb{F}$.*

We need to give a projective closure to an affine space. For simplicity, we shall define affine spaces as modules. In the classical case, the affine part of a projective space is given by a function on the underlying vector space, so given a module M and its closure $\mathbb{P}N$, there should be a natural map $N \to \mathbb{F}$, with the preimage of 1 isomorphic to M. The most natural way to do this is if $N = M \times \mathbb{F}$.

Definition 2.18. *Given an $\mathbb{F}$-module M, $\mathbb{P}(M \times \mathbb{F})$ is the* ***projective closure****, and M is the* ***affine part*** *of $\mathbb{P}(M \times \mathbb{F})$.*

There is a straightforward way to define homogeneous functions of a fixed degree on a projective space, and we can use it to define functions on its affine part.

Definition 2.19. *Given a module M, the* ***homogeneous functions of degree*** *n on the projective space $\mathbb{P}M$ is given by $\mathsf{Sym}^n M^*$.*

Proposition 2.20. *Given a module M whose projective closure is $\mathbb{P}N$ with $N = M \times \mathbb{F}$, the homogeneous functions of degree n are in a bijection with the module $\sum_{k=0}^{n} \mathsf{Sym}^k M^*$.*

Proof. Since $N \cong M \times \mathbb{F}$, $N^* \cong M^* + \mathbb{F}$. Recall that $(A + B) \otimes C \cong (A \otimes C) + (B \otimes C)$, hence $\bigotimes^n (M^* + \mathbb{F}) \cong \sum_{k=0}^{n} \bigotimes^k M^* \otimes \bigotimes^{n-k} \mathbb{F} \cong \sum_{k=0}^{n} \bigotimes^k M^*$. Symmetrization does not identify terms from different components, hence $\mathsf{Sym}^n(M^* + \mathbb{F}) \cong \sum_{k=0}^{n} \mathsf{Sym}^k M^*$. □

This proposition provides us with a natural definition for a ring of functions.

Definition 2.21. *Given a module M, the* ***symmetric ring*** *of M is defined as $\mathsf{Sym}\, M := \sum_{n=0}^{\infty} \mathsf{Sym}^n M$. The* ***ring of functions*** *over M is defined as $\mathbb{F}[M] := \mathsf{Sym}^n M^*$.*

Proposition 2.22. *The free ring in n variables, $\mathbb{F}[x_1, \ldots, x_n]$ is the ring of functions over the module $\prod_{i=1}^{n} \mathbb{F}$. The ring of functions over the module $\sum_{i=1}^{n} \mathbb{F}$ is $\sum_{n=0}^{\infty} \prod^n \mathbb{F}$.*

3 Ordered structure

Recall from Proposition 2.2 that an $\mathbb{F}$-module for a given $\mathbb{F}_\infty$-division algebra has a natural partial order. It has many of the usual properties of an ordered algebraic structure:

Proposition 3.1. *Given an $\mathbb{F}$-module M and elements a, b, $c \in M$ such that $a \leq b$, we have $a+c \leq b+c$ and $ac \leq bc$, and if $c \leq d \in M$, we have $a+c \leq b+d$ and $ac \leq bd$. In particular, if $a \leq b$ then $-a \leq -b$ as well. Also, if $a \leq b$ and $a \leq c$ then $a \leq b + c$.*

Proof. These are elementary consequences of the definition, the idempotence of additivity and distributivity. □

Such a module is in fact a **semilattice** with respect to the meet-operation, $+_2$. It has clearly no lattice structure, since if a, $-a \leq x$ for some x and $a \neq 0$, we would have $a \leq -x$ and $a \leq x + -x = 0$, a contradiction. This can be salvaged by the introduction of a largest element.

Definition 3.2. *For an $\mathbb{F}$-module M, we will denote by $\overline{M}$ the set $\{\omega\} \cup M$ where $\omega > a$ for all $a \in M$, and call it the **order closure** or **closure** of M. We may extend the operations as partial operations via $a + \omega = a$ and $\lambda\omega = \omega$ for $\lambda \neq 0$. 0ω is undefined.*

Definition 3.3. *An $\mathbb{F}$-module M is called a **lattice** if the order closure $\overline{M}$ of M has a lattice structure. This means that for any a, $b \in M$, there is an upper bound $a \cup b \in \overline{M}$.*

Theorem 3.4. *A finitely generated $\mathbb{F}$-module M is a lattice.*

Proof. If M is finitely generated, then there is a finite set G of generators, and the sum $a \cup b := \sum\limits_{\substack{x \in G \\ x \geq a,b}} x$ is finite and well-defined. Now assume that $d \geq a$, b. Since M is finitely generated, there is a finite subset $G(d) \subseteq G$ such that $d = \sum_{x \in G(d)} x$. Then $x \geq a$, b for all $x \in G(d)$, hence $d \geq a \cup b$. Therefore $a \cup b$ is a lower bound. □

The lattice structure permits us to construct a **dual lattice**, one where $+$ and $\cup$ switch places. For finite modules, it turns out that the dual lattice has a natural algebraic meaning: the module of linear functions to $\mathbb{F}$. This can be expressed through the natural duality.

Definition 3.5. *For an $\mathbb{F}$-module M, there is a **natural duality** $(\cdot,\cdot)\colon (M \setminus \{0\}) \times M \to \mathbb{F}$ defined as $(a, b) = \varepsilon$ if $b \geq \varepsilon a$, and 0 if no such ε exists. We extend it to $(a, b)\colon \overline{M} \times \overline{M} \setminus \{(0, 0), (\omega, \omega)\} \to \overline{\mathbb{F}}$, defined via $(\omega, a) = 0$, $(a, \omega) = \omega$, $(a, 0) = \omega$.*

Proposition 3.6. *The natural duality on M is well defined, and in particular, the map $a^* := (a, \cdot)$ is a homomorphism from M to $\mathbb{F}$ for all $a \in \overline{M} \setminus \{0\}$. Also, $(\mu a, b) = \mu^{-1}(a, b)$ for $\mu \in \mathbb{F}^\times$.*

Proposition 3.7. *If M is a finite module, then there is a natural order-reversing bijection between $\overline{M}$ and $\overline{M^*}$ where $M^* := \mathsf{Hom}(M, \mathbb{F})$, and the addition on M^* is given by $\cup$.*

Proof. Any element $a \in \overline{M} \setminus \{0\}$ gives a natural map $a^* \colon M \to \mathbb{F}$. Consider a function $f \colon M \to \mathbb{F}$ that is not trivially zero. Then the sum $F = \sum\{c \mid f(c) = 1\}$ is well-defined, and $F^* = f$. □

Now let us look at how to define dual modules for infinite modules. The following propositions show the naïve way of looking at homomorphic maps to the base field.

Proposition 3.8. *For a given $\mathbb{F}$-module M, homomorphic maps $f \colon M \to \mathbb{F}$ are in a bijection with filters F, given by $a \in F \Leftrightarrow f(a) = 1$.*

Proposition 3.9. *The set of filters F on a given $\mathbb{F}$-module M form an $\mathbb{F}$-module M^F, given by $0_{M^F} = \emptyset$, $F_1 + F_2 = F_1 \cap F_2$ and $\varepsilon \cdot F = \{\varepsilon^{-1} a \mid a \in F\}$ for $\varepsilon \in \mathbb{F}^\times$.*

Proposition 3.10. *There is a natural injection $M \to (M^F)^F$, given by sending a to $\hat{a} := \{F \in M^F \mid a \in F\}$. This is not always a bijection.*

This is in contrast to the finite case, when M and $(M^*)^*$ are isomorphic. By introducing a weak form of topology, we can define a better concept of dual module.

Definition 3.11. *A **principal filter** of an $\mathbb{F}$-module M is a filter of the form $F_a = \{x \in M \mid a \leq x\}$, and it is said to be **generated by** a. We say that an $\mathbb{F}$-module M has a **topology with respect to filters** if all principal filters are closed. A **topology with respect to the order** is such that F_a and all sets of the form $L_a = \{x \in M \mid a \geq x\}$ are closed.*

When no topology is specified, we may assume the discrete topology where all filters are closed.

Given a filter F and an element $a \in M$, we will denote by $F(a) = \varepsilon \in \mathbb{F}^\times$ if $a \in \varepsilon F$, and $F(a) = 0$ if no such ε exists. This is compatible with the natural duality for principal filters: $F_a(b) = (a, b)$.

Definition 3.12. *If M is an $\mathbb{F}$-module M with topology with respect to filters, let us denote by M^* the set of closed filters. It is called the **dual module** of M. M^* is an $\mathbb{F}$-module, where $0_{M^*} := \emptyset_M$, $F_1 + F_2 = F_1 \cap F_2$, $\lambda \cdot F = \{\lambda^{-1} \cdot a \mid a \in F\}$. Its **filter-topology** has a closed basis given by $C_a := \{\Phi \in M^* \mid a \in \Phi\}$ for all $a \in M$, and is a topology with respect to filters. Its **weak topology** is generated by all C_a and their complements $\overline{C_a}$, and is a topology with respect to the order.*

Proposition 3.13. *Given a descending sequence $(x_i)_{i \in I}$ in M^* indexed by a directed set I, the intersection is an accumulation point with respect to either the filter-topology or the weak topology.*

Proof. Consider the point $x = \bigcap_{i \in I} x_i$. To prove that it is an accumulation point, we need to show that every open set containing x contains all x_i for $i \geq i_0$ for some $i_0 \in I$. Since an open basis is given by the complement $\overline{C_a}$ of C_a, all open sets containing x must contain an open set of the form $\bigcap_{a \in S} \overline{C_a}$ for a finite set $S \subseteq M$, hence it is enough to show this statement for open sets of this form. Since $x \in C := \bigcap \overline{C_a}$, this is equivalent to $a \notin x$ for all $a \in S$, and since x is the intersection of all x_i, there is an i_a for all a such that $a \notin x_{i_a}$. Being a directed set, I contains an index i_0 such that $i_0 \geq i_a$ for all $a \in S$, because S is finite, and since (x_i) is descending, $a \notin x_i$ for all $i \geq i_0$ and $a \in S$. Hence $x_i \in C$. The case of weak topology is similar, but open sets of the form C_a may also appear in the intersection C. □

Corollary 3.14. *Given a closed filter Φ in either the filter-topology or the weak topology on M^*, and a subset $S \subseteq \Phi \subseteq M^*$, the infinite intersection $\bigcap_{s \in S} s$ exists and is an element of Φ.*

Proof. Since the elements of M^* are closed filters on M, their intersection is also a closed filter, hence an element of M^*. We only need to show that it is an element of Φ. This can be proven by transfinite recursion on the cardinality of S. When S is finite, it is a trivial consequence of the definition of a filter. When S is infinite, let I be the powerset of S, and for $i \subseteq S$, let $s_i := \bigcap_{s \in i} s$. By transfinite recursion, all s_i exist and are contained in Φ. Then $(s_i)_{i \in I}$ is a descending sequence, and the intersection $\bigcap_{s \in S} s$ is its accumulation point. Therefore it is in Φ. □

Theorem 3.15. *Given an $\mathbb{F}$-module, there is a natural embedding $M \to (M^*)^*$, given by $\hat{a} := \{F \in M^* \mid a \in F\}$.*

Proof. This is a homomorphism since $\widehat{a + b} = \hat{a} \cap \hat{b}$, an embedding since $\Phi_a := \{x \in M \mid a \leq x\}$ is such that $\Phi_a \in \hat{b}$ if and only if $a \leq b$, so if $\hat{a}$ and $\hat{b}$ both contain Φ_a and Φ_b, then $a = b$. □

Definition 3.16. *A module M is* **complete** *if every closed filter is principal.*

Theorem 3.17. *A complete module is a lattice, and it admits an order reversing isomorphism to its dual.*

Proof. The second part of the statement is a trivial consequence of the definition of a complete module. Consider a complete module M and two elements a, $b \in M$. The filter $F := F_a \cap F_b$ is closed and contains all elements x such that a, $b \leq x$. Since M is complete, F is principal, generated by c, hence a, $b \leq c$ and for all $x \in F$, $c \leq x$. □

Proposition 3.18. *Every finite module is complete with respect to the discrete topology.*

Proof. Every filter is finite, hence it is generated by the sum of its elements. □

Theorem 3.19. *The module M^* is complete and is a lattice, with respect to either the filter-topology or the weak topology.*

Proof. Given a closed filter $\Phi \subseteq M^*$, the intersection $\bigcap \Phi$ is an element of Φ. Since $\bigcap \Phi \leq a$ for all $a \in \Phi$, Φ is the principal filter generated by $\bigcap \Phi$. □

Since the closed filters of M^* are the same in the filter-topology and the weak topology, $(M^*)^*$ is isomorphic as an $\mathbb{F}$-module whether M^* is endowed with one or the other. Since there is an isomorphism $M \cong (M^*)^*$ for complete modules M, the weak topology can be defined for them as well.

Proposition 3.20. *Every complete module M with a topology with respect to filters has a refined topology with respect to the order, referred to as its **weak topology**, and the order reversing bijection $\overline{M} \to \overline{M^*}$ is continuous.*

Proposition 3.21. *Consider two $\mathbb{F}$-modules M_1 and M_2, with either the discrete topology, or a topology with respect to filters. Let us define the closed filters of $M_1 \otimes M_2$ to be those filters F where $\{a \mid a \otimes b \in F\}$ and $\{b \mid a \otimes b \in F\}$ are closed. Then $(M_1 \otimes M_2)^* \cong \mathsf{Hom}(M_1, M_2^*)$, where $\mathsf{Hom}(M_1, M_2^*)$ is the module of continuous homomorphisms to M_2 with the topology with respect to filters.*

Proof. Elements of $(M_1 \otimes M_2)^*$ are closed filters on $M_1 \otimes M_2$, while elements of $\mathsf{Hom}(M_1, M_2^*)$ are continuous maps from M_1 to closed filters of M_2. Given a filter F on $M_1 \otimes M_2$ and a map $\varphi\colon M_1 \to M_2^*$, we will identify them if for any $m_1 \in M_1$ and $m_2 \in M_2$, $m_1 \otimes m_2 \in F$ if and only if $\varphi(m_1) \ni m_2$. It can be checked that this defines a bijection between filters on $M_1 \otimes M_2$ and maps $M_1 \to M_2^*$.

Now assume that there is corresponding pair of a filter F and a map φ. Given an element $m_1 \in M_1$, we need to see when $\varphi(m_1)$ is closed. It consists of those m_2 where $m_1 \otimes m_2 \in F$, which is a closed set if F is closed. To make φ continuous, let us fix a closed set from the basis of topology of M_2^*, C_{m_2} for some $m_2 \in M_2$. Then $\varphi^{-1}(C_{m_2}) = \{m_1 \mid \varphi(m_1) \in C_{m_2}\}$. Since $\Phi \in C_{m_2}$ if and only if $m_2 \in \Phi$, we get $\varphi^{-1}(C_{m_2}) = \{m_1 \mid m_2 \in \varphi(m_1)\} = \{m_1 \mid m_1 \otimes m_2 \in F\}$, which is true if F is closed. Furthermore, if φ maps pointwise to closed filters and is continuous, then F is closed as well. □

Proposition 3.22. $(A + B)^* \cong A^* \times B^*$, $(A \times B)^* \cong A^* + B^*$.

Proof. Since $A \to A^*$ defines a contravariant functor from the category of $\mathbb{F}$-modules to itself, and the product and coproduct are dual to each other, these equalities hold. □

Definition 3.23. *Given a module M with a topology, we say that **all sums exist** if for any set $S \subseteq M$ there is a lower bound.*

In particular, finite modules (with the discrete topology) and complete modules with the weak topology are such that all sums exist.

Proposition 3.24. *Assume that all sums exist in M_1. A homomorphism $\varphi\colon M_1 \to M_2$ admits a natural dual $\varphi^*\colon M_2^* \to M_1^*$, identified by $\varphi^*(\mu) = (\sum\{m \in M_1 \mid \varphi(m) \geq \mu^*\})^*$ where μ^* is defined through $(\mu^*)^* = \mu$.*

Proof. There is a natural map $\varphi^*\colon M_2^* \to M_1^*$ defined as $\varphi^*(\mu)(m) = \mu(\varphi(m))$, so we just have to prove that it is indeed given by the above identification. Consider the φ^* defined as in the statement, and denote $\mu_0 := \sum\{x \in M_1 \mid \varphi(x) \geq \mu^*\}$. We have $\varphi(x) \geq \mu^*$ if and only if $\mu(\varphi(x)) = 1$. We need to prove that $\mu_0^*(x) = \mu(\varphi(x))$ for all $x \in M_1$.

Consider a $\varepsilon \in \mathbb{F}^\times$. The set $\{x \in M_1 \mid \varphi(x) \geq \mu^*\}$ is in fact a filter generated by μ_0, since φ is order preserving, hence $\mu_0^*(x) = \varepsilon$ if and only if $\varepsilon^{-1}x \geq \mu_0$. Since μ_0 is the sum of all elements in F_{μ_0}, this is equivalent to $\varphi(\varepsilon^{-1}x) \geq \mu^*$, and by the definition of μ^*, this is $\mu(\varphi(x)) = \varepsilon$. Since this is an equivalence, this also entails that $\mu^*(x) = 0$ if and only if $\mu(\varphi(x)) = 0$. □

Given two finite modules, M_1 and M_2, a homomorphism is certainly determined if the image of generators of M_1 are given. However, not all such maps on the generators extends to the whole M_1.

Lemma 3.25. *Let M_1 and M_2 be modules, and G_1 be a set of generators of M_1 closed under multiplication, and G_2 a set of generators of M_2^* closed under multiplication. There is a bijection between homomorphisms $\varphi\colon M_1 \to M_2$ and pairs of operation-preserving maps $u\colon G_1 \to M_2$ and $v\colon G_2 \to M_1^*$ such that $u(g) \geq \gamma$ in M_2 if and only if $g \geq v(\gamma)$ in M_1 for $g \in G_1$ and $\gamma \in G_2$.*

Proof. If there is a homomorphism φ, then clearly $u := \varphi|_{G_1}$ and $v := \varphi^*|_{G_2}$ satisfy the condition. Conversely, a map $u\colon G_1 \to M_2$ extends to a homomorphism if and only if for every pair of sums $\sum_i g_i = \sum_i g_i'$ with g_i and $g_i' \in G_1$, we have $\sum_i u(g_i) = \sum_i u(g_i')$. Consider such a pair, and denote $A := \sum_i u(g_i)$ and $B := \sum_i u(g_i')$. If $A \neq B$, there is at least a single $\gamma \in G_2$ such that $A \geq \gamma$ but $B \ngeq \gamma$ in M_2, or vice versa. Since $u(g) \geq \gamma$ for some $g \in G_2$ if and only if $g \geq v(\gamma)$, clearly $g_i \geq v(\gamma)$ and $g_i' \ngeq v(\gamma)$. However, by our assumption, $v(\gamma) \leq \sum_i g_i = \sum_i g_i' \ngeq v(\gamma)$, a contradiction. □

The following theorem shows which homomorphisms exist.

Theorem 3.26. *Let M_1 and M_2 be modules, either finite with the discrete topology, or complete with the weak topology. Let G_1 be a set of generators of M_1 closed under multiplication, and G_2 a set of generators of M_2^*. Given a map $f\colon G_1 \to M_2$ that preserves operations, this extends to a homomorphism from M_1 if and only if for each $\gamma \in G_2$, $F_\gamma := f^{-1}(\{x \in M_2 \mid x \geq \gamma\})$ is such that for any finite subset $S \subseteq F_\gamma$ and $g \in G_1$, if $g \geq \sum_{s \in S} s$ then $g \in F_\gamma$.*

Proof. Clearly if such a map φ exists, $\varphi^{-1}(\{x \in M_2 \mid x \geq \gamma\})$ is closed under addition, and all its elements are generated by F_γ. Conversely, let us construct a map $v\colon G_2 \to M_1^*$ by defining $v(\gamma) = \sum \varphi^{-1}(\{x \in M_2 \mid x \geq \gamma\})$. If M_1 is finite or complete with the weak topology, such a sum exists. Also, if $f(g) \geq \gamma$, then $g \in \varphi^{-1}(\{x \in M_2 \mid x \geq \gamma\})$, hence $g \geq v(\gamma)$, satisfying the conditions of the previous lemma. Hence a homomorphism exists. □

4 Congruences and ideals

4.1 Congruences

A congruence in an $\mathbb{F}_\infty$-module M or $\mathbb{F}_\infty$-algebra A is an equivalence relation compatible with the natural algebraic structure.

Definition 4.1. *A congruence C in an $\mathbb{F}_\infty$-module M is a set of pairs (a, b) where a, $b \in M$ so that*

- *for every $a \in M$, $(a, a) \in C$,*
- *if $(a, b) \in C$ and $(b, c) \in C$, then $(a, c) \in C$,*
- *if $(a, b) \in C$, then $(b, a) \in C$, and finally*
- *if $(a, b) \in C$, then for every $c \in M$ we have that $(a + c, b + c) \in C$.*

A congruence C in an $\mathbb{F}_\infty$-algebra A is a congruence on the underlying module that furthermore satisfies

- *if $(a, b) \in C$, then for every $c \in A$ we have that $(ac, bc) \in C$.*

Clearly, the smallest congruence, Δ, is the set of diagonal pairs, $\Delta := \{(a, a)|a \in A\}$, for either modules or algebras. The maximal congruence is the set of all pairs. Moreover, notice that if C is a congruence of an $\mathbb{F}_\infty$-module M, then M/C is also an $\mathbb{F}_\infty$-module. Likewise, if C is a congruence of an $\mathbb{F}_\infty$-algebra, A/C is also an $\mathbb{F}_\infty$-algebra.

Restricting our study to algebras, annihilators of elements of A give rise to congruences.

Lemma 4.2. *Let $a \in A$ and C a congruence in A. Then the set of pairs*

$$Ann_C(a) = \{(b, c)|(ab, ac) \in C\}$$

is a congruence.

Proof. We leave the proof of this statement to the reader. □

4.2 Ideals

Since modules are partially ordered sets, we may define their ideals and filters. Note that ideals will be defined differently for modules and algebras. Let us fix an $\mathbb{F}$-module M.

Definition 4.3. *An* ***ideal of a module****, I is such that for $I + M \subseteq I$ and $\mathbb{F} \cdot I \subseteq I$ and $0 \in I$. A* ***filter of a module****, F is such that if $a + b \in F$ then $a \in F$ and $b \in F$, and also $0 \notin F$.*

Definition 4.4. *The* ***ideal*** *(or* ***kernel****) of a congruence C is the equivalence class of 0. The* ***maximal congruence*** *for an ideal I, if it exists, is the maximal congruence whose ideal is I.*

Definition 4.5. *A* ***maximal filter with respect to an ideal*** *I is a maximal filter among filters that do not intersect I. A* ***maximal filter*** *is one that is maximal with respect to the trivial ideal $\{0\}$. A module is* ***separable with respect to the order*** *or just* ***separable*** *if for any pair of distinct elements a, $b \in M$, there is a maximal filter F such that $a \in F$ and $b \notin F$, or vice versa.*

Lemma 4.6. *For an ideal I and an element x, there is a maximal filter with respect to I that does not contain x.*

Proof. Zorn's lemma. □

Theorem 4.7. *In a module M, every ideal has a corresponding maximal congruence C, characterized by the property that M/C is separable.*

Proof. Every ideal I has a corresponding minimal congruence such that $a \sim b$ if and only if $a = b$ or a, $b \in I$. Therefore, by passing to M/I, it is enough to check the statement for $I = \{0\}$.

Let us denote by $\mathcal{F}(a)$ the set of maximal filters containing a. Let us define the equivalence relation C as $a \sim b$ if and only if $\mathcal{F}(a) = \mathcal{F}(b)$. This is a congruence, since $\mathcal{F}(\lambda a) = \{\lambda F \mid F \in \mathcal{F}(a)\}$, and $\mathcal{F}(a + b) = \mathcal{F}(a) \cap \mathcal{F}(b)$. Furthermore, M/C is separable.

We only need to show that this is in fact the maximal congruence. We may pass to the module M/C via the assumption $M/C = M$, meaning that M is separable. Assume that there is a non-trivial congruence C whose ideal is trivial, meaning that $a \sim b$ for some distinct pair of elements. Since M is separable, we have a maximal filter F such that, for instance, $a \in F$ and $b \notin F$. Since F is maximal, the filter generated by F and b contains 0, that is $x + b \leq 0$ for some $x \in F$. Under the congruence C, we get $0 = x + b \sim x + a$. Since x, $a \in F$, and F is a filter, $x + a \in F$ as well, and so $x + a \neq 0$. Then the ideal of C contains a non-zero element $x + a$, contradicting our assumption. □

A similar result can achieved for algebras. Let us fix an algebra A.

Definition 4.8. *An* ***ideal of an algebra****, I is such that it is an ideal of the module, furthermore $A \cdot I \subseteq I$. A maximal filter with respect to an ideal is a maximal filter of the underlying module. A* ***quasimaximal filter with respect to an ideal*** *I, Φ is such that there is a maximal filter F and an $a \in A$ (possibly $a = 1$) such that $\Phi = \{x \in A \mid ax \in F\}$. A* ***quasimaximal filter*** *is one that is quasimaximal with respect to the trivial ideal $\{0\}$. An algebra is* ***quasiseparable*** *if for any pair of distinct elements a, $b \in M$, there is a quasimaximal filter F such that $a \in F$ and $b \notin F$, or vice versa.*

We shall denote the set $\{x \in A \mid ax \in F\}$ by $F : a$.

Theorem 4.9. *In an algebra A, every ideal has a corresponding maximal congruence C, characterized by the property that M/C is quasiseparable.*

Proof. The proof is similar to the case of modules. Every ideal I has a corresponding minimal congruence, therefore, by passing to A/I, it is enough to check the statement for $I = \{0\}$.

Let us denote by $\mathcal{F}(a)$ the set of quasimaximal filters containing a. Let us define the equivalence relation C as $a \sim b$ if and only if $\mathcal{F}(a) = \mathcal{F}(b)$. Clearly $\mathcal{F}(\lambda a) = \{\lambda F \mid F \in \mathcal{F}(a)\}$, $\mathcal{F}(a+b) = \mathcal{F}(a) \cap \mathcal{F}(b)$. Furthermore if $\mathcal{F}(a) = \mathcal{F}(b)$, we need to prove $\mathcal{F}(ac) = \mathcal{F}(bc)$. The antecendent means that $ua \in F$ if and only if $ub \in F$ for all F maximal filters and $u \in A$. In particular, this holds for $u = vc$ for any $v \in A$, hence $v(ac) \in F$ if and only if $v(bc) \in F$. This determines that $\mathcal{F}(ac) = \mathcal{F}(bc)$. Also, A/C is quasiseparable.

To show that this is in fact the maximal congruence, we pass to the algebra A/C. Let us assume that A is quasiseparable and C is the trivial congruence. Assume that there is a non-trivial congruence C whose ideal is trivial, meaning that $a \sim b$ for some distinct pair of elements. Since A is quasiseparable, we have a maximal filter F and $u \in A$ such that, for instance, $ua \in F$ and $ub \notin F$. Since F is maximal, the filter generated by F and ub contains 0, that is $x + ub = 0$ for some $x \in F$. Under the congruence C, we get $0 = x + ub \sim x + ua \in F$, and $x + ua \neq 0$. Then the ideal of C contains a non-zero element $x + ua$, contradicting our assumption. □

4.3 Congruences in semifields

In this section we investigate fields over $\mathbb{F}_\infty$ and we prove some elementary statements which are needed for our proof of the prime decomposition.

Definition 4.10. *We say that an $\mathbb{F}_\infty$-algebra is a field, if for every $a \neq 0$ has a multiplicative inverse.*

Fields over $\mathbb{F}_\infty$ can have non-trivial congruences, on the other hand, the kernel of these congruences are always trivial.

Lemma 4.11. *Let F be a field over $\mathbb{F}_\infty$, and C a proper congruence. Then the kernel of C is trivial.*

Proof. Assume that $(a, 0) \in C$ for some $a \neq 0$. Then, a is a unit, hence $(1, 0) \in C$ implying that C cannot be proper. □

Therefore, by Theorem 4.9, the field has to have a unique maximal (proper) congruence. We construct this unique maximal congruence.

Proposition 4.12. *Let F be a field over $\mathbb{F}_\infty$. Then, the set $C = \{(a, b) | a \neq 0, b \neq 0, a + b \neq 0\} \cup \{(0, 0)\}$ is a congruence.*

Proof. We begin with proving transitivity. Assume that $(a, b) \in C$ and $(b, c) \in C$, we prove that $(a, c) \in C$. It is enough to show that whenever $a + b \neq 0$ and $a + c \neq 0$, then $b + c \neq 0$. Indeed consider

$$b(1 + ab^{-1})(1 + ca^{-1}) = b + c + ...$$

and since every element on the left hand side is a unit, thus the right hand side cannot be 0.

Next we show that if $(a,b) \in C$ and $(c,d) \in C$, then $(a+c, b+d) \in C$. Indeed, it is enough to show that whenever $a+b \neq 0$ and $c+d \neq 0$, then either $a+b+c+d \neq 0$ or $a+c = b+d = 0$. Consider the following product

$$(a+c)(1+ba^{-1})(1+dc^{-1}) = a+b+c+d+...$$

We see that if $a+b+c+d=0$, then $a+c=0$.

Finally, we show that if $(a,b) \in C$ for $a+b \neq 0$ and $c \in F$ then $(ac, bc) \in C$. Clearly either $ac+bc = c(a+b) \neq 0$ or $c=0$ and in this case $(ac,bc) = (0,0) \in C$. □

The above congruence is indeed maximal, since if $(a,b) \in C$ for some $a \neq 0$ and $a+b=0$, then $(0,b) = (a+b,b) \in C$ and by Lemma 4.11 it cannot be proper.

Now, we characterize all congruences. Notice that a congruence C of a field F can be characterized by the equivalence class of 1.

Proposition 4.13. *Let C be a congruence. Then, if x and y are in the equivalence class of 1, then so are xy^{-1}, xy, $\lambda x + \mu y$ for every $\lambda, \mu \in F$ satisfying $\lambda + \mu = 1$.*

Proof. The first two assertions are trivial. We prove the third one. Since $(x,1) \in C$ and $(y,1) \in C$, therefore $(\lambda x, \lambda)$ and $(\mu y, \mu)$ are in C, and thus so is $(\lambda x + \mu y, 1)$. □

Actually this completely characterizes a congruence.

Proposition 4.14. *Let S be a subset of $F \setminus 0$ so that whenever $x, y \in S$, then xy^{-1}, xy and $\lambda x + \mu y$ are in S as well for every $\lambda, \mu \in F$ so that $\lambda + \mu = 1$. Then, the set*

$$C = \{(a,b) | a \neq 0, b \neq 0, ab^{-1} \in S\} \cup \{(0,0)\}$$

is a congruence.

Proof. The only assertion which is not trivial is that if $(a,b) \in C$ and $(c,d) \in C$ then $(a+c, b+d) \in C$. If $b+d \neq 0$, then $b(b+d)^{-1} + d(b+d)^{-1} = 1$, and hence $ab^{-1}b(b+d)^{-1} + cd^{-1}d(b+d)^{-1} = (a+c)(b+d)^{-1} \in S$, and hence $(a+c, b+d) \in C$. Otherwise, if $b+d=0$, then by symmetry we get that $a+c=0$ and we are done. □

An easy corollary of the above characterization is the following.

Corollary 4.15. *Let $x \neq 0$, then the equivalence class of 1 in congruence generated by $(x,1)$ is the set*

$$\left\{ \frac{\sum_{i=1}^{n} \lambda_i x^i}{\sum_{j=1}^{k} \mu_j x^j} : \sum_{i=1}^{n} \lambda_i = \sum_{j=1}^{k} \mu_j = 1 \right\}$$

Proof. We see that these elements have to be in the equivalence class and we also see that this set is closed under the operations listed in Proposition 4.14. □

5 Prime congruences

In this section we define prime congruences and we prove some simple statements about them. We also explicitly compute all prime congruences of $\mathbb{F}_\infty[x]$. We begin with the motivation.

In the work of Dániel Joó and Kalina Mincheva ([5]), prime congruences were defined in additively idempotent semirings in a very straightforward manner. If the semiring were a ring, and C a congruence in it, $(a, b) \in C$ would hold if and only if $(a-b, 0) \in C$. For any pairs $(a-b, 0)$ and $(c-d, 0)$, their product $((a-b)(c-d), 0) \in C$ if and only if $(ac+bd, ad+bc) \in C$. Therefore they defined C to be a prime if $(ac+bd, ad+bc) \in C$ entails that either $(a, b) \in C$ or $(c, d) \in C$, and this definition holds in semirings in general.

Unfortunately, for our semirings, this condition is too strong, since choosing $c = 0$, $ac+bd = ad+bc = 0$, and $(0, 0) \in C$, hence all $(a, b) \in C$. For intuition, we turned to the ring $\mathbb{Z}_\infty$. In Nikolai Durov's work ([3]), $\mathbb{Z}_{(\infty)}$ is isomorphic to the closed interval $[-1, 1]$, and instead of addition, we have convex combinations, such as $\frac{a+b}{2}$. To avoid the absorbing properties of 0, let us interpret the condition $(a, b) \in C$ for some congruence as the harmonic difference $a \star b := \frac{1}{\frac{1}{a}-\frac{1}{b}}$, instead of the standard difference $a-b$. Then $(ac+bd)(ad+bc)(a\star b)(c\star d) = abcd((ac+bd)\star(ad+bc))$. This motivates the following preliminary definiton for a prime congruence.

Definition 5.1. *We say that a proper congruence C is prime if the following two conditions hold*

1. *Whenever $abcd(ac+bd, ad+bc) \in C$ then either*
   - $(a, b) \in C$ *or*
   - $(c, d) \in C$ *or*
   - $(ac+bd, 0) \in C$ *or*
   - $(ad+bc, 0) \in C$.
2. *Whenever $abc(ac, bc) \in C$ then either*
   - $(a, b) \in C$ *or*
   - $(ac, 0) \in C$ *or*
   - $(bc, 0) \in C$.

Remarks:

- Once prime congruences are specified, we can define Spec of any $\mathbb{F}_\infty$-algebra (as a topological space).

- The reason that there are two conditions is that the direct sum contains other elements than pairs of elements.

Lemma 5.2. *Let C be a prime congruence. Then $(ab, 0) \in C$ implies that $(a, 0) \in C$ or $(b, 0) \in C$.*

Proof. Assume first that $(x^2, 0) \in C$ holds for a prime congruence C. Applying the second condition for $a = 1$, $b = -1$ and $c = x$ that either $(x, 0)$ or $(-x, 0)$ holds in C.

Now, assume that $(ab, 0) \in C$ holds for a prime congruence C. Applying the second condition for $c = 1$, we get that either $(a, b) \in C$, or $(a, 0)$ or $(b, 0) \in C$. If $(a, b) \in C$, then $(a^2, 0) \in C$, therefore $(a, 0) \in C$. □

Lemma 5.3. *Let C be a prime congruence. Assume that neither $(ac, 0)$ nor $(bc, 0)$ holds in C. Then $(ac, bc) \in C$ implies that $(a, b) \in C$.*

Proof. Trivial. □

The above lemmas show that we can simplify our notion of a prime congruence to the following equivalent definition.

Definition 5.4. *We say that a proper congruence C is prime if the following two conditions hold*

1. *Whenever $(ac + bd, ad + bc) \in C$ then either*
   - *$(a, b) \in C$ or*
   - *$(c, d) \in C$ or*
   - *$(ac + bd, 0) \in C$ or*
   - *$(ad + bc, 0) \in C$.*
2. *Whenever $(ac, bc) \in C$ then either*
   - *$(a, b) \in C$ or*
   - *$(c, 0) \in C$.*

From now on, we use this definition for a prime congruence. Instead of writing $(ac+bd, ad+bc)$ we will write $(a, b)(c, d)$. We proceed with some simple lemmas needed to characterize the prime congruences of $\mathbb{F}_\infty[x]$.

Lemma 5.5. *Let C be a prime congruence. Then for any two elements $a, b \in A$ we have that $a \geq b$ or $a \leq b$ or $a + b = 0$ in A/C.*

Proof. We can assume that neither a nor b is identified with 0 in A/C. Consider the following identity

$$(a + b, a)(a + b, b) = ((a + b)^2, (a + b)^2).$$

From the first condition, we obtain that either $((a+b)^2, 0)$, $(a+b, a)$ or $(a+b, b)$ is in P for all $a, b \in A$. □

As a consequence we see that if C is a prime congruence, then A/C is a union of totally ordered chains with sums of elements in different chains being 0.

Lemma 5.6. *Let C be a prime congruence in an $\mathbb{F}_\infty$-algebra A so that in A/C we have that $a > b$ and $c > d$. Then either $ac > bd$ or $(ac, 0) \in C$.*

Proof. The statements $ac \geq ad \geq bd$ and $ac \geq bd \geq bd$ hold for any congruence. On the other hand if $ac = bd$, then $ac = ad = bc = bd$ has to hold as well, and hence $(a, b)(c, d) = (ac{+}bd, ad{+}bc) \in C$. The latter implies that $(ac, 0) \in C$. □

Moreover we can take roots in prime congruences.

Lemma 5.7. *Let C be a prime congruence of an $\mathbb{F}_\infty$-algebra A. Assume that $(a^n, b^n) \in C$ for some $(a, b) \notin C$. Then $(a + b, 0) \in C$.*

Proof. Since C is a prime congruence, therefore in A/C, we have $a > b$ or $b > a$ or $a + b = 0$. The first two cases cannot hold, since $a^n = b^n$. □

Now, we characterize the prime congruences of $\mathbb{F}_\infty[x]$. Recall that elements of $\mathbb{F}_\infty[x]$ are 0 and polynomials of the form $\sum_{i \in I} \lambda_i x^i$ where $\lambda_i = \pm 1$ and $I \subseteq \mathbb{Z}$ is finite. We begin with a simple lemma.

Lemma 5.8. *Let A be an $\mathbb{F}_\infty$-algebra and assume that $(1 + x^n, 1) \in C$ and $(1 + x^m, 1) \in C$ hold for a congruence C for some $n > m$. Then $(1 + x^{n+m}, 1) \in C$. Moreover if C is prime, then $(1 + x^{n-m}, 1)$ is also in C.*

Proof. Since $(1 + x^n, 1) \in C$ and $(1 + x^m, 1) \in C$, therefore

$$(1 + x^n + x^m + x^{n+m}, 1)$$

also holds in C which implies that $(1 + x^{n+m}, 1) \in C$.

Now, assume that C is prime. Consider 1 and x^{n-m}. Since C is prime, one of the following holds in C:

- $(1 + x^{n-m}, 0)$: In this case we get that $(x^m + x^n, 0)$ holds, but this cannot be true, since $1 + x^n = 1 + x^m = 1$ in A/C.
- $(1 + x^{n-m}, x^{n-m})$: In this case $1 + x^{n-m} + x^{2(n-m)} + ... + x^{m(n-m)} = x^{m(n-m)}$ and also it equals to $1{+}x^{m(n-m)} = 1$ in A/C, therefore $(x^{m(n-m)}, 1)$ holds in A/C, meaning that $(x^{m-n}, 1)$ holds in A/C, and we are done.
- $(1 + x^{n-m}, 1)$: We are done.

□

We are ready to compute the prime congruences of $\mathbb{F}_\infty[x]$.

Theorem 5.9. *The prime congruences of $\mathbb{F}_\infty[x]$ are the following.*

1. *The congruence generated by $(1 + x, x)$.*

2. *The congruence generated by* $(x, 1)$.

3. *The congruence generated by* $(x, 0)$.

4. *The congruence generated by* $(1 + x, 1)$.

5. *The congruence generated by* $(-1 + x, x)$.

6. *The congruence generated by* $(x, -1)$.

7. *The congruence generated by* $(-1 + x, -1)$.

8. *Every* $n > 0$*, the prime congruence* P *generated by* $(1 \pm x, 0)$*,* $(1 \pm x^2, 0)$*, ...* $(1 \pm x^{n-1}, 0)$ *and* $(1 + x^n, x^n)$.

9. *Every* $n > 0$*, the prime congruence* P *generated by* $(1 \pm x, 0)$*,* $(1 \pm x^2, 0)$*, ...* $(1 \pm x^{n-1}, 0)$ *and* $(1 + x^n, 1)$.

10. *Every* $n > 0$*, the prime congruence* P *generated by* $(1 \pm x, 0)$*,* $(1 \pm x^2, 0)$*, ...* $(1 \pm x^{n-1}, 0)$ *and* $(-1 + x^n, x^n)$.

11. *Every* $n > 0$*, the prime congruence* P *generated by* $(1 \pm x, 0)$*,* $(1 \pm x^2, 0)$*, ...* $(1 \pm x^{n-1}, 0)$ *and* $(-1 + x^n, -1)$.

12. *Every* $n > 0$*, the prime congruence* P *generated by* $(1 \pm x, 0)$*,* $(1 \pm x^2, 0)$*, ...* $(1 \pm x^{n-1}, 0)$ *and* $(x^n, 1)$.

13. *Every* $n > 0$*, the prime congruence* P *generated by* $(1 \pm x, 0)$*,* $(1 \pm x^2, 0)$*, ...* $(1 \pm x^{n-1}, 0)$ *and* $(x^n, -1)$.

14. *The prime congruence* P *generated by* $(1 \pm x, 0)$*,* $(1 \pm x^2, 0)$*, ...*

Proof. Let P be a prime congruence. We have three cases:

1. $1 + x = x$ holds in $\mathbb{F}_\infty[x]/P$

2. $1 + x = 1$ holds in $\mathbb{F}_\infty[x]/P$

3. Neither of the above, in particular $1 + x = 0$ holds in $\mathbb{F}_\infty[x]/P$.

We investigate all cases:

1. $1 + x = x$: Let P be the smallest congruence so that $1 + x = x$ holds in $\mathbb{F}_\infty[x]/P$. In this case, we can replace any polynomial with its highest degree term in $\mathbb{F}_\infty[x]/P$ if all coefficients are equal, otherwise 0. We see that the corresponding smallest congruence is indeed prime, because degree is additive.

   Is there any prime congruence Q containing P? If Q is any other congruence, then either $(x^n, x^m) \in Q$ or $(x^n, 0) \in Q$. (If $(x^n, -x^m) \in Q$, then $x^n - x^m = 0$ implies that $(x^n, 0) \in Q$) If $(x^n, x^m) \in Q$ then $(1, x^{m-n}) \in Q$ (without loss of generality, we can assume $m > n$), but $x \geq 1$, so $(x, 1) \in Q$ and in this case $\mathbb{F}_\infty[x]/Q = \mathbb{F}_\infty$. Similarly, if $(x^n, 0) \in Q$, then $(x, 0) \in Q$, and in this case $\mathbb{F}_\infty[x]/Q = \mathbb{F}_\infty$.

2. $1+x=1$: Let P be the smallest congruence so that $1+x=1$ holds in $\mathbb{F}_\infty[x]/P$. In this case, we can replace any polynomial with its smallest degree term in $\mathbb{F}_\infty[x]/P$ if all coefficients are equal, otherwise 0. We see that the corresponding smallest congruence is indeed prime, because degree is additive.

   Is there any prime congruence Q containing P? If Q is any other congruence, than either $(x^n, x^m) \in Q$ or $(x^n, 0) \in Q$. If $(x^n, x^m) \in Q$ then $(1, x^{m-n}) \in Q$ (without loss of generality, we can assume that $m > n$), but $x \leq 1$, so $(x, 1) \in Q$ and in this case $\mathbb{F}_\infty[x]/Q = \mathbb{F}_\infty$. If $(x^n, 0) \in Q$, then $(x, 0) \in Q$, which contradicts $1+x=1$.

3. Last case: In this case, neither of the above holds. We can also assume that neither $-1+x=x$ nor $-1+x=-1$ holds because we can replace x by $-x$ and we receive one of the cases above. Let P be any prime congruence in this case. We have basically three cases: $(1 \pm x^n, 0) \in P$ for every n or $(1+x^n, 1) \in P$ for some n or $(1+x^n, x^n) \in P$ for some n or $(-1+x^n, -1) \in P$ for some n or $(-1+x^n, x^n) \in P$ for some n. First, we assume that there is an expression $1 \pm x^n$ which is not 0. Let n be a smallest such n, and moreover assume that we have $(1+x^n, 1) \in P$. Then, by Lemma 5.8, the m's satisfying $(1+x^m, 1) \in P$ have to be divisible by this n. We see that the smallest congruence satisfying this condition is prime. Can a congruence Q contain this congruence? We see that it can only happen if $x^n = 1$ in that congruence. We leave to the reader to complete the cases when $(-1 \pm x^n, -1)$ or $(\pm 1 + x^n, x^n)$ is in P.

   Finally, we have the case that $(1 \pm x^n, 0)$ holds for every n. We can see that the smallest such congruence P is prime. Can there be any prime congruence Q containing P? Since every polynomial containing at least 2 monomials is identified with 0, hence the only possibility is that x^n is identified with x^m. In that case we get that $x^n = 0$ or $x^{n-m} = 1$ (this cannot hold). Therefore $x = 0$.

□

Geometrically, the prime congruences generated by $(x, \pm 1)$ correspond to evaluation at $x = \pm 1$, and the prime congruence generated by $(x, 0)$ corresponds to evaluation at $x = 0$. Furthermore the prime congruences listed in 12. and 13. are listed in Section 2 in the Example part. These are finite field extensions of $\mathbb{F}_\infty$.

Therefore, we obtain that the geometry of $\mathsf{Spec}\,\mathbb{F}_\infty[x]$ is very similar to $\mathsf{Spec}\,\mathbb{Z}/p\mathbb{Z}[x]$, for instance the closed points of $\mathsf{Spec}\,\mathbb{F}_\infty[x]$ correspond to elements of $\mathbb{F}_\infty$ and some finite extensions of $\mathbb{F}_\infty$.

6 Krull dimension

In this section we prove that the Krull dimension of a polynomial algebra over $\mathbb{F}_\infty$ is the number of indeterminants.

We say that an $\mathbb{F}_\infty$-algebra A has Krull dimension n if the longest chain of prime congruences has length $n+1$. We begin with an easy lemma.

Lemma 6.1. *Let A be an $\mathbb{F}_\infty$-algebra of Krull dimension n. Then the dimension of $A[x]$ is at least $n+1$.*

Proof. Let P be the minimal element of a maximal chain of prime congruences of A. Then $\mathsf{dim}\, A/P = \mathsf{dim}\, A$. Moreover $\mathsf{dim}\, A/P[x] \geq \mathsf{dim}\, A/P + 1$, since the congruence generated by $(x, 0)$ is prime. Therefore

$$\mathsf{dim}\, A[x] \geq \mathsf{dim}\, A/P[x] \geq \mathsf{dim}\, A/P + 1 = \mathsf{dim}\, A + 1.$$

□

Theorem 6.2. *Let A be an $\mathbb{F}_\infty$-algebra of Krull dimension n. Then either*

- *$A[x]$ is of dimension $n+1$.*
- *$A[x]$ is of dimension at most $n+2$, furthermore in this case there exists a chain of prime congruences of length $n+3$ and four prime congruences in this chain $P_1 \subset P_2 \subset P_3 \subset P_4$ so that $(x, 0) \in P_4 \setminus P_3$, and there exist $a, b \in A$ so that $(a, 0)$, $(b, 0)$ are in P_3 and for some j, $(ax^j, b) \in P_2 \setminus P_1$.*

Proof. Let $P_1 \subset P_2 \subset P_3 \subset P_4$ be prime congruences of $A[x]$ so that $P_1|_A = P_2|_A$ and $P_3|_A = P_4|_A$ (using the natural map $A \to A[x]$). If we can conclude that either $P_1 = P_2$ or $P_3 = P_4$ happens, then we see that $A[x]$ has to have dimension $n+1$. Let's check what happens when $P_1 \neq P_2$ and $P_3 \neq P_4$.

Since each prime congruence contains $(a+b, a)$, $(a+b, b)$ or $(a+b, 0)$ for any elements $a, b \in A[x]$, hence we can assume that for any $(p(x), q(x)) \in P_2 \setminus P_1$, we have that $p(x)$ and $q(x)$ are either monomials or one of them is 0. The same holds for any pair $(p(x), q(x)) \in P_4 \setminus P_3$. Notice that if $(ax^n, 0) \in P_{i+1} \setminus P_i$ (for $i = 1$ or 3), then from the prime property we get that either $(a, 0) \in P_{i+1} \setminus P_i$ (which contradicts our original assumptions) or $(x, 0) \in P_{i+1} \setminus P_i$. We separate cases.

1. First, we assume that there are monomials so that we have that

$$(ax^n, bx^m) \in P_2 \setminus P_1$$

and

$$(cx^k, dx^l) \in P_4 \setminus P_3$$

and furthermore $(x, 0)$ does not hold in any of the congruences. Then, we can use the cancellation property and we obtain that (assuming that $n \geq m$ and $k \geq l$)

$$(ax^{n-m}, b) \in P_2 \setminus P_1$$

and

$$(cx^{k-l}, d) \in P_4 \setminus P_3.$$

We see that

$$(a^{k-l}c^{n-m}x^{(n-m)(k-l)}, b^{k-l}c^{n-m}) \quad \text{and} \quad (a^{k-l}c^{n-m}x^{(n-m)(k-l)}, d^{n-m}a^{k-l})$$

are contained in P_4, therefore $(b^{k-l}c^{n-m}, d^{n-m}a^{k-l}) \in P_4$. Since P_4 and P_3 are the same once they are restricted to A, therefore

$$(b^{k-l}c^{n-m}, d^{n-m}a^{k-l}) \in P_3$$

implying that

$$(b^{k-l}c^{n-m}x^{(n-m)(k-l)}, d^{n-m}a^{k-l}x^{(n-m)(k-l)}) \in P_3.$$

Furthermore, since $(ax^{n-m}, b) \in P_2 \subset P_3$ we obtain that

$$(b^{k-l}c^{n-m}x^{(n-m)(k-l)}, d^{n-m}b^{k-l}) \in P_3$$

so

$$(c^{n-m}x^{(n-m)(k-l)}, d^{n-m}) \in P_3.$$

So either $(cx^{k-l}, d) \in P_3$ or $(cx^{k-l} + d, 0) \in P_3$, but none of these options is possible.

2. If $(x, 0) \in P_2 \setminus P_1$, then clearly $(cx^k, dx^l) \in P_4 \setminus P_3$ cannot hold.

3. If $(x, 0) \in P_4 \setminus P_3$, then $(ax^n, bx^m) \in P_2 \setminus P_1$ implies that $(ax^{n-m}, b) \in P_2 \setminus P_1$, so $(b, 0) \in P_4$ and thus in P_3 as well. In this case we see that $\mathsf{dim}\, A[x] \leq n + 2$, because for any chain of prime congruences in $A[x]$: $Q_1 \subset Q_2 \subset Q_3 \subset Q_4 \subset Q_5 \subset Q_6$, $(x, 0) \in Q_{i+1} \setminus Q_i$ can only hold once. Hence we obtain the second part of our statement.

□

Corollary 6.3. *The Krull dimension of* $\mathbb{F}_\infty[x_1, ..., x_n]$ *is exactly* n.

Proof. We proceed by induction. For $n = 0$, we are done. Assume that $\mathbb{F}_\infty[x_1, ..., x_{n-1}]$ is of dimension $n-1$, then we would like to prove that $\mathbb{F}_\infty[x_1, ..., x_n]$ is of dimension n. We prove that any chain of prime congruences is of length $n + 1$. Since $\mathbb{F}_\infty[x_1, ..., x_n] = \mathbb{F}_\infty[x_1, ..., x_{n-1}][x_n]$ we obtain that if the dimension of $\mathbb{F}_\infty[x_1, ..., x_n]$ is not n, then there exists a chain of prime congruences of length $n + 2$ so that for four prime congruences $P \subset Q \subset R \subset S$ we have

- $(x_n, 0) \in S \setminus R$
- $(ax_n^j, b) \in Q \setminus P$ for some $a, b \in \mathbb{F}_\infty[x_1, ..., x_{n-1}]$
- $(a, 0)$ and $(b, 0)$ are in $R \setminus Q$.

We prove that this chain is of length $n+1$. Replacing x_n by any x_i we see that all x_i are identified with 0 eventually in the chain. Moreover, since $(a, 0)$ and $(b, 0)$ are not in Q, therefore we can assume that a and b are monomials. On the other hand $(a, 0)$, $(b, 0)$ are in R, hence $(x_i, 0)$ (for some $i \neq n$) has to hold in R. Without loss of generality we can assume that $(x_1, 0)$ holds first in our chain, meaning that $(x_1, 0) \in T$ where T is a prime congruence in our chain and if $(x_i, 0) \in T'$ for some $i \neq 1$ and T' in our chain, then T' contains T. But then $\mathbb{F}_\infty[x_1, ..., x_n] = \mathbb{F}_\infty[x_2, ..., x_n][x_1]$ and the second condition of the previous theorem cannot hold for our chain of prime congruences. We are done. □

7 Prime decomposition

We begin with some definitions.

Definition 7.1. *We say that a congruence C is radical, if whenever $(a, b)(a, b) \in C$, then $(a, b) \in C$ or $(a^2 + b^2, 0) \in C$ or $(ab, 0) \in C$.*

Definition 7.2. *We say that a congruence C is cancellative, if whenever $(ab, ac) \in C$, then $(a, 0) \in C$ or $(b, c) \in C$.*

Notice that if C is prime, then C is radical and cancellative. Moreover

Lemma 7.3. *Let C be a cancellative congruence, then C is radical.*

Proof. Assume that $(a, b)(a, b) = (a^2 + b^2, ab) \in C$. Then

$$(a + b)(a + b, a) = ((a + b)^2, a^2 + ab).$$

Since $(a^2 + b^2, ab) \in C$, therefore we obtain that $(a + b)(a + b, a) \in C$, which implies that either $(a + b, 0)$ or $(a + b, a) \in C$. If the first statement holds then $(ab, 0) \in C$. If $(a + b, a) \in C$ holds, then by a symmetric line of thoughts we obtain that $(a + b, b) \in C$, so $(a, b) \in C$. □

Annihilators with respect to radical congruences are always radical.

Lemma 7.4. *Let C be a radical congruence of an $\mathbb{F}_\infty$-algebra A. Then, for every $c \in A$, $Ann_C(c)$ is radical.*

Proof. Assume that $(a, b)^2 c \in C$. Then, clearly $((a, b)c)^2 \in C$, therefore $(a, b)c \in C$. □

We can also define annihilators of pairs (c, d) as $Ann_C(c, d) := \{(a, b)|(a, b)(c, d) \in C$. This set is basically never a congruence, on the other hand, it is radical in the sense that if $(a, b)^2 \in Ann_C(c, d)$, then $(a, b) \in Ann_C(c, d)$ for every radical congruence C.

In cancellative congruences, we can take roots of elements as explained in the following lemma.

Lemma 7.5. *Let C be a cancellative congruence of an $\mathbb{F}_\infty$-algebra A. Then, if $(a,b)(c,d) \in C$, and $(a+b,0) \notin C$ and $(c+d,0) \notin C$, then for every n, $(a^n,b^n)(c,d) \in C$.*

Proof. We prove the statement by induction. For $n=1$, it is trivial. For $n=2$, we consider $(a+b)(a^2,b^2)(c,d)$, or in other words,

$$(a^3c+ab^2d+a^2bc+b^3d, ab^2c+a^3d+b^3c+a^2bd).$$

Since $(ac+bd,ad+bc) \in C$, hence in A/C,

$$(a^3c+ab^2d+a^2bc+b^3d) = (a^3c+ab^2c+a^2bd+b^3d) =$$

$$= (a^3c+ab^2d+b^3c+a^2bd) = (a^3d+ab^2d+b^3c+a^2bc) =$$

$$= (ab^2c+a^3d+b^3c+a^2bd).$$

Since C is cancellative, we obtain that $(a^2,b^2)(c,d) \in C$.

We assume that the statement is true up to $n-1$, and we would like to prove it for n. Consider $(a^{n-1}+b^{n-1})(a^n,b^n)(c,d)$, or in other words,

$$(a^{2n-1}c+a^{n-1}b^nd+a^nb^{n-1}c+b^{2n-1}d, a^{2n-1}d+a^{n-1}b^nc+a^nb^{n-1}d+b^{2n-1}c).$$

Since $(ac+bd,ad+bc) \in C$ and by the inductive hypothesis

$$(a^{n-1}c+b^{n-1}d, a^{n-1}d+b^{n-1}c) \in C,$$

we have that in A/C, the following equations hold

$$(a^{2n-1}c+a^{n-1}b^nd+a^nb^{n-1}c+b^{2n-1}d) =$$

$$= (a^{2n-1}c+a^nb^{n-1}d+a^{n-1}b^nc+b^{2n-1}d) =$$

$$= (a^{2n-1}c+a^nb^{n-1}d+a^{n-1}b^nd+b^{2n-1}c) =$$

$$= (a^{2n-1}d+a^nb^{n-1}c+a^{n-1}b^nd+b^{2n-1}c) =$$

$$= (a^{2n-1}c+a^{n-1}b^nc+a^nb^{n-1}d+b^{2n-1}c),$$

and we are done. □

As a Corollary we obtain the following surprising statement.

Corollary 7.6. *Let F be a field over $\mathbb{F}_\infty$, and assume that $(a,b)(c,d) \in \Delta$ for some elements such that $a+b \neq 0$ and $c+d \neq 0$. Then any pair (x,y) of the congruence generated by (a,b) is annihilated by (c,d), in other words, $(x,y)(c,d) \in \Delta$.*

Proof. By Corollary 4.15 the congruence generated by (a, b) consists of pairs of the form

$$\Big(u(\sum \lambda_i (ab^{-1})^i), u(\sum \mu_j (ab^{-1})^j)\Big)$$

for some $u \in F$, and some coefficients λ_i, μ_j so that $\sum \lambda_i = \sum \mu_j = 1$. Therefore every pair is of the form

$$\Big(u(\sum \lambda_i (\sum \mu_j)(ab^{-1})^i, u(\sum \mu_j (\sum \lambda_i)(ab^{-1})^j)\Big)\,.$$

Hence, after foiling out we see that any pair in the congruence generated by (a, b) can be written as a sum of

$$c_i(a^i, b^i)$$

for some $c_i \in F$. By the previous statement, our Corollary follows. □

The following proposition enables us to work with fields instead of cancellative algebras.

Proposition 7.7. *Let A be an $\mathbb{F}_\infty$-algebra, then if C is a cancellative congruence, then A/C embeds into a field.*

Proof. We leave it to the reader that the standard construction of a fraction field works here. □

One big advantage of working with fields is that we can more easily construct prime congruences.

Lemma 7.8. *Let F be an $\mathbb{F}_\infty$-field and $1 \neq x \in F$. Then, a maximal congruence among all radical congruences which does not contain $(x, 1)$ is a prime congruence.*

Proof. First of all, to make sense of the statement, we see that Δ is a radical congruence not containing $(x, 1)$, and hence, by Zorn lemma, there is a maximal radical congruence, and we denote it by P.

If $1 + x = 0$, then $(x, 1) \in C$ implies that $(0, 1) \in C$. Since a field has a unique maximal congruence which is prime, we are done in this case.

We assume that $1 + x \neq 0$. We show that P is prime. Suppose the contrary. One of the two assertions of being a prime has to fail. Assume that there exists $a, b, c, d \in F \setminus \{0\}$ such that $(a, b)(c, d) \in P$, but $(a, b) \notin P$, $(b, c) \notin P$, $(ac + bd, 0) \notin P$ and $(ad + bc, 0) \notin P$. The latter two conditions imply that $(a + b, 0) \notin P$ and $(c + d, 0) \notin P$. We leave it to the reader to show that the second assertion of being a prime cannot fail.

For simplicity, we look at F/P. In this field, any non-trivial radical congruence contains $(x, 1)$. Consider the congruence generated by $(ab^{-1}, 1)$. By Corollary 7.6, any (u, v) in the congruence generated by $(ab^{-1}, 1)$ is annihilated by (c, d). Even though the annihilator of (c, d) is not a congruence, it is radical. We know also that (c, d) is not contained in the annihilator of (c, d), since P is radical, therefore the radical of the congruence generated by $(ab^{-1}, 1)$ is a proper radical congruence, therefore $(x,1)$ is contained in it. So we obtain that $(x,1)(c,d) \in \Delta$ in F/P. By a similar argument to above one, using that $1+x \neq 0$, we obtain that $(x,1)^2 \in \Delta$ which is a contradiction. □

We are ready to prove our main theorems of this section.

Theorem 7.9. *Let F be an $\mathbb{F}_\infty$-field. Then the trivial congruence Δ is the intersection of prime congruences.*

Proof. Assume that it is not, hence the intersection of all prime congruences contains a tuple (x,y) where $x \neq y$. Without loss of generality we can assume that $y = 1$, and using the above Lemma, we obtain that there is a prime not containing our tuple. This is a contradiction. □

Theorem 7.10. *Let C be a cancellative congruence in $\mathbb{F}_\infty$-algebra A. Then C is the intersection of all prime congruences containing C.*

Proof. This follows from Lemma 7.7 and Theorem 7.9. □

References

[1] Suren Yurevich Arakelov. *Intersection theory of divisors on an arithmetic surface.* Math. USSR Izv (1974), **8** (6): 1167–1180.

[2] Suren Yurevich Arakelov. *Theory of intersections on an arithmetic surface.* Proc. Internat. Congr. Mathematicians Vancouver (1975), **1**, Amer. Math. Soc., pp. 405–408.

[3] Nikolai Durov. *New Approach to Arakelov Geometry.* PhD Thesis. 2007.

[4] Gerd Faltings. *Diophantine Approximation on Abelian Varieties*, Annals of Mathematics (1991), Second Series, 133 (3): 549–576

[5] Dániel Joó, Kalina Mincheva. *Prime congruences of idempotent semirings and a Nullstellensatz for tropical polynomials.* Preprint. 2014.

[6] Dániel Joó, Kalina Mincheva. *On the dimension of polynomial semirings.* Preprint. 2015.

[7] Paul Vojta. *Siegel's Theorem in the Compact Case*, Annals of Mathematics, (1991) Vol. 133, No. 3, 133 (3): 509–548