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

May 13, 2020

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, $F_\infty$. 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 $\text{Spec} \, \mathbb{Z}$, 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 [3] and [4] 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 $\text{Spec} \, \mathbb{Z}$.

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 analogous formulation for $\text{Spec} \, \mathbb{Z}$ 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 \(|.|_p\) 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 \( \text{Spec} \mathbb{Z} \), however, the Archimedean valuation, called for analogical reasons the valuation at the infinite place or infinity, is missing from \( \text{Spec} \mathbb{Z} \).

Durov uses this idea to complete \( \text{Spec} \mathbb{Z} \), and, among others, he defines the residue field corresponding to the valuation at infinity. In general, for a prime \( p \), we introduce \( \mathbb{Z}_p(\infty) = \{ q \in \mathbb{Q} \mid |q|_p \leq 1 \} \) and the open unit ball \( U_p := \{ q \in \mathbb{Z}_p \mid |q|_p < 1 \} \), and define the residue field as the quotient \( \mathbb{F}_p = \mathbb{Z}_p(\infty) / U_p \). 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 algebra over this generalized ring. Explicitly, this generalized ring has three elements: \(-1,0,1\), equipped with three operations: \( +, \cdot \) and a unary \(-\) so that

- \( + \) is idempotent: \( a + a = a \) for every element \( a \),
- 0 is an absorbing element: \( a + 0 = 0 \) for every element \( a \),
- \( + \) is commutative and associative,
- \( -(1) = -1, -(\infty) = 0, \)
- \( -1 + 1 = 0, \)
- \( \cdot \) is commutative, associative, and distributive with respect to \( + \),
- 1 is a multiplicative identity,
- 0 is absorbing with respect to \( \cdot \) as well,
- \( (\infty) \cdot (\infty) = 1. \)

For instance, we clearly see that \( \mathbb{F}_\infty \) is not a ring in the usual sense, it lacks of an additive identity, and, as a consequence, of additive inverses. On the other hand, it is not very far from being a ring itself. One purpose of this paper is to show that algebraic geometry over \( \mathbb{F}_\infty \) looks similar to algebraic geometry over finite fields.

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 \( \mathbb{F}_\infty \)-fields, 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 \( 3.11 \) \( 3.12 \) \( 3.13 \), and use this to understand dual modules \( 3.17 \) \( 3.18 \) and \( \text{Hom} \)-modules \( 3.20 \), 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 $F_\infty$-fields, 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 $F_\infty$. 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 prime congruences are more natural objects to study than prime ideals. The authors study tropical geometry using prime congruences instead of prime ideals, and they prove a version of Hilbert’s Nullstellensatz in the realm of tropical geometry. We follow this key idea and we define prime congruences in algebras over $F_\infty$ 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 $F_\infty$ with the theory of classical finite fields.

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

We would also like to thank an anonymous referee for their invaluable comments.

2 Modules and algebras over $F_\infty$

First, let us recall what the object $F_\infty$ is (see [3], 5.1.16).

**Definition 2.1.** The **generalized field** or **field** $F_\infty$ has as set the elements $\{-1, 0, 1\}$, with three operations: a unary $\cdot$, and a binary $\dot{+}$ and $\cdot$, with the following properties:

- $(a + b) \dot{+} c = a \dot{+} (b + c), \quad a + b = b + a$;
- $0 \dot{+} a = a \dot{+} 0 = 0$, hence 0 is an **absorbing element**;
- $a \dot{+} a = a$;
- $a \dot{+} (-a) = 0$;
- $-(1) = -1, \quad -(1) \dot{+} 1 = 1, \quad -0 = 0$;
- $(a \cdot b) \cdot c = a \cdot (b \cdot c), \quad a \cdot b = b \cdot a$;
- $1 \cdot a = a \cdot 1 = a$;
- $(1) \cdot (1) = 1$. 

2
Note in particular that the operator ˙+ is unlike the typical addition in that 0 is an absorbing element and that −a is not the additive inverse of a. The notations were chosen this way because of the way Durov defined these structures in [3], and since in his development, ˙+ is derived as a convex combination. Durov chose the notation ∗ for this operator, but we wanted to preserve its connection to addition. Also note that 0 is absorbing for both operations.

Intuitively, a module over the field at infinity, $F_\infty$, corresponds to the faces of a symmetric polyhedron, where the binary operation is the smallest face containing both. Then the field $F_\infty$ 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 cannot be realized as actual symmetric polyhedra, this can be a useful visualization.

In the following definitions, we will denote by indices the arity of the operations. In [3], modules over generalized rings are described in 4.3.7. Here we give a more direct description for $F_\infty$.

**Definition 2.2.** An $F_\infty$-module is a structure $(V, 0, 0, 1, ˙+)$ 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.

Proposition 2.3. 0 is an absorbing element in an $F_\infty$-module.

**Proof.** $0 = a ˙+ (−a) = a ˙+ a ˙+ (−a) = a ˙+ 0$.

Example. The set $F_\infty = \{-1, 0, 1\}$ is an $F_\infty$-module, defined uniquely by the module axioms.

Proposition 2.4. An $F_\infty$-module has a natural partial order defined by $a ≤ b$ if $a ˙+ b = a$, with 0 being the smallest element, i.e. $0 ˙+ x = 0$.

**Proof.** Reflexivity arises from idempotence, symmetry from commutativity. If $a ≤ b ≤ c$, then $a ˙+ b = a$ and $b ˙+ c = b$, hence $a ˙+ c = (a ˙+ b) ˙+ c = a ˙+ b = a$, therefore $a ≤ c$.

**Definition 2.5.** 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 $F_\infty$: [4]
Definition 2.6. An $\mathbb{F}_\infty$-algebra or ring is an $\mathbb{F}_\infty$-module $A$ with a semigroup structure $(A, \cdot)$ 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 subalgebra, congruence, quotient algebra and algebra homomorphism are defined as usual.

A unital algebra is a monoid structure $(V, 1, \cdot)$ such that $a \cdot 1 = 1 \cdot a = a$.

An invertible element $a$ is such that there is an $a^{-1}$ such that $a \cdot a^{-1} = 1$, and the group of invertible elements is denoted by $A^\times$. The unital algebra is a division algebra if $(V \setminus \{0\}, 1, \cdot)$ is a group, and a $\mathbb{F}_\infty$-field if it is a commutative group.

Recall once again that 0 is not a neutral element for addition:

Proposition 2.7. 0 is an absorbing element in an $\mathbb{F}_\infty$-algebra.

Proposition 2.8. In a finite unital algebra, all invertible elements are incomparable.

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

Remark. Note that our usage of $\mathbb{F}_\infty$-algebra is more in line with what Durov refers to as unary algebras over $\mathbb{F}_\infty$, as defined in 5.1.15 in [3], referred to as such because what we describe as elements, he refers to them as unary operations (4.3.9). A proof for this will be sketched in [2.12]. What he refers to as algebras, described in 5.1.9, are more general structures, and may have additional operations of higher arity.

Example.

- The field $\mathbb{F}_\infty$ is a commutative division $\mathbb{F}_\infty$-algebra.
- $\mathbb{F}_{\infty^k}$ is the $\mathbb{F}_\infty$-field generated by $\zeta_k$ such that $\zeta_k^k = -1$ (for the definition of a freely generated algebra, see [2.29] and [2.22]). Its elements are $\{\zeta_k^i \mid i \in \{0, 1, \ldots, 2k - 1\}\}$, and by [2.9] we have $a + b = 0$ unless $a = b$. 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 $F_{\infty k}$ into $F_{\infty \ell}$, given by $\zeta_{k} = \zeta_{\ell}^{\ell/k}$. The field $F_{\infty} := \varprojlim F_{\infty k}$ 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 $k$th roots of unity. The Euclidean closure of $F_{\infty k}$ in $\mathbb{C}$ is given as $F_{\infty k} := \mathbb{T} \cup \{0\} = \{z \in \mathbb{C} \mid |z| = 1\} \cup \{0\}$. Using the multiplication on $\mathbb{C}$ and defining addition as $a + b = 0$ unless $a = b$, this gives a field structure to the set $F_{\infty k}$.

We may also consider the extension with $\zeta_{k} = 1$. In this case, its elements are $\pm \zeta^{i}$ for $i \in \{0, \ldots, k\}$. These and $F_{\infty k}$ will appear later as quotients of the polynomial ring $F_{\infty}[x]$ in §10.

More generally, given a group $G$ and a field $F$, the group algebra $F[G]$ consists of elements 0 and $\lambda g$ with $\lambda \in F^\times$ 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 $F_{\infty}[\mathbb{Z}/k\mathbb{Z}]$.

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

For an example of a $F_{\infty}$-field 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 2.10.** 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 $a, b \in \mathbb{A}, m \in M$;
- $a \cdot (m \cdot n) = a \cdot (m \cdot n)$ and $(a \cdot b) \cdot m = a \cdot m \cdot b \cdot m$ 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 $a \in \mathbb{A}, m, n \in M$.

**Lemma 2.11.** The category theoretic free module $\mathbb{A}(n)$ over $\mathbb{A}$, generated by $x_1, \ldots, x_n$, consists of elements $\bigoplus_{i \in I} \lambda_i x_i$ for $I \subseteq \{1, \ldots, n\}$, $\lambda_i \in \mathbb{A} \setminus \{0\}$, and the element 0. The operation $\bigoplus_{i \in I} \lambda_i x_i + \bigoplus_{j \in J} \mu_j x_j = \bigoplus_{i \in I \setminus J} (\lambda_i + \mu_i) x_i \bigoplus \bigoplus_{i \in I \cap J} \lambda_i x_i \bigoplus \bigoplus_{j \in J \setminus I} \mu_j x_j$ with $0x_i = 0$ and $0 \cdot a = 0$ for any $a$.

This is a consequence of 2.15 that we will announce later.
**Theorem 2.12.** Any $F_\infty$-algebra $\mathbb{A}$ (defined as in 2.6) can be given a generalized ring structure, as defined in 3.1, and the categories of modules and algebras over it are equivalent to the categories of modules and unary algebras over $\mathbb{A}$, respectively, the latter as defined in 3.1. Also, $\mathbb{A}$ is an $F_\infty$-algebra, in the sense of 2.6.

**Proof.** Here we will sketch the proof, referring to sections in 3.1, denoted by bold numerals.

Durov defines generalized rings in 5.1 as a commutative algebraic monad. In 4.3, an algebraic monad $\Sigma$ is described by defining $\Sigma(n)$, which is a free module generated by $n$ elements, as shown in 4.6.5, and several natural maps $\mu^{(k)}_n : \Sigma(k) \times \Sigma(n)^k \to \Sigma(k)$, which satisfy certain natural relations. In 4.3.7, modules $M$ are defined through maps $\alpha^{(k)} : \Sigma(k) \times M^k \to M$ with a similar description.

In our case, we already have $\mathbb{A}(n)$, consisting of terms in variables $x_1, \ldots, x_n$. We may define $\mu_n(k)(t, s_1, \ldots, s_n)$ and $\alpha^{(k)}(t, \sigma_1, \ldots, \sigma_n)$ for $t \in \mathbb{A}(n)$, $s_i \subseteq \mathbb{A}(k)$ and $\sigma_i \subset M$ by replacing each $x_i$ by $s_i$ and $\sigma_i$, respectively, in $t$. Then the relations and commutativity may be checked directly. It can be checked that the homomorphisms are identical to those defined in 2.3 as well by noting that all elements of $\mathbb{A}(n)$ can be written using + and the variables $x_1, \ldots, x_n$.

It is also worth noting that in general, every universal algebraic variety containing no relations (i.e., a category of algebras satisfying a certain set of equalities) gives rise to an algebraic monad, hence the variety of $\mathbb{A}$-modules is also trivially an algebraic monad, giving equivalent categories. The only condition needing to be checked separately is the commutativity, which is a very simple corollary of 5.1.7 and the fact that $\mathbb{A}$ is generated by operations of arity at most 2.

Since any $F_\infty$-algebra $\mathbb{A}$, according to our definition, can be generated by adding elements $a_i \in \mathbb{A}$ and relations $f_i = g_i$ between terms in $a_i$, these are exactly what Durov refers to as unary algebras in 5.1.15, as all of $a_i$, $f_i$ and $g_i$ are unary operations, according to 4.3.9. Furthermore, as announced in 5.3.8 and 5.3.13, the category of unary $\mathbb{A}$-algebras is equivalent to the category of algebras in the category of $\mathbb{A}$-modules, and by 5.3.9, this is identical to how we defined $\mathbb{A}$-algebras and homomorphisms in 2.6.

In 5.1.9, an algebra $\Sigma$ over $\Lambda$ is defined by the existence of a ring homomorphism $\Lambda \to \Sigma$, and given an $\Lambda$-algebra $M$, we have a natural map $\Lambda \to M$. □

Henceforth we will consider only unital algebras.

Let $F$ denote an $F_\infty$-field. Recall that $F^\times = F \setminus \{0\}$.

**Definition 2.13.** The **dimension** of an $F$-module $M$, denoted by $\dim M$, 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 $F_\infty$-module structure with $P = 0$, $-v_i = v_{i+n}$ 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 adjacent 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 \( f \oplus f' \) 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 2.14.** 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. The coproduct of several modules is de-
noted by \( \sum_{i=1}^n M_i \).
\( M_1 \times M_2 \) is the **Cartesian product**, with operations evaluated coordinate-wise.
The product of several modules is denoted by \( \prod_{i=1}^n M_i \).
The free module generated by \( n \) elements is given by \( \mathbb{F}^n \).
The free module generated by elements of a set \( S \) is denoted by \( \mathbb{F}(S) \).
The set of module-homomorphisms is denoted by \( \text{Hom}(M_1, M_2) \).

**Proposition 2.15.** The coproduct, Cartesian product and free module are the
category theoretical coproduct, product and free object. Also, the free module \( \mathbb{F}(S) \) generated by a set \( S \) is isomorphic to the coproduct \( \sum_{s \in S} \mathbb{F} \) (Note that if
\( S \) is infinite, the coproduct is infinite as well).

**Proof.** These are all trivial consequences of theorems in universal algebra. \( \square \)

**Proposition 2.16.** \( \text{Hom}(M_1, M_2) \) has a natural \( \mathbb{F} \)-structure.

**Proof.** The pointwise sum and scalar multiple of two homomorphisms is a ho-
omorphism. \( \square \)

**Remark.** This notion of \( \text{Hom} \) is identical to the definition in \[\text{[3], 4.6.3, further elaborated in 5.3.1.}\]

**Definition 2.17.** 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 \( M_1 \times \mathbb{M}_2 \rightarrow M_1 \otimes M_2 \) where \( M_1 \times M_2 \) is the set of pairs, such that for any bilinear map \( M_1 \times M_2 \rightarrow N \) for some other
module \( N \), there is exactly one map \( M_1 \otimes M_2 \rightarrow N \) that makes the diagram
\( M_1 \times M_2 \rightarrow M_1 \otimes M_2 \rightarrow N \) commute.

**Proposition 2.18.** 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 dia-
gram chasing. We can prove the existence by constructing \( M_1 \otimes M_2 \) ex-
plicitly. 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
\( (m_1 + m_1') \otimes m_2 \sim m_1 \otimes m_2 + m_1' \otimes m_2, \lambda(m_1 \otimes m_2) \sim (\lambda m_1) \otimes m_2 \sim m_1 \otimes (\lambda m_2) \).
Lemma 2.22. Noted by F 5.3.22 the definition in [3], affine space. First let us introduce the polynomial ring in \( n \in \mathbb{N} \) in 5.3.18.

The ear maps \( M \to A \otimes \mathbb{F} \equiv A, (A + B) \otimes C \equiv (A \otimes C) + (B \otimes C) \).

Proof. Since elements of \( \text{Hom}(M_1, \text{Hom}(M_2, N)) \) correspond naturally to bilinear maps \( M_1 \times M_2 \to N \), there is a natural embedding to \( \text{Hom}(M_1 \otimes M_2, N) \). On the other hand, a map \( \varphi : M_1 \otimes M_2 \to M_3 \) restricts to a map \( \varphi' : M_1 \times M_2 \to M_3 \) that is bilinear. Therefore \( \varphi'(m) \) for \( m \in M_1 \) is a homomorphism, and \( \varphi' \) 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 \((a + b, c) \mapsto (a \otimes c) + (b \otimes c)\), 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 coproduct.

Remark. Tensor products are in fact defined in [3], 5.3.5 using adjunction.

Definition 2.20. Let \( M \) be an \( \mathbb{F} \)-module. Then \( \bigotimes^n M \) or \( M^\otimes_n \) denotes the tensor product \( M \otimes \cdots \otimes M \), and \( \bigotimes^0 M = \mathbb{F} \). The congruence generated by \( a_1 \otimes a_2 \otimes a_3 \otimes a_4 \sim a_1 \otimes a_3 \otimes a_2 \otimes a_4 \) for \( a_1 \in M^{\otimes n_1}, a_4 \in M^{\otimes n_2} \) for \( n_1 + n_2 + 2 = n \) and \( a_2, a_3 \in M \) is the kernel of the surjective map \( M^{\otimes n} \to \text{Sym}^n M \) that defines the symmetric power of \( M \). Furthermore, there are natural maps \( \bigotimes^{n_1} M \otimes \bigotimes^{n_2} M \to \bigotimes^{n_1+n_2} M \) and \( \text{Sym}^{n_1} M \otimes \text{Sym}^{n_2} M \to \text{Sym}^{n_1+n_2} M \).

Given a module \( M \), the tensor algebra and the symmetric ring of \( M \) are graded rings defined as \( \bigotimes M := \sum_{n=0}^{\infty} \bigotimes^n M \) and \( \text{Sym} M := \sum_{n=0}^{\infty} \text{Sym}^n M \), respectively, and multiplication is given by the above maps.

Remark. In [3], the tensor algebra and symmetric ring are defined identically, in 5.3.18 and 5.3.19, respectively.

To do algebraic geometry, we need to construct the coordinate ring of an affine space. First let us introduce the polynomial ring in \( n \) variables, following the definition in [3], 5.3.22.

Definition 2.21. The polynomial ring in \( n \) variables \( x_1, \ldots, x_n \) over \( \mathbb{F} \), denoted by \( \mathbb{F}[x_1, \ldots, x_n] \), is defined as the symmetric product \( \text{Sym} \mathcal{F}(\{x_1, \ldots, x_n\}) \).

Lemma 2.22. The polynomial ring generated by \( \{x_1, \ldots, x_n\} \) is isomorphic to

\[
\sum_{\mu : \{1, \ldots, n\} \to \mathbb{N}} (x_1^{\mu_1} \cdots x_n^{\mu_n}) \mathbb{F},
\]

where \( \mu \) is a function from \( \{1, \ldots, n\} \) to \( \mathbb{N} \).
as a module, and the ring structure may be defined as the extension of multiplication of monomials \(x_1^{p_1} \cdots x_n^{p_n}\).

**Proof.** First let us write \(M = \mathcal{F}(\{x_1, \ldots, x_n\})\) as the coproduct \(\sum_{i=1}^n x_i \mathcal{F}\). By 2.19 we may write \(\otimes^k M\) as \(\sum_{\sigma \in S} (x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(k)}) \mathcal{F}\) where \(S\) is the set of maps from \(\{1, \ldots, k\}\) to \(\{1, \ldots, n\}\). By symmetrizing, we get that \(\text{Sym} M\) is isomorphic to the above description. \(\square\)

**Proposition 2.23.** The polynomial ring in \(n\) variables is the free object generated by \(\{x_1, \ldots, x_n\}\) in the category of \(\mathbb{F}\)-algebras. Then every finitely generated algebra is the quotient of a polynomial ring.

**Proof.** Proving this universal property for the polynomial ring amounts to showing that given an algebra \(A\) with certain elements \(a_i \in A\) for \(1 \leq i \leq n\), there is a unique map \(\mathbb{F}[x_1, \ldots, x_n] \rightarrow A\) that sends \(x_i\) to \(a_i\).

Every monomial of the form \(x_1^{p_1} \cdots x_n^{p_n}\) has a well-defined image. Since the polynomial ring is the category theoretical coproduct of the modules \((x_1^{p_1} \cdots x_n^{p_n}) \mathcal{F}\), each freely generated by a monomial, maps from these modules define a (unique) map from the polynomial ring. Since this map preserves multiplication on monomials, it preserves all products.

For the second part of the theorem, we may send the variables \(x_i\) to the generators of the algebra. \(\square\)

Then we may define the affine space as the set of homomorphisms from the polynomial ring to the underlying field, analogously with classical fields. Note that this is not what we will refer to as the algebraic variety, since it is not a spectrum of a ring.

**Definition 2.24.** The affine space of dimension \(n\), \(\mathbb{A}^n\), is the set consisting of ring homomorphisms from \(\mathbb{F}[x_1, \ldots, x_n]\) to \(\mathbb{F}\). We will call \(\mathbb{F}[x_1, \ldots, x_n]\) the ring of functions of \(\mathbb{A}^n\).

**Lemma 2.25.** The points of the affine space \(\mathbb{A}^n\) are in a bijection with the elements of the module \(A := \prod_{i=1}^n \mathbb{F} = \mathbb{F} \times \cdots \times \mathbb{F}\), and the homogeneous degree 1 elements of the polynomial ring \(\mathbb{F}[x_1, \ldots, x_n]\) are in a canonical bijection with \(A^* := \text{Hom}(A, \mathbb{F})\).

**Proof.** A map \(\mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{F}\) is defined by giving the images of the variables \(x_1, \ldots, x_n\), since the polynomial ring is the free object. If the images are denoted by \(\varepsilon_1, \ldots, \varepsilon_n\), this gives an element \((\varepsilon_1, \ldots, \varepsilon_n) \in A\), and since the \(\varepsilon_i\) may be arbitrary, this defines the bijection.

The degree 1 part of \(\mathbb{F}[x_1, \ldots, x_n]\) is isomorphic to the free coproduct of modules \(\sum_{i=1}^n x_i \mathcal{F}\). To see that its elements give linear maps on the module \(A\), it is sufficient to check for the generators of this module, \(f = x_1\). In fact, it is enough to check for a single variable \(f = x_1\). Consider two points \(p, q \in \mathbb{A}^n\), identified by \(\hat{p} := (p(x_1), \ldots, p(x_n))\) and \(\hat{q} := (q(x_1), \ldots, q(x_n)) \in A\). Their images under \(x_1\) are \(p(x_1)\) and \(q(x_1)\). Given a linear combination \(\lambda \hat{p} + \mu \hat{q} \in A\), its image is \(\lambda p(x_1) + \mu q(x_1)\) under \(x_1\), since \(+\) is evaluated coordinate-wise in
the product $A$. This is equal to the linear combination of the images. Later we will prove \[3.22\] and as a consequence the finite module $A^*$ is isomorphic to the free coproduct $\sum_{i=1}^n F$, and it is in fact generated by the linear functions $x_i$. □

As is usual in the theory of classical fields, any vector space can be given a natural affine space structure by forgetting the origin of the space. Unfortunately, contrary to the theory of classical fields, the $n$-dimensional module is not unique. However, since any finitely generated ring is a quotient of a polynomial ring, the different spaces all arise as affine subvarieties of $A^n$, and we may study them as such. Nevertheless, we will present a general definition for the coordinate ring of such spaces arising from a module, and we will call them affine cones.

With the symmetric product, we may define the ring of functions over an affine cone arising from a module $M$. We want the homogeneous linear functions on this affine cone to be isomorphic to $M^*$, as was the case for $M = \prod_{i=1}^n F$, which motivates our following definition.

**Definition 2.26.** The ring of functions over $M$, as an affine cone, is defined as $F[M] := \text{Sym} M^*$. Then the associated affine cone, denoted by $|M|$, is the set consisting of ring homomorphisms $F[M] \to F$.

**Example.** For instance, consider the module $M$ generated by $u, v$, such that $u + v = u - v = 0$. This is a module consisting of 5 elements: $\{0, u, v, -u, -v\}$. Then the ring of functions is isomorphic to $F[x, y]/\{x + y \sim 0, x - y \sim 0\}$. It is a simple verification that $|M|$ is in a bijection with $M$, hence it gives rise to an affine cone that is not isomorphic to $A^n$.

Note that contrary to the case of classical rings, an affine cone based on a module preserves its origin: any non-constant function of $\text{Sym} M^*$ evaluates to 0 in the origin, while as we will see in later chapters, there is at least one linear function for every other point that does not send it to 0.
3 Ordered structure

Recall from Proposition 2.4 that an \( F \)-module for a given \( F_\infty \)-field \( F \) has a natural partial order. It has many of the usual properties of an ordered algebraic structure:

**Proposition 3.1.** Given an \( F \)-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. \( \square \)

Such a module is in fact a **semilattice** with respect to the meet-operation, \( \dot{+} \). 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 \( F \)-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 \( M \).

**Definition 3.3.** An \( F \)-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 \( F \)-module \( M \) is a lattice.

**Proof.** If \( M \) is finitely generated, then there is a finite set \( G \) of generators, and the sum \( a \cup b := \sum_{x \geq a, b} x \) 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 to \( d \). \( \square \)

The lattice structure permits us to construct a **dual lattice**, one where \( \dot{+} \) 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 \( F \). This can be expressed through the natural duality.

**Definition 3.5.** For an \( F \)-module \( M \), there is a **natural duality** \( (\cdot, \cdot) : (M \setminus \{0\}) \times M \to F \) defined as \( (a, b) = \varepsilon \) if \( b \geq \varepsilon a \), and \( 0 \) if no such \( \varepsilon \) exists. We extend it to \( (a, b) : \overline{M} \times \overline{M} \setminus \{(0,0), (\omega, \omega)\} \to F \), 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 \( F \) for all \( a \in \overline{M} \setminus \{0\} \). Also, \( (\mu a, b) = \mu^{-1} (a, b) \) for \( \mu \in F^\times \).
Proposition 3.7. If $M$ is a finite module, then there is a natural order-reversing bijection between $\overline{M}$ and $\overline{M^*}$ where $M^* := \text{Hom}(M, \mathbb{F})$, and the addition on $M^*$ is given by $\cup$.

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

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

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

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 $\varepsilon$ 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 $0_{M^*} := 0_M$, $F_1 + F_2 = F_1 \cap F_2$, $\lambda \cdot F = \{ \lambda^{-1} a \mid a \in F \}$.

Its filter-topology has a closed basis given by $C_a := \{ F \in M^* \mid a \in F \}$ 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 \( C_{a} \) of \( C_{a} \), all open sets containing \( x \) must contain an open set of the form \( \bigcap_{a \in S} C_{a} \) for a finite set \( S \subseteq M \), hence it is enough to show this statement for open sets of this form. Since \( x \in C := \bigcap C_{a} \), 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 \( \Phi \) in either the filter-topology or the weak topology on \( M^* \), and a subset \( S \subseteq \Phi \subseteq M^* \), the infinite intersection \( \bigcap_{a \in S} \Phi_a \) exists and is an element of \( \Phi \).

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 \( \Phi \). 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 \( s_i := \bigcap_{a \in i} \Phi_a \). By transfinite recursion, all \( s_i \) exist and are contained in \( \Phi \). Then \( (s_i)_{i \in I} \) is a descending sequence, and the intersection \( \bigcap_{i \in S} s_i \) is its accumulation point. Therefore it is in \( \Phi \).

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 \( \hat{a} + \hat{b} = \hat{a} \cap \hat{b} \), an embedding since \( \Phi_a := \{ x \in M \mid a \leq x \} \) is such that \( \Phi_a \subseteq \hat{b} \) if and only if \( a \leq b \), so if \( \hat{a} \) and \( \hat{b} \) both contain \( \Phi_a \) and \( \Phi_b \), 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 $\Phi$. Since $\bigcap \Phi \leq a$ for all $a \in \Phi$, $\Phi$ is the principal filter generated by $\bigcap \Phi$. \(\square\)

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 $(M_1 \otimes M_2)^* \cong \text{Hom}(M_1, M_2^*)$, where $\text{Hom}(M_1, M_2^*)$ 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 $\text{Hom}(M_1, M_2^*)$ 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 $\varphi: M_1 \to M_2^*$, 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 $\varphi(m_1) \supseteq m_2$. 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 $\varphi$. 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 $\varphi$ 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 $\Phi \subseteq C_{m_2}$ 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 closed if $F$ is closed. Furthermore, if $\varphi$ maps pointwise to closed filters and is continuous, then $F$ is closed as well. \(\square\)

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. \(\square\)

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 $\varphi: M_1 \to M_2$ admits a natural dual $\varphi^*: M_2^* \to M_1^*$, identified by $\varphi^*(\mu) = (\sum\{m \in M_1 \mid \varphi(m) \geq \mu^*\})^*$ where $\mu^*$ is defined through $(\mu^*)^* = \mu$.

Proof. There is a natural map $\varphi^*: M_2^* \to M_1^*$ 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 $\varphi^*$ 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 $\varepsilon \in F^{\times}$. The set $\{x \in M_1 \mid \varphi(x) \geq \mu^*\}$ is in fact a filter generated by $\mu_0$, since $\varphi$ is order preserving, hence $\mu_0^*(x) = \varepsilon$ if and only if $\varepsilon^{-1}x \geq \mu_0$. Since $\mu_0$ is the sum of all elements in $F_{\mu_0}$, this is equivalent to $\varphi(\varepsilon^{-1}x) \geq \mu^*$, and by the definition of $\mu^*$, 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 extend 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 $\varphi: M_1 \to M_2$ and pairs of operation-preserving maps $u: G_1 \to M_2$ and $v: G_2 \to M_1^*$ 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 $\varphi$, then clearly $u := \varphi|_{G_1}$ and $v := \varphi^*|_{G_2}$ satisfy the condition. Conversely, a map $u: G_1 \to M_2$ 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 $B \not\geq \gamma$ 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 $g_i' \not\geq v(\gamma)$. However, by our assumption, $v(\gamma) \leq \sum_i g_i = \sum_i g_i'$, 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 $f: G_1 \to M_2$ 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 $\varphi$ exists, $\varphi^{-1}(\{x \in M_2 \mid x \geq \gamma\})$ is closed under addition, and all its elements are generated by $F_\gamma$. Conversely, let us construct a map $v: G_2 \to M_1^*$ 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, $\Delta$, 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

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

is a congruence.

Proof. We leave the proof of this statement to the reader. \qed

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 $I + M \subseteq I$ 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 $I$. 

18
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 $x \notin I$, 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 $F(a)$ the set of maximal filters containing $a$. Let us define the equivalence relation $C$ as $a \sim b$ if and only if $F(a) = F(b)$. This is a congruence, since $F(\lambda a) = \{\lambda F \mid F \in F(a)\}$, and $F(a + b) = F(a) \cap F(b)$. 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 be 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 $I$, $\Phi$ 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 antecedent 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 \( \mathbb{F}_\infty \)-fields

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. Recall from [2.6] the following.

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

Fields over \( \mathbb{F}_\infty \) can have non-trivial congruences, on the other hand, the kernels 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
\[
\left\{ \frac{x^n}{\sum_{j=1}^{k} \mu_j x^j} : \sum_{i=1}^{n} \lambda_i = \sum_{j=1}^{k} \mu_j = 1 \right\}
\]

**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 $F_{\infty}[x]$. 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 $F_{\infty}$-algebras, 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 $a+b$. To avoid the absorbing properties of 0, let us interpret the condition $(a, b) \in C$ for some congruence as the harmonic difference $a \ast b := \frac{1}{\frac{1}{a} + \frac{1}{b}}$, instead of the standard difference $a - b$. Then $(ac+bd)(ad+bc)(a \ast b)(c \ast d) = abcd((ac+bd) \ast (ad+bc))$. This motivates the following preliminary definition 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
   - $(bc, 0) \in C$.

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

Once prime congruences are specified, we can define $\text{Spec}$ of any $F_{\infty}$-algebra (as a topological space) as follows:

**Definition 5.2.** Given a congruence $C$ in $F_{\infty}$-algebra $A$ we denote the set of all prime congruences containing $C$ by $V(C)$. Let $\text{Spec}A$ be the spectrum of $A$, consisting of prime congruences. The closed sets of $\text{Spec}A$ are generated by those of the form $V(C)$ where $C$ is a congruence.
Lemma 5.3. 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 5.4. 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 congru-
ence to the following equivalent definition.

Definition 5.5. 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 \( F_\infty[x] \).

Lemma 5.6. 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.

23
Lemma 5.7. 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 5.8. Let $C$ be a prime congruence of an $\mathbb{F}_\infty$-algebra $A$. Assume that $(a^n, b^n) \in C$ for some $(a, b) \not\in C$. Then $(a^n + b, 0) \in C$.

Proof. Since $C$ is a prime congruence, therefore in $\mathbb{A}/C$, 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 5.9. 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 $(x^{n+m} + x^n, 0)$ 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 $1 + x^{n-m} + x^{2(n-m)} + \ldots + x^{m(n-m)} = x^{m(n-m)}$ 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 5.10. 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 $(x, 0)$.

24
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 $(1 \pm x, 0), (1 \pm x^2, 0), \ldots (1 \pm x^{n−1}, 0)$ and $(1 + x^n, x^n)$.

9. Every $n > 0$, the prime congruence $P$ generated by $(1 + x, 0), (1 + x^2, 0), \ldots (1 + x^n, 1)$.

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

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

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

13. Every $n > 0$, the prime congruence $P$ generated by $(1 + x, 0), (1 + x^2, 0), \ldots (1 + x^n, 0)$ and $(x^n, −1)$.

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

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 $\mathbb{F}_\infty[x]/Q = \mathbb{F}_\infty$. 

25
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 5.9 the \(m\)'s satisfying \((1 + x^n, 1) \in P\) 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 \(x = 0\).

\[\square\]

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 \(\mathbb{F}_\infty\) in the Example part. These are finite field extensions of \(\mathbb{F}_\infty\).

Therefore, we obtain that the geometry of \(\text{Spec} \mathbb{F}_\infty[x]\) is very similar to \(\text{Spec} \mathbb{Z}/p\mathbb{Z}[x]\), for instance the closed points of \(\text{Spec} \mathbb{F}_\infty[x]\) 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 $\dim A/P = \dim A$. Moreover $\dim A/P[x] \geq \dim A/P + 1$, since the congruence generated by $(x, 0)$ is prime. Therefore

$$\dim A[x] \geq \dim A/P[x] \geq \dim A/P + 1 = \dim A + 1.$$ 

\[ \square \]

The next theorem gives a criterion when the dimension of $A[x]$ exceeds $n+1$.

**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 least $n + 2$, furthermore in this case there exist four distinct prime congruences in this chain $P_1 \subset P_2 \subset P_3 \subset P_4$ so that 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.** If the Krull dimension of $A[x]$ is at least $n + 2$, then there exist prime congruences $P_1 \subset P_2 \subset P_3 \subset P_4$ of $A[x]$ so that $P_1|_A = P_2|_A$ and $P_3|_A = P_4|_A$ (using the natural map $A \to A[x]$) so that $P_1 \neq P_2$ and $P_3 \neq P_4$. (Note that we do not assume that $P_2$ and $P_3$ are distinct).

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. On the other hand if $(p(x), 0) \in P_2 \setminus P_1$, then $p(x)$ can be replaced by a monomial in $P_1$ and hence in $P_2$ as well. Hence, we can always assume that for any $(p(x), q(x)) \in P_2 \setminus P_1$ we have that $p(x)$ and $q(x)$ are 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

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

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 $k \geq t$)

$$(ax^{n-m}, b) \in P_2 \setminus P_1.$$
and 
\[(cx^{k-l}, d) \in P_4 \setminus P_3.\]

We see that 
\[(a^{k-l}e^{n-m}x^{(n-m)(k-l)}, b^{k-l}e^{n-m}) \quad \text{and} \quad (a^{k-l}e^{n-m}x^{(n-m)(k-l)}, d^{n-m}a^{k-l})\]
are contained in \(P_4\), therefore \((b^{k-l}e^{n-m}, d^{n-m}a^{k-l}) \in P_4\). Since \(P_4\) and \(P_3\) are the same once they are restricted to \(A\), therefore 
\[(b^{k-l}e^{n-m}, d^{n-m}a^{k-l}) \in P_3\]
implying that 
\[(b^{k-l}e^{n-m}x^{(n-m)(k-l)}, d^{n-m}a^{k-l}x^{(n-m)(k-l)}) \in P_3.\]

Furthermore, since \((ax^{n-m}, b) \in P_2 \subset P_3\) we obtain that 
\[(b^{k-l}e^{n-m}x^{(n-m)(k-l)}, d^{n-m}b^{k-l}) \in P_3.\]

Now, assume that \((b, 0) \not\in P_3\), then 
\[(c^{n-m}x^{(n-m)(k-l)}, d^{n-m}) \in P_3.\]

In this case, either \((cx^{k-l}, d) \in P_3\) or \((cx^{k-l} + d, 0) \in P_3\). The first possibility is clearly impossible. If \((cx^{k-l} + d, 0) \in P_3\), then since \((cx^{k-l}, d) \in P_4\), we obtain \((d, 0) \in P_4\). This implies that \((d, 0) \in P_3\), so \((cx^{k-l}, 0) \in P_3\) which yields contradiction.

Therefore we have that \((b, 0) \in P_3\), which implies that \((a, 0) \in P_3\) as well.

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 \((ax^n, bx^n) \in P_2 \setminus P_1\) 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. This implies that \((a, 0) \in P_3\) and hence the statement holds.

\[\square\]

**Remark.** If for a monomial \(p(x_1, \ldots, x_n)\) of \(\mathbb{F}_\infty[x_1, \ldots, x_n]\) and a prime congruence \(P\) we have \((p(x_1, \ldots, x_n), 0) \in P\), then for one of the variables \(x_i\) of \(x_1, \ldots, x_n\) we have \((x_i, 0) \in P\).

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

**Proof.** We proceed by induction. For \(n = 0\), we are done. Assume that \(\mathbb{F}_\infty[x_1, \ldots, x_{n-1}]\) is of dimension \(n-1\), then we would like to prove that \(\mathbb{F}_\infty[x_1, \ldots, x_n]\) is of dimension \(n\). We prove that any chain of prime congruences is of length \(n + 1\). Assume the contrary, hence, we have a chain \(L\) of prime congruences of length at least \(n + 2\):

\[L : P_0 \subseteq P_1 \subseteq \ldots \subseteq P_{n+1} \subseteq \ldots\]

We have two cases.

28
1. Assume that none of the $P_j$ of the the chain $L$ of prime congruence contains any of the $(x_i, 0)$. Then, the second case of Theorem 6.2 cannot hold because of the above remark implying the statement of the Corollary for $A = F_\infty[x_1, \ldots, x_{n-1}]$ and $x = x_n$.

2. One of the prime congruences $P$ contains one of the $(x_i, 0)$. Let $P_j$ be the minimal prime congruence of the chain $L$ which contains one of the $(x_i, 0)$. We can assume that it is $(x_n, 0)$. Let us denote $F_\infty[x_1, \ldots, x_{n-1}]$ by $A$. Then for any $P_k$ and $P_l$ for $k, l \geq j$ we have that $P_k|_A = P_l|_A$ if and only if $P_k = P_l$. Furthermore the second condition of Theorem 6.2 cannot hold for four prime congruences of index at most $j$ again by the previous remark. Hence the chain

$$P_0|_A \subseteq P_1|_A \subseteq \ldots \subseteq P_{n+1}|_A \subseteq \ldots$$

consists of distinct prime congruences except $P_{j-1}|_A = P_j|_A$. By induction, 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 $(a, 0) \in C$. If $(a + b, a) \in C$ holds, then by a symmetric line of thoughts we obtain that $(a + b, b) \in C$, so $(a, b) \in C$. \qed

Note that in an $F_\infty$-field every congruence is cancellative, hence radical. Moreover, annihilators with respect to radical congruences are always radical.

**Lemma 7.4.** Let $C$ be a radical congruence of an $F_\infty$-algebra $A$. Then, for every $c \in A$, $Ann_C(c)$ is radical.
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, \((a^{2n-1}c + a^{n-1}b^n d + a^n b^{n-1} c + b^{2n-1}d, a^{2n-1}d + a^{n-1}b^n c + a^n b^{n-1}d + b^{2n-1}c)\).

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

\[
(a^{2n-1}c + a^{n-1}b^n d + a^n b^{n-1}c + b^{2n-1}d) = \\
= (a^{2n-1}c + a^n b^{n-1}d + a^{n-1}b^n c + b^{2n-1}d) = \\
= (a^{2n-1}c + a^n b^{n-1}d + a^{n-1}b^n d + b^{2n-1}c) = \\
= (a^{2n-1}d + a^n b^{n-1}c + a^{n-1}b^n d + b^{2n-1}c) = \\
= (a^{2n-1}c + a^{n-1}b^n c + a^n b^{n-1}d + b^{2n-1}c),
\]

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

\[
\left( u\left( \sum \lambda_i(ab^{-1})^i \right), u\left( \sum \mu_j(ab^{-1})^j \right) \right)
\]

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

\[
\left( u\left( \sum \lambda_i\mu_j(ab^{-1})^i \right), u\left( \sum \mu_j\lambda_i(ab^{-1})^j \right) \right).
\]

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 congruences which does not contain \((x, 1)\) is a prime congruence.

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

If \( 1 + x = 0 \), then \((x, 1) \in P\) 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 \((a, b) \not\in P\), \((b, c) \not\in P\), \((ac + bd, 0) \not\in P\) and \((ad + bc, 0) \not\in P\). The latter two conditions imply that \((a + b, 0) \not\in P\) and \((c + d, 0) \not\in P\). 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 congruence contains \((x, 1)\). Consider the congruence generated by \((ab^{-1}, 1)\). By Corollary
any \((u, v)\) in the congruence generated by \((ab^{-1}, 1)\) is annihilated by \((c, d)\). So we obtain that \((x, 1)(c, d) \in \Delta\) in \(F/P\). By a similar argument, using that \(1+x \neq 0\), we obtain that \((x, 1)^2 \in \Delta\) which is a contradiction because every congruence in an \(\mathbb{F}_\infty\)-field is radical.

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 \(\Delta\) 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 the \(\mathbb{F}_\infty\)-algebra \(A\). Then \(C\) is the intersection of all prime congruences containing \(C\).

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

Nikolai Durov in his thesis ([3]) defines a family of spectra. The minimal spectrum, the one he refers to as the unary spectrum (6.1) is a straight-forward generalization of the spectrum given by prime ideals. Theorem 7.10 shows that our prime spectrum, given by prime congruences, is a refinement of Durov’s unary spectrum, as every prime ideal gives rise to a congruence generated by it that is cancellative.

**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, 1974, 1, Amer. Math. Soc., pp. 405–408. (1975)

[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.* Selecta Mathematica, pp 1–27, (2017).

[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.