# Languages, automata and computation II
# Tutorial 10 – Ideals, varieties, and polynomial automata

Winter semester 2024/2025

In this tutorial we explore ideals, varieties, and polynomial automata. Recall that an *ideal* of a ring $R$ is a subset $I \subseteq R$ which is 1) closed under sum $I + I \subseteq I$, and 2) closed under under product with elements from the ring $R \cdot I \subseteq I$. For a set of vectors $A \subseteq \overline{\mathbb{Q}}^k$, let $I(A) \subseteq \overline{\mathbb{Q}}[x_1, \ldots, x_k]$ be the set of polynomials vanishing on $A$. (This is an ideal, justifying the notation). For a set of polynomials $P \subseteq \overline{\mathbb{Q}}[x_1, \ldots, x_k]$, let $V(P) \subseteq \overline{\mathbb{Q}}^k$ be the set of vectors where all polynomials in $P$ vanish simultaneously. The *Zariski closure* of a set of vectors $A$ is defined as

$$\overline{A} := V(I(A)).$$

**Exercise 1.**
1. Show that $A \subseteq \overline{A}$, for every $A \subseteq \overline{\mathbb{Q}}^k$.
2. Find a set of vectors $A \subseteq \overline{\mathbb{Q}}^k$ where the inclusion in the previous point is strict. Can such a set $A$ be finite?

**Exercise 2** (zero polynomial vs. zero polynomial function)**.** Show that $p : \overline{\mathbb{Q}}[x_1, \ldots, x_k]$ is the zero polynomial iff as a function $\overline{\mathbb{Q}}^k \to \overline{\mathbb{Q}}$ it is constantly zero. Is this true if we replace $\overline{\mathbb{Q}}$ by $\mathbb{F}_2$ (the field consisting just of the elements $\{0, 1\}$)?

**Exercise 3.** Show that $I$ is an ideal of $R[x]$ iff $I$ is a vector subspace of $R[x]$ over $R$ (i.e., $I + I \subseteq I$ and $aI \subseteq I$ for every $a \in R$) s.t. $xI \subseteq I$.

**Exercise 4.** We have seen that $I(A)$ is an ideal of $\overline{\mathbb{Q}}[x_1, \ldots, x_k]$ for every $A \subseteq \overline{\mathbb{Q}}^d$. Is every ideal of this ring of this form?

## Principal ideal rings

Recall that a ring $R$ is a *principal ideal ring* if every ideal of $R$ is generated by one element.

**Exercise 5.** Are the following principal ideal rings?

1. The field of rational numbers $\mathbb{Q}$.
2. The ring of integers $\mathbb{Z}$.

3. The ring of univariate polynomials over the rationals $\mathbb{Q}[x]$.

4. The ring of univariate polynomials over the integers $\mathbb{Z}[x]$.

5. The ring of bivariate polynomials over the rationals $\mathbb{Q}[x, y]$.

6. The quotient ring $\mathbb{Q}[x, y]/\langle x - y \rangle$.

**Exercise 6.** If $R$ is a principal ideal ring, does the same hold for $R[x]$?

## Noetherian rings

A ring $R$ is *Noetherian* if every ideal $I \subseteq R$ is finitely generated. In the following problem we explore ways to construct Noetherian rings.

**Exercise 7.** 1. Fields are Noetherian.

2. Finite rings are Noetherian.

3. Principal ideal rings are Noetherian.

4. If $R$ is Noetherian and $I \subseteq R$ is an ideal, then $R/I$ is Noetherian.

5. If $R$ is Noetherian, then $R[x]$ is Noetherian. Does the converse hold?

6. If $R$ is Noetherian, then $R[\![x]\!]$ is Noetherian.

**Exercise 8.** Are the following rings Noetherian?

1. Ring of polynomials with countably many variables: $\mathbb{Q}[x_1, x_2, \dots]$.

2. Ring of power series: $\mathbb{Q}[\![x]\!]$.

3. Ring of rational power series: $\mathbb{Q}[\![x]\!] \cap \mathbb{Q}(x)$.

4. Noncommutative ring of power series in noncommuting variables: $R := \Sigma^* \to \mathbb{Q}$, $|\Sigma| \geq 2$, with sum and convolution (Cauchy) product.

**Exercise 9.** For every of the following sets $A$ check that it is a ring. Is it Noetherian?

1. $A = x \cdot \mathbb{Q}[x] \subseteq \mathbb{Q}[x]$.

2. $A = \mathbb{Z} + x \cdot \mathbb{Q}[x] \subseteq \mathbb{Q}[x]$.

## Polynomial automata

Recall that a *polynomial automaton* is a tuple

$$A = (d, \Sigma, Q, q_I, p, F)$$

where $d \in \mathbb{N}$ is the *dimension*, $\Sigma$ is a finite alphabet, $Q = \overline{\mathbb{Q}}^d$ is the set of *states*, $q_I \in Q$ is the *initial state*, $p : \Sigma \to \mathbb{Q}[d]^d$ is a collection of tuples of polynomials inducing a polynomial action on states

$$q \in Q \mapsto q \cdot a \in Q, \quad \text{for every } a \in \Sigma,$$

where $q \cdot a := p^a(q) = (p_1^a(q), \ldots, p_d^a(q))$, and $F : Q \to \overline{\mathbb{Q}}$ is the polynomial *output function*. The action of $\Sigma$ is extended to words $w \in \Sigma^*$ homomorphically: $q \cdot \varepsilon := q$ and $q \cdot (a \cdot w) := (q \cdot a) \cdot w$. The *semantics* of state $q \in Q$ is the mapping $[\![q]\!] : \Sigma^* \to \overline{\mathbb{Q}}$ defined as

$$[\![q]\!]_w = F(q \cdot w), \quad \text{for every } w \in \Sigma^*.$$

The semantics of the automaton $A$ is $[\![A]\!] = [\![q_I]\!]$. The automaton is *zero* if $[\![A]\!] = 0$.

The set $\Sigma^* \to \mathbb{Q}$ has the structure of a commutative ring w.r.t. addition and Hadamard product (pointwise product). This gives us an alternative presentation of the semantics of polynomial automata.

**Exercise 10.** Show that a function $f : \Sigma^* \to \mathbb{Q}$ is recognisable by a polynomial automaton iff its reversal $f^R$ belongs to a finitely generated subring of $\Sigma^* \to \mathbb{Q}$ closed under left quotients $u^{-1}(\cdot)$.

**Exercise 11.** Consider the following computational model $B$. States are tuples of polynomials $S = \mathbb{Q}[d]^d$, with $p_I := (x_1, \ldots, x_d)$ being the initial state and $F : S \to \mathbb{Q}$ a polynomial output function. The update function is described by a tuple of polynomials $p^a = (p_1^a, \ldots, p_d^a) \in \mathbb{Q}[d]^d$, one for each $a \in \Sigma$, by polynomial substitution as follows:

$$p \mapsto p \cdot a := p(p^a) \in S, \quad \text{for every } a \in \Sigma.$$

In other words, in the current state $p$ we replace $x_1$ by $p_1^a$, $\ldots$, $x_d$ by $p_d^a$. This is extended homomorphically to $\Sigma^* \to S$. For instance $p_I \cdot ab = p^a(p^b)$ and $p_I \cdot abc = p^a(p^b)(p^c) = p^a(p^b(p^c))$. The output on reading $w$ is $[\![B]\!]_w = F(p_I \cdot w)$. Decide zeroness for $B$.

A *variety* is a subset $V \subseteq \overline{\mathbb{Q}}^d$ which is the set of common zeros of a set of polynomials: $V = V(P)$ for some $P \subseteq \mathbb{Q}[x_1, \ldots, x_d]$.

**Exercise 12.** For $d = 2$ find a non-trivial infinite variety.

**Exercise 13.** Let $V \subseteq \overline{\mathbb{Q}}^d$ be a variety.

1. Let $g : \overline{\mathbb{Q}}^e \to \overline{\mathbb{Q}}^d$ be a polynomial map. Is $g^{-1}(V) \subseteq \overline{\mathbb{Q}}^e$ a variety?
2. Let $g : \overline{\mathbb{Q}}^d \to \overline{\mathbb{Q}}^e$ be a polynomial map. Is $g(V) \subseteq \overline{\mathbb{Q}}^e$ a variety?

**Exercise 14.** Show that all real varieties $V \subseteq \mathbb{R}^d$ are generated by *a single* polynomial. Is this true for varieties of $\mathbb{C}^d$?

**Exercise 15.** Let $U, V \subseteq \overline{\mathbb{Q}}^d$ be a varieties. Are the following varieties?

1. $U \cap V$. What about possibly infinite intersections?
2. $U \cup V$. What about possibly infinite intersections?
3. $U \setminus V$.

**Exercise 16.** For each direction of the statements below, prove it if it holds, or find a counter-example otherwise.

1. For sets $A, B \subseteq \overline{\mathbb{Q}}^d$: $A \subseteq B$ iff $I(B) \subseteq I(A)$.
2. For sets of polynomials $P, Q \subseteq \overline{\mathbb{Q}}[x_1, \ldots, x_d]$: $P \subseteq Q$ iff $V(Q) \subseteq V(P)$.
3. For varieties $U, V \subseteq \overline{\mathbb{Q}}^d$: $U \subseteq V$ iff $I(V) \subseteq I(U)$.

In the next problem we explore an algorithm to decide zeroness of polynomial automata.

**Exercise 17.** Consider the set of states $V_n \subseteq Q$ which give zero after reading words of length $\leq n$:

$$V_n = \left\{ q \in Q \mid \forall w \in \Sigma^{\leq n} : q \cdot w = 0 \right\}.$$

1. Show that the automaton is zero iff $q_I \in \bigcap_n V_n$.
2. Show that $V_0 \supseteq V_1 \supseteq \cdots \supseteq \bigcap_n V_n$ is a nonincreasing chain of varieties. Conclude that the chain stabilises at some finite level: There is $N \in \mathbb{N}$ s.t. $V_N = V_{N+1} = \cdots = \bigcap_n V_n$.
3. Show that for every $n \in \mathbb{N}$, $V_n = V_{n+1}$ implies $n = N$.
4. Let $P_n$ be a finite set of polynomials s.t. $V_n = V(P_n)$. Show that we can compute a finite set of polynomials $P_{n+1}$ s.t. $V_{n+1} = V(P_{n+1})$.
5. Show how to decide $V(P) = V(Q)$ for two finite set of polynomials $P, Q \subseteq \mathbb{Q}[d]$.
6. Conclude with an algorithm for zeroness.

**Exercise 18.** Provide a coRP algorithm (randomised polynomial time) for the following problem: Given a polynomial automaton $A$ and an input word $w \in \Sigma^*$, decide whether $[\![A]\!]_w = 0$.

**Exercise 19.** Give an algorithm for the following problem: In input we are given a polynomial automaton $A$ and a finite automaton $B$ recognising a regular language $L \subseteq \Sigma^*$. In output we answer whether for every $w \in L$ we have $[\![A]\!]_w = 0$.