Ingo Blechschmidt
University of Antwerp

Master course
Winter term 2024

Algebraic function fields

Exercise sheet 1: Algebraic preliminaries

Exercise 1.1. *Algebraically closed rings are infinite*

Let A be an algebraically closed ring, i. e. every monic polynomial of positive degree has a zero. Let $x_1, \ldots, x_n \in A$. Show that there is an element $y \in A$ which is apart from all the x_i.

Note. Elements $x, y \in A$ are *(strongly) apart* iff $x - y$ is invertible.

Solution. For $n = 0$, pick $y := 0$. For $n \geq 1$, use as y any zero of the monic polynomial $(X - x_1) \cdots (X - x_n) + 1$ of positive degree. (Factors of invertible elements are themselves invertible.)

Exercise 1.2. *Infinitude of the irreducible polynomials*

Let k be a field. Let $f_1, \ldots, f_n \in k[X]$ be irreducible polynomials. Assuming that every nonzero polynomial can be factored into irreducible polynomials, show that there is an irreducible polynomial distinct from the given f_i.

Hint. Adapt Euclid's proof of the infinitude of the primes.

Solution. If $n = 0$, use the polynomial X.

If $n \geq 1$, consider $f_1 \cdots f_n + 1$. *to be continued*

Exercise 1.3. *Vanishing of polynomials*

(a) Let A be a ring. Let $f \in A[X]$ be a polynomial of degree $\leq n$. Show: If f has $n + 1$ pairwise weakly apart zeros, then $f = 0$.

Note. Elements $x, y \in A$ are *weakly apart* iff $x - y$ is regular. An element $u \in A$ is called *regular* if and only if $uv = 0$ implies $v = 0$ for all $v \in A$.

(b) Let A be an infinite integral domain. Let $f \in A[X_1, \ldots, X_n]$. Suppose $f(x_1, \ldots, x_n) = 0$ for all $x_1, \ldots, x_n \in A$. Show that $f = 0$.

Note. That A is *infinite* means that given elements $a_1, \ldots, a_n \in A$, there is always a distinct element $b \in A$.
Hint. Write f as a polynomial in X_n over $A[X_1, \ldots, X_{n-1}]$ and use induction and (a).

(c) Mine your proof of (b) to give a more quantitative version: How many and which zeros does a multivariate polynomial need to have in order for it be the zero polynomial?

Solution.

(a) The case $n = 0$ is immediate. Let $n \geq 1$ and let $a \in A$ be a zero of f. By expanding $f((X - a) + a)$ we observe that $f(X) = (X - a)g(X)$ for some polynomial $g \in A[X]$ of degree $\leq n - 1$. Every zero of f weakly apart from a is also a zero of g. Hence we can conclude by the induction hypothesis.

(b) The case $n = 0$ is immediate. For $n \geq 1$, write $f = \sum_{i=0}^{d} g_i(X_1, \ldots, X_{n-1}) X_n^i$ as a polynomial in X_n. We claim that all the coefficients g_i are zero in $A[X_1, \ldots, X_{n-1}]$. To this end, it suffices by the induction hypothesis to verify that $g_i(a_1, \ldots, a_{n-1}) = 0$ for every point $(a_1, \dots, a_{n-1}) \in A^{n-1}$. This follows from part (a) as the univariate polynomial $f(a_1, \dots, a_{n-1}, X_n) = \sum_{i=0}^{d} g_i(a_1, \dots, a_{n-1}) X_n^i$ has more than d zeros, and because A is an integral domain distinctness implies weak apartness.

Alternative solution. For every element $a \in A$, the polynomial $f(X_1, \dots, X_{n-1}, a)$ is zero in $A[X_1, \dots, X_{n-1}]$ by the induction hypothesis. Hence, viewed as an univariate polynomial in X_n, the polynomial f has more zeros than its formal degree. So $f = 0$ by part (a) applied to the integral domain $A[X_1, \dots, X_{n-1}]$.

(c) A quantitative result is the following. Let A be a ring. Let $f \in A[X_1, \dots, X_n]$ be a polynomial of total degree $\leq d$. If there is a set $M \subseteq A$ of $d + 1$ weakly apart elements such that f is zero on M^n, then $f = 0$.

Exercise 1.4. *Examples for irreducible polynomials*

Which of the following polynomials over a field k are irreducible? Do the answers depend on k?

(a) $Y - X^2$

(b) $XY - 1$

(c) $X^2 + Y^2$

Note. A regular element f is *irreducible* iff $f \sim g_1 \cdots g_n$ implies $f \sim g_i$ for some i, where $a \sim b$ (“a and b are associated”) means that $a = ub$ for some unit b. *Hint.* Use $k[X, Y] \cong (k[X])[Y]$.

Solution.

(a) As a polynomial in Y, it is monic linear, hence irreducible.

(b) As a polynomial in Y, it is linear with the ideal $(X, -1)$ of its coefficients being improper, hence irreducible.

Ingo Blechschmidt
University of Antwerp

Master course
Winter term 2024

Algebraic function fields

Exercise sheet 2: Algebraic sets

Exercise 2.1. *Examples for algebraic sets*

Let k be a field.

(a) Show that the *twisted cubic* $C = \{(t, t^2, t^3) \mid t \in k\} \subseteq \mathbb{A}^3_k$ is algebraic. Can you do describe it using only quadratic equations?

(b) Observe that the set $\{M \in k^{n \times n} \mid M^t M = E_n\}$ of orthogonal matrices is algebraic.

Note. We identify $k^{n \times n}$ with k^{n^2}.

(c) Show that the set $\mathbb{A}^2_k \setminus \{(0,0)\}$ is not algebraic, if k is infinite.

Solution.

(a) We have $\{(t, t^2, t^3) \mid t \in k\} = V(Y - X^2, Z - X^3) = V(Y - X^2, Z - XY)$.

(b) Expanding the condition $M^t M = E_n$ in terms, we observe that the given set is clearly cut out by quadratic equations in the coefficients of M.

(c) Assume that $\mathbb{A}^2 \setminus \{(0,0)\} = V(f_1, \ldots, f_r)$. As k is infinite, there is a set $M \subseteq k \setminus \{0\}$ consisting of more distinct elements than the maximum of the formal degrees of the polynomials f_i. By assumption, the polynomials f_i vanish on M^2. Hence Exercise 1.3(c) implies that they are identically zero. Thus $V(f_1, \ldots, f_r) = V(0) = \mathbb{A}^2$, a contradiction.

Exercise 2.2. *On the size of algebraic sets*

Let k be a field.

(a) Show that every finite subset $\{x_1, \ldots, x_r\} \subseteq \mathbb{A}^n_k$ of r distinct points is algebraic.

(b) Show that at most $\mathbb{A}^1_k$ itself is an infinite algebraic subset of $\mathbb{A}^1_k$.

Note. Similar to Exercise 1.3(c), there is also a quantitative version of this result.

(c) For a suitable choice of k, give an example for a countable union of algebraic sets which is not algebraic.

Solution.

(a) Singleton sets are algebraic ($\{(a_1, \ldots, a_n)\} = V(X_1 - a_1, \ldots, X_n - a_n)$) and the union of pairwise disjoint algebraic sets is algebraic.

(b) Let $M = V(f_1, \ldots, f_r)$ be an algebraic subset of $\mathbb{A}^1_k$. Let $d_1, \ldots, d_r$ be bounds on the total degrees of the polynomials $f_1, \ldots, f_r$. If M contains $\max\{d_1, \ldots, d_r\} + 1$ distinct (hence weakly apart) points, then all the f_i have more zeros than their degree and hence vanish by Exercise 1.3(a), so then $M = \mathbb{A}^1_k$.

(c) For $k = \mathbb{Q}$, the union $\bigcup_{n \in \mathbb{N}} \{n\}$ of singleton (hence algebraic) sets is not algebraic in view of (b).

Exercise 2.3. *Lines intersecting curves*

Let k be a field. Let $C = V(f) \subseteq \mathbb{A}^2_k$ be an affine plane curve, where $f \in k[X, Y]$ is a polynomial of degree $\leq n$. Let $L \subseteq \mathbb{A}^2_k$ be a line. Show: If $C \cap L$ contains more than n points, then $L \subseteq C$.

Hint. Suppose $L = V(Y - (aX + b))$ and consider $f(X, aX + b) \in k[X]$.

Exercise 2.4. *A first exercise in fibered thinking*

Let k be an infinite field. Let $f \in k[X_1, \ldots, X_n]$.

(a) Let $n \geq 1$. Show: If $D(f)$ is inhabited at all, then $D(f)$ is infinite.

(b) Let $n \geq 2$. Let k be algebraically closed with decidable equality. Show that $V(f)$ is infinite, if f is of positive degree.

Note. Recall that a set X has *decidable equality* iff for all $x, y \in X$, either $x = y$ or $x \neq y$. Anonymously—disregarding algorithmic implementability and stability in families—every set has decidable equality.

Exercise 2.5. *Discriminating functions*

Let k be a field. Let $M \subseteq \mathbb{A}^n_k$ be an algebraic set.

(a) Let $p \notin M$. Show that there is a polynomial $f \in I(M)$ with $f(p) = 1$.

(b) Let $p_1, \ldots, p_r \notin M$ be distinct points. Find polynomials $f_1, \ldots, f_r \in I(M)$ with $f_i(p_j) = \delta_{ij}$.

Note. The Kronecker delta δ_{ij} is 1 if $i = j$, and 0 otherwise.

Ingo Blechschmidt
University of Antwerp

Master course
Winter term 2024

Algebraic function fields

Exercise sheet 3: Varieties

Exercise 3.1. *Examples for varieties*

Let k be an infinite field which is also an integral domain.

(a) Verify that $I(V(Y - X^2)) = (Y - X^2)$. Conclude that $V(Y - X^2) \subseteq \mathbb{A}^2_k$ is irreducible.

(b) Assuming that $2 \neq 0$ in k, decompose $V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) \subseteq \mathbb{A}^2_k$ into irreducible components.

(c) Determine $I(C)$ where C is the twisted cubic of Exercise 2.1(a) and verify that C is irreducible.

(d) Determine $I(\mathbb{A}^1_K)$ and decompose $\mathbb{A}^1_K$ into irreducible components in the case $K = \mathbb{F}_p$.

Exercise 3.2. *On the intersection of plane curves*

Let k be a field with decidable equality. Let $f, g \in k[X, Y]$ be polynomials of positive degree with $\gcd(f, g) = 1$.

(a) Find polynomials $d \in k[X]$, $e \in k[Y]$ of positive degree such that $V(f, g) \subseteq V(d) \times V(e)$.

Note. The following algebraic preliminaries are useful. As k has decidable equality, so has $k(X)$ and hence $k(X)[Y]$ is a Bézout ring. By a lemma of Gauß, we have $\gcd(f, g) = 1$ not only in $k[X][Y]$ but also in $k(X)[Y]$.

(b) Conclude that there is a number $r \in \mathbb{N}$ such that it is not the case that $V(f, g)$ contains more than r distinct points.

Exercise 3.3. *The many forms of the affine line*

Let k be an algebraically closed field with decidable equality. Which of the following algebraic sets are isomorphic to $\mathbb{A}^1_k$?

(a) $V(Y - X^2) \subseteq \mathbb{A}^2_k$

(b) $C \subseteq \mathbb{A}^3_k$ from Exercise 2.1(a)

(c) $V(XY - 1) \subseteq \mathbb{A}^2_k$

(d) $V(Y^2 - X^3) \subseteq \mathbb{A}^2_k$

Exercise 3.4. *Functions on the point*

Let k be a field. Let $M \subseteq \mathbb{A}^n_k$ be an algebraic set. Consider the following statements:

(1) $M = \{p\}$ for some point $p \in \mathbb{A}^n_k$.

(2) The canonical morphism $k \to \Gamma M$ is an isomorphism.

(3) The k-vector space ΓM is finitely generated.

Prove:

(a) $(1) \Rightarrow (2) \Rightarrow (3)$.

(b) $(2) \Rightarrow (1)$.

(c) $(3) \Rightarrow (2)$, if k is algebraically closed and an integral domain and if M is irreducible.

Hint (Cayley–Hamilton). Let A be a ring. Let B be an A-algebra which is generated as an A-module by d elements. Let $u \in B$. Then there is a monic polynomial $f \in A[X]$ of degree d such that $f(d) = 0$.

(d) $(3) \Rightarrow$ anonymously (1), if k is an integral domain and M is irreducible.

Hint. Show that it is impossible for M to be infinite, by using the following result of the class: If an algebraic set V contains r distinct points, then there is a linearly independent family of r vectors in ΓV.

Ingo Blechschmidt
University of Antwerp

Algebraic function fields

Exercise sheet 4: Noether normalization

Exercise 4.1. *Examples for finite and non-finite maps*

Which of the following ring homomorphisms mapping f to $[f]$ are finite? Provide proofs.

(a) $k[X] \to k[X,Y]/(Y-X^2)$
(b) $k[X] \to k[X,Y]/(X-Y^2)$
(c) $k[X] \to k[X,Y]/((Y-X)(Y+X))$
(d) $k[X] \to k[X,Y]/(XY)$
(e) $k[X] \to k[X,Y]/(XY-1)$

Hint. In order to form an opinion of the morphisms being finite, it may be useful to picture them geometrically and check whether the fibers are finite. For instance, the first morphism corresponds to the projection map $V(Y-X^2) \to \mathbb{A}^1_k$, $(x,y) \mapsto x$.

Exercise 4.2. *A concrete Noether normalization*

Let k be a field. Find a finite injective k-algebra homomorphism

$$k[T] \longrightarrow k[X,Y]/(XY-1)$$

and interpret your result geometrically.

Exercise 4.3. *Linear substitutions suffice*

Let k be an infinite field with decidable equality. Let $f \in k[X_1,\ldots,X_n,T]$ be a polynomial in which T actually occurs. Show that there exist numbers $\mu, \lambda_1, \ldots, \lambda_n \in k$ such that the polynomial $\mu f(X_1 + \lambda_1 T, \ldots, X_n + \lambda_n T, T)$ is monic of positive degree in T.

Hint. Write f as the sum of its homogeneous components and consider the highest-degree component.

Exercise 4.4. *First steps with integral extensions*

(a) Let A be a ring. Let $x \in A$ such that $x^2 - 3x + 1 = 0$. Let $y \in A$ such that $y^2 + 5y - 2 = 0$. Find a monic polynomial $f \in \mathbb{Z}[T]$ such that $f(x+y) = 0$.
(b) Let $A \subseteq B$ be an integral ring extension (i. e. A is a subring of B such that every element of B is the zero of a monic polynomial with coefficients from A). Let $x \in A$. Show: If x is invertible in B, then also in A.

Exercise 4.5. *The strong and the weak Nullstellensatz*

(a) Let A be a ring. Show that a polynomial $f = \sum_i a_i T^i \in A[T]$ is invertible iff $a_0 \in B$ is invertible and $a_1, a_2, \ldots$ are nilpotent.

   Note. The direction "$\Rightarrow$" admits a direct elementary proof, but it might be simpler to employ Krull's theorem: To verify that an element is nilpotent, show that it is contained in all prime ideals. In this form Krull's theorem is not constructive; this drawback can be healed by using the *generic prime ideal*.

(b) Let $\mathfrak{a} \subseteq A$ be an ideal in a ring A. Let $g \in A$. Let $\mathfrak{b} := \mathfrak{a}[T] + (1 - gT) \subseteq A[T]$. Prove: $g \in \sqrt{a} \Longleftrightarrow 1 \in \mathfrak{b}$.
(c) Let $n \in \mathbb{N}$. Let A be a ring such that

$$1 \in \mathfrak{b} \quad \vee \quad V(\mathfrak{b}) \text{ inhabited}$$

   for all finitely generated ideals $\mathfrak{b} \subseteq A[X_1,\ldots,X_n,T]$. Show that

$$g \in \sqrt{\mathfrak{a}} \quad \vee \quad V(\mathfrak{b}) \cap D(g) \text{ inhabited}$$

   for all finitely generated ideals $\mathfrak{a} \subseteq A[X_1,\ldots,X_n]$ and all polynomials $g \in A[X_1,\ldots,X_n]$.

Ingo Blechschmidt
University of Antwerp

Master course
Winter term 2024

Algebraic function fields

Exercise sheet 5: Unsorted drafts

Exercise 5.1. *Consequences of the duality axiom*

Recall that the ring R in synthetic algebraic geometry fulfills the following duality axiom: Given any polynomials $f_1, \ldots, f_r \in R[X_1, \ldots, X_n]$, the canonical R-algebra homomorphism

$$\begin{array}{rcl} R[X_1, \ldots, X_n]/(f_1, \ldots, f_r) & \longrightarrow & R^{V(f_1, \ldots, f_n)} \\ [g] & \longmapsto & (p \mapsto g(p)) \end{array}$$

where $V(f_1, \ldots, f_n) = \{p \in R^n \mid f_1(p) = \ldots = f_r(p) = 0\}$ is an isomorphism. Show that this axiom implies the following consequences.

(a) For every map $f : R \to R$, there is a unique polynomial $g \in R[X]$ such that $f(x) = g(x)$ for all $x \in R$.

(b) Let $f_1, \ldots, f_r \in R[X]$ by polynomials with no common zero. Then $1 \in (f_1, \ldots, f_r)$.

(c) Let $x \in R$ be not invertible. Then x is nilpotent.

Hint. Consider the polynomial $f(Y) = xY - 1$.

(d) Let $f \in R[X]$ be monic of positive degree. Then it's impossible for f to have no zero.

(e) Let $x_1, \ldots, x_n \in R$. There it's not the case that there is no $y \in R$ apart from all x_i.