ENS de Lyon 2017 - 2018

MASTER 1–ALGEBRAIC GEOMETRY WEEK 1, 16.01.2018

TD 1-Noether normalization, Nullstellensatz and applications

All rings will be commutative with 1, all ring maps send 1 to 1. k will always be a field. A map of rings $f : A \to B$ is called

• **integral** if any $b \in B$ is integral over A, i.e. satisfies an equation $b^n + a_{n-1}b^{n-1} + ... + a_1 b + a_0 = 0$ with $a_i \in A$ (we use f to see B as A-algebra).

• **finite** (resp. **of finite type**) if it turns B into a finitely generated A-module (resp. A-algebra).

0.1 Basic things on integrality

Make sure you know the following things **very well**, since we will use them constantly.

1. Prove that any finite map of rings is integral. Moreover, an integral map $f : A \to B$ is finite if and only if it is of finite type, if and only if B is generated as A-algebra by finitely many elements integral over A.
2. Prove that a composition of finite (resp. integral, resp. of finite type) rings maps is also finite (resp...). Moreover, if $A \to B$ is integral (resp...), then for any map $A \to C$ the natural map $C \to C \otimes_A B$ is integral (resp...).
3. (a recurrent trick) Suppose that $f : A \to B$ is an injective integral map of rings. Prove that A is a field if and only if B is a field.

0.2 Noether's normalization lemma

This result is absolutely fundamental, make sure you understand it!

1. (preparation) Let R be a ring and let $f \in R[X_1, ..., X_n] \setminus R$. Prove that if e is large enough, then we can find $d > 0$, $a \in R \setminus \{0\}$ and $a_0, ..., a_{d-1} \in R[X_1, ..., X_{n-1}]$ such that
$$f(X_1 + X_n^{e^{n-1}}, X_2 + X_n^{e^{n-2}}, ..., X_{n-1} + X_n^e, X_n) = aX_n^d + a_{d-1}X_n^{d-1} + ... + a_0.$$
2. Prove **Noether's normalization lemma** : let A, B be integral domains and let $f : A \to B$ be an injective map of finite type. Then we can find $x_1, ..., x_d \in B$ and $f \in A \setminus \{0\}$ such that the natural $A[1/f]$-algebra map $A[1/f][T_1, ..., T_d] \to B[1/f], T_i \mapsto x_i$ is injective and finite.
   Hint : pick the smallest d for which there are $f \in A \setminus \{0\}$ and $x_1, ..., x_d \in B$ such that the previous map is integral, and show that up to replacing f by a multiple of it, $x_1, ..., x_d$ work, using the preparation result.
3. State in a comprehensible way what this result says about finitely generated algebras over a field and over $\mathbf{Z}$.

0.3 Zariski's lemma

Let k be a field. We want to prove (in several ways) **Zariski's lemma** : if a finitely generated k-algebra A is a field, then A is a finite extension of k.

1. Give a proof using Noether normalization and the recurrent trick in exercise 1.
2. For a second proof, we will prove by induction on n the following statement : if A is a k-algebra generated by n elements, say $x_1, ..., x_n$, and if A is a field, then $x_1, ..., x_n$ are algebraic over k.
   a) Treat the case $n = 1$. Suppose now that the result holds for algebras generated by at most $n - 1$ elements (over any field!) and that x_1 is not algebraic over k.

b) Prove that we can find $a \in k[x_1] \subset A$ nonzero such that $ax_2, ..., ax_n$ are integral over $k[x_1]$. **Hint** : note that $A = k(x_1)[x_2, ..., x_n]$.

c) Prove that if $b \in k[x_1]$ is nonzero, then for d large enough $\frac{a^d}{b}$ belongs to $k[x_1, ax_2, ..., ax_n]$. Conclude that $\frac{a^d}{b} \in k[x_1]$ and finish the proof.

3. a) Prove the following result of Artin and Tate : let $A \subset B \subset C$ be rings, with A noetherian and C finitely generated as A-algebra and finitely generated as B-module, then B is a finitely generated A-algebra. Hint : using generators of C as A-algebra and B-module, cook up a finitely generated A-algebra $D \subset B$ such that C is a finite D-module, then deduce that B is a finite D-module.

   b) Use this result to give yet another proof of Zariski's lemma.

   c) Use a) to prove the following theorem of Noether : if R is a finitely generated k-algebra (k being a field), and if G is a finite group acting on R by k-algebra automorphisms, then the ring of invariants R^G is also finitely generated over k.

0.4 Maximal ideals in $k[X_1, ..., X_n]$ and $\mathbf{Z}[X_1, ..., X_n]$

Let k be a field.

1. Prove that if m is a maximal ideal of $k[X_1, ..., X_n]$, then $k[X_1, ..., X_n]/m$ is a finite extension of k.
2. If k is algebraically closed, give a natural bijection between maximal ideals of $k[X_1, ..., X_n]$ and k^n. In general, prove that the maximal ideals of $k[X_1, ..., X_n]$ are in canonical bijection with the G-orbits on $\bar{k}^n$, where $\bar{k}$ is an algebraic closure of k and $G = \mathrm{Gal}(\bar{k}/k)$.
3. (**weak Nullstellensatz**) The polynomials $f_1, ..., f_d \in k[X_1, ..., X_n]$ have no common zero in an algebraic closure of k. Prove that we can find polynomials $g_1, ..., g_d \in k[X_1, ..., X_n]$ such that

$$f_1 g_1 + ... + f_d g_d = 1.$$

4. Prove that if m is a maximal ideal of $\mathbf{Z}[X_1, ..., X_n]$, then $\mathbf{Z}[X_1, ..., X_n]/m$ is a finite field.
5. Prove that a family of polynomials $f_i \in \mathbf{Z}[X_1, ..., X_n]$ generates the unit ideal in $\mathbf{Z}[X_1, ..., X_n]$ if and only if the equations $f_i(x_1, ..., x_n) = 0$ have no common solution in any finite field.
6. (more difficult) Let $(f_i)_{i \in I}$ be a family of polynomials in $\mathbf{Z}[X_1, ..., X_n]$. Prove that the following statements are equivalent :
   - these polynomials have a common zero in $\mathbf{C}^n$.
   - for all but finitely many primes p the f_i's have a common zero in $\overline{\mathbf{F}}_p$.
   - same as before, but with infinitely many primes instead.
7. (more difficult) Prove that any maximal ideal of $k[X_1, ..., X_n]$ can be generated by n elements, more precisely it is generated by elements of the form $f_1(X_1), f_2(X_1, X_2), ..., f_n(X_1, ..., X_n)$.
8. (more difficult) a) Let A be an integral domain and let $\bar{K}$ be an algebraic closure of its fraction field K. A polynomial $P \in A[X_1, ..., X_n]$ has the property that P is irreducible in $\bar{K}[X_1, ..., X_n]$. Prove that there is $a \in A \backslash \{0\}$ such that for all maps $\varphi : A_f \to L$, with L a field, the corresponding polynomial $P^\varphi \in L[X_1, ..., X_n]$ is irreducible.

   b) State this in a comprehensible way when $A = \mathbf{Z}$.

0.5 The Nullstellensatz

Let k be a field.

1. Let $f : A \to B$ be a morphism of finitely generated k-algebras. Prove that the inverse image of any maximal ideal of B is a maximal ideal of A.
2. Prove that if A is a finitely generated k-algebra, then for all ideals I of A, $\sqrt{I}$ is the intersection of all maximal ideals of A containing I. **Hint** : reduce to $I = 0$, then apply the first item to the map $A \to A[1/f]$ (for suitable f).
3. Deduce **Hilbert's Nullstellensatz** : if $f, g_1, ..., g_d \in k[X_1, ..., X_n]$ and f vanishes at each common zero of $g_1, ..., g_d$ in an algebraically closed extension of k, then for N large enough $f^N \in (g_1, ..., g_d)$.

0.6 Some fun applications

1. (A very special case of the Ax-Grothendieck theorem) Let k be an algebraically closed field and write X for $(X_1, ..., X_n)$, so $k[X] = k[X_1, ..., X_n]$, $k[X, Y] = k[X_1, ..., X_n, ..., Y_n]$, etc. Let $P_1, ..., P_n \in k[X]$ be such that the induced map

$$f : k^n \to k^n,\ f(x_1, ..., x_n) = (P_1(x_1, ..., x_n), ..., P_n(x_1, ..., x_n)).$$

   is injective. We will prove that f is surjective.

   a) Suppose that this is not the case. Prove that we can find $N \geq 1$ and polynomials $H_{ij} \in k[X, Y]$ such that for $i = 1, ..., n$

$$(X_i - Y_i)^N = \sum_{j=1}^{n} H_{ij}(X, Y)(P_j(X) - P_j(Y)).$$

   Also prove that there are $a_1, ..., a_n \in k$ and polynomials $G_1, ..., G_n \in k[X]$ such that

$$G_1(P_1 - a_1) + ... + G_n(P_n - a_n) = 1.$$

   b) Let A be the subring of k generated by the coefficients of all polynomials P_i, G_j, H_{ij}, as well as by $a_1, ..., a_n$. Using a maximal ideal of A, obtain a contradiction.

2. (more difficult) a) Prove the following theorem of Malcev : a finitely generated group of matrices G over a field is residually finite, i.e. for any $g \in G \setminus \{1\}$ there is a finite-index normal subgroup of G not containing g.

   b) Prove Selberg's lemma : a finitely generated group of matrices over a field of characteristic zero has a torsion-free subgroup of finite index.

0.7 Nullstellensatz and Jacobson rings

This exercise is rather challenging. A ring R is called a **Jacobson ring** if for all ideals I of R, $\sqrt{I}$ is the intersection of all maximal ideals of R containing I. For instance, $\mathbf{Z}$ and any field (or even a finitely algebra over that field) are Jacobson rings, but a discrete valuation ring is not.

1. (preliminary) Let $A \to B$ be an inclusion of integral domains, with B a field, finitely generated as A-algebra and [1] such that B is algebraic over $\mathrm{Frac}(A)$. Prove that there is some nonzero $a \in A$ for which $A[1/a]$ is a field.
2. Prove that the following statements are equivalent
   - R is Jacobson.
   - If a quotient A of R is an integral domain and $A[1/a]$ is a field for some nonzero $a \in A$, then A is a field.
   - for any maximal ideal m of $R[T]$, $m \cap R$ is maximal in R.
3. (generalization of Nullstellensatz) Prove that if A is a Jacobson ring, then so is any finitely generated A-algebra B, and for any maximal ideal m of B, the inverse image n of m in A is maximal and the extension $A/n \to B/m$ is finite.

1. Using Zariski's lemma, one easily shows that the next hypothesis is a consequence of the others, but you can do the whole exercise without using Zariski's lemma...