Prof. Dr. U. Görtz **WS 2018/19**
F. Gora

Seminar on the Weil conjectures for curves — Supplementary notes on Talk 3

Let k be a perfect field, and let $\overline{k}$ be an algebraic closure of k.

In the talk, we made the following definition (following [Ha]):

Definition. We say that an affine algebraic set $V \subseteq \mathbb{A}^n(\overline{k})$ is *defined over* k if it is of the form $V(\mathfrak{a})$ where $\mathfrak{a} \subseteq \overline{k}[X_1, \dots, X_n]$ is an ideal which has a system of generators in $k[X_1, \dots, X_n]$.

Note that an ideal $\mathfrak{a}$ has a system of generators in $k[X_1, \dots, X_n]$ if and only if

$$\mathfrak{a} = (\mathfrak{a} \cap k[X_1, \dots, X_n])\overline{k}[X_1, \dots, X_n],$$

i.e., $\mathfrak{a}$ is equal to the ideal generated by $\mathfrak{a} \cap k[X_1, \dots, X_n]$ in $\overline{k}[X_1, \dots, X_n]$.

This is the natural definition[1] of an algebraic set defined over k, however we will need to know that in this case the ideal $I(V)$ also has a system of generators in $k[X_1, \dots, X_n]$. For $V = V(\mathfrak{a})$ we have $I(V) = \mathrm{rad}(\mathfrak{a})$ (using Hilbert's Nullstellensatz). So the statement above boils down to the following

Proposition. Let $\mathfrak{a}_0 \subset k[X_1, \dots X_n]$ be a radical ideal. Then the ideal $\mathfrak{a} := \mathfrak{a}_0\overline{k}[X_1, \dots, X_n]$ generated by $\mathfrak{a}_0$ in $\overline{k}[X_1, \dots, X_n]$ is also a radical ideal.

Proof. We sketch a proof (but will use more advanced commutative algebra than is used in the seminar; what we did in the Commutative Algebra course last term is enough, or see [Atiyah-Macdonald] or another book on commutative algebra). We have $\overline{k}[X_\bullet]/\mathfrak{a} = k[X_\bullet]/\mathfrak{a}_0 \otimes_k \overline{k}$. By assumption, $k[X_\bullet]/\mathfrak{a}_0$ is reduced, and we want to show that the tensor product $k[X_\bullet]/\mathfrak{a}_0 \otimes_k \overline{k}$ is also reduced.

Since $\mathfrak{a}_0$ is a radical ideal, it is equal to the intersection of the prime ideals in $k[X_1, \dots, X_n]$ containing it. Of course, it is enough to take the intersection of the minimal prime ideals among these, and since $k[X_1, \dots, X_n]$ is Noetherian, there are only finitely many such prime ideals. Therefore,

$$\mathfrak{a}_0 = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_m$$

is a finite intersection of prime ideals $\mathfrak{p}_i$. This shows that we can embed $k[X_1, \dots, X_n]/\mathfrak{a}$ into the product $\prod_i k[X_1, \dots, X_n]/\mathfrak{p}_i$ of domains, and passing to fraction fields, into a product of fields. Since tensor product is compatible with finite products this means that it is enough to show the following

Claim. Let L/k be an extension field (not necessarily algebraic). Then $L \otimes_k \overline{k}$ is reduced.

[1] The alternative would be defining that V is defined over k if $I(V)$ has a system of generators in $k[X_1, \dots, X_n]$ — we could work in the sequel with this definition, but we would not know that writing down a system of polynomial equations with coefficients in k would give rise to an affine algebraic set defined over k.

To prove the claim, it is enough to prove that $L \otimes_k k'$ is reduced for every finite field extension k'/k. Since k is assumed to be perfect, we can apply the Theorem of the Primitive Element and write $k' \cong k[T]/(f)$ for a separable irreducible polynomial $f \in k[T]$. Then we have

$$L \otimes_k k' \cong L[X]/(f).$$

Since f is separable, the factorization into irreducible polynomials over any extension field (such as L) does not have multiple factors. The Chinese Remainder Theorem then shows that $L[X]/(f)$ is a product of fields, hence reduced.

Remark.

(1) Note that we need that k is perfect. (Can you see an example where the proposition fails for a non-perfect field k?)

(2) It is not true in general that, with notation as above, $\mathfrak{a}$ is a prime ideal for $\mathfrak{a}_0$ a prime ideal. (Can you find an example?)

In the end, I stated, but did not have time to prove, the following proposition:

Proposition Let $V \subseteq \mathbb{A}^n(\overline{k})$ be an affine variety which is defined over k. Let $k(V)$ be its field of rational functions. Then k is algebraically closed in $k(V)$.

Proof. To make the proof more transparent, we will use tensor products of k-algebras. With some effort, one could translate the proof into more elementary terms, of course.

With notation as above, we have $k(V) = \mathrm{Frac}(A)$, where $A = k[X_1, \ldots, X_n]/\mathfrak{a}_0$ is the affine coordinate ring of V over k. We want to show that there does not exist an intermediate field k' of the extension $k(V)/k$ which is finite over k but $\neq k$.

Let k' be an intermediate field of $k(V)/k$ which is finite over k. Since k is perfect, k' is separable over k, so as before we write it as $k' \cong k[T]/(f)$ for an irreducible polynomial k. Since $k' \subset k(V)$ and since $\overline{k}$ is flat over k, tensoring gives us an *inclusion*

$$\overline{k}[T]/(f) \cong k' \otimes \overline{k} \to k(V) \otimes \overline{k}.$$

To proceed, we will first prove:

Claim. We have

$$k(V) \otimes \overline{k} \cong \overline{k}(V).$$

More or less by definition we have $k[V] \otimes_k \overline{k} \cong \overline{k}[V]$. Letting $S = k[V] \backslash \{0\}$, so $k(V) = S^{-1}k[V]$, we then obtain

$$k(V) \otimes \overline{k} = S^{-1}k[V] \otimes \overline{k} \cong S^{-1}\overline{k}[V].$$

From this point there are different ways to prove the claim. Using the theory of integral ring homomorphisms, it can be done as follows: The map $k \mapsto \overline{k}$ is an integral ring homomorphism Since the tensor product $- \otimes_k k[V]$, and the localization with respect to S preserve this property, the inclusion $k(V) \to S^{-1}\overline{k}[V]$ is again integral. Since $\overline{k}[V]$ is a domain, this is an injective integral ring homomorphism between domains. In this situation we know that one

of the two is a field if and only if the other one is. It follows that $S^{-1}\overline{k}[V]$ is a field, so it must be equal to $\mathrm{Frac}(\overline{k}[V]) = \overline{k}(V)$.

The claim being proved, we now have an inclusion

$$\overline{k}[T]/(f) \to \overline{k}(V).$$

The left hand side decomposes, since f is separable, as a product of copies of $\overline{k}$ (once again, by the Chinese Remainder Theorem). The number of copies is the degree of f, so since the right hand side is a domain, the degree must be $= 1$, whence $k' = k$.

Literatur

[Ha] S. H. Hansen, *Rational Points on Curves over Finite Fields*, Lect. Notes Ser., Aarhus Univ. Mat. Institute, 1995. Available online.