Universität Konstanz
Fachbereich Mathematik und Statistik
Prof. Dr. Salma Kuhlmann
Mitarbeiter: Dr. Mickaël Matusinski
Büroraum F 409
mickael.matusinski@uni-konstanz.de

Übungen zur Vorlesung Reelle algebraische Geometrie

Blatt 3 - Lösung.

Theorem 0.1 (Puiseux theorem) *The set $\mathcal{P}$ is a real closed field.*

1. Firstly, we show that $\mathcal{K}$ is a field.
   Let $A(X) = \sum_{i=m}^{\infty} a_i X^i$ and $B(X) = \sum_{i=n}^{\infty} b_i X^i$ be two elements of $\mathcal{K}$, with for instance $m \leq n$. We have:

   - stability by addition: $A(X)+B(X) = \sum_{i=m}^{n} a_i X^i + \sum_{i=n}^{\infty}(a_i+b_i)X^i$ is an element of $\mathcal{K}$;

   - the addition is associative and commutative: this follows directly from the preceding formula and the commutativity and associativity of the coefficients that are real numbers;

   - the neutral element is 0: we have $0 + A(X) = A(X) + 0 = A(X)$ in $\mathcal{K}$;

   - existence of an additive inverse: the element $-A(X) = \sum_{i=m}^{\infty} -a_i X^i$ is the inverse of $A(X)$ in $\mathcal{K}$;

   - stability by multiplication: note that for any $i \geq m+n$, the number of couples of integers (j,k) such that $j \geq m, k \geq n$ and $j+k=i$, is finite. Then $A(X).B(X) = \sum_{i=m+n}^{\infty} \sum_{j+k=i} a_j b_k X^i$ is well defined and is an element of $\mathcal{K}^*$;

   - the multiplication is associative and commutative: this follows directly from the preceding formula and the commutativity and associativity of the coefficients that are real numbers;

   - the neutral element is 1: we have $1.A(X) = A(X).1 = A(X)$ in $\mathcal{K}^*$;

- existence of the multiplicative inverse: suppose $A(X) \neq 0$. Factorizing by the term with lowest degree $a_m X^m$, we get $A(X) = a_m X^m(1 + U(X))$ where $U(X) \in \mathbb{R}[[X]]$ such that $U(0) = 0$. Then we define

$$\begin{aligned} \frac{1}{A(X)} &:= a_m^{-1} X^{-m} \frac{1}{1 + U(X)} \\ &= a_m^{-1} X^{-m} \sum_{k=0}^{\infty} (-1)^k U(X)^k \text{ by Euler's formula} \end{aligned}$$

Since $U(0) = 0$, we can factor X in $U(X)$. So for any k, $U(X)^k$ has **order (= least exponent**) at least k. So by a straightforward induction, one shows that only finitely many terms $U(X)^k$ give a contribution to a given power X^i. Therefore $\sum_{k=0}^{\infty} (-1)^k U(X)^k = 1 - U(X) + U(X)^2 - \cdots$ is well-defined and is an element of $\mathbb{R}[[X]]$;

- the set $T := \mathcal{K}_{\geq 0} = \left\{ A(X) = \sum_{i=m}^{\infty} a_i X^i \mid a_m \geq 0 \right\} \cup \{0\}$ is a positive cone: provided $A(X)$,$B(X) \in P$, we have
• $A(X) + B(X) = a_m X^m + \cdots \in T$,
• $A(X).B(X) = a_m b_n X^{m+n} + \cdots \in T$,
• for any $A(X) \in \mathcal{K}$, $A(X)^2 = a_m^2 X^{2m} + \cdots \in T$.
So T is a preordering.
Moreover, $-1 \notin T$. So T is a proper preordering.
Finally, given any non zero $A(X) = \sum_{i=m}^{\infty} a_i X^i \in \mathcal{K}$, either $a_m > 0$ and so $A(X) \in T$, or $a_m < 0$ and so $-A(X) \in T$. Thus T is an ordering in $\mathcal{K}$.

2. Let $A(X) = \sum_{i=m}^{\infty} a_i X^{i/N_1}$ and $B(X) = \sum_{i=n}^{\infty} b_i X^{i/N_2}$ be two Puiseux series. Writing $i/N_1 = iN_2/(N_1N_2)$ and $i/N_2 = iN_1/(N_1N_2)$, we rewrite $A(X)$ and $B(X)$ as series with exponents that have same denominator (N_1N_2). Then, by the change of variable $X^{1/(N_1N_2)} = \xi$, we have $A(X) = \tilde{A}(\xi)$ and $B(X) = \tilde{B}(\xi)$ which are elements of $\mathcal{K}$ (here the quotient field of $\mathbb{R}[[\xi]]$). Then the results of the preceding question apply, making $\mathcal{P}$ into a field.

3. We consider a polynomial equation

$$(I) \qquad P(X,Y) = A_0(X)Y^n + A_1(X)Y^{n-1} + \cdots + A_{n-1}(X)Y + A_n(X) = 0$$

with coefficients in $\mathcal{P}$. We denote by N_i the denominator of the exponents in A_i, and $N := lcm(N_i, i = 0, \ldots, n)$. We perform the change of variable $\tilde{X} := X^{1/N}$. A Puiseux series $Y(X) \in \mathcal{P}$ is a solution of (I) if and only if $\tilde{Y}(\tilde{X}) := Y(\tilde{X}^N) \in \mathcal{P}$ is a solution of

$$\begin{aligned} (II) \qquad P(\tilde{X}^N,\tilde{Y}) &= A_0(\tilde{X}^N)\tilde{Y}^n + A_1(\tilde{X}^N)\tilde{Y}^{n-1} + \cdots + A_{n-1}(\tilde{X}^N)\tilde{Y} + A_n(\tilde{X}^N) = 0 \\ \Leftrightarrow \quad \tilde{P}(\tilde{X},\tilde{Y}) &= B_0(\tilde{X})\tilde{Y}^n + B_1(\tilde{X})\tilde{Y}^{n-1} + \cdots + B_{n-1}(\tilde{X})\tilde{Y} + B_n(\tilde{X}) = 0 \end{aligned}$$

which has coefficients $B_1(\tilde{X})$ in $\mathcal{K}$.

Define m_i to be the order of B_i and

$$k := \max\{l \in \mathbb{Z} \mid nl + m_0 \leq (n-i)l + m_i, \forall i = 1, \ldots, n\}.$$

Then putting $\tilde{Y} = \tilde{X}^k \hat{Y}$ and dividing by X^{nk+m_0}, we get that $\tilde{Y}$ is solution of (II) in $\mathcal{P}$ if and only if $\hat{Y}$ is solution of

$$(III) \qquad \hat{P}(\tilde{X},\hat{Y}) = C_0(\tilde{X})\hat{Y}^n + C_1(\tilde{X})\hat{Y}^{n-1} + \cdots + C_{n-1}(\tilde{X})\hat{Y} + C_n(\tilde{X}) = 0$$

with coefficients that are in $\mathbb{R}[[X]]$, in particular with $C_0(0) \neq 0 \Leftrightarrow C_0(\tilde{X}) = c_0 + U(X)$ with $U(0) = 0$.

Finally, divide this equation by $C_0(\tilde{X})$ and use the Euler formula as above to conclude that this equation (III) is equivalent to an equation

$$(IV) \qquad Q(\tilde{X},\hat{Y}) = \hat{Y}^n + D_1(\tilde{X})\hat{Y}^{n-1} + \cdots + D_{n-1}(\tilde{X})\hat{Y} + D_n(\tilde{X}) = 0$$

defined by $Q(\tilde{X},\hat{Y})$ which is a monic polynomial in $\hat{Y}$ with coefficients $D_k(\tilde{X})$ in $\mathbb{R}[[(\tilde{X})]]$.

4. Since $P(Y)$ and $Q(Y)$ are relatively prime, by the cited lemma, we have:

$$1 = A_0(Y)P(Y) + B_0(Y)Q(Y).$$

for some polynomials $A_0(Y)$ and $B_0(Y)$.Thus we have

$$F(Y) = F(Y)A_0(Y)P(Y) + F(Y)B_0(Y)Q(Y).$$

Then using the Euclidean division, we can write

$$\begin{aligned} F(Y)A_0(Y) &= C_1(Y)Q(Y) + A(Y) \\ F(Y)B_0(Y) &= C_2(Y)P(Y) + B(Y). \end{aligned}$$

where the degree of $A(Y)$, respectively $B(Y)$, is strictly less than $q = \deg Q(Y)$, respectively $p = \deg P(Y)$. Thus we have

$$F(Y) = [C_1(Y) + C_2(Y)]P(Y)Q(Y) + A(Y)P(Y) + B(Y)Q(Y).$$

Since $\deg(P(Y)Q(Y))$ is $p+q$, which is bigger than $\deg F(Y)$, then we must have $C_1(Y) + C_2(Y) = 0$.

5. Consider $C_1(X_1,\ldots,X_n),\ldots,C_p(X_1,\ldots,X_n)$ and $D_1(X_1,\ldots,X_n),\ldots,D_q(X_1,\ldots,X_n)$ as in the cited lemma. We notice that for all i,j, $C_i(a_1,\ldots,a_n)$ and $D_j(a_1,\ldots,a_n)$ are well defined, where $a_k = A_k(0)$ for all k. Set the n-tuple $A(X) = (A_1(X),\ldots,A_n(X))$. Since for all k, $A_k(X) = a_k + U_k(X)$ with $U(0) = 0$, the expressions $C_i(A(X))$ and $D_j(A(X))$ are also well defined (using for instance multivariate Taylor expansion). Then we can define:

$$\begin{aligned} P(X,Y) &:= Y^p + C_1(A(X))Y^{p-1} + \cdots + C_p(A_n(X)) \\ Q(X,Y) &:= Y^q + D_1(A(X))Y^{p-1} + \cdots + D_q(A_n(X)). \end{aligned}$$

6. (a) Consider $A(X) = \sum_{i=m}^{\infty} a_i X^i \in \mathbb{R}[[X]]$ (thus $m \geq 0$) with $a_m > 0$, and the equation

$$Y^2 - A(X) = 0.$$

with solutions $Y(X) \in \mathcal{P}$. Applying the change of unknown $\tilde{Y} = \dfrac{Y}{X^{m/2}}$, we equivalently get an equation

$$F(X,\tilde{Y}) = \tilde{Y}^2 - (a_m + a_{m+1}X + \cdots) = 0$$

for which $F(0,\tilde{Y}) = \tilde{Y}^2 - a_m = (\tilde{Y} - \sqrt{a_m})(\tilde{Y} + \sqrt{a_m})$ and the solutions $\tilde{Y}(X) \in \mathcal{P}$. By Hensel's lemma, there exist $P(X,\tilde{Y}) = \tilde{Y} - B_1(X)$ and $Q(X,\tilde{Y}) = \tilde{Y} - C_1(X)$ with $B_1(X), C_1(X) \in \mathbb{R}[[X]]$ such that $(\tilde{Y} - B_1(X))(\tilde{Y} - C_1(X)) = \tilde{Y}^2 - (a_m + a_{m+1}X + \cdots)$. So $B_1(X) = -C_1(X)$ and $B_1(X)^2 = C_1(X)^2 = a_m + a_{m+1}X + \cdots = \dfrac{A(X)}{X^m}$. Say for instance that $B_1(X) > 0$. Then $X^{1/2}B_1(X) = \sqrt{A(X)} \in \mathcal{P}$.
Note: we have $B_1(X) = \sqrt{a_m} + U_1(X)$ with $U_1(0) = 0$.

(b) We proceed by induction on $p \in \mathbb{N}$ where $2p + 1 = n$.

For $p = 0 \Leftrightarrow n = 2p + 1 = 1$, we consider an equation $Y - A_1(X) = 0$ that has a unique solution $Y(X) = A_1(X) \in \mathcal{P}$.

For $p > 0 \Leftrightarrow n = 2p + 1 > 1$, we suppose that any poynomial equation over $\mathcal{P}$ of odd degree less than or equal to $2p - 1$ has a root in $\mathcal{P}$. Then we consider a polynomial equation

$$(I) \quad F(X,Y) = Y^n + A_1(X)Y^{n-1} + \cdots + A_n(X) = 0$$

of degree $n = 2p + 1$. We notice that $F(0,Y) = Y^n + a_{n-k}Y^k + \cdots + a_{n-l}Y^l$ for eventually some $1 \le k,l \le n$ and some coefficients $a_i \in \mathbb{R}$. Since $\mathbb{R}$ is real closed and $F(0,Y)$ has an odd degree, then $F(0,Y)$ has at least one real root, say α, that has some multiplicity r. There are two cases:

• either $r < n$, which means that $F(0,Y) = (Y - \alpha)^r Q_0(Y)$ with $(Y - \alpha)^r$ and $Q_0(Y)$ that are relatively primes. Then we apply Hensel's lemma and get that $F(X,Y) = P(X,Y)Q(X,Y)$ for some $P(X,Y), Q(X,Y)$ that are polynomials in Y with coefficients that are formal series in X. Since $\deg F(X,Y)$ is odd, then either $\deg P(X,Y)$ or $\deg Q(X,Y)$ is odd. Therefore we apply the induction hypothesis to the one with odd degree and we get a root in $\mathcal{P}$ of $F(X,Y)$.

• or $r = n$ meaning that $F(0,Y) = (Y - \alpha)^n$. We perform the Tschirnhausen transform $Y(X) =: Y_1(X) - \dfrac{A_1(X)}{n}$ in the equation (I). After expansion, we equivalently get an equation polynomial in Y_1

$$(II) \quad F_1(X,Y_1) = Y_1^n + B_2(X)Y_1^{n-1} + \cdots + B_n(X) = 0$$

which has coefficient $B_1(X) \equiv 0$.
Then we set $d := \min\left\{\dfrac{\deg B_k(X)}{k} \mid k = 2, \ldots, n\right\}$ and we perform in (II) the change of unknown $Y_1(X) =: X^d Y_2(X)$. After dividing by X^{nd}, we get an equation

$$(III) \quad F_2(X,Y_2) = Y_2^n + C_2(X)Y_2^{n-1} + \cdots + C_n(X) = 0$$

such that $F_2(0,Y_2) = Y_2^n + c_2Y_2^{n-1} + \cdots + c_n = 0$ with some $c_k \neq 0$. Thus this equation splits into two relatively prime factors (it cannot be $(Y - \beta)^n$ since we have the coefficient $c_{n-1} = 0$). Then we are back to the preceding case.

7. Criterion (*iii*) of Artin-Schreier's theorem says that a field K is real closed if and only if it is real, it has no proper algebraic extension of odd degree and $K^* = (K^*)^2 \cup -(K^*)^2$. Equivalently, K is ordered, any polynomial equation of

odd degree with coefficients in K has a root in K, and any positive element in K has a square root (see Corollary 2 in the Lecture of the 03/11/09). That is what we prove in question 3 (for the ordering) and in question 6, thanks to the changes of variable described in question 3.