

# Theorem G of Taylor's article

## *Remarks on a conjecture of Fontaine and Mazur*

Lecture by Gunther Cornelissen — Notes written with Peter Bruin

### Notation and statement of the theorem

Let  $K$  be a number field, and let  $S$  be a finite set of places of  $K$ . Let  $K_S$  be the maximal algebraic extension of  $K$  (inside a fixed algebraic closure  $K^{\text{ac}}$  of  $K$ ) in which all places in  $S$  split completely. For a given place  $v$  of  $K$ , write  $K_v$  for the completion of  $K$  at  $v$ . Finally, let  $X$  be a geometrically irreducible quasi-projective scheme over  $K$ .

With this notation, we will prove the following theorem (Theorem ‘‘G’’ in [5]):

**Theorem ‘‘G’’.** *If  $X(K_v)$  contains a smooth point for all  $v \in S$ , then  $X(K_S)$  is Zariski dense, i.e., the only rational function on  $X$  vanishing on  $X(K_S)$  is the zero function. In particular,  $X(K_S) \neq \emptyset$ .*

**Examples.** Here are three examples/applications of the theorem:

1. If  $S = \emptyset$ , then  $K_S = K^{\text{ac}}$ . The theorem says that  $X(K^{\text{ac}})$  is not empty (we have assumed  $X$  to be geometrically irreducible, hence non-empty, so that there exist non-zero functions on  $X$ ). This is equivalent to Hilbert's Nullstellensatz.
2. If  $K = \mathbf{Q}$  and  $S = \{\infty\}$ , then  $K_S$  is the maximal totally real extension of  $\mathbf{Q}$  inside  $\mathbf{Q}^{\text{ac}}$ . The theorem therefore implies that any variety with a real point also has a totally real algebraic point.
3. In [5], Taylor will apply Theorem G to a moduli space for which he knows local existence of points at three places ( $p$ ,  $l$ , and  $\infty$ ).

**Remark.** The theorem is a corollary of a much more general statement known as ‘Skolem-type theorems’, due to Moret-Bailly [1] and Rumely, also called ‘Rumely’s local-global principle’.

We will give a more direct proof of the theorem following an appendix to an article by Florian Pop [2]. This article refers to an article by B. Green, F. Pop and P. Roquette [3] for some topological results.

### Overview of the lecture

#### 1. Preliminaries

We will use the following topological theorems without proof:

- Continuity of roots of algebraic functions
- A  $v$ -adic implicit function theorem

#### 2. Topologising Jacobians

#### 3. Proof of Theorem G

The proof consists of a sequence of reductions to an easy topological problem:

- Reduction to the case of curves
- Reduction to a ‘moving lemma’ for divisors
- Reduction to a ‘moving lemma’ for sums in topological groups
- Proof of the moving lemma

### 1. Preliminaries

Fix a place  $v$  of  $K$ . Let  $F$  be the function field of a curve  $X$  over  $K_v$ . Every finite-dimensional  $K_v$ -vector space  $M \subset F$  gets a  $v$ -adic topology from the  $v$ -adic topology on  $K_v$ , and  $F$  inherits a  $v$ -adic topology by declaring the topology of  $F$  to be the finest topology for which all inclusions  $M \hookrightarrow F$  are continuous. We adopt the following convention for the divisor of zeros and the divisor of poles of a function  $f \in F \setminus \{0\}$ : we write  $(f)_0$  and  $(f)_\infty$  for the unique effective divisors such that the supports of  $(f)_0$  and  $(f)_\infty$  are disjoint and the divisor of  $f$  equals  $(f)_0 - (f)_\infty$ .

**1.1 Theorem (Continuity of roots of algebraic functions).** *For each  $f \in F \setminus \{0\}$  the following statements are true:*

- *There exists a neighbourhood  $U \subset F$  of  $f$  such that  $(f)_\infty \leq (g)_\infty$  for all  $g \in U$ .*
- *Let  $P_1, \dots, P_m$  be the distinct zeros of  $f$  in  $X((K_v)^{\text{ac}})$ , and let  $n_1, \dots, n_m$  be their multiplicities. Let  $\mathcal{U}_k$  be arbitrary disjoint neighbourhoods of  $P_k$  ( $1 \leq k \leq m$ ) in  $X((K_v)^{\text{ac}})$  with the  $v$ -adic topology. Then there exists a neighbourhood  $V$  of  $f$  in  $F$  such that every function  $g \in V$  has at least  $n_k$  zeros in each  $\mathcal{U}_k$  (counted with multiplicities).*

In particular, if  $\deg g = \deg f$  it follows that  $g$  has exactly  $n_k$  zeros in each  $\mathcal{U}_k$ , and that  $(f)_\infty = (g)_\infty$ .

**1.2 Theorem (Implicit function theorem).** Fix a place  $v$  of  $K$ . Let  $X$  be a geometrically irreducible scheme of dimension  $d$  over  $K_v$ , let  $x \in X(K_v)$  be a non-singular point, and let  $\mathbf{t} = (t_1, \dots, t_d)$  be a system of local parameters around  $x$ . Then there exist a  $v$ -adic neighbourhood  $U$  of  $x$  in  $X(K_v)$  and a  $v$ -adic neighbourhood  $V$  of  $0$  in  $K_v^d$  such that

$$\mathbf{t}|_U: U \rightarrow V$$

is a homeomorphism. In particular, the set  $X(K_v)$  is Zariski dense.

**1.3 (A note about the proof)** If  $x \in X(K_v)$  is non-singular, the completed local ring  $\hat{\mathcal{O}}_{X,x}$  is a regular local ring. This means that every minimal set of generators of its maximal ideal contains exactly  $d$  elements  $(t_1, \dots, t_d)$ . Then there exists an affine neighbourhood of  $x$  which is a (local) complete intersection with respect to  $\mathbf{t}$ .

The theorem is proved in the non-Archimedean case by applying the following version of Hensel's lemma to this complete intersection:

**1.4 Theorem (Hensel's lemma in higher dimension).** Let  $K_v$  be the completion of a field  $K$  with respect to a non-Archimedean valuation  $v$ , and let  $\mathcal{O}_v$  be the corresponding valuation ring. For  $\mathbf{x} = (x_1, \dots, x_r) \in K_v^r$ , define

$$v(\mathbf{x}) = \min_{1 \leq i \leq r} v(x_i).$$

Suppose  $r$  functions  $\mathbf{f} = (f_1, \dots, f_r) \in \mathcal{O}_v[X_1, \dots, X_r]^r$  are given, and  $\mathbf{x} \in K_v^r$  is a point such that

$$2v \left( \det \left( \frac{\partial f_k}{\partial X_j}(\mathbf{x}) \right)_{j,k=1}^r \right) < v(\mathbf{x}).$$

Then there exists a unique point  $\mathbf{y} \in K_v^r$  such that

$$\mathbf{f}(\mathbf{y}) = 0 \quad \text{and} \quad v(\mathbf{x} - \mathbf{y}) > v \left( \det \left( \frac{\partial f_k}{\partial X_j}(\mathbf{x}) \right)_{j,k=1}^r \right).$$

For the proof, see M. J. Greenberg, *Lectures on Forms in Many Variables*, Benjamin, New York, 1969.

## 2. Topologising Jacobians

Suppose  $X$  is a smooth projective curve of genus  $g$  over  $K$ . Let

$$\phi: X^g \rightarrow X^{(g)}$$

be the quotient map from the  $g$ -fold product of  $X$  with itself to the  $g$ -fold symmetric product  $X^{(g)} = X^g/S_g$ . This last space represents effective divisors of degree  $g$  on  $X$  with coordinates in a given extension of  $K$ : for every extension field  $L$  of  $K$  we have a natural isomorphism

$$\text{Div}^g(X_L) \simeq X^{(g)}(L).$$

The map  $\phi$  is unramified at all points  $(Q_1, \dots, Q_g)$  for which the  $Q_i$  are distinct. We define  $J_L$  as the group  $\text{Jac}(X_L)$  of divisor classes of degree 0 on  $X_L$ .

**2.1 Lemma.** Let  $L$  be an extension field of  $K$ . For all  $P_0 \in X(L)$ , the map

$$\begin{aligned} \varphi: X^{(g)}(L) &\rightarrow J_L \\ [Q_1, \dots, Q_g] &\mapsto \left[ \sum_{i=1}^g Q_i - gP_0 \right] \end{aligned}$$

is surjective. On the set of non-special points of  $X(L)$  it is also injective.

**2.2 Remark.** Notice that the map  $\varphi$  is different from the map  $\phi: X^g \rightarrow X^{(g)}$  defined earlier, but as this notation stems from [2], we stick to it. We also remark that the first part of the lemma remains valid if  $g$  is replaced by any integer  $n \geq g$ , but we will not need this fact.

*Proof.* Given a divisor class  $[D] \in J_L$ , the Riemann–Roch theorem says

$$\begin{aligned} h^0(\mathcal{O}(D + gP_0)) &= 1 - g + \deg(D + gP_0) + h^1(\mathcal{O}(D + gP_0)) \\ &= 1 + h^0(\mathcal{O}(D_{\text{can}} - D - gP_0)), \end{aligned}$$

where  $D_{\text{can}}$  is a canonical divisor. We conclude that there exists a function  $f \in \mathcal{O}(D + gP_0) \setminus \{0\}$  for which the divisor

$$Q = D + gP_0 + (f)$$

of degree  $g$  is effective, say

$$Q = \sum_{i=1}^g Q_i$$

with  $Q_i \in X(L)$ . The element  $[Q_1, \dots, Q_g]$  of  $X^{(g)}(L)$  now maps to  $[D]$  under  $\varphi$ :

$$\varphi([Q_1, \dots, Q_g]) = [D + gP_0 - (f) - gP_0] = [D].$$

Since  $h^0(\mathcal{O}(D_{\text{can}} - D - gP_0)) = 0$  unless  $D - gP_0$  (or, equivalently,  $Q$ ) is a *special* divisor, the divisor  $Q$  (and hence the point  $[Q_1, \dots, Q_g]$  of  $X^{(g)}(L)$ ) is unique if  $Q$  is non-special.  $\square$

We now turn to the ‘topological’ situation, where  $L$  is a completion  $K_\nu$  of  $K$ . We equip the set  $X(K_\nu)$  with the  $\nu$ -adic topology and  $X^g(K_\nu)$  with the product topology;  $X^{(g)}(K_\nu)$  and  $J_{K_\nu}$  get the quotient topology via the maps

$$X^g(K_\nu) \xrightarrow{\phi} X^{(g)}(K_\nu) \xrightarrow{\varphi} J_{K_\nu}.$$

The topological spaces in the above sequence are all compact; they are also non-empty for all  $\nu \in S$ , since  $X(K_\nu) \neq \emptyset$  by assumption.

The  $\nu$ -adic implicit function theorem from Section 1 implies that  $X(K_\nu)$  is Zariski dense. From this it follows that  $X^{(g)}(K_\nu)$  has non-singular points (namely, those corresponding to points  $(Q_1, \dots, Q_g) \in X^g(K_\nu)$  with all  $Q_i$  distinct). Another application of the implicit function theorem shows that  $X^{(g)}(K_\nu)$  is Zariski dense. Therefore,  $X^{(g)}(K_\nu)$  contains points corresponding to divisors  $Q = \sum_{i=1}^g Q_i$  on  $X(K_\nu)$  with all  $Q_i$  distinct,  $K_\nu$ -valued and such that  $Q$  is non-special.

Furthermore, with respect to the  $\nu$ -adic topology  $\varphi$  is locally a homeomorphism at points corresponding to non-special divisors, and  $J_{K_\nu}$  is a compact topological group with respect to addition of divisor classes (see [2] for details).

### 3. Proof of Theorem G

#### A. Reduction to the case where $X$ is a curve

Suppose  $\dim X > 1$ . We embed  $X$  in a projective space  $\mathbf{P}_K^n$ . The ‘scheme of hyperplanes’ of  $\mathbf{P}_K^n$  contains a dense subset  $E$  with the property that for each point  $\xi \in E$  the intersection  $Y_\xi$  of the corresponding hyperplane with  $X$  is geometrically irreducible (see Proposition 4.3 of [4]). Since the set of smooth  $K_\nu$ -valued points in  $X$  is Zariski dense,  $E$  contains a dense subset consisting of points  $\xi$  such that  $Y_\xi$  is geometrically irreducible and contains a smooth  $K_\nu$ -valued point. If  $Y_\xi(K_S)$  is Zariski dense for all these  $\xi$ , then so is  $X(K_S)$ . By applying this fact  $\dim(X) - 1$  times, we are left with the case where  $X$  is a curve with a smooth  $K_\nu$ -valued point for all  $\nu \in S$ , and it remains to be proved that  $X(K_S)$  is Zariski dense.

#### B. Reduction to a moving lemma for divisors

From now on we assume  $X$  to be a curve. Fix an effective divisor  $D$  on  $X$  and pick, for every  $\nu \in S$ , a non-empty open set  $\Omega_\nu \subseteq X(K_\nu)$  (in the  $\nu$ -adic topology). The following lemma, which will be proved using a reduction to another moving lemma, now implies Theorem G:

**3.1 Moving divisor lemma.** *There exist a positive integer  $n$  and functions  $f_\nu \in K_\nu(X)$  (one for each  $\nu \in S$ ) such that*

$$(f_\nu)_\infty = nD \quad \text{and} \quad (f_\nu)_0 \text{ is reduced with support inside } \Omega_\nu.$$

Here we say an effective divisor  $\sum_{P \in X} n_P P$  is *reduced* if  $n_P \leq 1$  for all  $P \in X$ .

We first describe how Theorem G (in the case where  $X$  is a curve) follows from the lemma. Consider the natural inclusion

$$H^0(X, \mathcal{O}(nD)) \hookrightarrow \prod_{\nu \in S} H^0(X_{K_\nu}, \mathcal{O}(nD))$$

of  $K$ -vector spaces. Give each  $K_\nu$ -vector space  $H^0(X_{K_\nu}, \mathcal{O}(nD))$  the topology described in the theorem on continuity of roots of algebraic functions from Section 1. Put the product topology on the product and the subspace topology on  $H^0(X, \mathcal{O}(nD))$ . Then  $H^0(X, \mathcal{O}(nD))$  is dense in  $\prod_{\nu \in S} H^0(X_{K_\nu}, \mathcal{O}(nD))$ . Together with the theorem on continuity of roots of algebraic functions, this implies that there exist non-zero functions  $f \in K(X)$  such that  $(f)_\infty = nD$  and the points of  $(f)_0$  lie arbitrarily close to the points of  $(f_\nu)_0$  for each  $\nu \in S$ . It follows that for suitable  $f \in K(X)$ , the divisor  $(f)_0$  is reduced with support in  $\Omega_\nu$  for all  $\nu \in S$ .

Let  $x$  be a zero of  $f$ . Since  $f \in K(X)$  is defined over  $K$ , for any embedding  $\sigma$  of  $K^{\text{ac}}$  into  $K_\nu^{\text{ac}}$ ,  $\sigma(x)$  is also a zero of  $f$ . As by construction, the zeros of  $f$  are  $K_\nu$ -rational, we find that  $\sigma(x) \in K_\nu$  for any  $\sigma$ . This means that  $\nu$  splits completely in  $K(x)$ , and thus the zeros of  $f$  are  $K_S$ -rational, where  $K_S$  is the maximal extension of  $K$  inside  $K^{\text{ac}}$  in which all the places  $\nu \in S$  split completely.

### C. Reduction to a moving lemma for topological groups

First assume that the genus of  $X$  is zero. Since  $X(K_v)$  is non-empty by assumption,  $X_{K_v}$  is isomorphic to  $\mathbf{P}_{K_v}^1$ . This implies that  $D$  is linearly equivalent to any effective divisor of degree  $\deg D$ . Now take one that is reduced and has support inside  $\Omega_v$ ; this is possible since  $\Omega_v$  is infinite.

Now assume  $X$  has genus  $g > 0$ . Consider one of the places  $v \in S$ . As before, let  $\Omega_v$  be a given non-empty  $v$ -adic open subset of  $X(K_v)$ . Choose  $g$  distinct points  $Q_{v,1}, \dots, Q_{v,g} \in \Omega_v$  such that the divisor  $\sum_{i=1}^g Q_{v,i}$  is non-special, and write  $Q_v = (Q_{v,1}, \dots, Q_{v,g})$ . Recall that

$$\phi: X^g(K_v) \rightarrow X^{(g)}(K_v)$$

is locally at  $Q_v$  a homeomorphism by the  $v$ -adic implicit function theorem, and that the non-speciality of  $\sum_{i=1}^g Q_{v,i}$  implies that

$$\varphi: X^{(g)}(K_v) \rightarrow J_{K_v}$$

is locally at  $[Q_v]$  a homeomorphism. Therefore, the subset

$$\varphi\phi(\Omega^g) - \varphi\phi(Q_v)$$

is a  $v$ -adic open neighbourhood of 0 in  $J_{K_v}$  for sufficiently small  $\Omega_v$ .

Let us temporarily denote the maps  $\phi: X^g(K_v) \rightarrow X^{(g)}(K_v)$  and  $\varphi: X^{(g)}(K_v) \rightarrow J_{K_v}$  by  $\phi_v$  and  $\varphi_v$ , respectively, to prevent confusion. Now let  $\mathbf{J}_S$  be the product space  $\prod_{v \in S} J_{K_v}$ , and let  $\Phi$  denote the product map

$$\Phi = \prod_{v \in S} \varphi_v \phi_v: \prod_{v \in S} X^g(K_v) \rightarrow \mathbf{J}_S.$$

Put  $d = \deg D$ , and set

$$x = \left( \left[ gD - d \sum_{i=1}^g Q_{v,i} \right]_{v \in S} \right) \in \mathbf{J}_S.$$

Since  $\mathbf{J}_S$  is compact, the sequence  $(mx)_{m>0}$  has a convergent subsequence, say  $(m_k x)_{k>0}$ . Setting  $n_k = m_{k+1} - m_k$ , the sequence  $(n_k)_{k>0}$  converges to 0 in  $\mathbf{J}_S$ . From this we conclude that for some large value of  $m = n_k$ ,

$$mx \in \Phi \left( \prod_{v \in S} \Omega_v^g \right) - \Phi((Q_v)_{v \in S}).$$

This means that there is some  $(Q'_v)_{v \in S} \subset \prod_{v \in S} \Omega_v^g$  such that  $mx = \Phi((Q'_v)_{v \in S}) - \Phi((Q_v)_{v \in S})$ ; equivalently, for all  $v \in S$  we have

$$mgD \sim (md - 1) \sum_{i=1}^g Q_{v,i} + \sum_{i=1}^g Q'_{v,i}$$

with  $\sim$  standing for linear equivalence of divisors. We conclude that for each  $v \in S$ , the divisor  $nD$  (with  $n = mg$ ) is linearly equivalent to an effective divisor  $E$  with support in  $\Omega_v$ . A function  $f$  such that  $nD + (f) = E$  satisfies the conditions of the moving divisor lemma, except that  $(f)_0 = E$  need not be reduced. We will deal with this final obstacle in the next section.

### D. Proof of the topological moving lemma

We conclude the proof of Theorem G by proving the following lemma:

**3.2 Lemma.** *Let  $G = \prod_{k=1}^t G_k$  be the direct product of a finite number of commutative topological groups which are Hausdorff and non-discrete. Any finite sum  $\sum_{i=1}^n g_i$  with  $n \geq 0$  and  $g_i \in G$  can be written as  $\sum_{i=1}^n h_i$  such that each  $h_i$  is arbitrarily close to  $g_i$  and such that for  $k = 1, \dots, t$  the  $k$ -th components of  $h_1, \dots, h_n$  are all distinct.*

*Proof.* If  $g_i$  and  $g_j$  have a common component for two distinct indices  $i, j$ , we call this a failure. We decrease the number of failures inductively by replacing, for each pair of distinct indices  $(i, j)$  such that  $g_i$  and  $g_j$  having a common component, the elements  $g_i$  and  $g_j$  by  $h_i = g_i + \varepsilon$  and  $h_j = g_j - \varepsilon$ , with  $\varepsilon$  in a sufficiently small punctured neighbourhood of zero (without introducing new failures).  $\square$

## References

- [1] L. Moret-Bailly. Groupes de Picard et problèmes de Skolem, II. *Ann. sci. ENS* **22** (1989), no. 2, 181–194.
- [2] F. Pop. Embedding problems over large fields. *Ann. Math.* **144** (1996), 1–34.
- [3] B. Green, F. Pop and P. Roquette. On Rumely’s local-global principle. *Jahresber. Deutsch. Math.-Verein.* **97** (1995), no. 2, 43–74.
- [4] P. Blass and J. Blass, A. Grothendieck’s EGA V: Translation and Editing of his ‘prenotes’, available online at [www.jmilne.org/math/Documents/EGA-V.pdf](http://www.jmilne.org/math/Documents/EGA-V.pdf).
- [5] R. Taylor, Remarks on a conjecture of Fontaine and Mazur, *J. Inst. Math. Jussieu* **1** (2002), 1–19, available online at [abel.math.harvard.edu/~rtaylor/](http://abel.math.harvard.edu/~rtaylor/)

Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht, Nederland,  
email: [cornelis@math.uu.nl](mailto:cornelis@math.uu.nl)