

# Number Theory 2009

Yuri Bilu

## Exercise list 4: more on valuations

1. In this exercise we determine the fields complete with respect to archimedean absolute values.
- (a) (*Banach-valued analytic functions*) Let  $X$  be a complex Banach space and  $D$  an open subset of  $\mathbb{C}$ . A function  $f : D \rightarrow X$  is called *analytic* if in a neighborhood of any  $\alpha \in D$  it can be represented by a convergent (by norm) power series; precisely, for any  $\alpha \in D$  there exists  $r > 0$  such that for  $|z - \alpha| < r$  we have

$$f(z) = a_0 + a_1(z - \alpha) + a_2(z - \alpha)^2 + \dots,$$

where  $a_0, a_1, a_2, \dots \in X$ . Show that Banach-valued analytic functions satisfy the Cauchy formula, the mean-value theorem, and the Liouville theorem (a bounded analytic on  $\mathbb{C}$  function is constant).

- (b) (*the Gelfand theorem*) A *Banach algebra* is a commutative  $\mathbb{C}$ -algebra  $A$ , supplied with a norm  $\|\cdot\|$  satisfying  $\|ab\| \leq \|a\| \cdot \|b\|$  for any  $a, b \in A$  and complete with respect to this norm. Show that for any  $a \in A$  there exists  $z \in \mathbb{C}$  such that  $a - z$  is not invertible in  $A$ . (Hint: assume the contrary and consider the analytic function  $\mathbb{C} \rightarrow A$  defined by  $z \mapsto (a - z)^{-1}$ .)
- (c) Let  $K$  be a field complete with respect to an archimedean absolute value. We denote by  $\mathbb{R}$  the completion of the simple subfield of  $K$ , by  $i$  a square root of 1 in the algebraic closure of  $K$  and by  $\mathbb{C}$  the field  $\mathbb{R}(i)$ . Prove that  $K = \mathbb{C}$  if  $i \in K$  and  $K = \mathbb{R}$  if  $i \notin K$ .
2. (*polynomials over complete fields*) Let  $K$  be a field complete with respect to a non-archimedean valuation  $v$ . We fix an algebraic closure of  $K$  and extend  $v$  to this algebraic closure (see Exercise 3(a) below).

- (a) (*Krasner's lemma*) Let  $\alpha$  and  $\beta$  be algebraic elements over  $K$  with the following property: if  $\alpha' \neq \alpha$  is conjugate to  $\alpha$  over  $K$ , then  $|\alpha - \beta|_v < |\alpha' - \beta|_v$ . Show that  $\alpha \in K(\beta)$ .

For a polynomial  $f(x) = a_n x^n + \dots + a_0$  define  $|f|_v = \max\{|a_0|_v, \dots, |a_n|_v\}$ .

- (b) (*continuity of roots*) Let  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in K[x]$  be a separable monic polynomial. Show that for every sufficiently small  $\varepsilon > 0$  there exists  $\delta > 0$  with the following property. Let  $g(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0 \in K[x]$  be a monic polynomial such that  $|f - g|_v < \delta$ . Then for every root  $\alpha$  of  $f$  (in the algebraic closure of  $K$ ) there exists exactly one root  $\beta$  of  $g$  such that  $|\alpha - \beta|_v \leq \varepsilon$ .
- (c) Assume that  $f$  from the previous question is irreducible over  $K$ . Then all monic polynomials over  $K$  in some neighborhood  $f$  are irreducible over  $K$  and generate the same extension of  $K$  as  $f$ .
- (d) Show that  $\mathbb{Q}_p$  has only finitely many extensions of any given degree.
3. (a) Let  $K$  be a field complete with respect to some absolute value. Show that the absolute value extends in a unique way to the algebraic closure of  $K$ .

- (b) Let  $F$  be a field admitting separable extensions of arbitrarily high degree. Show that the unramified closure and the algebraic closure of the field  $F((t))$  are not complete.
- (c) More generally, let  $K$  be a field complete with respect to a discrete valuation. Assume that its residue field admits separable extensions of arbitrarily high degree. Show that the unramified closure and the algebraic closure of  $K$  are not complete. In particular, the unramified closure and the algebraic closure of  $\mathbb{Q}_p$  are not complete.
- (d) Let  $K$  be a field complete with respect to a discrete valuation, admitting totally ramified extensions of arbitrarily high degree. Show that the algebraic closure of  $K$  is not complete. Give examples.
- (e) Let  $K$  be an algebraically closed field, supplied with an absolute value. Show that the completion of  $K$  is algebraically closed.
4. This is a preparatory exercise for the Eisenstein theorem. Let  $K$  be a field with a non-archimedean valuation  $v$ , and let a polynomial  $f(x) = a_n x^n + \cdots + a_0 \in K[x]$  have  $n$  roots  $\alpha_1, \dots, \alpha_n \in K$ .

- (a) Assume that all the roots, except *exactly* one, are of absolute value strictly smaller than 1: say,  $|\alpha_1|_v \geq 1 > \max\{|\alpha_2|_v, \dots, |\alpha_n|_v\}$ . Show that in this case  $a_{n-1}$  is the biggest coefficient; more precisely,

$$|a_{n-1}|_v \geq |a_n|_v, \quad |a_{n-1}|_v > \max\{|a_0|_v, \dots, |a_{n-2}|_v\}.$$

- (b) Assume now that all the roots, except *exactly* one, are of absolute value strictly bigger than 1: say,  $|\alpha_1|_v \leq 1 < \min\{|\alpha_2|_v, \dots, |\alpha_n|_v\}$ . Show that in this case  $a_1$  is the biggest coefficient; more precisely,

$$|a_1|_v \geq |a_0|_v, \quad |a_1|_v > \max\{|a_2|_v, \dots, |a_n|_v\}.$$

5. In this exercise we prove the *Eisenstein theorem* on algebraic power series. A formal series  $x(t) = \sum_{k=0}^{\infty} a_k t^k \in \mathbb{Q}[[t]]$  is called *algebraic power series* if it is algebraic over the field  $\mathbb{Q}(t)$ , viewed as a subfield of  $\mathbb{Q}((t))$ .

- (a) Prove that the coefficients  $a_0, a_1, a_2, \dots$  of an algebraic power series belong to some number field (a finite extension of  $\mathbb{Q}$ ).

In the sequel  $x(t) = \sum_{k=0}^{\infty} a_k t^k$  is an algebraic power series. Let  $K$  be a number field containing the coefficients. The Eisenstein theorem asserts that for all  $v \in M_K$  the  $v$ -values  $|a_k|_v$  grow at most exponentially in  $k$ , and for almost all<sup>1</sup>  $v \in M_K$  we have  $|a_k|_v \leq 1$  for all  $k$ . Precisely: *to every  $v \in M_K$  one can associate a real number  $A_v$  such that*

- $A_v \geq 1$  for all  $v \in M_K$ ;
  - $A_v = 1$  for almost all  $v \in M_K$ ;
  - $|a_k|_v \leq A_v^{k+1}$  for all  $v \in M_K$  and all  $k = 0, 1, 2, \dots$
- (b) (independence of the number field) Show that if a series satisfies the Eisenstein theorem over some number field  $K$ , then it satisfies it over any other number field containing the coefficients.
- (c) (the non-degenerate case) Assume that the series  $x(t)$  satisfies the polynomial equation  $F(x(t), t) = 0$ , where  $F(x, t)$  is a polynomial with coefficients in some number field  $K$ , satisfying  $F'_x(a_0, 0) \neq 0$ .

- i. Show that the coefficients of  $x(t)$  belong to the field  $L = K(a_0)$ .

---

<sup>1</sup>Here and below “almost all” means “all but finitely many”.

- ii. Use the implicit function theorem from the complex analysis to show that the  $v$ -adic convergence radius of  $x(t)$  is positive for every archimedean  $v \in M_L$ . Deduce from this the existence of the numbers  $A_v$  for the archimedean  $v$ .

From now on we work with non-archimedean  $v$ , which is the main contents of the Eisenstein theorem (see the remarks below). In the sequel we assume (as we may) that  $a_0 = 0$  and that the coefficients of  $F(x, t)$  are algebraic integers. Put  $\delta = F'_x(0, 0)$ .

- iii. Denote by  $x_k(t)$  the  $k$ -th partial sum of  $x(t)$ :

$$x_k(t) = a_1 t + \cdots + a_k t^k.$$

Show that for  $k \geq 1$

$$a_k = \frac{-t^{-k} F(x_{k-1}(t), t) \Big|_{t=0}}{\delta}.$$

Deduce from this that the coefficients  $a_k$  are algebraic integers when  $\delta = 1$ .

- iv. Show that in general the numbers  $\delta^{2k-1} a_k$  are algebraic integers. (Hint: consider the series  $\delta^{-1} x(\delta^2 t)$  and the polynomial  $\delta^{-2} F(\delta x, \delta^2 t)$ .) Conclude.
- (d) (the general case) Here we establish the Eisenstein theorem in full generality, reducing it to the non-degenerate case. We consider on the field  $\mathbb{Q}((t))$  the additive valuation  $\text{ord}_t$  ( $t$ -adic order), and we extend it to the algebraic closure of  $\mathbb{Q}((t))$ .
- i. Let  $K$  be a number field containing the coefficients of  $x(t)$ . Prove the Eisenstein theorem under the following assumption: *every conjugate  $y(t)$  of  $x(t)$  over the field  $K(t)$ , except  $x(t)$  itself, satisfies  $\text{ord}_t y(t) < 0$ .* (Hint: use Exercise 4 to show that this is the non-degenerate case.)
- ii. Show that for sufficiently large  $m$  the “tail” series

$$a_m + a_{m+1} t + a_{m+2} t^2 + \dots$$

has the property from the previous question (all its conjugates, except itself, are of negative  $t$ -adic order). Conclude.

## Remarks

- (i) We say that a formal power series with coefficients in a number field  $K$  has the “Eisenstein property” if there exists numbers  $A_v$  as in the Eisenstein theorem. Obviously, the Eisenstein property implies that the  $v$ -adic convergence radius of the series is positive for all  $v$  and is 1 for almost all  $v$ . This “convergence property” does not formally imply the Eisenstein property: consider the logarithmic series  $\sum x^k/k$ . However, for the algebraic power series it is easy to deduce the Eisenstein property from the convergence property. Modern proofs of the Eisenstein theorem go along these lines.
- (ii) Eisenstein himself proved only the degenerate case. The general case was established later (probably, by Heine).
- (iii) Eisenstein actually proved that there exist a non-zero integer  $\Delta$  (the “Eisenstein constant”) such that  $\Delta^{k+1} a_k$  is an algebraic integer for all  $k$ . This is equivalent to the Eisenstein property with  $M_K$  replaced by  $M_K^0$  (the non-archimedean part of  $M_K$ ).
- (iv) Sharp quantitative versions of the Eisenstein theorem are available<sup>2</sup>.

---

<sup>2</sup>B. M. DWORK AND A. J. VAN DER POORTEN, The Eisenstein Constant, *Duke Math. J.* **65**(1) (1992), 23–43.