LECTURE 6

Date of Lecture: August 29, 2019

As usual, K is a complete non-archimedean field (with non-trivial $|\cdot|$) and $k = \widetilde{K}$, i.e., $k = \mathscr{O}_K/\mathfrak{m}_K$. And as before $\mathbf{N} = \{0, 1, 2, \ldots, m, \ldots\}$. Rings mean commutative rings with 1.

1. The Weierstrass Division and Preparation Theorems

1.1. Euclidean Division over arbitrary rings. It is not necessary to assume that the coefficients of of polynomials come from a fixed field for the Euclidean algorithm to be valid. It is enough that the polynomial one is dividing by is monic. In more precise detail:

Theorem 1.1.1. *Let A be a ring and $g = a_0 + a_1X + \cdots + a_{d-1}X^{d-1} + X^d \in A[X]$ a monic polynomial. Then for any $f \in A[X]$ there exist unique elements q and r in $A[X]$ with $\deg r < d$ such that*

$$f = qg + r.$$

Proof. Let us first prove uniqueness. If $gq+r = 0$, where $q, r \in A[X]$ with $\deg r < d$, then as g is monic, q and r must be zero.

It remains to prove existence. We proceed by induction on $m = \deg f$. Let $m = \deg f$ and a the leading coefficient of f. If $m < d$ then we may pick $r = f$ and $q = 0$. If $m \geq d$ then set $f_1 = f - aX^{m-d}g$. Then $\deg f_1 < \deg f$ and by induction we may assume that $f_1 = q_1g + r$ with $\deg r < d$. Set $q = aX^{m-d} + q_1$. Then $f = qg + r$. $\square$

1.2. The Weierstrass Theorems. Recall (see Definition 2.1.1 of Lecture 5) that an element $f \in T_n$ is said to be *ζ_n-distinguished of order s* if in the decomposition $f = \sum_{\nu\in\mathbf{N}} g_\nu\zeta_n^\nu$ with $g_\nu \in T_{n-1}$, the following hold:

(i) g_s is a unit in T_{n-1}.

(ii) $\|g_s\| = \|g\|$ and $\|g_s\| > \|g_\nu\|$ for $\nu > s$.

Theorem 1.2.1. (The Weierstrass Division Theorem) *Let $g \in T_n$ be ζ_n-distinguished of order s. For each $f \in T_n$ there exist unique elements $q \in T_n$ and $r \in T_{n-1}[\zeta_n]$ with $\deg_{\zeta_n}(r) < s$ such that*

$$f = qg + r.$$

Moreover, the following equality holds:

$$\|f\| = \max\{\|qg\|, \|r\|\}.$$

If in addition f and g are in $T_{n-1}[\zeta_n]$ then q is also a polynomial in $T_{n-1}[\zeta_n]$.

Proof. We first prove that if the relation $(*)$ below holds for an $f \in T_n$

$$(*) \qquad f = qg + r, \qquad (q \in T_n \text{ and } \deg_{\zeta_n}(r) < s)$$

then

$$(\dagger) \qquad \|f\| = \max\{\|qg\|, \|r\|\}.$$

Suppose (f, q, r) satisfies $(*)$. It is certainly true that

$$\|f\| \leq \max\{\|qg\|, \|r\|\}.$$

If $\max\{\|qg\|, \|r\|\} = 0$ then $(\dagger)$ is trivially true. So suppose the maximum is not zero. Without loss of generality we may assume

$$\|g\| = 1 \quad \text{and} \quad \max\{\|q\|, \|r\|\} = 1.$$

Then $\|f\|, \|q\|, \|r\| \leq 1$ and hence f, q, and r lie in T_n°. We then have

$$\tilde{f} = \tilde{q}\tilde{g} + \tilde{r}$$

with $\deg_{\zeta_n}(\tilde{r}) < s$. If $\|f\| < 1$ then $\tilde{f} = 0$, and by the uniqueness assertion for Euclidean Division in the ring $R[\zeta_n]$, with $R = k[\zeta_1, \ldots, \zeta_{n-1}]$,[1] we must have $\tilde{q} = \tilde{r} = 0$. This contradicts the fact that $\max\{\|q\|, \|r\|\} = 1$. Thus $\|f\| = 1 = \max\{\|q\|, \|r\|\}$. This proves that (f, q, r) satisfies $(\dagger)$.

One consequence of what we proved is that if $f \in T_n$ has a representation as in $(*)$, then the representation is unique. Indeed, if $qg + r = 0$ with $\deg_{\zeta_n}(r) < s$, then by $(\dagger)$ we must have $\max\{\|qg\|, \|r\|\} = 0$, whence $q = r = 0$.

It only remains to show that every $f \in T_n$ has a representation of the form $(*)$. We may assume without loss of generality that $\|g\| = 1$. Let

$$B = \left\{qg + r \,\middle|\, q \in T_n,\ \deg_{\zeta_n}(r) < s\right\}.$$

We will show that $B = T_n$. As a first step, we will show that B is closed in T_n. Note that B is an additive subgroup of $(T_n, +)$. If $\{f_m\}$ is a Cauchy sequence in B, say $f_m = q_m g + r_m$ with $\deg_{\zeta_n}(r_m) < s$, then for each $\epsilon > 0$ there exists $N \in \mathbf{N}$ such that $\|f_m - f_\nu\| \leq \epsilon$ whenever $m, \nu \geq N$. Applying $(\dagger)$ to the relation $f_m - f_\nu = (q_m - q_\nu)g + (r_m - r_\nu)$, we get that $\|q_m - q_\nu\| \leq \epsilon$ and $\|r_m - r_\nu\| \leq \epsilon$. In other words $\{q_m\}$ and $\{r_m\}$ are also Cauchy. Let f, q, and r be the limits in T_n of $\{f_m\}$, $\{q_m\}$, and $\{r_m\}$ respectively. Clearly $f = qg + r$ and $\deg_{\zeta_n}(r) < s$. Thus $f \in B$. It follows that B is complete, and hence closed in T_n.

We will show that B is dense in T_n. This will prove that $B = T_n$, and hence prove that every $f \in T_n$ can be represented as in $(*)$. Let

$$\varepsilon = \max_{\nu > s} \|g_\nu\|.$$

Since $\|g_\nu\| < \|g_s\| = \|g\| = 1$ for $\nu > s$, it is clear that $\varepsilon < 1$. Set

$$K_\varepsilon := \{x \in K \mid |x| \leq \varepsilon\}$$

and

$$k_\varepsilon = K/K_\varepsilon.$$

We have an obvious ring map

$$\tau_\varepsilon \colon T_n^\circ \longrightarrow k_\varepsilon[\zeta_1, \ldots, \zeta_n]$$

with $\ker \tau_\varepsilon = \{f \in T_n^\circ \mid \|f\| \leq \varepsilon\}$.

For $f \in T_n^\circ$, by Euclidean division on $k_\varepsilon[\zeta_1, \ldots, \zeta_n] = k_\varepsilon[\zeta_1, \ldots, \zeta_{n-1}][\zeta_n]$ we have, for each $f \in T_n^\circ$, elements $q \in T_n^\circ$ and $r \in T_{n-1}^\circ[\zeta_n]$ with $\deg_{\zeta_n}(r) < s$ such that

$$\tau_\varepsilon(f) = \tau_\varepsilon(q)\tau_\varepsilon(g) + \tau_\varepsilon(r).$$

We are using the fact that $1 = \|g\| = \|g_s\|$ whence $\tau_\varepsilon(g_s)$ is a unit, making $\tau_\varepsilon(g)$ a unitary polynomial (i.e. essentially monic) in $k_\varepsilon[z_1, \ldots, \zeta_{n-1}]][\zeta_n]$. It follows that

[1] see Theorem 1.1.1

for $f \in T_n^\circ$ there exists $b \in B$ ($b = qg + r$ in this case) such that $\|f - b\| \leq \varepsilon$. This means that for $f \in T_n$, there exists $b \in B$ such that

$$(\ddagger) \qquad \|f - b\| \leq \varepsilon \|f\|.$$

In order to show that B is dense in T_n, we have to show that for each $f \in T_n$, $d(f, B) = 0$ where $d(f, B)$ is the distance from f to B, i.e. $d(f, B) = \inf_{b \in B} \|f - b\|$. Suppose there is an f in T_n such that $d(f, B) > 0$. Since $\varepsilon^{-1} > 1$, there exists $b_1 \in B$ such that $\|f - b_1\| < \varepsilon^{-1} d(f, B)$. Applying ($\ddagger$) to $f - b_1$ we find that there exists $b_2 \in B$ such that

$$\|f - (b_1 + b_2)\| = \|(f - b_1) - b_2\| \leq \varepsilon \|f - b_1\| < \varepsilon\varepsilon^{-1} d(f, B) = d(f, B).$$

This contradicts the definition of $d(f, B)$. Hence $d(f, B) = 0$ for all $f \in T_n$, i.e. B is dense in T_n. $\square$

As a corollary we have:

Corollary 1.2.2. (The Weierstrass Preparation Theorem) *Let $g \in T_n$ be ζ_n-distinguished of order s. Then there exist a unique representation*

$$g = ew$$

of g with e a unit in T_n and w a monic polynomial of degree s in $T_{n-1}[\zeta_n]$. Moreover, $\|w\| = 1$ and hence w is ζ_n-distinguished or order s. If $g \in T_{n-1}[\zeta_n]$ then e is also an element of $T_{n-1}[\zeta_n]$.

Proof. Without loss of generality we may assume $\|g\| = 1$. Apply Weierstrass division to ζ_n^s to get $q \in T_n$ and $r \in T_{n-1}[\zeta_n]$ with $\deg(r) < s$ such that

$$\zeta_n^s = qg + r.$$

Set $w = \zeta_n^s - r$. Then w is a monic polynomial in $T_{n-1}[\zeta_n$ and of degree s. Moreover, we have $\max\{\|q\|, \|r\|\} = \|\zeta_n^s\| = 1$, whence q and r lie in T_n°. It follows that in $k[\boldsymbol{\zeta}]$ we have $\zeta_n^s = \tilde{q}\tilde{g} + \tilde{r}$. Since $\deg_{\zeta_n}(\zeta_n^s) = \deg_{\zeta_n}(\tilde{g}) = s$ and $\tilde{g}$ is unitary as a polynomial in ζ_n over $k[\zeta_1, \ldots, \zeta_{n-1}]$, we have $\tilde{q} \in k^*$, which means q is a unit in T_n° and hence in T_n. Let $e = q^{-1}$. Then $g = ew$. It is clear that $\|w\| = 1$.

We now prove the uniqueness of the representation $g = ew$ of e. If we set $q = e^{-1}$ and $r = \zeta_n^s - w$ we get $g = qg + r$ with $r \in T_{n-1}[\zeta_n]$ and $\deg r < s$. This determines q and r by the uniqueness part of the Weierstrass Division Theorem, and hence determines e and w.

The last part of the statement of the Corollary is obvious from the last part of the Weierstrass Division Theorem. $\square$