Seminar on Iwasawa Theory of Elliptic Curves
4. The Iwasawa Algebra

Marcel Mohyla

14. Mai 2008

In this section we will establish the link between $\mathbb{Z}_p[[T]]$ and $\mathbb{Z}_p[[G]]$, where the first one denotes the ordinary ring of power series in T and the second one is the projective limit of certain $\mathbb{Z}_p-$algebras. This enables us to understand the structure of $\mathbb{Z}_p[[G]]$ in detail. Additionally, the description of the set of irreducible elements will be given explicitly.
In the following let p be a prime number and $\Lambda := \mathbb{Z}_p[[T]]$. Remember that Λ defines a local ring whose maximal ideal is generated by p and T. Further we have

$$\Lambda^* = \left\{ \sum_{i=0}^{\infty} a_i T^i \in \Lambda \,\middle|\, a_0 \in \mathbb{Z}_p^* \right\}.$$

As well, $\mathbb{Z}_p$ is a local ring and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$. This leads to an isomorphism $\Lambda/p\Lambda \cong \mathbb{F}_p[[T]]$.
Now we give the first definitions needed in this scope.

Definition 4.1 *Let $g \in \mathbb{Z}_p[T]$ be normalized of degree d, $g = T^d + \sum_{i=0}^{d-1} a_i T^i$, such that $a_i \in p\Lambda$ for $0 \leq i < d$. Then g is said to be a distinguished polynomial of degree d. The whole set of distinguished polynomials of arbitrary degree is denoted by Δ. Further let*

$$\Psi := \left\{ f = p^m \cdot u \cdot g \in \Lambda \,\middle|\, \big(m = 1 \textit{ and } g = 1\big) \ \underline{\textit{or}}\ \big(m = 0 \textit{ and } g \textit{ is irreducible as element in } \mathbb{Q}_p[T]\big), u \in \Lambda^*, g \in \Delta \right\}.$$

We will see later that Ψ denotes the set of irreducible elements. Before this, we state a quite useful theorem.

Theorem 4.2 *Let $g \in \Lambda \setminus p\Lambda$ and $f \in \Lambda$ arbitrary. Denote by d the smallest integer such that the coefficient a_d of g is a unit where $g = \sum_{i=0}^{\infty} a_i T^i$. There exist uniquely determined $h \in \Lambda$ and $r \in \mathbb{Z}[T]$ such that*

$$f = gh + r$$

with $\text{degree}(r) < d$.

Proof: Let $f := \sum_{i=0}^{\infty} b_i T^i$. We take a look at the projection map

$$\bar{\cdot} : \mathbb{Z}_p[[T]] \twoheadrightarrow \mathbb{F}_p[[T]] : \sum_{i=0}^{\infty} c_i T^i \mapsto \sum_{i=0}^{\infty} \overline{c_i} T^i.$$

By the assumption on g, we have $\overline{a_d} \neq 0$ and $\overline{a_i} = 0$ for all $0 \leq i < d$, hence $\overline{g} = T^d \cdot u$ for $u \in (\mathbb{F}_p[[T]])^*$. Since $\overline{f} := T^d \left(\sum_{i=d}^{\infty} \overline{b_i} T^{i-d}\right) + \sum_{i=0}^{d-1} \overline{b_i} T^i$ and $T^d \left(\sum_{i=d}^{\infty} \overline{b_i} T^{i-d}\right) \in (\overline{g}) = (T^d)$, one has $\overline{f} = \overline{g}\overline{h_1} + \overline{r_1}$ for certain $h_1 \in \Lambda$ and $r_1 := \sum_{i=0}^{d-1} b_i T^i \in \mathbb{Z}_p[T]$. In particular, we have $f \equiv gh_1 + r_1 \bmod p\Lambda$ and consequently $f = gh_1 + r_1 + pf_1$ for $f_1 \in \Lambda$. In the same way one gets $f_1 = gh' + r' + pf_2$ and obtains $f = gh_2 + r_2 + p^2 f_2$, where $h_2 := h_1 + ph'$ and $r_2 := r_1 + pr'$. This leads to $f = gh_n + r_n + p^n f_n$ in general. Let $h_n := \sum_{i=0}^{\infty} a_i(h_n) T^i$ and $r_n := \sum_{i=0}^{d-1} b_i(r_n) T^i$. Note that the congruences

$$a_i(h_n) \equiv a_i(h_{n+1}),\ i = 0, 1, \ldots, \infty, \text{ and}$$

$$b_i(r_n) \equiv b_i(r_{n+1}) \ mod\ p^n \mathbb{Z}_p, i = 1, \ldots d-1,$$

hold for all $n > 0$. By construction, the limits exist in $\mathbb{Z}_p$, denote them by a_i, respectively b_i. Letting $h := \sum_{i=0}^{\infty} a_i T^i$ and $r := \sum_{i=0}^{d-1} b_i T^i$, one receives $f = gh + r$ as desired.
It remains to show the uniqueness of h and r. To do this, assume that

$$f = gh + r = gh' + r',$$

hence $s := r' - r \equiv 0 \ mod\ g$. If $s \neq 0$, let $s = p^m s_1$, so that $s_1 \notin p\Lambda$. We get $g | s_1$ and since $\overline{g} = T^d \cdot \tilde{s}$, $\tilde{s} \in \mathbb{F}_p[[T]]$, one concludes $T^d | \overline{s_1}$. This is a contradiction to degree$(s) < d$. Finally, $r' = r$ leads to $h' = h$ directly. ∎

Corollary 4.3 *Let $g \in \Lambda \smallsetminus p\Lambda$. Then $\Lambda/(g)$ and $\mathbb{Z}_p^d$ are isomorphic regarded as $\mathbb{Z}_p-$modules. In particular, $\Lambda/(g)$ is free of rank d.*

Proof: We identify $\mathbb{Z}_p^d$ with $\left\{ f \in \mathbb{Z}_p[T] \middle| \ degree(f) < d \right\}$ in the obvious manner. By (4.2) we get a well defined homomorphism of $\mathbb{Z}_p-$modules defined as follows:

$$\Lambda \to \mathbb{Z}_p^d : f = gh + r \mapsto r.$$

Passing to the quotient proves the corollary. ∎

We need a further description of $g \in \Lambda/p\Lambda$.

Corollary 4.4 *Let $g \in \Lambda \smallsetminus p\Lambda$. There exists a uniquely determined polynomial $\tilde{g} \in \Delta$ that satisfies $g = u\tilde{g}$ where $u \in \Lambda^*$.*

Proof: By (4.3) we know that $\Lambda/(g)$ is a free $\mathbb{Z}_p-$module of rank d. Therefore let $\tilde{g}$ denote the characteristic polynomial of the endomorphism

$$\Lambda/(g) \to \Lambda/(g) : g \mapsto g \cdot T.$$

We have degree$(\tilde{g})$ = rank$(\Lambda/(g)) = d$ and $\tilde{g} \cdot \Lambda/(g) = \{0\}$, hence $\Lambda/(g) \subseteq \Lambda/(\tilde{g})$. Applying (4.3) to $\tilde{g}$ shows equality and therefore $(g) = (\tilde{g})$, i.e. $g = u \cdot \tilde{g}$. This shows $\tilde{g} \in \Delta$. Now assume there is another $g' \in \Delta$ satisfying $g = u'g'$, $u' \in \Lambda^*$. Since $\Lambda/(\tilde{g}) = \mathbb{Z}_p[T]/(\tilde{g})$, one has $\mathbb{Z}_p[T]/(\tilde{g}) = \mathbb{Z}_p[T]/(g')$ and hence degree$(\tilde{g})$ = degree(g_1). In addition, we have $g' \cdot \mathbb{Z}_p[T]/(\tilde{g}) = \{0\}$. That means $g' \equiv 0 \bmod \tilde{g}$, i.e. $\tilde{g} | g'$. One concludes $\tilde{g} = g'$. ∎

Theorem 4.5 *Let* $0 \neq g \in \Lambda$.

(i) There exist uniquely determined $m \in \mathbb{N},\ u \in \Lambda^*$ *and* $\tilde{g} \in \Delta$, *such that* $g = p^m u\tilde{g}$.

(ii) Ψ *is the set of irreducible elements in* Λ.

PROOF: (i) This is an easy consequence of (4.4). If needed, write $g = p^m g_1$ and apply the corollary to g_1.

(ii) If g is irreducible in Λ, then $g \notin p\Lambda$ or $g = p \cdot u$ with $u \in \Lambda^*$. By (i), we have $g = p^m u\tilde{g}$ for $\tilde{g} \in \Delta,\ u \in \Lambda^*$. Therefore we can restrict to the case $m = 0$ and $\tilde{g}$ is irreducible in $\mathbb{Q}_p[[T]]$. Assume first that $\tilde{g}$ is reducible in Λ. Following (4.4) there exist $g_1, g_2 \in \Delta$ such that $\tilde{g} = g_1 g_2$, hence $\tilde{g}$ is reducible in $\mathbb{Q}_p[T]$. Otherwise, if $\tilde{g}$ is reducible in $\mathbb{Q}_p[T]$, then it is also reducible in $\mathbb{Z}_p[T]$. This proves the statement. ∎

We see that we can reduce the problem of deciding whether $f \in \Lambda$ is irreducible or not to the corresponding situation in $\mathbb{Z}_p[T]$.

Definition 4.6 *Let* G *denote a topological group.*

(i) $\gamma \in G$ *is called a topological generator if the cyclic subgroup* $< \gamma >$ *is a dense subgroup of* G, *i.e.* $\overline{< \gamma >} = G$.

(ii) If G *denotes a profinite group, i.e.* $G = \varprojlim G_n$ *for* $n \in \mathbb{N}$, *we define the* $\mathbb{Z}_p-$*algebra* $\mathbb{Z}[[G]]$ *as the projective limit:*

$$\mathbb{Z}_p[[G]] := \varprojlim \mathbb{Z}_p[G_n].$$

$\mathbb{Z}_p[[G]]$ *is called the completed group ring for* G *over* $\mathbb{Z}_p$.

In this context, we are interested in the case that G satisfies: $G \cong \mathbb{Z}_p$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and is generated by 1, there always exists a topological generator, e.g. γ equals the preimage of 1. Further, γG^{p^n} generates G/G^{p^n} for every $n \in \mathbb{N}$. In fact, every topological generator will do this. For chosen γ, we define $\gamma^n := \gamma G^{p^n}$.
Regarding the second definition, one should mention that the defining homomorphisms of G can be extended linearly to $\mathbb{Z}_p-$algebra homomorphisms that define $\mathbb{Z}_p[[G]]$.

Corollary 4.7 *Let* $G \cong \mathbb{Z}_p$ *and let* γ *be a generator of* G. *We have:*
Let $w_n := (1+T)^{p^n} - 1$. *The map*

$$\sigma_n : \Lambda/(w_n) \to \mathbb{Z}_p[G/G^{p^n}] : 1 + T + (w_n) \mapsto \gamma^{(n)}$$

defines an isomorphism.

PROOF: Obviously, we have $w_n \in \Delta$ for each $n \in \mathbb{N}$. With regard to (4.3) the set $\{(1+T)^i + (w) \big|\ 0 \leq i < p^n\}$ forms a $\mathbb{Z}_p-$basis for the module $\Lambda/(w_n)$. The basis is generated by $\overline{1+T} \in \Lambda/(w_n)$ and we have $\overline{1+T}^{p^n} = \overline{1}$. So σ_n is well defined for all n and clearly an isomorphism since $\#G/G^{p^n} = p^n$. ∎

To prove the next proposition we recall some useful statements concerning profinite groups.

Theorem 4.8 *Let G, H denote profinite groups and let π_i denote the projection mapping of G to the $i-$th component for $G := \varprojlim G_i$. We get:*

(i) A group homomorphism $f : G \to H$ is continuous if and only if there exist continuous maps φ_i such that the diagramm

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi_i"'] & H \arrow[d, "\pi_i"'] \\ G_i \arrow[r, dashed, "\varphi_i"] & H_i \end{tikzcd}$$

commutes for all $i \in \mathbb{N}$.

(ii) $X \subset G$ is a dense subset if and only if $\pi_i(X) = G_i$ for all $i \in \mathbb{N}$.

Proof: See .... . ∎

One should note that $\mathbb{Z}_p[G/G^{p^n}] \cong \mathbb{Z}_p^{p^n}$ as $\mathbb{Z}_p-$modules. Therefore $\mathbb{Z}_p[G/G^{p^n}]$ is compact and $\mathbb{Z}_p[[G]]$, too. The compactness of Λ is also obvious.

Now everything is prepared to state the last result.

Proposition 4.9 *Let γ be an topological generator of $G \cong \mathbb{Z}_p$. There is an isomorphism of $\mathbb{Z}_p-$algebras*

$$\eta : \Lambda \to \mathbb{Z}_p[[\Gamma]]$$

where η is uniquely determined by $\eta(T) = \gamma - 1$. In addition, η is continuous.

Proof: Taking the maps of (4.7), we have surjective, continuous maps

$$\sigma_n' : \Lambda \to \mathbb{Z}_p[G/G^{p^n}] : T \to \gamma_n - 1$$

for all $n \in \mathbb{N}$. Since $\gamma_n \equiv \gamma_{n+1} \ mod \ G^{p^n}$, we get an induced map $\eta : \Lambda \to \mathbb{Z}_p[[G]]$. Applying $(4.8)(i)$, we see that γ is continuous. As a conclusion of $X := \eta(\Lambda)$ in $(4.8)(ii)$, we get that $\eta(\Lambda)$ is a dense subgroup of $\mathbb{Z}_p[[T]]$. It follows that η is surjective, since both, Λ and $\mathbb{Z}_p[[G]]$, are compact.
Finally, let $g \in ker(\eta)$. That means $g \in (w_n)$ for all n, but $\cap_{n \in \mathbb{N}}(w_n) = \{0\}$. So η is injective and the statement follows. ∎

Literature

Ralph Greenberg, Introduction to Iwasawa Theory for Elliptic Curves, http://www.math.washington.edu/ greenber/Park.ps

Lawrence Washington, Introduction to Cyclotomic Fields, Springer