Algebraic Number Theory

Problem sheet 11

The following problems build on each other. The main goal is the definition of the Lubin–Tate formal groups and the construction of Lubin–Tate extensions of local fields using them.

1. (6 points) Let R be a commutative ring with identity. A (one-parameter) commutative formal group law is by definition a two-variable power series $F(X,Y) \in R[[X,Y]]$ satisfying the following properties:

   (i) $F(X,Y) = X + Y$+terms of higher degree;

   (ii) $F(X, F(Y,Z)) = F(F(X,Y),Z)$ (associative);

   (iii) there exists a power series $\iota_F(X) \in XR[[X]]$ such that $F(X, \iota_F(X)) = 0$ (inverse);

   (iv) $F(X,Y) = F(Y,X)$ (commutative).

   (v) $F(X,0) = X$ and $F(0,Y) = Y$

   Prove that (iii) and (v) follow from (i) and (ii). Also prove that (iv) follows from (i) and (ii) if R has no torsion nilpotent elements. Show that if $R = \mathcal{O}_K$ is the valuation ring in a complete nonarchimedean field and $\mathcal{M}_K$ is the maximal ideal then $\mathcal{M}_K$ is a group with respect to the operation $a +_F b := F(a,b)$. Further verify that the power series $F(X,Y) = X+Y$, resp. $F(X,Y) = X+Y+XY$ define commutative formal groups. What is $(\mathcal{M}_K, +_F)$ isomorphic to in these two cases?

2. (3 points) A homomorphism between the formal group laws F and G is a power series $h(T) \in TR[[T]]$ such that $h(F(X,Y)) = G(h(X), h(Y))$. Show that in case $F = G$ the set $\mathrm{End}(F) := \mathrm{Hom}(F,F)$ is a ring with respect to the addition $+_F$ and composition as multiplication. Show further that $h_n(T) = (T+1)^n - 1$ is an endomorphism of the formal group law $F(X,Y) = X+Y+XY$ for any integer $n \geq 1$.

3. (4 points) From now on put $R = \mathcal{O}_K$ where $K/\mathbb{Q}_p$ is a finite extension and $\pi \in \mathcal{O}_K$ is a prime element (unique upto multiplication by a unit). Denote by $\mathcal{F}_\pi$ the set of power series $f(X) \in \mathcal{O}_K[[X]]$ such that $f(X) = \pi X$+terms of higher degree and $f(X) \equiv X^q \pmod{\pi}$ where $q = p^f$ is the cardinality of the residue field $k = \mathcal{O}_K/\mathcal{M}_K$. Let $f, g \in \mathcal{F}_\pi$ and $\phi_1(X_1, \dots, X_n) \in \mathcal{O}_K[X_1, \dots, X_n]$ be a homogeneous polynomial of degree one. Show that there exists a unique formal power series $\phi(X_1, \dots, X_n) \in \mathcal{O}_K[[X_1, \dots, X_n]]$ in n variables such that $\phi(X_1, \dots, X_n) = \phi_1(X_1, \dots, X_n)$+terms of higher degree and $f(\phi(X_1, \dots, X_n)) = \phi(g(X_1), \dots, g(X_n))$.

4. (3 points) Show that for all $f \in \mathcal{F}_\pi$ there exists a unique formal group law $F_f(X,Y) \in \mathcal{O}_K[[X,Y]]$ such that f is an endomorphism of F_f. (Such formal groups are called Lubin–Tate formal groups.)

5. (3 points) Let a be arbitrary in $\mathcal{O}_K$ and $f, g \in \mathcal{F}_\pi$. Verify that there exists a unique power series $[a]_{g,f}(T) \in T\mathcal{O}_K[[T]]$ such that $[a]_{g,f}(T) = aT$+terms of higher degree and $[a]_{g,f} \circ f = g \circ [a]_{g,f}$. Moreover, $[a]_{g,f}$ is a homomorphism from F_f to F_g. In particular, F_f and F_g are isomorphic.

6. (2 points) Verify that the map $\mathcal{O}_K \to \mathrm{End}(F_f)$, $a \mapsto [a]_f := [a]_{f,f}$ is an injective ring homomorphism such that $[\pi]_f = f$. (This makes F_f into a *formal $\mathcal{O}_K$-module.*)

7. (3 points) Let $f \in \mathcal{F}_\pi$ be arbitrary (by Problem 5 we may assume for sake of simplicity that $f(T) = \pi T + T^q$) put Λ_n for the set of roots of the polynomial $f^{(n)} = \underbrace{f \circ \dots \circ f}_{n}$ in the algebraic

closure of $\mathbb{Q}_p$. Show that Λ_n has cardinality q^n and it is an $\mathcal{O}_K$-module with respect to the addition $+_{F_f}$ and multiplication $a \cdot_{F_f} \lambda := [a]_f(\lambda)$ ($a \in \mathcal{O}_K$, $\lambda \in \Lambda_n$). Verify the isomorphism $\Lambda_n \cong \mathcal{O}_K/(\pi^n)$ as $\mathcal{O}_K$-modules.

8. (4 points) Let $K_{\pi,n} := K(\Lambda_n)$ be the splitting field of $f^{(n)}$ over K. Show that we have $\mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/(\pi^n))^\times$ and that $K_{\pi,n}/K$ is totally ramified. Further, $K_{\pi,n}$ does not depend on the choice of $f \in \mathcal{F}_\pi$ and π is the norm of a suitable element in $K_{\pi,n}$.

The field $K_{\pi,n}$ is called the nth Lubin–Tate extension of K (with respect to the uniformizer π). For p-adic number fields other than $\mathbb{Q}_p$ these play the role of the analogs of the p-power cyclotomic extensions. Indeed, the following generalization of the local Kronecker–Weber theorem holds:

Theorem. *Let $K/\mathbb{Q}_p$ be a finite and $\pi \in K$ be a uniformizer. Let L/K be a Galois extension with abelian Galois group $\mathrm{Gal}(L/K)$. Then there exists a positive integer n such that $L \subseteq K_{\pi,n}K_n^{ur}$ where K_n^{ur} is the (unique) unramified extension of K of degree n. In other words $K_{\pi,\infty}K_\infty^{ur}$ is the maximal abelian extension of K where $K_{\pi,\infty} = \bigcup_n K_{\pi,n}$ and $K_\infty^{ur} = \bigcup_n K_n^{ur}$. Moreover, we have $\mathrm{Gal}(\overline{K}/K)^{ab} = \mathrm{Gal}(K_{\pi,\infty}K_\infty^{ur}/K) \cong \mathcal{O}_K^\times \times \hat{\mathbb{Z}}$.*