TCC COURSE ON IWASAWA THEORY
ASSIGNEMENT 1
Óscar Rivero, Oscar.Rivero-Salgado@warwick.ac.uk

This is the first of 3 problem sheets for this course, covering material from lectures 1 and 2. Questions are assessed out of a total of 100. Students taking this course for credit should submit their solutions to me (by email) by **noon on Monday 8th November**.
Some of the problems (specially those addressed to review previous background) may be found as known results in books in algebraic number theory. Those of you with a more solid background in the topic can safely skip the first exercises. Recall that you only need a minimum of 40 points in each problem sheet.

1 Review of local fields

Problem 1 (10 points)**.** Let p be a prime number. Find all the quadratic extensions of $\mathbb{Q}_p$.
Hint: distinguish the cases p odd and $p = 2$.

Problem 2 (8 points)**.** Let L be an algebraic extension of $\mathbb{Q}_p$, and let ℓ stand for its residue field. Show that the map $K' \mapsto k'$ sending an unramified extension K' of $\mathbb{Q}_p$ contained in L to its residue field k' is a one-to-one correspondence between finite and unramified extensions over $\mathbb{Q}_p$ contained in L and finite extensions over $\mathbb{F}_p$ contained in ℓ.
Hint. You can use the following result (a variant of Hensel's lemma). Let A be a complete discrete valuation ring and π a generator of the maximal ideal. Let $f(x) \in A[x]$ and let a_0 be a simple root of $f(X)$ modulo π. Then, there is a unique root a of $f(x)$ with $a \equiv a_0$ modulo π.

Problem 3 (7 points)**.** Let L be a finite extension of $\mathbb{Q}_p$. Show that $L/\mathbb{Q}_p$ is totally ramified if and only if $L = K(\alpha)$, with α a root of an Eisenstein polynomial.

2 Review of algebraic number theory

Problem 4 (12 points)**.** Let E/F be a finite Galois extension, with $G = \mathrm{Gal}(E/F)$. Let H_E stand for the Hilbert class field of E. The aim of this problem is showing that H_E/F is a Galois extension.

(a) Let $\tilde{H}_E$ denote the Galois closure of H_E as an extension of F. For $\sigma \in G$, let $\tilde{\sigma}$ denote a lift of σ to $\mathrm{Gal}(\tilde{H}_E/F)$. Show that

$$\tilde{H}_E = \prod_{\sigma \in G} \tilde{\sigma}(H_E).$$

(b) Let I_v be the inertia group at a prime v of E in the abelian extension $\mathrm{Gal}(\tilde{H}_E/E)$. Show that $I_v = 0$.

(c) Conclude that H_E/F is a Galois extension.

Let E/F be a finite Galois extension. Define

$$j_{E/F} : \mathrm{Cl}_F \longrightarrow \mathrm{Cl}_E, \quad j_{E/F}([\mathfrak{a}]) = [\mathfrak{a}\mathcal{O}_E],$$

and consider also the norm map

$$N_{E/F} : \mathrm{Cl}_E \longrightarrow \mathrm{Cl}_F, \quad N_{E/F}([\mathfrak{a}]) = \Big(\Big(\prod_{\sigma \in G} \sigma(\mathfrak{a})\Big) \cap \mathcal{O}_F\Big).$$

For the following problem, we use the following notations:

- For a G-module A, the group of invariants is

$$A^G = \{a \in A \text{ such that } g \cdot a = a \text{ for all } g \in G\},$$

  which is to say the largest submodule of A fixed by G.

- The augmentation ideal I_G is the ideal of $\mathbb{Z}[G]$ generated by the set $\{g - 1 \text{ with } g \in G\}$.

- For a G-module A, the group of coinvariants is

$$A_G = A/I_G A,$$

  which is to say the largest quotient of A fixed by G.

Problem 5 (10 points)**.** Let p be a prime, and let A_K denote the p-part of the class group of any number field K. Assume that the order of G is prime to p.

(a) Determine $N_{E/F} \circ j_{E/F}$.

(b) Show that the map $A_F \longrightarrow A_E^G$ induced by $j_{E/F}$ is an isomorphism. *Hint.* Let $\mathbb{Z}' = \mathbb{Z}[|G|^{-1}]$ and consider the idempotent $\epsilon_G = \frac{1}{|G|} N_G \in \mathbb{Z}'[G]$. What can we deduce from $\epsilon_G A_E = A_E^G$?

(c) Show that the map $(A_E)_G \to A_F$ induced by the norm is an isomorphism. *Hint.* Note that A_E is finite. Is there any relation between the orders of $(A_E)_G$ and $(A_E)^G$?

Problem 6 (8 points)**.** Let E/F be a Galois extension of number fields with Galois group G. Show that the cokernel of $N_{E/F}$ is isomorphic to the Galois group of the maximal unramified abelian subextension of F inside E.

3 Structure theory

Problem 7 (15 points)**.** The objective of this problem is proving the p-adic Weierstrass preparation theorem: *Let $f(T) \in \Lambda$ be a non-zero power series. Then, there exists a unique distinguished polynomial $P(T)$, a unique unit $U(T) \in \Lambda^\times$, and a unique non-negative integer m such that*

$$f(T) = p^m P(T) U(T).$$

The first step is establishing the so-called division lemma: *if $f(T), g(T) \in \Lambda$ and $f(T) = a_0 + a_1 T + \ldots$ is such that $p \mid a_i$ for all $0 \leq i \leq n-1$ and $a_n \in \mathbb{Z}_p^\times$, then we may uniquely write*

$$g(T) = q(T) f(T) + r(T),$$

with $r(T) \in \mathbb{Z}_p[T]$ and $\deg r(T) < n$ (with the convention that $\deg 0 = -\infty$).

(a) Establish the uniqueness of both $g(T)$ and $r(T)$.

(b) Define $\tau = \tau_n : \Lambda \to \Lambda$ by

$$\tau\Big(\sum_{i=0}^{\infty} b_i T^i\Big) = \sum_{i=n}^{\infty} b_i T^{i-n}.$$

Show that τ is $\mathbb{Z}_p$-linear and that $\tau(T^n h(T)) = h(T)$ for all $h(T) \in \Lambda$. Further, show that $\tau(h(T)) = 0$ if and only if $h(T) \in \mathbb{Z}_p[T]$ with $\deg h \leq n-1$.

(c) Justify that we may write

$$f(T) = pP(T) + T^n U(T),$$

where $P(T)$ is a polynomial of degree less than n and $U(T) = a_n + a_{n+1} T + \ldots = \tau(f(T))$.

(d) Consider the polynomial

$$q(T) = \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j p^j \Big(\tau \circ \frac{P}{U}\Big)^j \circ \tau(g).$$

Show that $q(T)$ is a well-defined power series in Λ. Conclude from here the proof of the division lemma.

Now we are ready to prove the Weierstrass preparation theorem.

(e) Justify that we may assume that f has a non-zero coefficient not divisible by p. If a_n is the smallest such coefficient, and $g(T) = T^n$, apply the division lemma and conclude that $P(T) = T^n - r(T)$ is a distinguished polynomial of degree n.

(f) Conclude the proof.

Problem 8 (10 points)**.** Let $f = \sum_{i=0}^{\infty} a_i T^i \in \Lambda$, with $a_0 \neq 0$.

(a) Prove that $f \in \mathbb{Q}_p[[T]]^{\times}$.

(b) Write $f^{-1} = \sum_{i=0}^{\infty} b_i T^i$, with $b_i \in \mathbb{Q}_p$. Prove that $\mathrm{ord}_p(b_i) \geq -(i+1)\,\mathrm{ord}_p(a_0)$.

(c) Conclude that the fraction field of Λ is strictly contained in the Laurent series ring $\mathbb{Q}_p((T))$.

Problem 9 (10 points)**.** Let $\Lambda = \mathbb{Z}_p[[T]]$ and M be a finitely generated torsion Λ-module. Suppose that we are given a sequence $g_n \in \Lambda$ of distinguished polynomials with $\lim_{n\to\infty} \deg g_n = \infty$. If the sequence $\{\dim_{\mathbb{F}_p} M/(g_n, p)M\}_n$ is bounded, prove that $\mu(M) = 0$.

Problem 10 (10 points)**.** There is a slightly different approach to the structure theorem, on the realm of commutative algebra. Recall that for an integral domain R we say that an R-module homomorphism $f : A \longrightarrow B$ is a pseudo-isomorphism if it has pseudo-null kernel and cokernel. Nevertheless, we can make the following definition, which does provide an equivalence relation: we say that two modules A and B over R are pseudoisomorphic if $A_{\mathfrak{p}} \cong B_{\mathfrak{p}}$ for all height one prime ideals $\mathfrak{p}$ of R.

(a) Let $f : A \longrightarrow B$ be a pseudo-isomorphism of R-modules, where R is an integral domain. Show that A and B are pseudo-isomorphic.

(b) Show that any torsion module over a noetherian ring R has only finitely many height one prime ideals in its support.

(c) We assume now that $R = \mathbb{Z}_p[[T]]$. Let A and B finitely generated, torsion $\mathbb{Z}_p[[T]]$-modules. Let X be the finite set of height one prime ideals in the support of A and B. Set $S = \Lambda - \cup_{\mathfrak{p}\in X} \mathfrak{p}$. Let $f : A \longrightarrow B$ be a $\mathbb{Z}_p[[T]]$-module homomorphism. Then, show that f is a pseudo-isomorphism if and only if the localized map

$$S^{-1}f : S^{-1}A \longrightarrow S^{-1}B$$

is an isomorphism.

If you are interested in commutative algebra or feel comfortable with the previous notions, you can try to write proofs of the following results (not for credit). See either Bourbaki's Commutative Algebra or Serre's exposé *Classes des corps cyclotomiques*.

(a) Prove that pseudo-isomorphism is an equivalence relation in the category of finitely generated $\mathbb{Z}_p[[T]]$-modules.

(b) Suppose that

$$0 \longrightarrow M \longrightarrow N \longrightarrow K \longrightarrow 0$$

is a short exact sequence of finitely generated torsion $\mathbb{Z}_p[[T]]$-modules. If there are no height-one primes of $\mathbb{Z}_p[[T]]$ contained in $\mathrm{supp}(M) \cap \mathrm{supp}(K)$, show that N is pseudo-isomorphic to $M \oplus K$.