NOTES ON MATHEMATICS

ASVIN GOTHANDARAMAN

CONTENTS

1. DISTINGUISHED POLYNOMIALS

Let $\Lambda = \mathbb{Z}_p[[t]]$. This is a two dimensional local ring. We say that a polynomial is distinguished if it is of the form $p(t) \equiv t^n \pmod{p}$. These will be our building blocks.

Theorem 1 (Weierstrass Preparation Theorem)**.** *Any power series $f(t) \in \Lambda$ can be factored uniquely into the form $p^n P(t)U(t)$ where $P(t)$ is distinguished and $U(t)$ is a unit.*

The proof requires a version of the Euclidean Divison algorithm"

Theorem 2 (Division Algorithm)**.** *Let $f(t) \in \Lambda$ be such that $f(t) \equiv T^n +$ higher order terms $\pmod{p}$. Then, for any $g(t) \in \Lambda$, we can find $q(t), r(t)$ uniquely such that:*

$$g(t) = q(t)f(t) + r(t)$$

where $r(t)$ is a polynomial of degree less than n.

It is easy to prove uniqueness but I don't understand how to prove existence. I will assume this theorem for now.

We can use this to prove the preparation theorem:

Proof. Assume that $p \nmid f(t)$ and that it is of the form assumed in the division algorithm. Other notation also carries over from that statement.

Take $g(t) = t^n$ and so we have $t^n - r(t) = q(t)f(t)$. Reducing modulo p one sees that $t^n - r(t)$ is distinguished. Expanding and comparing coefficients, one sees that $q(t)$ is invertible modulo p and hence in $\mathbb{Z}_p$ (by Hensel).

This completes the proof. □

This result is very useful for a lot of reasons. For one, it lets us classify the spectrum of Λ:

Date:

Theorem 3. *The prime ideals of Λ are of the following form: $(P(t))$, for P a distinguished irreducible polynomial or (p) or (p, T). The last one is the unique maximal ideal.*

Proof. Let $\mathfrak{p}$ be a prime ideal and $f(t) \in \mathfrak{p}$. Then continuing the notation, either $p \in \mathfrak{p}$ or $P(t) \in \mathfrak{p}$ for some $P(t)$ distinguished polynomial dividing f. If $p \in \mathfrak{p}$, everything follows easily.

Assume $p \notin \mathfrak{p}$. ... □

Also, it is clear from the factorization that any power series has finitely many roots (since Λ is an integral domain and units can't have roots).

This lets us prove the following result:

Theorem 4. *For $P(t)$ a distinguished polynomial, $P(t)$ divides a power series $f(t)$ as a power series if and only if it divides it as a polynomial.*

Proof. A root λ of $P(t)$ has to have absolute value less than 1 (extend $\mathbb{Z}_p$ if necessary to include all roots in the base ring). Therefore a root of $P(t)$ is a root of $f(t)$ and use this to factor $x - \lambda$ out of both $P(t)$ and $f(t)$. □

All of this has been building up to the following big theorem:

Theorem 5. *Let $G = \mathbb{Z}_p$. We have an isomorphism:*

$$\mathbb{Z}_p[[G]] = \varprojlim \mathbb{Z}_p[G/H] \cong \Lambda$$

where the inverse limit is over open subgroups of G which sends the topological generator γ to $T+1$.

Proof. We need to show that $\varprojlim \mathbb{Z}_p[[\mathbb{Z}/p^n]] \cong \mathbb{Z}_p[[t]]$. Note that

$$R_n = \mathbb{Z}_p[[\mathbb{Z}/p^n]] = \mathbb{Z}_p[t]/((1+t)^{p^n} - 1).$$

Define $P_n(t) = (1+t)^{p^n} - 1$. Note that this is a distinguished polynomial. The division algorithm (with $f(t) = P_n(t)$) gives us a map $\Lambda \longrightarrow R_n$ that sends $g(t) \longrightarrow g_n(t) = r(t)$.

We need to verify that $g_{n+1}(t) \equiv g_n(t) \pmod{P)_n(t}$ to show that we can glue the maps together. This follows from the fact that $P_{n+1}(t)/P_n(t)$ is a polynomial and Theorem 4.

Then we need to show that it is injective and surjective.

Injectivity follows from the fact that $P_n(t) \in (p,t)^n$ (prove by induction) and so $f(t) \in \bigcap_n P_n(t)$ implies that it is 0

To show that it is surjective, we use the fact that Λ is complete and take the limit of the sequence.

To verify this choice, let $f = \lim f_n$ and note that for $m \geq n$, $f_m - f_n = P_n q_{m,n}$ and after rearranging and letting $m \longrightarrow \infty$, one sees that $\lim_{m \longrightarrow \infty} q_{m,n} \in \Lambda$ and so $f = P_n(\lim_{m \longrightarrow \infty} f_{m,n}) + f_n$.

□

2. Structure Theorem for Λ -modules:

For M a finitely generated Λ module, there is an exact sequence of Λ-modules the form:

$$0 \longrightarrow A \longrightarrow M \longrightarrow \Lambda^r \oplus_i \Lambda/(f_i(t)^{m_i}) \oplus_j \Lambda/(p^{n_j}) \longrightarrow B \longrightarrow 0)$$

where A, B are finite and f_i are distinguished and irreducible.

3. Growth of class groups in a $\mathbb{Z}_p$ extension

Let $K_0 = K$ be a number field and K_∞/K be a Galois extension such that it has Galois group $\Gamma = \mathbb{Z}_p$. This is equivalent to requiring that there is a sequence of number fields K_n such that each of them has Galois group $\mathbb{Z}/p^n$ over K.

The ur-example is obtained in the following manner: Let $M_n = \mathbb{Q}(\mu_n)$. Then $\mathrm{Gal}(M_\infty/M) = \mathbb{Z}_p^\times$ and therefore there is a unique sub extension K_∞ of M_∞ with Galois group $\mathbb{Z}_p$ as required.

This also gives us a way to generate $\mathbb{Z}_p$ extensions for any number field in a similar way by adjoining roots of unity and taking subfields.

We are interested in $X_n = \mathrm{Cl}(K_n)[p]$. This is naturally a module over $\Gamma_n = \mathrm{Gal}(K_n/K) = \mathbb{Z}/p^n$ and a module over $\mathbb{Z}_p$ (since we are taking the p-part). It makes sense to look at it as a module over the group ring $R_n = \mathbb{Z}_p[\mathbb{Z}/p^n]$.

Iwasawa's great idea was to see that it would be easier to study the modules if we considered all of them at the same time by forming the inverse limit.

We will also make use of the fact that there is a unique abelian unramified extension L_n of K_n such that $X_n = \mathrm{Gal}(L_n/K_n)$ through the Frobenius map. Putting every thing together, consider the following set up:

We have the extension of fields $L/K_\infty/K$ such that $L = \bigcup L_n$. Let $X = \mathrm{Gal}(L/K_\infty)$ and $G = \mathrm{Gal}(L/K)$ so that X is a subgroup of G and Γ is a quotient of G.

Since Γ_n acts on X_n (for $\gamma \in \Gamma_n$, lift it to $\tilde{\gamma} \in \mathrm{Gal}(L_n/K)$ and define the action by $\gamma \circ x = \tilde{\gamma} x \tilde{\gamma}^{-1}$) in a way compatible with the restriction maps, we have an action of Γ on X. As before, X is also a $\mathbb{Z}_p$ module and so X is a L module.

Now if we could show that X is finitely generated and find some way to relate X to X_n, we could leverage the structure theorem to prove things about the growth of the size of X_n.

First, we need to study the ramification in a $\mathbb{Z}_p$ extension:

3.1. **Ramification:**

Theorem 6. *A $\mathbb{Z}_p$ extension can be ramified only at places above p.*

Proof. Let I be an inertia group. Since I is closed, it has to be of the form $p^n\mathbb{Z}_p$. Since the inertia group at an infinite prime can only be finite, this rules out the archimedean case.

In the non archimedean case, if I corresponds to the inertia group of a prime over $l \neq p$, note that by local class field theory, I is a pro-l group. However $p^n\mathbb{Z}_p \cong \mathbb{Z}_p$ is pro-p and this is a contradiction. □

Corollary 7. *There are only finitely many primes ramified in K_∞/K.*

Corollary 8. *There is a finite extension K_e such that K_∞/K_e is totally ramified at every prime that ramifies.*

Proof. The intersection of all the inertia groups has finite index. □

Returning to the set up described at the beginning, let us make the assumption that K_∞ is totally ramified over K. Then, the restriction of the natural map $G \longrightarrow \Gamma$ to any inertia group is injective and surjective.

In particular, if $I_1, \dots I_n$ are the inertia groups, then $G = I_k X = X I_k$. Therefore, in defining the action of Γ on X, we might as well think of it as an action of I_k on X. Let σ_k be a topological generator of I_k that maps to $T + 1$.

Then, since $I_k \subset X I_1$, we have $\sigma_k = a_k \sigma_1$ for $a_k \in X$.

3.2. **Relating X to X_n:** Let us first make the assumption that K_∞ / K is totally ramified whenever it is ramified.

Let us first focus on X_0. This is the maximal abelian unramified sub extension of G and so:

$$X_0 = G / \overline{\langle [G, G], I_1, \dots, I_n \rangle}.$$

Let us work towards simplifying this. First, I claim that $[G, G] = TX = X^{\gamma_0 - 1}$.

Proof. Let $f = \alpha x, g = \beta y \in G$ be arbitrary elements with $\alpha, \beta \in I_1$ and $x, y \in X$. Then:

$$\begin{aligned}
[f, g] &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\
&= x^\alpha \alpha \beta y x^{-1} \alpha^{-1} \beta^{-1} \beta y^{-1} \beta^{-1} \\
&= x^\alpha (y x^{-1})^{\alpha\beta} y^{-\beta} \\
&= x^{\alpha(1-\beta)} y^{\beta(\alpha - 1)}
\end{aligned}$$

Taking $\alpha = \gamma, \beta = 1$, we see that $TX \subset [G, G]$. In the other direction, for arbitrary $\alpha \in I_k \cong \mathbb{Z}_p$, note that we can write $\alpha = \gamma^c$ for $c \in \mathbb{Z}_p$. Then:

$$\alpha - 1 = (1 + t)^c - 1 \in t\Lambda.$$

Similarly for β and so $[G, G] \subset TX$. □

Also, recall that $I_k = a_k I_1$ and $G = I_1 X$. Therefore:

$$X_0 = X / \overline{\langle a_2 \dots, a_n, TX \rangle}$$

Define $Y_0 = \overline{\langle a_2 \dots, a_n, TX \rangle}$. This is a $\mathbb{Z}_p$ module (since we are taking the closure) and also, T takes it to itself. Therefore, it is a Λ module.

Now let us try and see how to get X_n. The idea is that we will think of K_n as our new K_0 and see what changes. X remains unchanged. Γ gets replaced by the subgroup $p^n \mathbb{Z}_p \cong \Gamma$ and γ gets replaced by γ^n.

Similarly, I_k gets replaced by $p^n I_k$ and σ_k becomes $\sigma_k^{p^n}$. Therefore, since:

$$\sigma_k^m = (a_k \sigma_1)^m = a_k^{1 + \sigma_1 + \dots \sigma_1^{m-1}} \sigma_1^m$$

we know that a_k gets replaced by $v_n a_k$ where $v_n = 1 + \gamma + \gamma^2 \dots \gamma^{p^n - 1} = \frac{(1+t)^{p^n} - 1}{t} \in \Gamma$.

Finally, TX gets replaced by $((1 + T)^{p^n} - 1)X = v_n TX$. We see that effectively, we replace Y_0 by $v_n Y_0$.

That is, we have proven the following:

Theorem 9. *Let v_n and Y_0 be as above. Define $Y_n = v_n Y_0$ Then, $X_n = X / Y_n$.*

3.3. **Proving Finite Generation:** We will maintain our assumption for this section, see the next section to remove it.

We will need a lemma to get off the ground:

Note that X is compact since it is a profinite group.

Lemma 10. *If M is a compact Λ module, then M is finitely generated if and only if $M/(p,T)M$ is finite.*

Proof. One direction is clear. To show that M is finitely generated, let N be a finitely generated submodule of M such that $N/\mathfrak{m}N = M/\mathfrak{m}M$. We want to show that $P = M/N = 0$. We know that $P/\mathfrak{m}P = 0$.

We will prove it by showing that $P \subset \mathfrak{m}P$. Since $\bigcap_n \mathfrak{m}^n = 0$, this is sufficient.

The idea here is the following: For any open set U of 0 and any point $z \in P$, note that we can find some n such that $\mathfrak{m}^n U_z \subset U$ for some U_z since $\mathfrak{m}^n \longrightarrow 0$.

Since P is compact, we can use finitely many of these U_z to cover P and we have shown that $P = \mathfrak{m}^n P \subset U$. This completes the proof.

□

REMARK: This shows that M is Noetherian if it is finitely generated. In particular, Λ is finitely generated. This can also be seen directly by the Hilbert Basis Theorem since the generators of ideals are polynomials (by the preparation theorem).

Therefore, to show that X is compact, it suffices to show that $X/\mathfrak{m}X$ is finite. However, note that $v_1 \in \mathfrak{m}$ and so $X/\mathfrak{m}X$ is a quotient of $X/v_1 Y_0 = X_1$ which is finite.

This proves that X is finitely generated.

3.4. **Removing the assumption.** Finite generation is clear since passing to K_e means we are working with a smaller ring.

What we really need to change are the v_n. Note that passing to K_e replaces γ by γ^e. For $n \geq e$, it is easy to see that we need to replace v_n by:

$$v_{n,e} = 1 + \gamma^{p^e} + \gamma^{2p^e} + \cdots + \gamma^{(p^{n-e}-1)p^e} = \frac{v_n}{v_e}.$$

We have everything in place finally and we can begin calculating the class groups.

3.5. **Calculating the size of X_n:** Since X is finitely generated, we can apply the structure module. For the moment, let us assume that $A = B = 0$.

So $X = \Lambda^r \oplus_i \Lambda/(f_i(t)^{m_i}) \oplus_j \Lambda/(p^{n_j})$. We will calculate each quotient separately for each direct factor M:

Recall that $v_{n,e}$ is a distinguished polynomial since the quotient of distinguished polynomials is always distinguished (if it is a polynomial).

$M = \Lambda$. In this case, $M/(v_{n,e})M$ is infinite but $X/v_{n,e}X$ is finite, being a quotient of X_n. Therefore, this cannot occur and $r = 0$.

$M = \Lambda/(p^{n_j})$. In this case, $M/(v_{n,e})M = \Lambda/(p^{n_j}, v_{n,e}) = \mathbb{Z}/p^n[t]/(v_{n,e})$. Since $v_{n,e}$ has degree $p^n - p^e$, this set has $(p^{n_j(p^n-p^e)})$ elements.

$M = \Lambda/(f_i(t)^{m_j})$. This is the hardest case by far. First note that the quotient is infinite unless $(f_i(t), v_{n,e}) = 1$. We will prove the result the induction on n.

Let $g(t) = f_i(t)^{m_j}$. This is a distinguished polynomial and let it have degree d. Let $V = \Lambda/(g)$. We want to figure out the size of $V/v_{n,e}V$. Let this value be k_n.

Note that $k_{n+1}/k_n = |v_{n,e}V/v_{n+1,e}V|$.

Now, we see that $v_{n+1,e}/v_{n,e} = v_{n+1}/v_n = P_{n+1}/P_n$ where $P_n = (1+t)^{p^n} - 1$ is distinguished.

We then see that:

$$P_{n+1}(t) = (1 + (1+t)^{p^n} + (1+t)^{2p^n} \cdots + (1+t)^{(p-1)p^n})P_n(t).$$

Putting everything together, we see that $|E| = p^{mp^n+ln+c}$ for m, l, c constants and n large enough. E is the module approximating X_n.

Let $|X_n| = e_n$. So far we can only conclude that $e_n = mp^n + ln + c_n$ where c_n is bounded. The next lemma fixes this problem:

Lemma 11. *Suppose Y and E are Λ modules with $Y \sim E$ such that $Y/v_{n,e}Y$ is finite for all $n \geq e$. Then, for some constant c and large enough n, we have $|Y/v_{n,e}Y| = p^c|E/v_{n,e}E|$.*

Proof. □