1. Algebra

Lemma 1.0.1. Let R be a ring. Let M be an R-module. The following are equivalent.

(1) M is faithfully flat.
(2) M is flat, and for every R-module map $\alpha : N \to N'$ we have $\alpha = 0$ if and only if $\alpha \otimes_R \mathrm{id}_M = 0$.

Proof. Proof of (1) $\Rightarrow$ (2). Suppose $\alpha \otimes_R \mathrm{id}_M : N \otimes_R M \to N \otimes_R M'$ is zero. The exact sequence

$$0 \to \ker(\alpha) \to N \to N'$$

gives an exact sequence

$$0 \to \ker(\alpha) \otimes_R M \to N \otimes_R M \to N' \otimes_R M'$$

since M is flat. Then we have an exact sequence

$$0 \to \ker(\alpha) \otimes_R M \to N \otimes_R M \to 0,$$

which implies that

$$0 \to \ker(\alpha) \to N \to 0$$

is exact, i.e. $\alpha = 0$.

Proof of (2) $\Rightarrow$ (1). Let $N_1 \to N_2 \to N_3$ be a complex of R-modules. Suppose that

$$N_1 \otimes_R M \to N_2 \otimes_R M \to N_3 \otimes_R M$$

is exact. $\square$

Lemma 1.0.2. Let $A \to B$ be a flat ring map. The following are equivalent.

(1) $A \to B$ is faithfully flat.
(2) $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.
(3) The image of $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ contains every closed point.

Lemma 1.0.3. Let $R \to S$ be a flat ring map. Then it satisfies going down. In other words,

(1) For every $x' \rightsquigarrow x \in \mathrm{Spec}(R)$ (i.e. x is a generalization of x', or equivalently, $\mathfrak{p}_x \subset \mathfrak{p}_{x'}$) and $y' \in \mathrm{Spec}(S)$ mapping to x', there exists $y \in \mathrm{Spec}(S)$ mapping to x such that $y' \rightsquigarrow y$.
(2) For every primes $\mathfrak{p} \subset \mathfrak{p}'$ of R and $\mathfrak{q}'$ of S mapping to $\mathfrak{p}'$, there eixsts a prime $\mathfrak{q} \subset \mathfrak{q}'$ mapping to $\mathfrak{p}$.

The situation is illustrated in the following diagram

$$\begin{tikzcd}
\mathrm{Spec}(S) \arrow[d] & y' \arrow[r, rightsquigarrow] \arrow[d, mapsto] & \boxed{y} \arrow[d, mapsto] \\
\mathrm{Spec}(R) & x' \arrow[r, rightsquigarrow] & x
\end{tikzcd}$$

Lemma 1.0.4. Let A be a ring. Let $I \subset A$ be an ideal. Let A' be the localization of A along $V(I)$. Then

$$\mathrm{Spec}(A') = \bigcup_{\mathfrak{p} \in V(I)} \mathrm{Spec}(A_{\mathfrak{p}}).$$

Lemma 1.0.5. Let $A \to B$ be a ring map. Let $I \subset A$ be a principal ideal. Then IB is a principal ideala of B.

Proof. Suppose $I = dA$ with $d \in I \subset A$. Then

$$IB = dAB \subset dB,$$

and

$$dB \subset IB.$$

Hence $IB = dB$. $\square$

Lemma 1.0.6. Let $A \to B$ be a ring map. Let $I \subset A$ be a locally principal ideal. Then $IB \subset B$ is a locally principal ideal.

Proof. This is a direct corollary of the previous lemma. $\square$

2. Prisms

Lemma 2.0.1. Let A be a δ-ring. Let $d \in A$. Suppose $(d,p) \in \mathrm{jrad}(A)$. Then d is distinguished if and only if $p \in (d, \phi(d))$.

Recall the following result.

Lemma 2.0.2. Let A be a δ-ring. Let $I \subset A$ be a locally principal ideal with

(1) $(p,I) \subset \mathrm{jrad}(A)$.
(2) $p \in I + \phi(I)A$.

Then there exists a faithfully flat map $A \to A'$ of δ-rings that is an ind Zariski localization such that IA' is generated by a distinguished element $d \in A'$ with $(p,d) \subset \mathrm{jrad}(A')$.

Lemma 2.0.3. Let $(A,I) \to (B,J)$ be a map of prisms. Then the natural map $I \otimes_A B \to B$ induces an isomorphism

$$I \otimes_A B \to J$$

of B-modules. In particular, $IB = J$.

Proof. Choose faithfully flat maps $A \to A'$ and $B \to B'$ such that

$$IA' = (d), \quad JB' = (e)$$

with $(p,d) \subset \mathrm{jrad}(A')$ and $(p,e) \subset \mathrm{jrad}(B')$. Consider the following faithfully flat maps

$$B \to B' \to A' \otimes_A B'.$$

((TODO: δ-structure on tensor product))

Let B'' be the Zariski localization of $A' \otimes_A B'$ along $V(p, J(A' \otimes_A B'))$. We shall apply the previous lemma to the ring B'' and the ideal JB''. For this, we need

(1) The ideal JB'' is locally principal.
(2) $(p,J) \subset \mathrm{jrad}(B'')$.
(3) $p \in JB'' + \phi(JB'')B''$.

The first condition is clear as $J \subset B$ is locally principal. The second condition is ensured by the localization along $V(p, J(A' \otimes_A B'))$. The third one is also clear. Hence we obtain a faithfully flat map $B'' \to B'''$ of δ-rings that is an ind Zariski localization, and $JB''' = (e''')$ with $(p, e''') \subset \mathrm{jrad}(B''')$. Note that the ring map

$$B' \to A' \otimes_A B' \to B''$$

is flat. The image of $\mathrm{Spec}(B'') \to \mathrm{Spec}(A' \otimes_A B')$ contains $V(p, J(A' \otimes_A B'))$ by the localization. The restriction of $\mathrm{Spec}(A' \otimes_A B') \to \mathrm{Spec}(B')$ to

$$V(p, J(A' \otimes_A B')) \to V(p, JB')$$

is surjective, as it is the basechange of the faithfully flat map $A \to A'$ along

$$A \to B \to B' \to B'/JB'.$$

Hence $B' \to B''$ is faithfully flat, and thus the composition $B \to B'''$ is faithfully flat.

Replacing B' with B''', we have reduced to the following situation. We have a commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & A' \\ \downarrow & & \downarrow \\ B & \longrightarrow & B' \end{array}$$

where rows are faithfully flat, and we have

$$IA' = (d), \quad IB' = (e)$$

with $(p,d) \subset \mathrm{jrad}(A')$ and $(p,d) \subset \mathrm{jrad}(B')$. Note that the image of $d \in A'$ under $A' \to B'$ lies in (e), i.e. $d = ef$ for some $f \in B'$. We shall apply the lemma below to show that f is a unit in B'. It suffices to show that d is distinguished in A', which is clear as we have

(1) $(p,d) \subset \mathrm{jrad}(A')$.
(2) $p \in IA' + \phi(IA')A' = dA' + \phi(dA')A'$.

Hence
$$dA' \otimes_{A'} B' \simeq eB'.$$
Therefore we conclude that $I \otimes_A B \simeq J$ as the two ring maps $A \to A'$ and $B \to B'$ are faithfully flat. $\square$

Lemma 2.0.4. Let A be a δ-ring. Let $d \in A$ be an distinguished element. Suppose $d = fg$ with $f, g \in A$ and $(p, f) \subset \mathrm{jrad}(A)$. Then f is distinguished and g is a unit.

Proof. We have
$$\delta(d) = \delta(fg) = f^p\delta(g) + \delta(f)g^p + p\delta(f)\delta(g).$$
The left hand side is a unit, and the first and the third element in the right hand side lie in $\mathrm{jrad}(A)$. Hence $g^p\delta(f)$ is a unit. Therefore f is distinguished and g is a unit. $\square$

Remark 2.0.5. The condition $p \in I + \phi(I)A$ in the definition of a prism (A, I) says that the closed subschemes $\phi^{-1}(V(I))$ and $V(I)$ of $\mathrm{Spec}(A)$ meet only in characteristic p.

Definition 2.0.6. A prism (A, I) is called

(1) bounded, if A/I has bounded p^∞-torsion.

3. Iwasawa Theory

3.1. Review of Class Field Theory.

Lemma 3.1.1. Let K be a non-Archimedean local field with residue field k. Choose a uniformizer ϖ_K. Let G_K be the absolute Galois group of K. Let $I_K \subset G_K$ be the inertia subgroup, i.e. $I_K \simeq \mathrm{Gal}(K^s/K^{ur})$ where K^s is the separable closure and K^{ur} is the maximal unramified extension. We have an exact sequence
$$0 \to I_K \to G_K \to \mathrm{Gal}(\overline{k}/k) \to 0.$$
Note that k is a finite field, and hence $\mathrm{Gal}(\overline{k}/k) \simeq \widehat{\mathbb{Z}}$, and is generated by the Frobenius σ. The Frobenius gives a degree map $\deg : \mathrm{Gal}(\overline{k}/k) \to \widehat{Z}$. Let $W_K \subset G_K$ be the inverse image of $\mathbb{Z} \subset \widehat{\mathbb{Z}}$. Then there exists a unique map, called the reciprocity map, or the Artin map, denoted by $\mathrm{Art}_K : K^\times \to W_K^{\mathrm{ab}}$ such that

(1) $\mathrm{ord}_{\varpi_K}(\mathrm{Art}_K^{-1}(g)) = \mathrm{ord}(g)$ for all $g \in W_K^{\mathrm{ab}}$.
(2) For every Abelian extension L/K, we have a commutative diagram
$$\begin{array}{ccc} L^\times & \longrightarrow & W_L^{\mathrm{ab}} \\ \downarrow & & \downarrow \\ K^\times & \longrightarrow & W_K^{\mathrm{ab}} \end{array}$$
where $L^\times \to K^\times$ is the norm map, and $W_L^{\mathrm{ab}} \to W_K^{\mathrm{ab}}$ is the natural map.

Lemma 3.1.2 (local Kronecker–Weber)**.** The maximal Abelian extension of $\mathbb{Q}_p$ is obtained by adjoining all the roots of unity, i.e. $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p(\mu_\infty)$. The Artin map
$$\mathrm{Art}_{\mathbb{Q}_p} : \mathbb{Q}_p^\times \to W_{\mathbb{Q}_p}^{\mathrm{ab}}$$
can be described explicitly as follows. ((TODO))

Remark 3.1.3. For general K, we need Lubin–Tate formal group to describe K^{ab} explicitly. In the case $K = \mathbb{Q}_p$, this is $\mathrm{LT}_{\mathbb{Q}_p} = \mathbb{G}_m$.

Lemma 3.1.4. Let F be a number field with adele ring $\mathbb{A}_F$. Then there exists a unique map, called the global Artin map, denoted by Art_F,
$$\mathrm{Art}_F : \lim F^\times \backslash \mathbb{A}_F^\times / K \to G_F^{\mathrm{ab}}$$
where $K \subset \mathbb{A}_F^\times$ ranges through all the compact subgroups. It is characterized by the local-global compatibility
$$\begin{array}{ccc} F_v^\times & \longrightarrow & W_{F_v}^{\mathrm{ab}} \\ \downarrow & & \downarrow \\ \mathbb{A}_F^\times & \longrightarrow & G_F^{\mathrm{ab}} \end{array}$$

for each place v of F.

Lemma 3.1.5 (global Kronecker–Weber)**.** The maximal Abelian extension of $\mathbb{Q}$ is $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty)$.

Remark 3.1.6. For genearl F, this is Hilbert's 12-th problem. For F a imaginery quadratic field, we know (by the work of Shimura) that $F^{\mathrm{ab}} = F(j_E, E_{\mathrm{tor}})$ where E is a CM elliptic curve over F, and j_E is the j-invariant of E. Note that $F(j_E)$ is the Hilbert class field of F, i.e. maximal Abelian extension that is unramified everywhere (including Archimedean places), usually denoted by H_F. The elliptic curve E is an analogy of $\mathbb{G}_m$.

For recent progress, see Dasqupta–Kakde.

Lemma 3.1.7. Let H_F be the Hilbert class field of F. Then
(1) $\mathrm{Gal}(H_F/F) \simeq \mathrm{Cl}_F$.
(2) Every fractional ideal of F becomes principal in H_F.

3.2. **Introduction.**

Lemma 3.2.1. Let F be a number field. Let ζ_F be the Dedekind zeta function of F. Then

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2} R_F h_F}{w_F\sqrt{|D_F|}}$$

where r_1 (resp. r_2) is the number of real (resp. complex) places of F, R_F is the regulator of F, h_F is the class number of F, w_F is the number of roots of unity of F, and D_F is the discriminant of F. Using the functional equation for ζ_F, we have

$$\lim_{s\to 0}\frac{\zeta_F(s)}{s^{r_1+r_2-1}} = -\frac{R_F h_F}{w_F}.$$

Remark 3.2.2. Let $E/\mathbb{Q}$ be an elliptic curve with conductor N. Define an L-series by Euler product

$$L(E,s) = \prod_\ell P_\ell(\ell^{-s})^{-1}$$

where

$$P_\ell = \begin{cases} 1 - a_\ell \ell^{-s} + \ell^{1-2s} & \ell \not| N \\ 1 - a_\ell \ell^{-s} & \ell \mid N \end{cases}$$

Here $a_\ell = 1 + \ell - |\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_\ell)|$, where $\widetilde{E}$ is the mod ℓ reduction of E, and $(-)_{\mathrm{ns}}$ denotes the non-singular locus. By Weil bound, we have $|a_\ell| \le 2\sqrt{\ell}$. Hence $L(E,s)$ is absolutely convergent on $\Re(s) >> 0$. By the Taniyama–Shimura conjecture (which is a theorem by Wiles, Taylor, Breuil–Conrad–Diamond–Taylor), $L(E,s)$ is an entire function on $\mathbb{C}$. The BSD conjecture is
(1) $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. This rank is denoted by r.
(2) The refined BSD formula

$$\frac{L^{(r)}(E,s)}{r!} = \frac{|\mathrm{Sha}(E)|\Omega_E R_E \prod_\ell c_\ell(F)}{|E(\mathbb{Q})_{\mathrm{tor}}|^2}$$

where Ω_E is the period, R_E is the regulator, $\mathrm{Sha}(E)$ is the Shafarevich group, and c_ℓ is the Tamagawa number.

((TODO: definition of Shafarevich group))

Remark 3.2.3. We have the following analogies. number field; elliptic curves $\mathcal{O}_F^\times$; $E(\mathbb{Q})$ $r_1 + r_2 - 1$; r $(\mathcal{O}_E^\times)_{\mathrm{tor}}$; $E(\mathbb{Q})_{\mathrm{tor}}$ R_F; R_E $2^{r_1}(2\pi)^{r_2}$; Ω_E Cl_F; Sha_E

Remark 3.2.4. Class group and Shafarevich group. Let $\mathfrak{a}$ be a fractional ideal of F. There exists an extension L/F such that $\mathfrak{a}\mathcal{O}_L = (a)$ for some $a \in L^\times$. We can construct an isomorphism

$$\mathrm{Cl}_F \to \ker\left(H^1(F, \mathcal{O}_{F^s}^\times) \to \prod_v H^1(F_v, \mathcal{O}_{F_v^s}^\times)\right)$$

with

$$\mathfrak{a} \mapsto (\sigma \mapsto \sigma(a)/a).$$

See [Buzzard, "Why is an ideal class group a Tate–Shafarevich group"].

Let p be an odd prime.

Definition 3.2.5. Let $\mathbb{Q}_\infty/\mathbb{Q}$ be an $\mathbb{Z}_p$ extension. Since

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times (1+p\mathbb{Z}_p) \simeq \mathbb{F}_p^\times \times \mathbb{Z}_p,$$

we have $\mathbb{Q}_\infty \subset \mathbb{Q}(\mu_{p^\infty})$. Let $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$. Let $\mathbb{Q}_n$ be the subextension of $\mathbb{Q}_\infty/\mathbb{Q}$ such that

$$\Gamma_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Definition 3.2.6. The Iwasawa module is

$$\Lambda = \mathbb{Z}_p[[\Gamma]] = \lim_n \mathbb{Z}_p[[\Gamma_n]].$$

Lemma 3.2.7. There exists an isomorphism

$$\mathbb{Z}_p[[x]] \to \Lambda$$

sending x to a topological generator $\gamma \in \Gamma$.

Definition 3.2.8. Let $N \geq 1$ not divisible by p. Let $Q_{N,\infty}$ be $Q_\infty Q(\mu_N)$, and $Q_{N,n} = Q_n Q(\mu_N)$.

Lemma 3.2.9 (Iwasawa's theorem)**.** There exist integers λ, μ, and $c \geq 0$, and some n_0 such that for all $n > n_0$, the p-part of the class number of $Q_{N,n}$ is of p-order $\lambda n + \mu p^n + c$.

Remark 3.2.10. Write $A_{N,n}$ for the kernel of

$$\mathrm{Hom}_{\mathrm{cts}}(G_{Q_{N,n}}, \mathbb{Q}_p/\mathbb{Z}_p) \to \prod_v \mathrm{Hom}_{\mathrm{cts}}(I_v, \mathbb{Q}_p/\mathbb{Z}_p).$$

Here cts means continuous. By class field theory, we have

$$A_{N,n} \simeq \mathrm{Hom}(\mathrm{Gal}(H_{N,n}/Q_{N,n}), \mathbb{Q}_p/\mathbb{Z}_p) \simeq \mathrm{Hom}(\mathrm{Cl}_{Q_{N,n}}, \mathbb{Q}_p/\mathbb{Z}_p).$$

Define $A_{N,\infty} = \mathrm{colim}_n A_{N,n}$. Define $M_{N,\infty}$ as the Pontryagin dual $A^*_{N,\infty} = \mathrm{Hom}_{\mathrm{cts}}(A_{N,\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$. It carries an action of Γ, and thus it is a module over Λ.

Lemma 3.2.11 (Control theorem)**.**
(1) $M_{N,\infty}$ is a finitely generated torsion Λ-module.
(2) There exists a submodule Y of $M_{N,\infty}$ generated by

$$(xM_{N,\infty}, a_1, \ldots, a_s)$$

for some $a_1, \ldots, a_s \in M_{N,\infty}$ such that for every n,

$$\frac{M_{N,\infty}}{(((1+x)^{p^n}-1)/x)Y} \simeq M_{N,n}.$$

Lemma 3.2.12 (Structure theorem)**.** Let M be a finitely generated Λ-module. Then there exists a homomorphism

$$\iota_M : M \to \Lambda^r \oplus \bigoplus_{i=1}^m \Lambda/(f_i(x))^{b_i} \oplus \bigoplus_{j=1}^s \Lambda/(p^{n_i}\Lambda)$$

with kernel and cokernel both have finite cardinality, where $f_i(x)$ are distinguished polynomials (i.e. monic polynomials with non-leading coefficients divisible by p).

Remark 3.2.13. An old reference: GTM83.