Galois Deformations and Hecke Curves

B. Mazur

Following Andrew Wiles' announcement of his work, in June 1993, and in view of the immense interest it met with, I felt it reasonable to give a two semester graduate course [1] covering topics that might be helpful to people who want to understand, and possibly pursue, the subject.

In the Fall semester I covered the basic deformation theory of Galois representations (in detail) and Fontaine's theory (very briefly), all the material covered having been already available in published papers.

The Spring semester was entirely devoted to a study the methods of Flach's article[2] in some depth, these methods following on the work of Kolyvagin.

The pages below comprise a (**still very rough**) draft of a compilation of course notes for the Spring semester. I would like to extend these notes in future drafts, writing the unwritten sections, completing the unfinished sections[3], and adding a good deal more material (including a certain amount of numerical data). Nevertheless, incomplete as these notes are at present, I'm distributing them in the hope that they may be useful. Please let me know if you spot any errors, regret any omissions, or want any clarifications to be included in later drafts. I am thankful to Henri Darmon and

---

[1] Math 257z in the Fall and Math 257y in the Spring, at Harvard, 1993

[2] Flach, M.: A finiteness theorem for the symmetric square of an elliptic curve, Inv. Math. **109** (1992) 307-327.

[3] e.g., proofs for Lemmas 1 and 2 of §6 of Chapter 8 have not yet been written...

Alexander Beilinson for extensive comments on my first draft.

The first part of these notes is an "axiomatic" preview of the type of structures dealt with in Flach's article. The basic structure we call a "Flach System" and a stricter version of this type of structure we refer to as a "Cohesive Flach System". The mere existence of a "Cohesive Flach System" has rather extraordinary consequences which are examined in Part I.

In the second part of the course we study Flach's construction in some detail, and show that it does produce "Cohesive Flach Systems". We focus, in Chapter 9, on the context of modular curves and explicitly extract some of the direct consequences of the existence of Cohesive Flach Systems for the Galois representations attached to modular forms.

In the third part of the course we return to "axiomatics". We observe that Flach's construction yields something still stronger than a "Cohesive Flach System". We try to capture more fully the precise structure that his construction yields, by formulating a notion which we call a "Bilateral Flach Derivation".

Table of Contents

Part II : Constructions

Chapter eleven: Bilateral Flach Derivations

§1. The basic set-up for this Chapter.

§2. The $A \otimes_{\mathbb{Z}_p} A$-module $H \otimes_{\mathbb{Z}_p} H$ and its cohomology.

§3. (Bilateral) Flach Derivations connected to Galois representations.

* §4. Are the Bilateral Flach Derivations that we have constructed "canonical" ?

§5. The bilateral derivation of A associated to a Bilateral Flach Derivation.

* Glossary of notation
* References

Note: * means "not written, or not completely written".

Part I : Axiomatics

Chapter one: Local Preliminaries

A general reference: [Milne] Milne, J.S.: Arithmetic Duality Theorems Academic Press 1986. pp. 1-45.

§1. Conventions. All our rings will be assumed to have identity elements. If M is a module over a commutative ring A, and $I \subset A$ is an ideal, the notation M[I] will mean the "kernel of I in M", that is,

$$M[I] = \bigcap_{\gamma \in I} \ker \{ \gamma : M \to M \}.$$

If A is a Λ-algebra, if M is an A-module and B a Λ-module, the Λ-module $\mathrm{Hom}_\Lambda(M,B)$ is given a natural A-module structure compatible with its Λ-module structure by the rule: $a \cdot \varphi(m) = \varphi(a \cdot m)$ for $a \in A$, $\varphi \in \mathrm{Hom}_\Lambda(M,B)$, and $m \in M$.

Pairings: If Λ is a commutative ring, B a Λ-module, and M, N are two modules over a Λ-algebra A, and if we are given a Λ-bilinear pairing

$$(,): \quad M \times N \to B$$

we will say that A is **self-dual** (or synonymously: **Hermitian** [1]) with respect to the pairing if we have

$(a\cdot m,n) = (m,a\cdot n)$ for all $a\in A$, $m\in M$, $n\in N$. If so, then the pairing factors through a homomorphism of Λ-modules

$$M \otimes_A N \to B,$$

which we may also refer to as "the pairing" $(\ ,\ )$. The action of A is Hermitian if and only if the mappings $N\to \mathrm{Hom}_\Lambda(M,B)$ and $M\to \mathrm{Hom}_\Lambda(N,B)$ induced from the pairing are homomorphisms of A-modules. We say that the pairing is **perfect** if these mappings are isomorphisms.

Given pairings

$$(\ ,\ )_j : M_j \times N_j \to \mathbb{Q}/\mathbb{Z}$$

of *finite* A-modules indexed by j in $\mathbb{N}$ (or more generally, in a directed set of indices) with homomorphisms of A-modules $\varphi: M_j \to M_{j+1}$ and $\psi: N_{j+1} \to N_j$ for j in $\mathbb{N}$ we will say that the pairings $(\ ,\ )_j$, $j\in\mathbb{N}$, are **compatible** if for all j and $m\in M_j$, $n\in N_{j+1}$ we have

$$(m, \psi n)_j = (\varphi m, n)_{j+1}.$$

In such a case, the pairings $(\ ,\ )_j$ for $j \in \mathbb{N}$ "compile" in an evident way to provide a bilinear pairing,

$$(\ ,\ ) : \underset{j\in\mathbb{N}}{\text{lim. ind.}}\,(M_j) \times \underset{j\in\mathbb{N}}{\text{lim. proj.}}\,(N_j) \to \mathbb{Q}/\mathbb{Z}$$

with respect to which the action of A is Hermitian if it is so for all of the pairings $(\ ,\ )_j$. If the $(\ ,\ )_j$ are perfect

---

[1] anticipating the moment, which will not in fact come in these notes, when we have rings A with an anti-involution $a\mapsto a^*$ and pairings which are Hermitian in the standard sense, i.e., $(a\cdot m,n) = (m,a^*\cdot n)$; in these notes our rings A are commutative and our anti-involution $a \mapsto a^*$ is the identity.

pairings in the sense of Pontrjagin duality, then the compiled pairing (,) is also a perfect pairing in the category of topological abelian groups if the inductive limit of the M_j's and the projective limit of the N_j's are given their natural topologies; in particular, lim.ind. (M_j) is discrete, and lim.proj. (N_j) is profinite.

Group cohomology: Let G be a profinite group, and M a torsion G-module, the action of G on M being continuous. Then $H^i(G,M)$ will stand for i-dimensional group cohomology computed via continuous cocycles where M is given the discrete topology; equivalently it is the inductive limit of the i-dimensional cohomology over the inductive system of finite submodules of M.

§2. Finite fields. Let k be a finite field of characteristic ℓ, with $q = \ell^f$ elements. Let G_k be its Galois group, so: $G_k = \mathrm{Gal}(\bar{k}/k) \cong \hat{\mathbb{Z}}$ with $[\varphi: x \mapsto x^q] \in G_k$ identified with $1 \in \hat{\mathbb{Z}}$. Let M be a torsion G_k-module. Then:

$$H^i(G_k,M) = 0 \quad \text{for } i \neq 1,2$$

$$H^0(G_k,M) = M^{G_k} = M[1-\varphi]$$

$$H^1(G_k,M) = M_{G_k} = M/(1-\varphi)M,$$

with the correspondence between 1-cocycles representing classes in $H^1(G_k,M)$ and elements of $M/(1-\varphi)M$ being given by

$$[c:G_k \to M] \quad \text{--------} \to \quad c(\varphi) \mod (1-\varphi)M.$$

If M has trivial G_k-action, we have the canonical identifications $H^0(G_k,M) = H^1(G_k,M) = M$, and taking $M = \mathbb{Q}/\mathbb{Z}$ with trivial G_k-action, let us record the canonical

identification

$$H^1(G_k,\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}.$$

Now let M be finite, and denote its Pontrjagin dual

$$M\hat{} := \quad \mathrm{Hom}\,(M,\mathbb{Q}/\mathbb{Z}).$$

The perfect pairing $M \times M\hat{} \to \mathbb{Q}/\mathbb{Z}$ induces perfect pairings

$$M^{G_k} \times (M\hat{})_{G_k} \to \mathbb{Q}/\mathbb{Z} \quad \text{and} \quad M_{G_k} \times (M\hat{})^{G_k} \to \mathbb{Q}/\mathbb{Z},$$

and these are simply the pairings induced by cup-product on the cohomology groups

$$(1)\quad H^i(G_k,M) \times H^{1-i}(G_k,M\hat{}) \to H^1(G_k,\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z},$$

for i = 0, 1 respectively. So (1) is a perfect duality for all $i \in \mathbb{Z}$.

§3. Local fields. Let K be a finite extension of $\mathbb{Q}_\ell$ with residue field k. We have the basic facts of life of such K's:

$$\begin{array}{ccccccccc}
 & & & & & \overset{\mathrm{val}}{} & & & \\
0 & \to & \mathcal{O}_K^* & \to & K^* & \to & \mathbb{Z} & \to & 0 \\
 & & \cong\downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathcal{U} & \to & G_K^{ab} & \to & G_k & \to & 0 \\
 & & \uparrow & & \uparrow & & \uparrow = & & \\
0 & \to & I_K & \to & G_K & \to & G_k & \to & 0
\end{array}$$

where the downward arrows are given by local class field theory, the two unlabelled ones being injections which induce isomorphisms from the profinite completion of their respective domains to their respective ranges, and the right-most one inducing the isomorphism $\hat{\mathbb{Z}} \cong G_k$ described previously $(1 \mapsto \varphi)$.

§4. Tate Local Duality. Let μ denote the torsion subgroup of all roots of unity in $\overline{K}$. By Local Class Field Theory we have the canonical identification $H^2(G_K, \mu) \cong \mathbb{Q}/\mathbb{Z}$. Define the "Cartier" dual of a torsion G_K-module M to be $M^* := \mathrm{Hom}_{\mathbb{Z}}(M,\mu)$ with G_K-action given in the natural way, namely: if $f \in \mathrm{Hom}_{\mathbb{Z}}(M,\mu)$ and $g \in G_K$, then $(g\cdot f)(g\cdot m) = g\cdot(f(m))$. Now suppose that M is finite. Cup-product induces a pairing,

$$(2) \qquad H^i(G_K,M) \times H^{2-i}(G_K,M^*) \to H^2(G_K,\mu) = \mathbb{Q}/\mathbb{Z},$$

and by "Tate Local Duality" let us mean the assertion that the groups $H^i(G_K,M)$ are finite, and that (2) is a perfect pairing for all $i \in \mathbb{Z}$ (cf. **[Milne]** Chapter I, Cor. 2.3 for a slightly more general formulation). It follows that $H^i(G_K,M)$ vanishes if $i \neq 0,1,2$, and we have the following information about these intermediate dimensions:

$$H^0(G_K,M) = M^{G_K}, \quad H^2(G_K,M)\hat{} \cong (M^*)^{G_K} = \mathrm{Hom}_{G_K}(M,\mu),$$

and there is a perfect pairing,

$$(3) \qquad H^1(G_K,M) \times H^1(G_K,M^*) \to H^2(G_K,\mu) = \mathbb{Q}/\mathbb{Z}.$$

Example. Let $M = \mathbb{Z}/N\mathbb{Z}$ with trivial G_K-action. Then:

$$H^1(G_K,M) = \mathrm{Hom}(G_K, \mathbb{Z}/N\mathbb{Z}) \cong \mathrm{Hom}(K^*, \mathbb{Z}/N\mathbb{Z}),$$

where the isomorphsim is given by local Class Field Theory, and

$$H^1(G_K,M^*) = H^1(G_K,\mu_N) \cong K^*/K^{*N},$$

where the isomorphism is given by Kummer Theory.

In this situation, (3) is a perfect pairing

$$(4) \quad \mathrm{Hom}(K^*, \mathbb{Z}/N\mathbb{Z}) \times K^*/K^{*N} \to \mathbb{Q}/\mathbb{Z},$$

and we should make our sign conventions so that (4) comes out to be the natural pairing, not the negative of it.

§5. The "finite part" of 1-dimensional cohomology.

Keep M a finite G_K-module. The Hochschild-Serre Spectral Sequence (cf. **[Milne]** Ch. I, 0.7) for the normal subgroup $I_K \subset G_K$ reads:

$$H^p(G_k(H^q(I_K,M)) \Rightarrow H^{p+q}(G_K,M)$$

and gives an exact sequence

$$(5) \quad 0 \to H^1(G_k, M^{I_K}) \to H^1(G_K,M) \to H^1(I_K,M)^{G_k} \to 0,$$

the zero on the right because $H^2(G_k, M^{I_K})$ vanishes.

Suppose M **is unramified.** By this we mean that I_K acts trivially on M and therefore M may be viewed, in a natural way, as a G_k-module. Then (5) reads:

(6) $0 \to H^1(G_k, M) \to H^1(G_K, M) \to \mathrm{Hom}_{G_k}((I_K)^{ab}, M) \to 0.$

Suppose M **is unramified, and of cardinality a power of a prime number** $p \neq \ell$. Then two further things happen. First, M^* is also unramified. Second, any homomorphism $(I_K)^{ab} \to M$ factors through the p-primary component of the tame inertia group, i.e.,

$$\mathrm{Hom}_{G_k}((I_K)^{ab}, M) = \mathrm{Hom}_{G_k}(\mathbb{Z}_p(1), M) = M(-1)^{G_k},$$

so we may evaluate the exact sequence (6) for M and M^* as follows:

(7) $0 \to H^1(G_k, M) \to H^1(G_K, M) \to M(-1)^{G_k} \to 0$

(8) $0 \to H^1(G_k, M^*) \to H^1(G_K, M^*) \to (M\hat{})^{G_k} \to 0,$

where we have used the identification of $M^*(-1)$ with $M\hat{}$.

Proposition 1: Tate Local Duality "respects" the exact sequences (7) and (8) in that $H^1(G_k, M)$ and $H^1(G_k, M^*)$ are orthogonal complements with respect to the Tate pairing,

$$H^1(G_K, M) \times H^1(G_K, M^*) \to \mathbb{Q}/\mathbb{Z}$$

and the induced pairing

(9) $$H^1(G_k, M) \times (M\hat{})^{G_k} \to \mathbb{Q}/\mathbb{Z}$$

is the perfect pairing coming from Pontrjagin duality.

Note: The phrase "coming from Pontrjagin duality" in the statement of the Proposition is ambiguous perhaps, in

that there are two ways to think of (9) as coming "from Pontrjagin duality: Identifying $(M\hat{})^{G_k}$ with $H^0(G_k, M\hat{})$ we may pass from the left-hand side of (9) via cup-product to $H^1(G_k, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_k, \mathbb{Q}/\mathbb{Z})$, and this latter group we identify with $\mathbb{Q}/\mathbb{Z}$ by associating to a homomorphism $h \in \mathrm{Hom}(G_k, \mathbb{Q}/\mathbb{Z})$ the image of the Frobenius element in G_k under h. Alternatively, we may view the left factor, $H^1(G_k, M)$, of (9) as isomorphic to the module, M_{G_k}, of co-invariants of the action of G_k on M, via the identification of a class h in $H^1(G_k, M)$ with the image in M_{G_k} of the Frobenius element in G_k under a 1-cocycle representing h. The pairing (9) then becomes a pairing,

$$M_{G_k} \times (M\hat{})^{G_k} \quad \rightarrow \mathbb{Q}/\mathbb{Z}$$

which is obtained directly from the Pontrjagin duality pairing

$$M \times M\hat{} \quad \rightarrow \mathbb{Q}/\mathbb{Z},$$

by restricting to $(M\hat{})^{G_k}$ on the right, and passing to the quotient M_{G_k} on the left. These two descriptions of the pairing (9) are the same.

Proof of Proposition 1: See [Milne] Chapter I, Thm. 2.6. Briefly, the argument is as follows: that $H^1(G_k, M)$ and $H^1(G_k, M^*)$ are orthogonal can be seen by noting that the Tate pairing restricted to $H^1(G_k, M) \times H^1(G_k, M^*)$ factors through the cup-product mapping to $H^2(G_k, \mu)$ which vanishes. To finish, one must identify the induced pairing

(9). But if one is content not to actually identify (9) as the Pontrjagin pairing, but merely to see that it is a perfect pairing, this is easy: it follows from a simple argument using only that the Tate pairing is perfect, and the two groups $H^1(G_k, M)$ and $(M\hat{})^{G_k}$ have the same (finite) order.

□

Let us call the subgroup $H^1(G_k, M) \subset H^1(G_K, M)$ the **finite part** of the cohomology, and the quotient group $H^1(G_K,M) \to M(-1)^{G_k}$ the **singular "part"**. So, a necessary and sufficient condition for a class in $H^1(G_K, M)$ to lie in the "finite part" is for it to project to zero in the singular part, and if it does so, then a necessary and sufficient condition for it to vanish is for it to "cup" trivially with every element in the singular part of $H^1(G_K, M^*)$.

§6. Passage to the limit. For a moment, let G be any profinite group and M^* any (continuous) G-module whose underlying abelian group is a free $\mathbb{Z}_p$-modules of finite rank. The cohomology of M^* is then defined as the projective limit of cohomology,

$$H^i(G, M^*) = \text{proj. lim.}_{\nu \to \infty} H^i(G, M^*/p^\nu M^*)$$

viewed as $\mathbb{Z}_p$-module. If M is a G_K-module whose underlying abelian group is a p-divisible group of finite corank, then M^* is as above, and we have cohomology of both M and M^* defined. The entire discussion above goes through for the cohomology groups of M and M^*. Specifically, the exact sequences and dualities listed in (1) -(3) and (5), (6) all hold.

Suppose M is unramified, and of cardinality a power of $p \neq \ell$ Then (7)- (9) also hold. In particular, revisiting (7) and (8) in this new context, we have that the *singular part* of $H^1(G_K,M^*)$, i.e.: $(M\hat{})^{G_k}$, is a free $\mathbb{Z}_p$-module of finite rank (since it is a submodule of such) and the *finite part* of $H^1(G_K,M)$, i.e.: $H^1(G_k,M)$, is p-divisible.

§7. Suppose $\ell \neq p$ and M is allowed to be ramified.

If $I_{K,\ell} \subset I_K$ is the (unique) pro-ℓ-Sylow subgroup of I_K, then the quotient group $I_K/I_{K,\ell}$, called the **tame quotient** of I_K, is abelian, of (pro-) order prime to ℓ, and there is a canonical isomorphism

$$\delta: \; I_K/I_{K,\ell} \; \overset{\cong}{\rightarrow} \; \prod_{r \neq \ell} \mathbb{Z}_r(1)$$

where the product on the right is taken over all prime numbers $r \neq \ell$, and where $\mathbb{Z}_r(1) = \mathit{Tate}\,(\mu_{r^\infty})$, the Tate module of μ_{r^∞}. There are natural actions of G_k on domain and range, , the action on the tame quotient being induced from the action of G_k on $I_K{}^{ab}$ via conjugation by liftings of elements of G_k to G_K, and the isomorphism δ is G_k-equivariant. For a concise description of this structure theory for tame inertia, see pp. 262-265 of Serre's Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inv. Math 15 (1972) 259-331.

Projecting I_K to the factor $\mathbb{Z}_p(1)$ of the tame quotient, we get an exact sequence of profinite groups with G_K-actions,

$$(10) \qquad 0 \rightarrow \Gamma_K \rightarrow I_K \rightarrow \mathbb{Z}_p(1) \rightarrow 0$$

where Γ_K is the kernel of the projection $I_K \to \mathbb{Z}_p(1)$.

From now on, M will be a p-torsion G_K-module such that M[p] is finite.

Suppose that Γ_K acts trivially on M. Then M, M^*, and $M\hat{}$ have $\mathbb{Z}_p(1)$-actions induced from their I_K-module structures. Since Γ_K is a projective limit of finite groups prime to p, the exact sequence (10) gives us a degenerating Hochschild-Serre Spectral Sequence for the calculation of group cohomology of M. Thus $H^i(I_K, M) = H^i(\mathbb{Z}_p(1), M)$ for all i, so $H^i(I_K, M)$ vanishes for $i \neq 1,2$, and we have canonical isomorphisms:

$H^0(I_K, M) \cong M^{I_K} = M^{\mathbb{Z}_p(1)}$ and

$H^1(I_K, M^*) \cong H^1(\mathbb{Z}_p(1), M^*)$.

This latter group is canonically isomorphic to the module of $\mathbb{Z}_p(1)$-co-invariants of $\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(1), M^*) = M^*(-1) = M\hat{}$, i.e.,

(11) $H^1(I_K, M^*) \cong (M\hat{})_{\mathbb{Z}_p(1)} = (M\hat{})/(\gamma-1)(M\hat{})$,

where γ is any choice of topological generator of $\mathbb{Z}_p(1)$, and this isomorphism is "equivariant" for the natural action of G_k on each side.

Let us return to (5), written for both M and M^*,

(12) $0 \to H^1(G_k, M^{I_K}) \to H^1(G_K, M) \to H^1(I_K, M)^{G_k} \to 0$

(13) $0 \to H^1(G_k, M^{*I_K}) \to H^1(G_K, M^*) \to H^1(I_K, M^*)^{G_k} \to 0.$

Note that we have a natural Pontrjagin duality pairing,

$$M^{I_K} \times (M\hat{})_{I_K} \to \mathbb{Q}/\mathbb{Z},$$

from which the isomorphism of (11) gives the perfect pairing

$$M^{I_K} \times H^1(I_K, M^*) \to \mathbb{Q}/\mathbb{Z},$$

which, in turn, induces a perfect pairing:

(14) $H^1(G_k, M^{I_K}) \times H^0(G_k, H^1(I_K, M^*)) \to \mathbb{Q}/\mathbb{Z}.$

The "same" proof of Proposition 1 in §5 above gives:

Proposition 2: Tate Local Duality "respects" (12) and (13) in that $H^1(G_k, M^{I_K})$ and $H^1(G_k, M^{*I_K})$ are orthogonal complements with respect to the Tate pairing,

$$H^1(G_K, M) \times H^1(G_K, M^*) \to \mathbb{Q}/\mathbb{Z}$$

and Tate Duality induces the pairing (14) on the respective subgroup and quotient group.

Proof: This follows precisely the pattern of the proof of Proposition 1: one checks that the two groups $H^1(G_k, M^{I_K})$ and $H^1(G_k, M^{*I_K})$ are orthogonal because the Tate pairing, restricted to $H^1(G_k, M^{I_K}) \times H^1(G_k, M^{*I_K})$ factors through the cup-product mapping to $H^2(G_k, \mu)$ which vanishes, and then a counting argument will give that they are orthogonal complements, while a more detailed

calculation identifies the pairing (14).

Exercise and comment: Correctly worded, essentially the same Proposition and its proof work in complete generality... i.e., not assuming that Γ_K act trivially. As an exercise, work this out. But note that the hypothesis that "Γ_K acts trivially" is satisfied, for example, by the semi-stable Galois representations (we discussed last term) of G_K into $GL_N(A)$ where A is a complete noetherian local ring with finite residue field of characteristic p.

Terminology: We import, in this context, the same terminology as in the unramified case, i.e., the subgroup $H^1(G_k, M^{I_K})$ of $H^1(G_K,M)$ will be called the **finite part** of $H^1(G_K,M)$ and the quotient group $H^1(I_K,M)^{G_k}$ will be called the **singular part**, and similarly for M^*.

§8. Some notation, and the category $\mathfrak{M}(W)$. The letter A will stand for a complete local commutative finite faithfully flat $\mathbb{Z}_p$-algebra. For the definitions below we let $\ell \neq p$, or $\ell = p$. Let W^* be a free A-module of finite rank, with an A-linear continuous G_K-action. So W, the Cartier dual to W^*, is naturally endowed with the structure of p-divisible $A[G_K]$-module of finite corank. Define the category $\mathfrak{M}(W)$, a subcategory of the category of $A[G_K]$-modules, as follows. The objects M of $\mathfrak{M}(W)$ are the $A[G_K]$-submodules of W. The set of morphisms $\mathrm{Hom}_{\mathfrak{M}(W)}(M_1, M_2) \subset \mathrm{Hom}_{A[G_K]}(M_1, M_2))$ are those morphisms of $A[G_K]$-submodules obtainable by multiplication by elements a of A in W:

$$\begin{array}{ccc} M_1 & \to & M_2 \\ \downarrow & & \downarrow \\ W & \to & W \,. \end{array}$$

We want to specify the notion of **short exact sequence** in $\mathfrak{M}(W)$ in the following rather restricted way: A ("short") sequence in $\mathfrak{M}(W)$ is exact if and only if it is isomorphic to a sequence of the form

$$(*)\quad 0 \to W[\alpha] \xrightarrow{\iota} W[\alpha\cdot\beta] \xrightarrow{\alpha} W[\beta] \to 0$$

where $\alpha,\beta \in A$, α is a unit in $A\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$, and ι is the natural inclusion. These are short exact sequences in the category of $A[G_K]$-modules because W is p-divisible. We will say that a morphism in $\mathfrak{M}(W)$ is *injective* or *surjective* if it is isomorphic to a morphism labelled ι or α respectively in some short exact sequence $(*)$.

Define the category $\mathfrak{M}(W^*)$, which we will call the "**Cartier dual category**" to $\mathfrak{M}(W)$ to be formally just the *opposite* category to $\mathfrak{M}(W)$. If M is an object of $\mathfrak{M}(W)$ then its corresponding object in $\mathfrak{M}(W^*)$ we will denote M^*. Of course, we can also think of $\mathfrak{M}(W^*)$ as a category whose objects are quotient $A[G_K]$-modules of W^*, where M^* is indeed the Cartier dual of M, and its exact sequences are the Cartier duals of $(*)$.

§9. Clean ramification. Let W and $\mathfrak{M}(W)$ be as in §8, and suppose that $\ell\neq p$ and that Γ_K acts trivially on W.

Lemma: The following are equivalent conditions:

1) W^{I_K} is p-divisible.

2) The functor $M \mapsto M^{I_K}$ is "exact" on the category $\mathfrak{M}(W)$.

3) $H^1(I_K, W^*)$ is free as a $\mathbb{Z}_p$-module.

Proof: 1) $\Leftrightarrow$ 3) because W^{I_K} and $H^1(I_K, W^*)$ are dual; while 2) applied to the exact sequences

$$0 \to W[p^n] \to W \xrightarrow{p^n} W \to 0$$

for arbitrary n, yields **1)**. To see that **1)** implies **2)** consider the commutative diagram of exact sequences of $A[G_K]$-modules below,

$$\begin{array}{ccccccccc} 0 & \to & W[\alpha] & \to & W[\alpha\cdot\beta] & \xrightarrow{\alpha} & W[\beta] & \to & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \to & W[\alpha] & \to & W & \xrightarrow{\alpha} & W & \to & 0, \end{array}$$

and note that if $w \in W[\beta]$ then the full inverse image, $W_w \subset W$ of the element w under multiplication by α is contained in $W[\alpha\cdot\beta]$. By **1)** if w is I_K-invariant, there is an I_K-invariant element in W_w, and hence there is one in $W[\alpha\cdot\beta]$, i.e., $W[\alpha\cdot\beta]^{I_K} \to W[\beta]^{I_K}$ is surjective, giving 2).

Definition: If the equivalent properties of the lemma above hold, say that W is **cleanly ramified.**

§10. Formal pedantries. As a formal summary of what we have done so far, let us say that we have a **finite/singular structure** on 1-dimensional Galois cohomology over K for $\mathfrak{M}(W)$ if to each object M of $\mathfrak{M}(W)$ we are given an A-submodule, call it $H_f^1(G_K, M)$ in $H^1(G_K, M)$ and refer to it as the "**finite part**" in $H^1(G_K, M)$, this data being functorial on $\mathfrak{M}(W)$ and satisfying these two further properties.

1) $H_f^1(G_K,W)$ is p-divisible.

2) If $M_1 \to M_2$ is injective in $\mathfrak{M}(W)$, then the following diagram is Cartesian:

$$\begin{array}{ccc} H_f^1(G_K,M_1) & \to & H_f^1(G_K,M_2) \\ \downarrow & & \downarrow \\ H^1(G_K,M_1) & \to & H^1(G_K,M_2). \end{array}$$

To give such a structure, it suffices to stipulate $H_f^1(G_K,W)$:

Lemma: Given any p-divisible A-submodule $\mathcal{H} \subset H^1(G_K,W)$ there is a unique finite/singular structure on $\mathfrak{M}(W)$ with $H_f^1(G_K,W) = \mathcal{H}$.

Proof: For $M \subset W$ any sub $A[G_{\mathbb{Q}_\ell}]$-module, define $H_f^1(G_K,M)$ to be the sub-module of $H^1(G_K,M)$ making

$$\begin{array}{ccc} H_f^1(G_K,M) & \to & H^1(G_K,M) \\ \downarrow & & \downarrow \\ \mathcal{H} & \to & H^1(G_K,W) \end{array}$$

Cartesian. Axiom 1 is immediate, and Axiom 2 is directly verifiable.

□

Example: The most "stringent" finite/singular structure on $\mathfrak{M}(W)$ is given by stipulating $H_f^1(G_K,W) = 0$. For the finite/singular structure determined by this stipulation

one has $H_f^1(G_K,W[\alpha]) = H^0(G_K,W)/\alpha\cdot H^0(G_K,W)$ for any α in A. The "loosest" finite/singular structure is given by stipulating that $H_f^1(G_K,W)$ be the subgroup of divisible elements in $H^1(G_K,W)$.

Now let a finite/singular structure $M \mapsto H_f^1(G_K,M)$ on 1-dimensional Galois cohomology over K for $\mathfrak{M}(W)$ be given. For this finite/singular structure, and for any M in $\mathfrak{M}(W)$, we **define** the **singular quotient** $H_s^1(G_K,M)$ to be the quotient of $H^1(G_K,M)$ by $H_f^1(G_K,M)$ so that we have a functorial exact sequence of A-modules

$$(15)\quad 0 \to H_f^1(G_K,M) \to H^1(G_K,M) \to H_s^1(G_K,M) \to 0.$$

Proposition 3: Given an exact sequence in $\mathfrak{M}(W)$,

$$0 \to W[\alpha] \xrightarrow{\iota} W[\alpha\beta] \xrightarrow{\alpha} W[\beta] \to 0$$

the finite/singular structure "cleaves" the nine-term long exact sequence for G_K-cohomology into two six-term exact sequences, as follows, where the cohomology groups recorded in (16), (17) below are all understood to be "with respect to" G_K:

$$(16)\quad \begin{aligned} 0 \to\ & H^0(W[\alpha]) \to H^0(W[\alpha\beta]) \to H^0(W[\beta]) \to \\ \to\ & H_f^1(W[\alpha]) \to H_f^1(W[\alpha\beta]) \to H_f^1(W[\beta]) \to 0, \end{aligned}$$

and

$$(17)\quad \begin{aligned} 0 \to\ & H_s^1(W[\alpha]) \to H_s^1(W[\alpha\beta]) \to H_s^1(W[\beta]) \to \\ \to\ & H^2(W[\alpha]) \to H^2(W[\alpha\beta]) \to H^2(W[\beta]) \to 0. \end{aligned}$$

Proof: This is a straightforward diagram-chase, and uses only the two axioms for finite/singular structure.

Given a finite/singular structure on $\mathfrak{M}(W)$ we also *define* functorial exact sequences of A-modules for objects of the Cartier dual category $\mathfrak{M}(W^*)$ to $\mathfrak{M}(W)$,

$$(18)\quad 0 \to H_f^1(G_K,M^*) \to H^1(G_K,M^*) \to H_s^1(G_K,M^*) \to 0.$$

by the requirement that $H_f^1(G_K,M)$ and $H_f^1(G, M^*)$ be orthogonal complements under Tate Duality, thereby putting the pairs $H_f^1(G_K,M)$ **&** $H_s^1(G_K,M^*)$ and $H_f^1(G_K,M^*)$ **&** $H_s^1(G_K,M)$ in perfect duality, one with another. From 1) it follows that then $H_s^1(G_K,W^*)$ is also free over $\mathbb{Z}_p$. The "exact sequences" of $\mathfrak{M}(W^*)$ are simply the the dual exact sequences to those of $\mathfrak{M}(W)$, i.e.,

$$(19)\quad 0 \to W^*/\beta W^* \to W^*/\alpha\beta W^* \to W^*/\alpha W^* \to 0$$

for $\alpha,\beta \in A$, with α a non-zero divisor. We have the statement "dual" to Proposition 3:

Proposition 4: Given an exact sequence (19) in $\mathfrak{M}(W^*)$ the finite/singular structure "cleaves" the nine-term long exact sequence for G_K-cohomology into two six-term exact sequences, as follows, where the cohomology groups recorded in (20), (21) below are all understood to be "with respect to" G_K:

(20)

$$0 \to H^0(W^*/\beta W^*) \to H^0(W^*/\alpha\beta W^*) \to H^0(W^*/\alpha W^*) \to$$
$$\to H_f^1(W^*/\beta W^*) \to H_f^1(W^*/\alpha\beta W^*) \to H_f^1(W^*/\alpha W^*) \to 0,$$

and

(21)

$$0 \to H_s^1(W^*/\beta W^*) \to H_s^1(W^*/\alpha\beta W^*) \to H_s^1(W^*/\alpha W^*) \to$$
$$\to H^2(W^*/\beta W^*) \to H^2(W^*/\alpha\beta W^*) \to H^2(W^*/\alpha W^*) \to 0.$$

Proposition 5. When $\ell \neq p$, we have produced in the previous paragraphs a finite/singular structure on $\mathfrak{M}(W)$.

Proof: Axiom **1)** for finite/singular structures on $\mathfrak{M}(W)$ follows immediately from the hypothesis that W is cleanly ramified. As for Axiom **2)**, we must show that

$$\begin{array}{ccc} H^1(G_k, W[\alpha]^{IK}) & \to & H^1(G_k, W[\alpha\cdot\beta]^{IK}) \\ \downarrow & & \downarrow \\ H^1(G_K, W[\alpha]) & \to & H^1(G_K, W[\alpha\cdot\beta]) \end{array}$$

is Cartesian. But by the Lemma of §9, we have the following commutative diagram of short exact sequences of $A[G_K]$-modules,

$$\begin{array}{ccccccccc} 0 & \to & W[\alpha]^{IK} & \to & W[\alpha\cdot\beta]^{IK} & \to & W[\beta]^{IK} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & W[\alpha] & \to & W[\alpha\cdot\beta] & \to & W[\beta] & \to & 0, \end{array}$$

and writing the long exact sequence of G_k-cohomology for the top line, and of G_K-cohomology for the bottom line, a simple diagram-chase does it.

This finite/singular structure on $\mathfrak{M}(W)$ for W cleanly ramified ($\ell \neq p$) can be defined "cohomologically" :

Proposition 6: The inclusion $H_f^1(G_K, M) \to H^1(G_K, M)$ is isomorphic to the natural injection

$$H^1_{\text{ét}}(\text{Spec } \mathcal{O}_K, j_*M) \rightarrow H^1_{\text{ét}}(\text{Spec } K, M)$$

where the G_K-module M is viewed as sheaf for the étale topology over Spec K, and j: Spec K $\rightarrow$ Spec $\mathcal{O}_K$ is the natural morphism.

Hints for the proof: Perhaps the most down-to-earth way of seeing this is to use the explicit description of j_* (for the open immersion j: Spec K $\rightarrow$ Spec $\mathcal{O}_K$) given, e.g., in Example 3.15 of Chapter II of Milne's Etale Cohomology Princeton Univ. Press (1980); also, for a brief expository account, see my *Notes on étale cohomology of number fields* , Annales Sci. de l'E.N.S. **6** (1973) 521-556.

§11. The case $\ell = p$ (minimalist version). Now let W be a p-divisible $A[G_K]$-module such that W^* is free over A, and $\ell = p$. In place of the clean ramification condition, let us suppose that W is crystalline[2]. Let T denote the Tate module of W and $V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ so that we have an exact sequence of $A[G_K]$-modules

$$0 \rightarrow T \rightarrow V \rightarrow W \rightarrow 0.$$

---

[2] Here we rely on the brief expository account of this theory that was given last semester. But we should add two comments. The first is that crystalline issues will only begin to be germane in Chapter 4, and if you are willing to impose some definite finite/singular structure for $\ell = p$, nothing more specific than the axioms of "finite/singular structure" will be assumed about it until Chapter 4 (Theorem 2) at which point one will have to deal with crystalline matters. The second comment is that merely to give the *definition* which we give below, we need not logically assume that W is crystalline. But if we do not assume that W is crystalline, the finite/singular structure defined may not be connected to anything useful.

Define $H_f^1(G_K, V)$ to be the kernel of the morphism

$$H^1(G_K, V) \to H^1(G_K, V \otimes_{\mathbb{Q}_p} B_{crys})$$

and define $H_f^1(G_K, W)$ to be the image of $H_f^1(G_K, V)$ under the natural mapping $H^1(G_K, V) \to H^1(G_K, W)$. For $M \subset W$ a sub $A[G_K]$-module, define $H_f^1(G_K, M) \subset H^1(G_K, M)$ to be the inverse image of $H_f^1(G_K, W) \subset H^1(G_K, W)$ under the map $H^1(G_K, M) \to H^1(G_K, W)$.

Proposition 7. The above rule imposes a finite/singular structure on $\mathfrak{M}(W)$ (which we will refer to below as the **crystalline finite/singular structure**).

Proof: The group $H_f^1(G_K, W)$ is p-divisible since it is defined as the image of the vector space $H_f^1(G_K, V)$. Our Proposition then follows from the Lemma of §10.

□

Commentary: Later we will restrict to a subclass of crystalline representations W which are particularly relevant to us, and for these there is a slightly more down-to-earth description of H_f^1.

If it were sufficient for our purposes (it is *not*, unfortunately!) to deal only with modules that prolong to finite flat group schemes (or Barsotti-Tate groups) over the ring of integers of K, we could use the flat topology to define a reasonably satisfactory finite/singular structure. Here is a sketch of what one can do in that situation[3].

---

[3] What follows will not be used in the sequel.

If M is a finite G_K-module let us say that M **prolongs** to a finite flat group scheme $\tilde{M}$ over $\mathcal{O}_K$ if there is such a finite flat group scheme $\tilde{M}$ with an isomorphism of its generic fiber with M (which, for this purpose we we view as finite flat group scheme over Spec K). There may be many non-isomorphic prolongations, but for example, when $K = \mathbb{Q}_p$ and $p > 2$, a prolongation $\tilde{M}$, if it exists, is unique up to unique isomorphism. Similarly, if W is a p-divisible G_K module of finite corank, then we have the notion of W **prolonging** to a Barsotti-Tate group $\tilde{W}$ over $\mathcal{O}_K$ (and a theorem of Tate[4] guarantees that $\tilde{W}$, if it exists, is uniquely determined by W for any K finite over $\mathbb{Q}_p$, any p). If M prolongs to a finite flat group scheme or to a Barsotti-Tate group, $\tilde{M}$, over $\mathcal{O}_K$, define

$$H_f^1(G_K, \tilde{M}) := H_{fl}^1(\mathrm{Spec}(\mathcal{O}_K), \tilde{M}) \subset H^1(G_K, M)$$

where H_{fl}^1 refers to cohomology over $\mathrm{Spec}(\mathcal{O}_K)$ computed for the flat topology (cf. [**Milne**] Chap III) and $H_s^1(G_K, \tilde{M})$ is defined so as to make the sequence (15) exact. The group $H_f^1(G_K, \tilde{M})$ may depend upon $\tilde{M}$, the finite flat prolongation of M chosen, in general. The Local Flat Duality Theorem (loc. cit. Cor. 1.4) and the explicit description for p-divisible groups (loc. cit. Prop. 1.13) tell us, in effect, that this definition of H_f^1 and H_s^1 defines the *analogue* of a "finite/singular structure" for Galois modules M with prolongations to finite flat group schemes, or to Barsotti -Tate groups. If we then restrict our Galois modules to objects of the category $\mathfrak{M}(W)$ for W a fixed p-divisible Barsotti-Tate group, taking $\tilde{M}$ to be the

---

[4] Theorem 4 in:

Tate, J.: p-*Divisible groups* , pp. 158-183 in Proceedings of a Conference on Local Fields (NUFFIC Summer School held at Driebergen 1966) 1967, Springer-Verlag.

induced finite flat subgroup scheme on $\tilde{W}$ for every $M \in \mathfrak{M}(W)$ we do get a finite/singular structure on that category.

Chapter two: Global Preliminaries

A general reference: Milne, J.S.: Arithmetic Duality Theorems Academic Press 1986. pp. 60-81, and 200-212.

§1. Global cohomology.

Although we could work over arbitrary number fields with no retrenchment of statements in this §, let us focus on the case of particular interest to us, namely $\mathbb{Q}$. Fix $\overline{\mathbb{Q}}$, an algebraic closure, and, as usual, let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Having done this we may identify abelian sheaves for the étale topology over Spec $\mathbb{Q}$ with $G_{\mathbb{Q}}$-modules (sheaves $M \mapsto$ Galois modules $M(\overline{\mathbb{Q}})$) and we shall do this with no change of notation, i.e., we think of the M's in the parenthesis above alternatively as abelian sheaves for the étale topology and as Galois modules.

Let W be a p-divisible $G_{\mathbb{Q}}$-module of finite rank with a commutative $\mathbb{Z}_p$-algebra A of endomorphisms. Suppose that $p > 2$, and that the Cartier dual W^* is a free A-module of finite rank. Suppose further that W is unramified except at a finite set Σ of primes, and at each prime $\ell \neq p$ for which it is ramified, it is "cleanly ramified"; moreover, W viewed as $G_{\mathbb{Q}_p}$-module is assumed to be crystalline. Thus we have finite/singular structures for $\mathfrak{M}_\ell(W)$ where the subscript ℓ signifies that W is viewed as $A[G_{\mathbb{Q}_\ell}]$-module, for all prime numbers ℓ. Dually, we have finite/singular structures for $\mathfrak{M}_\ell(W^*)$ for all ℓ.[1]

---

[1] If you are not at ease with the theory of B_{crys} (and consequently with the finite/singular structure we have imposed on $\mathfrak{M}_p(W)$) you may put off the moment when you must deal with these crystalline matters by merely assuming, at present, that you have stipulated *some* specific finite/singular

Let $\underline{X}$ = Spec $\mathbb{Z}$ and $S \subset \underline{X}$ is a finite set of primes. For M any $A[G_{\mathbb{Q}}]$- submodule of W or $A[G_{\mathbb{Q}}]$-quotient module of W^*, define the A-module $H^1(\underline{X}\text{-}S, M)$ as follows:

(1) $H^1(\underline{X}\text{-}S, M) := \ker \{H^1(G_{\mathbb{Q}}, M) \to \prod_{\ell \notin S} H_s{}^1(G_{\mathbb{Q}_\ell}, M)\}$.

Let $G_{\mathbb{Q},\Sigma}$ denote the Galois group of the maximal Galois extension of $\mathbb{Q}$ which is unramified outside Σ (equivalently, the quotient of $G_{\mathbb{Q}}$ by the closed normal subgroup generated by all inertia subgroups at primes ℓ not lying in Σ). Then the $G_{\mathbb{Q}}$-actions on W and on M factor through the quotient $G_{\mathbb{Q},\Sigma}$. Viewing M as sheaf for the étale topology over Spec($\mathbb{Q}$) and letting j:Spec $\mathbb{Q} \to \underline{X}$-S denote the natural inclusion, form the direct image sheaf j_*M for the étale topology over $\underline{X}$-S. Our "cohomological notation" is meant to be suggestive, and, in fact, the special case when $p \in S$, we actually have a cohomological interpretation for $H^1(\underline{X}\text{-}S, M)$ as defined by (1). Namely,

Proposition 1: If $p \in S$, the injection

$$H^1{}_{\acute{e}t}(\underline{X}\text{-}S, j_*M) \to H^1(\text{Spec } \mathbb{Q}, M) = H^1(G_{\mathbb{Q}}, M)$$

identifies $H^1{}_{\acute{e}t}(\underline{X}\text{-}S, j_*M)$ with the sub A-module $H^1(\underline{X}\text{-}S, M)$ of $H^1(G_{\mathbb{Q}}, M)$ defined in (1) above.

If $\Sigma \subset S$, then we have the further identification:

---

structure at p. Absolutely *no property* of this finite/singular structure (beyond the fact that it satisfies the defining axioms of a finite/singular structure) will be relevant until Chapter 4.

$$H^1_{ét}(\underline{X}\text{-}S,\ j_*M) \cong H^1(\underline{X}\text{-}S,\ M) \cong H^1(G_{\mathbb{Q},S},M) \subset H^1(G_{\mathbb{Q}},M).$$

This Proposition is a good exercise in étale cohomology. For some hints of how to do the exercise, see my article: Notes on étale cohomology of number fields, Ann. Sci. Ecole. Norm. **6** (1973) 521-552.

Comment: We should guard against our cohomological notation suggesting too much. For instance, if p is not in S, *we have yet defined the analogous groups* $H^i(\underline{X}\text{-}S,\ M)$ for $i \geq 2$. To be explicit about this, the modules $H^i(\underline{X}\text{-}S,\ M)$ when $i \leq 1$, or when $p \in S$ are defined as follows:

$H^0(\underline{X}\text{-}S,\ M) = M^{G_{\mathbb{Q}}}$,
$H^1(\underline{X}\text{-}S,\ M)$ = as defined in (1) and if $p \in S$ it may also be identified with $H^1_{ét}(\underline{X}\text{-}S,\ j_*M)$ as submodule of $H^1(G_{\mathbb{Q}},M)$, and if further $\Sigma \subset S$, it may be identified with $H^1(G_{\mathbb{Q},S},M)$ as asserted in Prop. 1 above,
$H^i(\underline{X}\text{-}S,\ M)$ --for $i \geq 2$ -- is *only defined, so far* if $p \in S$, and then it is defined to be the étale cohomology group $H^i_{ét}(\underline{X}\text{-}S,\ j_*M)$.

I am thankful to Beilinson who pointed out that there is no problem in defining "good modules" $H^i(\underline{X}\text{-}S,\ M)$ in general, or at least the cases where M is given the crystalline (or ordinary) finite/singular structure at p. We will not be making any explicit use of this general definition (i.e., of $H^i(\underline{X}\text{-}S,M)$ for $i \geq 2$ when p is not in S) in these notes, but see §6 below for a sketch.

Proposition: If M is of finite type over A, the A-modules $H^i(\underline{X}\text{-}S,\ M)$ as defined above, when they are defined, are of finite type.

Proof: This is standard for the étale cohomology groups

over $\underline{X}$-S (cf. Milne, Chapter II, Thm. 3.1) so $H^i(\underline{X}\text{-}S, M)$ is of finite type over A when $p \in S$. But when $p \notin S$, $H^1(\underline{X}\text{-}S, M)$, is a submodule of the A-module of finite type $H^1(\underline{X}\text{-}(S \amalg \{p\}), M)$. Since A is noetherian $H^1(\underline{X}\text{-}S, M)$, is of finite type as well.

□

In particular, if M is finite, the groups $H^i(\underline{X}\text{-}S, M)$, when defined, are also finite.

§2. Basic exact sequences.

Let M be a sub $A[G_{\mathbb{Q}}]$-module of W or a quotient $A[G_{\mathbb{Q}}]$-module of W^*. Let $S \subset T$ be finite sets of primes. Then

$$(2) \quad 0 \to H^1(\underline{X}\text{-}S, M) \to H^1(\underline{X}\text{-}T, M) \to \prod_{\ell \in T-S} H_s^1(G_{\mathbb{Q}_\ell}, M)$$

is exact, a fact that follows immediately from the definition.

Proposition 2: For S a finite set of primes, and any exact sequence

$$0 \to W[\alpha] \to W[\alpha\beta] \to W[\beta] \to 0$$

(with $\alpha \in A$ a nonzero divisor, and $\beta \in A$) there is an associated exact sequence for "cohomology":

$$(3) \quad 0 \to W[\alpha]^{G_{\mathbb{Q}}} \to W[\alpha\beta]^{G_{\mathbb{Q}}} \to W[\beta]^{G_{\mathbb{Q}}} \to$$

$$\to H^1(\underline{X}\text{-}S, W[\alpha]) \to H^1(\underline{X}\text{-}S, W[\alpha\beta]) \to H^1(\underline{X}\text{-}S, W[\beta]).$$

obtained by pullback from the corresponding exact sequence for $G_{\mathbb{Q}}$-cohomology:

Proof: The beginning of the sequence (3) being clearly "defined" and exact, even at the "point" $W[\beta]^{G_{\mathbb{Q}}}$ of the

sequence, we may restrict our efforts to showing that the arrows of the top horizontal line of the following commutative diagram are defined, and that the top line is exact:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
W[\beta]^{G_{\mathbb{Q}}} & \to & H^1(\underline{X}\text{-}S, W[\alpha]) & \to & H^1(\underline{X}\text{-}S, W[\alpha\beta]) & \to & H^1(\underline{X}\text{-}S, W[\beta]) \\
= \downarrow & & \downarrow & & \downarrow & & \downarrow \\
W[\beta]^{G_{\mathbb{Q}}} & \to & H^1(G_{\mathbb{Q}}, W[\alpha]) & \to & H^1(G_{\mathbb{Q}}, W[\alpha\beta]) & \to & H^1(G_{\mathbb{Q}}, W[\beta]) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \Pi H_s^1(G_{\mathbb{Q}_\ell}, W[\alpha]) & \to & \Pi H_s^1(G_{\mathbb{Q}_\ell}, W[\alpha\beta]) & \to & \Pi H_s^1(G_{\mathbb{Q}_\ell}, W[\beta]).
\end{array}$$

Here the product Π occurring in the bottom line is over all prime numbers ℓ not dividing m. The vertical lines and the middle horizontal line is exact; so is the lower line (by Proposition 3 of Chapter 1). A diagram-chase gives our Proposition.

□

We also have the dual statement. For $m > 0$ an integer, and any exact sequence

$$0 \to W^*/\beta W^* \to W^*/\alpha\beta W^* \to W^*/\alpha W^* \to 0$$

(with $\alpha \in A$ a nonzero divisor, and $\beta \in A$) there is an associated exact sequence for "cohomology" obtained by pullback from the corresponding exact sequence for $G_{\mathbb{Q}}$-cohomology:

Proposition 3:

(4) $0 \to W^*/\beta W^{*G_{\mathbb{Q}}} \to W^*/\alpha\beta W^{*G_{\mathbb{Q}}} \to W^*/\alpha W^{*G_{\mathbb{Q}}} \to$
$\to H^1(\underline{X}\text{-}S, W^*/\beta W^*) \to H^1(\underline{X}\text{-}S, W^*/\alpha\beta W^*) \to$
$\to H^1(\underline{X}\text{-}S, W^*/\alpha W^*).$

Proof: The proof is almost identical to that of Proposition 2. The beginning of the sequence (4) again being clearly "defined" and exact, even at the "point" $W^*/\beta W^{*G_{\mathbb{Q}}}$ of the sequence, we may restrict our efforts to showing that the rest of the sequence is defined and exact, as in Prop. 2. But a straightforward diagram-chase with a diagram analogous to that which enters into the proof of Prop. 2, whose "bottom horizontal line" is the exact sequence

$$0 \to \Pi H_s^1(G_{\mathbb{Q}_\ell}, W^*/\beta W^*) \to \Pi H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha\beta W^*) \to$$

$$\to \Pi H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha W)$$

gives the proof.

□

§3. Recalling Global Class Field Theory, and Global Tate Duality.

Recall that $p > 2$. The fundamental facts about 2-dimensional Galois cohomology of μ_{p^∞}, which will play a dominant role in what follows are these.

The local invariant. For any prime number ℓ have a canonical isomorphism which we will call inv_ℓ

$$\begin{array}{ccc} & \text{inv}_\ell & \\ H^2(G_{\mathbb{Q}_\ell}, \mu_{p^\infty}) & \to & \mathbb{Q}_p/\mathbb{Z}_p \ ; \\ & \cong & \end{array}$$

if $h \in H^2(G_{\mathbb{Q}_\ell}, \mu_{p^\infty})$, then $\text{inv}_\ell(h)$ will be referred to as its "*(local) invariant* ".

Passage from global to local. There is an exact sequence

$$0 \to H^2(G_{\mathbb{Q}},\mu_{p^\infty}) \xrightarrow{\iota} \oplus H^2(G_{\mathbb{Q}_\ell},\mu_{p^\infty}) \xrightarrow{\Sigma} \mathbb{Q}_p/\mathbb{Z}_p \to 0\ ,$$

where ι is the direct sum of the natural restriction mapping from $G_{\mathbb{Q}}$-cohomology to $G_{\mathbb{Q}_\ell}$-cohomology, taken over all prime numbers ℓ, and where Σ is the summation of the local invariants.

In the discussion for the rest of this paragraph, let M be either an $A[G_{\mathbb{Q}}]$-submodule of W, or an $A[G_{\mathbb{Q}}]$-quotient module of W*, and M*, as usual, its Cartier dual. Until further notice S will refer to a finite set of primes containing the prime p. Define

$$(5)\quad Ш_S^i(M) = \ker\{ H^i(\underline{X}\text{-}S,M) \to \prod_{\ell\in S} H^i(G_{\mathbb{Q}_\ell},M)\}.$$

Note that, despite appearances to the contrary, $Ш_S^1(M)$ is a "contravariant functor" on the directed system of finite sets of primes S, and more specifically, if $S \subset T$, then we have a natural inclusion $Ш_T^1(M) \subset Ш_S^1(M)$. On the other hand, $Ш_S^2(M)$ is a covariant functor, and more specifically, if $S \subset T$, we have a natural surjection $Ш_S^2(M) \to Ш_T^2(M)$.

If $\mathcal{S}$ is any set of primes (possibly infinite)[2] containing p, put:

---

[2] our convention will be that script $\mathcal{S}$ refers to a possibly infinite collection of primes while Roman S refers only to finite sets of primes.

(6) $\underline{Ш}_{\mathcal{S}}^1(M) = \text{"proj. lim"}_{S \subset \mathcal{S}} \underline{Ш}_S^1(M) = \bigcap_{S \subset \mathcal{S}} \underline{Ш}_S^1(M)$

the projective limit taken over the system of all finite sets of primes S contained in $\mathcal{S}$, which can be also viewed as an intersection over all $S \subset \mathcal{S}$, where the $\underline{Ш}_S^1(M)$'s are all viewed as submodules in $H^1(G_{\mathbb{Q}},M)$. Alternatively, we may write:

(7) $\underline{Ш}_{\mathcal{S}}^1(M) = \ker \{H^1(G_{\mathbb{Q}},M) \to \prod_{\ell \in \mathcal{S}} H^1(G_{\mathbb{Q}_\ell},M) \times \prod_{\ell \notin \mathcal{S}} H_s^1(G_{\mathbb{Q}_\ell},M)\}.$

Also, for $\mathcal{S}$ any set of primes, put

(8) $\underline{Ш}_{\mathcal{S}}^2(M) = \text{"ind. lim"}_{S \subset \mathcal{S}} \underline{Ш}_S^2(M) = \bigcup_{S \subset \mathcal{S}} \underline{Ш}_S^2(M).$

Defining these groups analogously for M^*, Tate Global Duality establishes, if M and $\mathcal{S}=S$ are finite, a perfect pairing

(9) $\underline{Ш}_S^i(M) \times \underline{Ш}_S^{3-i}(M^*) \to \mathbb{Q}_p/\mathbb{Z}_p.$

(See Milne Chapter I §4), and passage to the limit yields a perfect pairing

(10) $\underline{Ш}_{\mathcal{S}}^1(M) \times \underline{Ш}_{\mathcal{S}}^2(M^*) \to \mathbb{Q}_p/\mathbb{Z}_p,$

for any set of primes $\mathcal{S}$.

If $\mathcal{S}$ is the set of all primes, abbreviate $\underline{Ш}_{\mathcal{S}}^i(M)$ as $\underline{Ш}^i(M)$, for i=1,2.

To analyze the structure of $\underline{Ш}^1(M)$ further in the case

where M is finite, let $K/\mathbb{Q}$ be the splitting field for the $G_{\mathbb{Q}}$-action on M so that we have the exact sequence $1 \to G_K \to G_{\mathbb{Q}} \to \Delta \to 1$ where Δ is a finite subgroup of $\mathrm{Aut}_A(M)$, and the action of $G_{\mathbb{Q}}$ on M is via projection to Δ. Consider the following exact sequence of A-modules obtained from the associated Hochschild-Serre Spectral Sequence:

$$(11) \qquad 0 \to H^1(\Delta, M) \to H^1(G_{\mathbb{Q}}, M) \xrightarrow{\psi} \mathrm{Hom}\,(G_K, M)^{\Delta}.$$

Note that the submodule $Ш^1(M) \subset H^1(G_{\mathbb{Q}}, M)$ maps to zero under ψ. The reason for this the following. Let $h \in Ш^1(M)$ and let $\varphi: G_K \to M$ be the Δ-invariant homomorphism $\psi(h)$. Since $h \mapsto 0$ in $H^1(G_{\mathbb{Q}_\ell}, M)$ for all ℓ, and in particular for all ℓ which are unramified in the $G_{\mathbb{Q}}$-action on M, we see that φ brings the Frobenius elements of G_K attached to all liftings of such primes ℓ to zero. But, by Cebotarev's Theorem, these Frobenius elements are topologically dense in G_K, and since φ is continuous, $\varphi = 0$. By what has just been discussed, and the duality (10) we have shown:

Proposition 4: The submodule $Ш^1(M)$ of $H^1(G_{\mathbb{Q}}, M)$ is contained in $H^1(\Delta, M) \subset H^1(G_{\mathbb{Q}}, M)$. The modules $Ш^1(M)$ and $Ш^2(M^*)$ vanish if $H^1(\Delta, M) = 0$.

§4. A lifting problem.

Let $\underline{X} = \mathrm{Spec}\,\mathbb{Z}$, and S a finite set of primes containing p. Here is the problem we wish to consider in this section. Suppose we are given an exact sequence:

$$0 \to W^*/\beta W^* \to W^*/\alpha\beta W^* \to W^*/\alpha W^* \to 0$$

with α a non-zero-divisor. Consider the mapping $H^1(\underline{X},\ W^*/\alpha\beta W^*) \to H^1(\underline{X},\ W^*/\alpha W^*)$, which is, of course, not necessarily surjective.

Is there an $S \subset \underline{X}$ *such that the image of* $H^1(\underline{X},W^*/\alpha W^*)$ *in* $H^1(\underline{X}\text{-}S,\ W^*/\alpha W^*)$ *lifts to* $H^1(\underline{X}\text{-}S,\ W^*/\alpha\beta W^*)$?

Relevant to this question is the commutative diagram:

$$\begin{array}{ccc} H^1(\underline{X},\ W^*/\alpha\beta W^*) & \to & H^1(\underline{X}\text{-}S,\ W^*/\alpha\beta W^*) \\ \downarrow & & \downarrow \\ H^1(\underline{X},\ W^*/\alpha W^*) & \to & H^1(\underline{X}\text{-}S,\ W^*/\alpha W^*) \\ \downarrow & & \downarrow \\ Ш_S^2(W^*/\beta W^*) & \to & H^2(\underline{X}\text{-}S,\ W^*/\beta W^*) \end{array} \tag{12}$$

where the right vertical sequence is simply a piece of the long exact sequence for étale cohomology, which is legitimate since S contains p. That an element of $H^1(\underline{X}\text{-}S,\ W^*/\alpha W^*)$ which is in the image of $H^1(\underline{X},\ W^*/\alpha W^*)$, when mapped to $H^2(\underline{X}\text{-}S,\ W^*/\beta W^*)$ actually lands in $Ш_S^2(W^*/\beta W^*)$ comes from the fact that the local coboundary mappings $H^1(G_{\mathbb{Q}_\ell},W^*/\alpha W^*) \to H^2(G_{\mathbb{Q}_\ell},W^*/\beta W^*)$ annihilate $H_f^1(G_{\mathbb{Q}_\ell},W^*/\alpha W^*)$, for all prime numbers ℓ (cf. Prop. 3 of §11 of Chapter 1).

Proposition 3: Suppose that $Ш^1(W[\beta])$ vanishes. Then there is a finite set S of prime numbers so that the elements of $H^1(\underline{X},W^*/\alpha W^*)$ in $H^1(\underline{X}\text{-}S,\ W^*/\alpha W^*)$ lift to $H^1(\underline{X}\text{-}S,W^*/\alpha\beta W^*)$.

Proof. This does follow directly from the above discussion concerning diagram (12), and from the perfect duality (10) of §3.

A sufficient criterion for the vanishing of $Ш^1(W[\beta])$ is given by Proposition 4 of §3; namely $Ш^1(W[\beta])=0$ if $H^1(\Delta, W[\beta])=0$, where Δ is the image of $G_{\mathbb{Q}}$ which acts faithfully on $W[\beta]$.

§5. The Bockstein pairing.

In this paragraph I would like to focus on a certain pairing which I believe will clarify a good deal of the formalism later. For reasons which will shortly become clear (I hope) it seems reasonable to call it the "Bockstein pairing" relative to (α,β).

Keep notation as in the previous paragraphs. In particular, let $\underline{X}$= Spec $\mathbb{Z}$; let α, β be elements of A with α a non-zero-divisor; and let Δ be the quotient of $G_{\mathbb{Q}}$ acting faithfully on $W[\beta]$. Let us suppose a hypothesis which we will call--

Δ-vanishing (for β) : $H^1(\Delta, W[\beta]) = 0$.

Now let $x \in H^1(\underline{X}, W[\beta])$ and $y \in H^1(\underline{X}, W^*/\alpha W^*)$. We wish to define an element which we will denote $\{x,y\}_{\alpha,\beta} \in \mathbb{Q}_p/\mathbb{Z}_p$. For this, we first define elements $\tilde{y}_\ell \in H_s^1(G_{\mathbb{Q}_\ell}, W^*/\beta W^*)$ for $\ell \in S$.

Note that our hypothesis of "Δ-vanishing" allows us to use Proposition 3 of §4. That is, there is a finite set of primes S (with $p \in S$) such that the image of y in $H^1(\underline{X}\text{-}S, W^*/\alpha W^*)$ lifts to an element $\tilde{y} \in H^1(\underline{X}\text{-}S, W^*/\alpha\beta W^*)$. For each prime number $\ell \in S$, let $\tilde{y}_\ell \in H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha\beta W^*)$ be the image of

the restriction of $\tilde{y}$ to ℓ, $\mathrm{res}_\ell \tilde{y} \in H^1(G_{\mathbb{Q}_\ell}, W^*/\alpha\beta W^*,)$ in the singular part. Recall the exact sequence (Proposition 3 of §11 of Chapter 1)

$$0 \to H_s^1(G_{\mathbb{Q}_\ell}, W^*/\beta W^*) \to H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha\beta W^*) \to$$
$$\to H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha W^*)$$

and note that since $y \in H^1(\underline{X}, W^*/\alpha W^*)$, the image of $\tilde{y}_\ell$ in $H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha W^*)$ is zero. It follows that $\tilde{y}_\ell$ lies in the submodule $H_s^1(G_{\mathbb{Q}_\ell}, W^*/\beta W^*)$ of $H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha\beta W^*)$, and from now on we will view $\tilde{y}_\ell$ as an element of $H_s^1(G_{\mathbb{Q}_\ell}, W^*/\beta W^*)$.

Now let x_ℓ denote the restriction of the class $x \in H^1(\underline{X}, W[\beta])$ to $H^1(G_{\mathbb{Q}_\ell}, W[\beta])$, and note that x_ℓ lies in $H_f^1(G_{\mathbb{Q}_\ell}, W[\beta]) \subset H^1(G_{\mathbb{Q}_\ell}, W[\beta])$. We view x_ℓ as an element of $H_f^1(G_{\mathbb{Q}_\ell}, W[\beta])$. Now we may invoke the pairing (which we will denote $\langle , \rangle_\ell$)

$$H_f^1(G_{\mathbb{Q}_\ell}, W[\beta]) \times H_s^1(G_{\mathbb{Q}_\ell}, W^*/\beta W^*) \to \mathbb{Q}_p/\mathbb{Z}_p$$

and define

$$\{x,y\}_{\alpha,\beta} = \sum_{\ell \in S} \langle x_\ell, \tilde{y}_\ell \rangle_\ell . \tag{13}$$

To see that this definition does not depend upon the lifting $\tilde{y}$, consider two such liftings, $\tilde{y}_1$ and $\tilde{y}_2$. Then the difference $\delta = \tilde{y}_1 - \tilde{y}_2$ maps to zero in $H^1(\underline{X}\text{-}S, W^*/\alpha W^*)$

and therefore comes from a class in $H^1(\underline{X}\text{-}S, W^*/\beta W^*)$ by Proposition 2 of §2. It then follows from the definitions that the difference between the computation of the right-hand side of (13) via the lifting $\tilde{y}_1$ and via $\tilde{y}_2$ is given by the sum of all local invariants of the image in the cohomology group $H^2(G_{\mathbb{Q}}, \mu_{p^\infty})$ of the cup-product of the two global cohomology classes $x \cup \delta \in H^2(\underline{X}\text{-}S, W[\beta] \otimes_{\mathbb{Z}_p} W^*/\beta W^*)$, and by "Global Class Field Theory" (cf. §3) this sum is zero. We have therefore a well-defined bilinear pairing,

$$(14) \qquad H^1(\underline{X}, W[\beta]) \times H^1(\underline{X}, W^*/\alpha W^*) \quad \rightarrow \quad \mathbb{Q}_p/\mathbb{Z}_p$$

which we will call the **Bockstein pairing** (relative to α,β). It is also evident from definition of the pairing that the image of

$$H^1(\underline{X}, W^*/\alpha\beta W^*) \quad \rightarrow \quad H^1(\underline{X}, W^*/\alpha W^*)$$

lies in the right-nullspace relative to the pairing (14).

Problems: I haven't yet worked this out, but I imagine that the definition is symmetric, and the same pairing could be defined by lifting the class $x \in H^1(X, W[\beta])$ to $H^1(X\text{-}S, W[\alpha\beta])$ and making a symmetrical construction, in which case one would also have that the image of $H^1(X, W[\alpha\beta])$ in $H^1(X, W[\beta])$ lies in the left-nullspace relative to the pairing (14) (?) What, in fact, are the precise nullspaces?

§6. Definition of $H^i(\underline{X}\text{-}S,M)$ "in general".

I am very thankful to Beilinson who suggested the definition of these cohomology modules which we will only very briefly sketch in this §. Here let us assume that $\mathfrak{M}(W)$ is given the crystalline finite/singular structure at p as in Chapter 1, §11. Let $\underline{X}$= Spec $\mathbb{Z}$, as usual, and $S \subset \underline{X}$ a finite subset, which we may as well assume *not* to contain p.

Let δ: Spec $\mathbb{Q} \to \underline{X}$-S-{p} and γ: $\underline{X}$-S-{p} $\to \underline{X}$-S and j:Spec $\mathbb{Q} \to \underline{X}$-S denote the natural (the only, in fact) open immersions. So $j = \gamma \circ \delta$.

Choose an algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$ and let $\mathbb{Q}_p{}^{nr}$ denote the maximal unramified extension of $\mathbb{Q}_p$, i.e., the field of fractions of $W(\overline{\mathbf{F}}_p)$. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p{}^{nr}$ and $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ the algebraic closure of $\mathbb{Q}$ in $\overline{\mathbb{Q}}_p$. Having made all these choices, we can identify the categories of étale sheaves over the relevant fields, with the corresponding categories of Galois modules.

Let $H^1_f(\mathbb{Q}_p{}^{nr},M)$, for $M \in \mathfrak{M}(W)$, denote the union of the images of $H^1_f(K,M)$ in $H^1(\mathbb{Q}_p{}^{nr},M)$ where K ranges through the finite extensions of $\mathbb{Q}_p$ contained in $\mathbb{Q}_p{}^{nr}$. The module $H^1_f(\mathbb{Q}_p{}^{nr},M)$ has a natural $G_{\mathbf{F}_p} = \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ action, and may be identified with a sheaf of A-modules for the étale topology over $\mathbf{F}_p$, or alternatively as a "skyscraper sheaf" supported at p on the étale topology of $\underline{X}$ = Spec $\mathbb{Z}$; it is a subsheaf of the skyscraper sheaf $R^1\gamma_*(\delta_* M)$ whose underlying $G_{\mathbf{F}_p}$-module is $H^1(\mathbb{Q}_p{}^{nr},M)$. Viewing $H^1_f(\mathbb{Q}_p{}^{nr},M)$ as such a sub-skyscraper sheaf, let us call it $R^1\gamma_*(\delta_* M)_f$.

Fixing an injective resolution $N_\cdot$ of the étale sheaf $\delta_* M$ on $\underline{X}$-S-{p} we have a complex of sheaves for the étale topology on $\underline{X}$,

$$\gamma_*(N_0) \xrightarrow{\partial_0} \gamma_*(N_1) \xrightarrow{\partial_1} \gamma_*(N_2) \to \cdots, \tag{15}$$

whose quasi-isomorphism class is independent of the choice

of injective resolution, and which represents $R\gamma_*(\delta_* M)$. We have a diagram where straight lines are exact:

$$\begin{array}{ccccccc} & & 0 & & & & \\ & & \downarrow & & & & \\ & & \text{image}(\partial_0) & & & & \\ & & \downarrow & & \partial_1 & & \\ 0 & \to & \ker(\partial_1) & \to & \gamma_*(N_1) & \to & \gamma_*(N_2) \\ & & \downarrow & & & & \\ & & R^1\gamma_*(\delta_* M) & & & & \\ & & \downarrow & & & & \\ & & 0. & & & & \end{array}$$

Defining $\gamma_*(N_1)_f \subset \gamma_*(N_1)$ to be the subsheaf given as the inverse image of $R^1\gamma_*(\delta_* M)_f \subset R^1\gamma_*(\delta_* M)$ in $\ker(\partial_1) \subset \gamma_*(N_1)$, we have a truncation of the complex (15) that we will refer to as $R\gamma_*(\delta_* M)_f$:

$$(16) \quad \gamma_*(N_0) \xrightarrow{\partial} \gamma_*(N_1)_f \, .$$

The quasi-isomorphism class of the complex $R\gamma_*(\delta_* M)_f$ is easily seen to be independent of the choice of (15) and its sheaf cohomology groups, $\mathcal{H}^\bullet(R\gamma_*(\delta_* M)_f)$, are as follows:

$$\mathcal{H}^0 = j_* M \, , \quad \mathcal{H}^1 = R^1\gamma_*(\delta_* M)_f \, , \text{ and } \mathcal{H}^j = 0 \text{ for } j \geq 2.$$

Definition: $H^i(\underline{X}\text{-}S, M) := H^i(\underline{X}\text{-}S, R\gamma_*(\delta_* M)_f)$, where $\mathbf{H}^i$ referes to the hypercohomology of the complex $R\gamma_*(\delta_* M)_f$ for the étale topology on $\underline{X}$-S .

These cohomology modules are A-modules of finite type; they fit into "long exact sequences" restricting to the exact sequences of §2 above. Beilinson has communicated to me

that for S empty one can show that cup-product,

$$\langle\ ,\ \rangle : \quad H^i(\underline{X},M) \otimes H^{3-i}(\underline{X},M^*) \to H^3(\underline{X},\mu_{p^\infty}) = \mathbb{Q}_p/\mathbb{Z}_p,$$

gives rise to a perfect three-dimensional duality pairing, and that using the above, one can obtain the Bockstein pairing without any Δ-vanishing assumption. Namely, we have a canonical pairing

$$(17) \quad \{\ ,\ \} : H^1(\underline{X},W) \otimes H^1(\underline{X},W^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \to \mathbb{Q}_p/\mathbb{Z}_p$$

defined by $\{x,y\} := \langle x,\partial y\rangle$ where

$$\partial : H^1(\underline{X},W^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(\underline{X},W^*)$$

is the coboundary mapping in the long exact sequence of cohomology coming from the short exact sequence of modules

$$0 \to W^* \to W^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to W^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \to 0\ .$$

To compare the pairing (17) to the Bockstein pairing defined in §5, let α,β be non-zero-divisors in A, and

$$x \in H^1(\underline{X},W[\alpha]) \qquad y \in H^1(\underline{X},W^*/\beta\cdot W^*).$$

Then, if the Δ-vanishing hypothesis holds for β,

$$(18) \quad \{x,y\}_{\alpha,\beta} = \{x,\ \beta^{-1}\cdot y\}$$

where the $\{\ ,\ \}_{\alpha,\beta}$ refers to the Bockstein pairing defined in §5, and the $\{\ ,\ \}$ on the right-hand side of (18) is the pairing (17) for x considered as an element of $H^1(\underline{X},W)$ and $\beta^{-1}\cdot y$ as an element of $H^1(\underline{X},W^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$.

Chapter three: The Symmetric Square of a rank two Galois representation

§1. Our basic set-up for this Chapter.

We will keep all of the notational conventions of the previous two chapters, and begin to restrict the type of $G_{\mathbb{Q}}$-modules W that we wish to consider. Recall that $p > 2$ and that the base ring of scalars A is a commutative local finite faithfully flat $\mathbb{Z}_p$-algebra. Let $m \subset A$ denote the maximal ideal, and $k = A/m$ the residue field.

Let H be a free A-module of rank 2 with continuous A-linear action of $G_{\mathbb{Q}}$, unramified outside a finite set Σ of prime numbers including p. This defines a continuous Galois representation, $\rho: G_{\mathbb{Q},\Sigma} \rightarrow GL_2(A)$, well-defined up to conjugation.

We make the following assumption about the determinant of the representation ρ.

(1) The p-cyclotomic determinant condition:

The determinant character $\det_A \rho : G_{\mathbb{Q}} \rightarrow A^*$ is the composition of the p-cyclotomic character, $\chi: G_{\mathbb{Q}} \rightarrow \mathbb{Z}_p^*$ with the natural inclusion $\mathbb{Z}_p^* \subset A^*$.

Let $T_\ell \in A$ denote the A-trace of the ℓ-Frobenius element Frob_ℓ on H, and let us call T_ℓ the ℓ-th "**Hecke operator**" in A. It follows from (1) that the action of Frob_ℓ on H satisfies the ("**Eichler-Shimura** -type") identity

$$(2) \qquad \mathrm{Frob}_\ell^2 - T_\ell \cdot \mathrm{Frob}_\ell + \ell = 0.$$

For any ideal J contained in the maximal ideal of A, let

$$\rho_J: G_{\mathbb{Q}} \rightarrow GL_2(A/J)$$

denote the reduction of ρ mod J, and let

$$\overline{\rho}: G_{\mathbb{Q}} \rightarrow GL_2(k)$$

be the reduction modulo the maximal ideal, i.e., $\overline{\rho} = \rho_m$ is the associated "residual representation".

It follows from (1) that $\overline{\rho}$ is an odd representation, i.e., that the image of a "complex conjugation" involution τ in $G_{\mathbb{Q}}$ under $\overline{\rho}$ is *not* a scalar matrix in $GL_2(k)$.

Assume that $\overline{\rho}$ is absolutely irreducible.

§2. Principal polarizations.

To give a $G_{\mathbb{Q}}$-equivariant skew-symmetric pairing

$$(3) \qquad (\ ,\ ): \ H \otimes_{\mathbb{Z}_p} H \rightarrow \mathbb{Z}_p(1)$$

with respect to which the action of A is self-dual is visibly the same as giving a $\mathbb{Z}_p[G_{\mathbb{Q}}]$-homomorphism

$$(4) \qquad \psi: \wedge_A{}^2(H) \rightarrow \mathbb{Z}_p(1).$$

It is *also* the same as giving a $\mathbb{Z}_p$-homomorphism (4) since $G_{\mathbb{Q}}$-equivariance of such a homomorphism is automatic: by the p-cyclotomic determinant condition, the action of $G_{\mathbb{Q}}$ on $\wedge_A{}^2(H)$ is via the p-cyclotomic character χ, which is precisely how $G_{\mathbb{Q}}$-acts on $\mathbb{Z}_p(1)$.

Refer to the pairing corresponding to ψ as $(\ ,\ )_\psi$.

Lemma: The following are equivalent:

i) The $G_{\mathbb{Q}}$-equivariant, A-Hermitian, skew-symmetric pairing

$$(,)_\psi : \quad H \otimes_{\mathbb{Z}_p} H \quad \to \quad \mathbb{Z}_p(1)$$

is *perfect* in the sense that the induced mapping

$$\begin{array}{lccc} \psi: & H & \to & \mathrm{Hom}_{\mathbb{Z}_p}(H, \mathbb{Z}_p(1)) \\ & m & \mapsto & [\, n \mapsto (m,n)_\psi \,] \end{array}$$

is an isomorphism of (equivalently)

a) $\mathbb{Z}_p$-modules,
b) A-modules, where $\mathrm{Hom}_{\mathbb{Z}_p}(H, \mathbb{Z}_p(1))$ is given its induced A-module structure, and of
c) $A[G_{\mathbb{Q}}]$-modules, where $\mathrm{Hom}_{\mathbb{Z}_p}(H, \mathbb{Z}_p(1))$ is given its induced $A[G_{\mathbb{Q}}]$-module structure.

ii) The A-module $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge_A{}^2(H) , \mathbb{Z}_p(1))$ is free of rank 1, generated by the element in $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge_A{}^2(H) , \mathbb{Z}_p(1))$, call it ψ_o: $\wedge_A{}^2(H) \to \mathbb{Z}_p(1)$, induced from $(,)_\psi$.

Proof: The equivalence of **a)** and **b)** in **i)** is clear and just put in for the record. That **c)** is equivalent to **b)** comes from the discussion right before the statement of the Lemma. Now suppose **i)** in the form of **c)**. We first show that $\psi_o \in \mathrm{Hom}_{\mathbb{Z}_p}(\wedge_A{}^2(H) , \mathbb{Z}_p(1))$ is a generator of the A-module $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge_A{}^2(H) , \mathbb{Z}_p(1))$. For, by Schur's Lemma (see the form of it proved in the appendix) since $\overline{\rho}$ has been assumed to be absolutely irreducible, any

$A[G_{\mathbb{Q}}]$- module homomorphism $f : H \to \mathrm{Hom}_{\mathbb{Z}_p}(H, \mathbb{Z}_p(1))$ is a scalar multiple of the $A[G_{\mathbb{Q}}]$-isomorphism ψ, i.e., there is an element $a \in A$, such that $f_o = a \cdot \psi_o$, where $f_o, \psi_o \in \mathrm{Hom}_{\mathbb{Z}_p}(\wedge_A{}^2(H), \mathbb{Z}_p(1))$ are the elements induced from f and ψ. The A-module $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge_A{}^2(H), \mathbb{Z}_p(1))$ is therefore cyclic; that it is free of rank 1 then follows from the fact that it is $\mathbb{Z}_p$-free of the same $\mathbb{Z}_p$-rank as A. Therefore **i)** implies **ii)**. To see that **ii)⇒i) b)** note that the $G_{\mathbb{Q}}$-action plays no role, so you can choose an A-basis x,y of H, and a $\mathbb{Z}_p$-generator ζ of $\mathbb{Z}_p(1)$ giving $\wedge_A{}^2(H) = x \wedge y \cdot A$, $\mathbb{Z}_p(1) = \zeta \cdot \mathbb{Z}_p$. A generator, then, ψ_o of the A-module $\mathrm{Hom}_{\mathbb{Z}_p}(\wedge_A{}^2(H), \mathbb{Z}_p(1))$ is given by $x \wedge y \cdot a \to \zeta \cdot tr\ (a)$ for $a \in A$, where $tr : A \to \mathbb{Z}_p$ is a *Gorenstein trace* for A over $\mathbb{Z}_p$, i.e., *tr* is a generator of the A-module $\mathrm{Hom}(A, \mathbb{Z}_p)$; cf. §8 below. Then the associated homomorphism ψ: $H \to \mathrm{Hom}_{\mathbb{Z}_p}(H, \mathbb{Z}_p(1))$ is seen to be

$$x \cdot A \oplus y \cdot A \ \to\ \mathrm{Hom}_{\mathbb{Z}_p}(y \cdot A, \zeta \cdot \mathbb{Z}_p) \oplus \mathrm{Hom}_{\mathbb{Z}_p}(x \cdot A, \zeta \cdot \mathbb{Z}_p)$$

$$x \cdot a + y \cdot b \ \mapsto\ a \cdot tr + b \cdot tr$$

(with the evident notational conventions) and this ψ is perfect.

□

Definition: A pairing satisfying any one of the equivalent conditions of the previous lemma is called a **principal polarization** of H. Since the only "polarizations" we consider in this course are principal, we shall drop the adjective "principal" and refer to a **principal polarization** simply as a **polarization**.

The following two Corollaries come immediately from

formulation **(ii)** of the Lemma:

Corollary 1: Let $(\ , \ )_\Psi : H \otimes_{\mathbb{Z}_p} H \ \rightarrow \ \mathbb{Z}_p(1)$ be a polarization. Then for any $G_\mathbb{Q}$-equivariant skew-linear pairing $(\ , \ )_\psi$ there is a unique element $a \in A$ such that $(x,y)_\psi = (a \cdot x, y)_\Psi$ for all $x,y \in H$.
The pairing $(\ , \ )_\psi$ is a polarization if and only if a is a unit in A ; it is a polarization if and only if ψ is a generator of the A-module $\mathrm{Hom}_{\mathbb{Z}_p[G_\mathbb{Q}]}(\wedge_A{}^2(H), \mathbb{Z}_p(1))$.

.

□

Corollary 2: The ring A is Gorenstein if and only if H admits a polarization.

□

We shall *not* be assuming the existence of a polarization, (or equivalently that A be Gorenstein) until §8 below.

§3. The symmetric square of H. Define W^* to be $\mathrm{Sym}_A{}^2(H)$ with its induced $A[G_\mathbb{Q}]$-module structure. Then W^* is a free A-module of rank three. Also, for any ideal $J \subset A$, we have that

$$W^*/J \cdot W^* \ \cong \ \mathrm{Sym}_{A/J}{}^2(H/J \cdot H)$$

is a free A/J- module of rank 3.

Lemma 1: Let $\mathrm{End}_A{}^\circ(H) = \mathrm{End}^\circ(H)$ denote the A-module of A-endomorphisms of H of trace zero. Then given a polarization $(\ , \ ) = (\ , \ )_\Psi$ of H, as in §2 above, there is a canonical isomorphism of A-modules

$$(4) \quad W \overset{\iota}{\cong} \mathrm{End}^{\circ}(H)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \subset \mathrm{Hom}_A(H, H\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)$$

$$w \longrightarrow [\, T_w : H \to H\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p) \,]$$

where, if w is an element of $W = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sym}_A{}^2(H), \mu_{p^\infty})$ and if we view w as a μ_{p^∞}-valued A-bilinear symmetric function $w(x,y)$ of "two variables" x, y on H, the transformation T_w is determined by the rule $w(x,y) = (x, T_w y)_\Psi$ where the pairing

$$(\ ,\ )_\Psi : H \times H\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Z}_p(1)\otimes\mathbb{Q}_p/\mathbb{Z}_p = \mu_{p^\infty}$$

is induced in the evident manner from the given polarization $(\ ,\ )_\Psi$. The canonical isomorphism is $G_{\mathbb{Q}}$-equivariant if we endow $\mathrm{End}^{\circ}(H)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p$ with the adjoint action induced from the $G_{\mathbb{Q}}$-module structure of H (explicitly: if $g \in G_{\mathbb{Q}}$ and $e \in \mathrm{End}^{\circ}(H)$ then:

$$\mathrm{Ad}(g)\cdot e = g\cdot e\cdot g^{-1} : H \to H\ ).$$

Proof: That the rule of passage $w \longleftrightarrow T_w$ described above gives an A-module isomorphism between A-bilinear functions of two variables $w(x,y)$ and elements $T_w \in \mathrm{Hom}_A(H, H\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)$ is straightforward, in view of the fact that our polarization gives us a perfect pairing. Let us see that the trace zero condition on T_w corresponds to the symmetry condition on w. For this, we can cheat and choose an A-basis x,y of H, a $\mathbb{Z}_p$-basis ζ of $\mathbb{Z}_p(1)$, writing T_w as a 2×2 matrix with coefficients a and d on the

diagonal, and writing the polarization Ψ as

$$\Psi: x \wedge y \cdot \alpha \mapsto \zeta \cdot tr\ (\alpha)$$

for $\alpha \in A$ and for *tr* some *Gorenstein trace* (cf. §8). Then the symmetry condition for w translates simply as the condition $(\alpha \cdot x, T_w y)_\Psi = (y, \alpha \cdot T_w x)_\Psi$ for all $\alpha \in A$, or equivalently, $tr\ (d \cdot \alpha) = -\ tr\ (a \cdot \alpha)$ for all $\alpha \in A$. Since *tr* is a Gorenstein trace, this latter condition is equivalent to requiring that a+d = 0.

□

Changing the polarization Ψ to $a \cdot \Psi$, for a unit $a \in A^*$ changes the identification ι above to $a \cdot \iota$. It will be useful in Chapter 4 to assume the existence of a polarization, to fix a polarization, and thereby identify the A-module W with $\mathrm{End}_A{}^{\circ}(H) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$.

Define $W = \mathrm{Hom}_{\mathbb{Z}_p}(W^*, \mu_{p^\infty})$, to be the Cartier dual of W^* with its induced $A[G_{\mathbb{Q}}]$-module structure, so that W and W^* are in accord with the notational conventions of the previous Chapters. For any ideal $J \subset m \subset A$, W[J] is the Cartier dual of $W^*/J \cdot W^*$, both modules given their induced $(A/J)[G_{\mathbb{Q}}]$-actions. In particular, W[m] is seen to be a 3-dimensional k-vector space, Cartier dual to W^*/mW.

We now assume that the 3-dimensional k-vector space $W^*/m \cdot W^*$ $(= \mathrm{Sym}_k{}^2 \bar{\rho})$ is **an irreducible $G_{\mathbb{Q}}$-representation**. It is equivalent to assume that W[m] be irreducible as $G_{\mathbb{Q}}$-representation.

We also assume that W is **cleanly ramified** when viewed as $A[G_{\mathbb{Q}_\ell}]$- module for all $\ell \neq p$ and we give W,

viewed as $A[G_{\mathbb{Q}_\ell}]$-module, its associated finite/singular structure at ℓ (cf. Chapter 1) for $\ell \neq p$. As for finite/singular structure at p, assume that W is crystalline when viewed as $G_{\mathbb{Q}_p}$-module, and give it its crystalline finite/singular structure (or, the relentless axiomatician may simply assume that a specific finite/singular structure has been imposed at p, whose particular properties will be irrelevant until Theorem 2 of Chapter 4). So our W has been endowed with finite/singular structures at all primes ℓ, and conforms to the running assumptions made in Chapter 1. In particular we have the machinery of global cohomology introduced in Chapter 2 which applies now to W, its submodules of the form $W[\alpha]$ for $\alpha \in A$, and for W^* and the analogous quotient modules.

Since W[m] is an irreducible 3-dimensional vector space, it has no fixed vectors under $G_{\mathbb{Q}}$ and therefore, for any finite set $S \subset \underline{X}$ (= Spec $\mathbb{Z}$), we have:

$$W^{G_{\mathbb{Q}}} = H^0(\underline{X}\text{-}S, W) = H^0(\underline{X}, W) = 0.$$

Lemma: $H^1(\underline{X}\text{-}S, W[\alpha]) = H^1(\underline{X}\text{-}S, W)[\alpha]$.

Proof: This comes from the long exact sequence of §2 of Chapter 2, and the fact that $H^0(\underline{X}, W)=0$.

§4. The singular depth at primes of type $\mathfrak{L}$.

If $J \subset m \subset A$ is an ideal, let $K_J/\mathbb{Q}$ denote the field extension which splits the representation ρ_J. So ρ_J maps $G_{\mathbb{Q}}$ onto $\mathrm{Gal}(K_J/\mathbb{Q})$ which injects to $GL_2(A/J)$. By a **"complex conjugation" involution**, call it $\tau=\tau_J$, in $\mathrm{Gal}(K_J/\mathbb{Q})$ we mean any representative of the conjugacy

class of the image of the nontrivial element of a decomposition group $Gal(\mathbb{C}/\mathbb{R})$ mapping naturally to $Gal(K_J/\mathbb{Q})$, i.e., corresponding to a complex imbedding of K_J.

Let $\mathcal{L}_J$ denote the set of prime numbers ℓ which are unramified for ρ and such that a Frobenius element $Frob_\ell$ is (contained in the $Gal(K_J/\mathbb{Q})$-conjugacy class of) the complex conjugation involution $\tau = \tau_J$. If $J_1 \subset J_2$ is an inclusion of ideals of A, both contained in the maximal ideal m, we have $\mathcal{L}_{J_1} \subset \mathcal{L}_{J_2} \subset \mathcal{L}_m$. Put $\mathcal{L} = \mathcal{L}_m$. By the Cebotarev Density Theorem, there are an infinity of primes in $\mathcal{L}_J$ for any ideal J of finite index in A.

If $\ell \in \mathcal{L}_J$ then $Frob_\ell$ satisfies the relation $Frob_\ell^2 - 1 \equiv 0$ mod J, so that (2) implies that $\ell \equiv -1$ mod J, and $T_\ell \equiv 0$ mod J. Recalling that $p > 2$, an application of Hensel's lemma gives us then that we have a factorization in A[X]:

$$(5) \qquad X^2 - T_\ell \cdot X + \ell = (X+u)\cdot(X+v)$$

for elements $u,v \in A$ with $u \equiv 1$ and $v \equiv -1$ mod J.

Lemma 2: Let $\ell \in \mathcal{L}$ and retain the notation above. We have a direct sum decomposition of the A-module

$$(6) \quad H = H_u \oplus H_v$$

where each of the A-modules H_u and H_v are free of rank 1, and $Frob_\ell$ acts as multiplication by u on H_u and multiplication by v on H_v.

Proof. Take

$H_u := (Frob_\ell - v)\cdot H$ and $H_v := (Frob_\ell - u)\cdot H$,

and note that $H_u \cap H_v = \{0\}$ since $Frob_\ell$ acts on any element in this intersection as, simultaneously, multiplication by +1 and by -1 modulo the maximal ideal (recall: $p > 2$). If $h \in H$, writing $h_u = (Frob_\ell - v)\cdot h$ and $h_v = -(Frob_\ell - u)\cdot h$, we see that $h_u + h_v = (u-v)\cdot h$ and since $u-v$ is a unit in A, we do have our direct sum decomposition $H = H_u \oplus H_v$. Neither H_u nor H_v can vanish, because if one did (say $H_u = 0$) then $Frob_\ell$ would act as multiplication by the scalar v on all of H, and hence its trace T_ℓ would be $2\cdot v$ which is not $\equiv 0$ mod m. Similarly, $2\cdot u$ is not $\equiv 0$ mod m, so H_v cannot vanish. Now, since the free rank two module H is a direct sum, $H_u \oplus H_v$ of two nonzero modules, it follows, counting dimensions over k, that $H_u \otimes_A k$ and $H_v \otimes_A k$ are both of dimension 1, and therefore, by an application of Nakayama's lemma, H_u and H_v are both cyclic A-modules. Since A is $\mathbb{Z}_p$-torsionfree, a necessary and sufficient condition for a cyclic A-module U to be free of rank one is that its tensor product $U \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ have the same dimension (as a vector space over $\mathbb{Q}_p$) as $A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ does. A simple dimension count shows that H_u and H_v satisfies this condition.

□

Lemma 3: With the above notation, if $\ell \in \mathcal{L}$, then the singular quotient at ℓ, $H_s^1(G_{\mathbb{Q}_\ell}, W^*) = H^1(I_{\mathbb{Q}_\ell}, W^*)^{G_{F_\ell}}$ is a free A-module of rank one. Moreover, for any ideal $J \subset A$, $H_s^1(G_{\mathbb{Q}_\ell}, W^*/JW^*) = H^1(I_{\mathbb{Q}_\ell}, W^*/JW^*)^{G_{F_\ell}}$ is a free A/J-module of rank one.

Proof: Since $H^1(I_{\mathbb{Q}_\ell}, W^*) = W^*(-1)$ as a Frob_ℓ-module, we use the decomposition (6) of Lemma 2 to give us a decomposition of W^* as a direct sum of three free A-modules of rank 1:

$$(7) \quad W^* = (H_u \otimes_A H_u) \oplus (H_u \otimes_A H_v) \oplus (H_v \otimes_A H_v)$$

and Frob_ℓ acts on the first as multiplication by u^2 the second as multiplication by $uv = \ell$ and the third as multiplication by v^2. It follows that it is only the second of these three factors that contribute to the Frob_ℓ-fixed space in $W^*(-1)$. The first assertion of our lemma follows. The second assertion follows from the analogous calculation made over A/J, noting that $u^2 \equiv v^2 \equiv 1 \bmod m$, and therefore that the first and third factors in (7) still fail to yield anything fixed by Frob_ℓ in $W^*/JW^*(-1)$.

If c is a cohomology class in $H^1(G_{\mathbb{Q}}, W^*)$ let $c_{s,\ell} \in H_s^1(G_{\mathbb{Q}_\ell}, W^*)$ denote the projection of $\mathrm{res}_\ell(c) \in H^1(G_{\mathbb{Q}_\ell}, W^*)$ to $H_s^1(G_{\mathbb{Q}_\ell}, W^*)$, the singular quotient.

Definition 1: If α is a nonzero-divisor in A, and ℓ is a prime number in $\mathcal{L}$ we will say that the cohomology class c has **singular depth**, at ℓ, **equal to** $\alpha \in A$ if we have isomorphisms of A-modules

$$H_s^1(G_{\mathbb{Q}_\ell}, W^*)/c_{s,\ell} \cdot A \cong A/\alpha A,$$

or, equivalently, if the annihilator of the cyclic A-module $H_s^1(G_{\mathbb{Q}_\ell}, W^*)/c_{s,\ell} \cdot A$ is equal to the ideal generated by α.

Remark: The tightness (and usefulness) of Definition 1 depends upon $H_s^1(G_{\mathbb{Q}_\ell}, W^*)$ being free of rank one over A, which, in turn, occurs (cf. Lemma 3 above) when $\ell \in \mathfrak{L}$. In particular, we have only defined the notion of "singular depth being equal to α" for primes $\ell \in \mathfrak{L}$. This is to be compared with the following looser notion, which makes sense for all prime numbers ℓ:

Definition 2: If α is a nonzero-divisor in A, and ℓ is *any* prime number we will say that the cohomology class c has **singular depth**, at ℓ, **divisible by** $\alpha \in A$ if the image of $c_{s,\ell}$ in $H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha \cdot W^*)$ vanishes.

§5. Systems of Flach type.

Keep the hypotheses and notation of §4.

If $\gamma \in A$ is a non-unit, non zero-divisor, let $K = K_\gamma$ be the splitting field of the $G_{\mathbb{Q}}$ action on $W[\gamma]$. Let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, so that the Hochschild-Serre Spectral Sequence yields an exact sequence

$$(8) \quad 0 \to H^1(\Delta, W[\gamma]) \to H^1(\underline{X}, W[\gamma]) \xrightarrow{\varphi} \mathrm{Hom}\,(G_K, W[\gamma])^\Delta,$$

and, consequently if $H^1(\Delta, W[\gamma])$ is assumed to be zero (the "Δ-vanishing hypothesis for γ" of Chapter 2) the homomorphism φ is injective, allowing us to identify $H^1(\underline{X}, W[\gamma])$ with a submodule of $\mathrm{Hom}\,(G_K, W[\gamma])^\Delta$; to any cohomology class $c \in H^1(\underline{X}, W[\gamma])$ let its image under φ be denoted φ_c, a Δ-equivariant homomorphism:

$$\varphi_c : G_K \to W[\gamma].$$

To be explicit here, the Δ-equivariance condition boils

down to the following. Since φ_c is a homomorphism to an abelian group, the homomorphism φ_c factors through the maximal abelian quotient G_K^{ab} of G_K. Let E be the fixed field of the kernel of $G_K \to G_K^{ab}$ so that $E/\mathbb{Q}$ is Galois, with Galois group fitting in the exact sequence,

$$1 \to G_K^{ab} \to \mathrm{Gal}(E/\mathbb{Q}) \to \Delta \to 1.$$

Denote the natural "conjugation-after-lifting" action of Δ on G_K^{ab} by exponentiation, i.e., the action is given by ${}^{\delta}g = \tilde{\delta}\cdot g\cdot\tilde{\delta}^{-1}$ for $\delta \in \Delta$, $g \in G_K^{ab}$, and $\tilde{\delta} \in \mathrm{Gal}(E/\mathbb{Q})$ denotes any lifting of δ.

Denote the action of Δ on $W[\gamma]$ by $\circ$, so that if $\delta \in \Delta$ and $w \in W[\gamma]$, then the action is given by $(\delta,w) \mapsto \delta\circ w$.

Then by Δ-equivariance of φ_c we have:

(9) $\varphi_c({}^{\delta}g) = \delta\circ\varphi_c(g)$.

It follows that the kernel of φ_c is stabilized by Δ. Let L/K denote the field fixed by the kernel of φ_c and $\Gamma = \mathrm{Gal}(L/K)$. The field extension $L/\mathbb{Q}$ is then a finite Galois extension, and we have the exact sequence

$$1 \to \Gamma \to \mathrm{Gal}(L/\mathbb{Q}) \to \Delta \to 1.$$

The homomorphism φ_c induces an injective homomorphism, which we again denote by $\varphi_c\colon \Gamma \to W[\gamma]$, and Δ-invariance then boils down to (9) again where now g is taken to be in Γ, and the exponential action is the evident action of Δ on Γ.

Definition: If $\alpha \in A$ is a non zero-divisor, let J denote the ideal (α) if α is not a unit, or the maximal ideal m if

α is a unit. A **Flach system of depth α** (relative to the $A[G_{\mathbb{Q}}]$-module H) is a rule which assigns to each prime number $\ell \in \mathfrak{L}$ a cohomology class $c(\ell) \in H^1(\underline{X}-\{\ell\}, W^*)$ which has singular depth α at ℓ (in the terminology of §4).

Let us assume that a Flach system of depth α, $\ell \mapsto c(\ell)$, is given. Consider the diagram

$$\begin{array}{ccc} c(\ell) & \in & H^1(\underline{X}-\{\ell\}, W^*) \\ & & \downarrow \\ H^1(\underline{X}, W^*/\alpha W^*) & \subset & H^1(\underline{X}-\{\ell\}, W^*/\alpha W^*) \end{array}$$

Lemma: For all $\ell \in \mathfrak{L}$, the image of $c(\ell)$ under the vertical mapping in the above diagram is contained in the submodule $H^1(\underline{X}, W^*/\alpha W^*) \subset H^1(\underline{X}-\{\ell\}, W^*/\alpha W^*)$.

Proof: The condition to be checked is in the singular quotient of $\mathbb{Q}_\ell$-cohomology, so let us recall the notation of §4 and pass from the above diagram to the corresponding diagram of singular quotients for $\mathbb{Q}_\ell$-cohomology,

$$\begin{array}{ccc} c(\ell)_{s,\ell} & \in & H_s^1(G_{\mathbb{Q}_\ell}, W^*) \\ & & \downarrow \\ & & H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha W^*), \end{array}$$

and note that by Lemma 3 of §4, $H_s^1(G_{\mathbb{Q}_\ell}, W^*)$ is free of rank one over A, and $H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha W^*)$ is the quotient of $H_s^1(G_{\mathbb{Q}_\ell}, W^*)$ modulo $\alpha \cdot H_s^1(G_{\mathbb{Q}_\ell}, W^*)$. Moreover, by

the defintion of "depth α", $c(\ell)_{s,\ell}$ lies in $\alpha \cdot H_s^1(G_{\mathbb{Q}_\ell}, W^*)$ so goes to zero in $H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha W^*)$.

□

Let $d(\ell) \in H^1(\underline{X}, W^*/\alpha W^*)$ be the unique class mapping to the image of the class $c(\ell)$ in $H^1(\underline{X}-\{\ell\}, W^*/\alpha W^*)$.

Define, for J and ideal in A of finite index:

(10) $\quad \Phi_J \subset H^1(\underline{X}, W^*/\alpha W^*)$

to be the sub A-module generated by the elements $d(\ell) \in H^1(\underline{X}, W^*/\alpha W^*)$ for all $\ell \in \mathfrak{L}_J$.

§6. Annihilation of cohomology.

The following theorem, up to change of language and axiomatic setting, is due to Flach, and its proof is simply copied from the proof of Proposition 1.1 of **[F]**.

Theorem 1 : We suppose our running hypotheses. We suppose that the Δ-vanishing hypothesis holds for all non zero-divisors $\gamma \in A$, i.e., $H^1(\Delta, W[\gamma]) = 0$ where Δ is as in the beginning of §5.

Then if a Flach system of depth α exists,

(11) $\quad H^1(\underline{X}, W[\alpha]) = H^1(\underline{X}, W)[\alpha] = H^1(X, W).$

Proof: The first equality is just from the lemma of §1. It is the second equality, giving that $H^1(\underline{X}, W)$ is annihilated by α that is the point of the Proposition. Let $x \in H^1(\underline{X},W)$. Since $H^1(\underline{X},W)$ is A-torsion, we may assume that x is annihilated by γ for some non zero-divisor and non-unit in A; we can (and do) fix such a γ to be a multiple of α.

By the lemma of §1, again, $x \in H^1(\underline{X},W[\gamma])$ and we must show that x is annihilated by α.

Lemma 1: If $\ell \in \mathfrak{L}$ the restriction $res_\ell(x) \in H^1(G_{\mathbb{Q}_\ell},W[\gamma])$ of the class x is annihilated by multiplication by α.

Proof: Let the image of x in $H^1(G_{\mathbb{Q}}, W[\gamma])$ be denoted $x_{\mathbb{Q}}$. Fix a prime number $\ell \in \mathfrak{L}$ and any scalar $\beta \in A$. Consider the cohomology class $\beta\cdot c(\ell) \in H^1(\underline{X}-\{\ell\}, W^*)$. let $\beta\cdot c(\ell)_{\mathbb{Q}} \in H^1(G_{\mathbb{Q}}, W^*/\gamma W^*)$ denote the image of this class after projecting the coefficient module to $W^*/\gamma W^*$, and passing to $G_{\mathbb{Q}}$-cohomology. Form the cup-product of the cohomology classes $x_{\mathbb{Q}}$ and $\beta.c(\ell)_{\mathbb{Q}}$:

$$x_{\mathbb{Q}} \cup \beta\cdot c(\ell)_{\mathbb{Q}} \quad \in \quad H^2(G_{\mathbb{Q}}, W[\gamma]\otimes_{\mathbb{Z}_p} W^*/\gamma W^*),$$

and, using the natural pairing $W[\gamma]\otimes_{\mathbb{Z}_p} W^*/\gamma W^* \to \mu_{p^\infty}$ we get a cohomology class which we will denote

$$(12) \quad x_{\mathbb{Q}} \smile \beta\cdot c(\ell)_{\mathbb{Q}} \quad \in \quad H^2(G_{\mathbb{Q}}, \mu_{p^\infty}).$$

If q is a prime number different from ℓ, then the local invariant at q of the cohomology class (12) is zero. This is because, by hypothesis and construction, the restriction of both classes $x_{\mathbb{Q}}$ and $\beta\cdot c(\ell)_{\mathbb{Q}}$ to $G_{\mathbb{Q}_q}$-cohomology lie in the *finite* parts of their respective cohomology groups and so these classes are orthogonal under cup-product. Since the sum of all the local invariants of the global cohomology class (12) is zero, we then get that the local invariant of (12) at the prime ℓ is zero, as well. In other words, the classes $res_\ell(x)$ and $\beta\cdot c(\ell)_{s,\ell}$ are mutually orthogonal in the pairing:

(13) $\quad H_f^1(G_{\mathbb{Q}_\ell}, W[\gamma]) \times H_s^1(G_{\mathbb{Q}_\ell}, W^*/\gamma W^*) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p.$

But A is Hermitian in the above pairing, and by Lemma 3 of §4, we may identify $H_s^1(G_{\mathbb{Q}_\ell}, W^*/\gamma W^*)$ with $A/\gamma A$, viewed as A module, and moreover, the identification can be made in such a way that $c(\ell)_{s,\ell}$ is identified with α. Via the duality (13) we may use the above identification to identify $H_f^1(G_{\mathbb{Q}_\ell}, W[\gamma])$ with the A-module

$$\mathrm{Hom}_{\mathbb{Z}_p}(A/\gamma A, \mathbb{Q}_p/\mathbb{Z}_p)$$

and the element $\mathrm{res}_\ell(x) \in H_f^1(G_{\mathbb{Q}_\ell}, W[\gamma])$ is identified with a "homomorphism" r: $A/\gamma A \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ such that $r(\beta\cdot\alpha)=0$. This being true for any $\beta \in A$, we have that $\alpha\cdot r=0$, i.e., $\mathrm{res}_\ell(x) \in H_f^1(G_{\mathbb{Q}_\ell}, W[\gamma])[\alpha]$.

□

Since the image of $\alpha\cdot x$ in $H_f^1(G_{\mathbb{Q}_\ell}, W[\gamma])$ is zero for all $\ell \in \mathcal{L}$, in the terminology of §3 of Chapter 2 we have that $\alpha\cdot x \in Ш_{\mathcal{S}}^1(W[\gamma])$ where $\mathcal{S}$ is the set of prime numbers $\mathcal{L}$. Since $\mathcal{L}_{(\gamma)} \subset \mathcal{L}$, we have that

$$Ш_{\mathcal{L}}^1(W[\gamma]) \subset Ш_{\mathcal{L}_{(\gamma)}}^1(W[\gamma])$$

and therefore Theorem 1 then follows from the following refinement of Prop. 4 of §3 of Chapter 2 (and the Δ-vanishing hypothesis for γ), where Δ is as defined there, or again in the discussion at the beginning of §5.

Lemma 2: $Ш_{\mathcal{S}}^1(W[\gamma]) \subset H^1(\Delta, W[\gamma])$, when $\mathcal{S}=\mathcal{L}_{(\gamma)}$.

Proof: Using the exact sequence (7) it suffices to show that if $c \in \underline{Ш}_{\mathcal{S}}^{1}(W[\gamma])$ then the Δ-invariant homomorphism $\varphi=\varphi_c: G_K \to W[\gamma]$ is zero.

Recalling the discussion at the beginning of §5, let $L/\mathbb{Q}$ be the finite Galois extension containing K, such that L is the field fixed by the kernel of φ, we have $\Gamma = Gal(L/K)$, and we denote by φ again the induced injective Δ-equivariant homomorphism $\varphi: \Gamma \to W[\gamma]$.

Choose $\tau \in Gal(L/\mathbb{Q})$ a complex conjugation. For every $g \in \Gamma = Gal(L/K)$ choose a prime number $\ell = \ell_g$ unramified for ρ such that there is a prime ν of L above $\ell = \ell_g$ in $\mathbb{Q}$ whose associated Frobenius element $Frob_{L/\mathbb{Q}}(\nu) \in Gal(L/\mathbb{Q})$ is equal to $\tau \cdot g$. Let λ be the prime of K lying under the prime ν of L. The projection of $Frob_{L/\mathbb{Q}}(\nu)$ to $Frob_{K/\mathbb{Q}}(\lambda)$ in $\Delta = Gal(K/\mathbb{Q})$ is equal to τ, and therefore the prime numbers $\ell = \ell_g$ are all in $\mathcal{L}_{(\gamma)} = \mathcal{S}$. The residue field degree of λ over ℓ is 2 (recall: τ is of order two) and therefore $Frob_{L/K}(\nu) = (\tau g)^2$. Since c is assumed to be in $\underline{Ш}_{\mathcal{S}}^{1}(W[\gamma])$, the restriction, $res_\ell(c)$, of c to $H^1(G_{\mathbb{Q}_\ell}, W[\gamma])$ vanishes. It follows that $\varphi(Frob_{L/K}(\nu)) = \varphi(\tau g \tau g) = 0$. But both $\tau g \tau = \tau g \tau^{-1}$ and g lie in Γ, and φ is a homomorphism, so therefore:

$$(14) \quad \varphi(\tau g \tau g) = \varphi(\tau g \tau^{-1}) + \varphi(g) = \varphi(^{\tau}g) + \varphi(g) = 0 \quad (g \in \Gamma).$$

Since φ is Δ-equivariant, $\varphi(^{\tau}g) = \tau \cdot \varphi(g)$, and therefore (14) gives us that the image, $\mathcal{H} = \varphi(\Gamma)$, of the homomorphism φ lies in $W[\gamma]^-$, the subspace of $W[\gamma]$ where τ acts as -1. Moreover, $\mathcal{H}$ is stable under the action of Δ.

Since γ is a non-unit in A, $W[m] \subset W[\gamma]$, and the action of

Δ stabilizes W[m]. As discussed previously, W[m], being the Cartier dual of $W^*/mW^* = \mathrm{Sym}_k^2(\overline{\rho})$ is a k-vector space of dimension 3, and is irreducible as a Δ-representation space.
To conclude the proof of Lemma 2 (and the Theorem) we must show that $\mathcal{H} = 0$. For this it suffices to show that $\mathcal{H} \cap W[m] = 0$. From the above discussion we have that $\mathcal{H} \cap W[m] \subset W[m]^-$ and since both $\mathcal{H}$ and W[m] are Δ-stable, so is $\mathcal{H} \cap W[m]$. But since $\det(\overline{\rho})$ is odd, $W[m]^-$ is a vector space of dimension 2 over k, and therefore can contain no nonzero Δ-stable sub-vector spaces. Therefore $\mathcal{H} \cap W[m] = 0$.

□

§7. Left nondegeneracy in the Bockstein pairing.

One can get a bit more out of the machinery of the proof of Theorem 1. For this, let us assume again that the Δ-vanishing hypothesis holds for all non zero-divisors $\gamma \in A$.

Now consider the Bockstein pairing relative to (α,α), denoted $\{-,-\}_{\alpha,\alpha}$, as introduced in (14) of §5 of Chapter 2:

$$(12) \qquad H^1(\underline{X}, W[\alpha]) \times H^1(\underline{X}, W^*/\alpha W^*) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

$$(x \ , \ y) \mapsto \{x,y\} = \{x,y\}_{\alpha,\alpha}$$

Suppose that we are given a Flach system of depth α, with $\Phi_{(\alpha)} \subset H^1(\underline{X}, W^*/\alpha W^*)$ the A-submodule generated by the images $d(\ell)$ of all the classes $c(\ell)$ for $\ell \in \mathfrak{L}_{(\alpha)}$. Consider the restriction of the Bockstein pairing (12) to

(15) $$H^1(\underline{X}, W[\alpha]) \times \Phi_{(\alpha)} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

$$(x \ , \ y) \mapsto \{x,y\}$$

Proposition 1: The restriction of the Bockstein pairing (15) is left-nondegenerate. That is, if $x \in H^1(\underline{X}, W[\alpha])$ has the property that $\{x,y\} = 0$ for all $y \in \Phi_{(\alpha)}$, then $x=0$. The left-nondegenerate pairing (15) induces an injection of A-modules,

(16) $$0 \rightarrow H^1(\underline{X},W) \rightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\Phi_{(\alpha)}, \mathbb{Q}_p/\mathbb{Z}_p).$$

Proof: Let $y \in \Phi$ be the image of a Flach class $c(\ell)$ for $\ell \in \mathcal{L}_{(\alpha)}$. Recall the definition of the Bockstein pairing associated to the exact sequence

$$0 \rightarrow W^*/\alpha W^* \rightarrow W^*/\alpha^2 W^* \rightarrow W^*/\alpha W^* \rightarrow 0.$$

According to the definition, we must first find a finite set S of primes such that the element $y \in H^1(\underline{X}, W^*/\alpha W^*)$ lifts to a $\tilde{y} \in H^1(\underline{X}\text{-}S, W^*/\alpha^2 W^*)$. But the Flach class itself is such a lifting, i.e., we may take $S = \{\ell\}$ and $\tilde{y} = c(\ell)$. Next we must restrict $\tilde{y}$ to the primes of S, which in our present case means ℓ, and project this restriction to the singular quotient getting an element we denote $\tilde{y}_\ell \in H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha^2 W^*)$. By Lemma 3 of §4, the $A/\alpha^2 A$-module $H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha^2 W^*)$ is free of rank one, and by the axioms for a Flach system, $\tilde{y}_\ell$ is of singular depth α, i.e., $\tilde{y}_\ell$ is a *generator* of the (free, rank one) $A/\alpha A$ - submodule

$$H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha W^*) \subset H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha^2 W^*).$$

Then, the Bockstein pairing $\{x, r\cdot y\}$ for $r \in A$ is given by

the value $\langle res_\ell(x), r\cdot\tilde{y}_\ell\rangle$ of the local pairing $\langle\ -\ ,\ -\ \rangle$:

$$H_f^1(G_{\mathbb{Q}_\ell}, W[\alpha]) \times H_s^1(G_{\mathbb{Q}_\ell}, W^*/\alpha W^*) \ \rightarrow\ \mathbb{Q}_p/\mathbb{Z}_p.$$

It follows from nondegeneracy of this pairing, that if x is an element in $H^1(\underline{X}, W[\alpha])$ which lies in the nullspace of Φ relative to the pairing (15), then $res_\ell(x)=0$ for all $\ell \in \mathcal{L}_{(\alpha)}$, i.e., $x \in Ш_{\mathcal{S}}^1(W[\alpha])$ where $\mathcal{S} = \mathcal{L}_{(\alpha)}$. Lemma 2 in the proof of Theorem 1 then allows us to conclude left-nondegeneracy of the $\{\alpha,\alpha\}$-Bockstein pairing, and, using Theorem 1 we get the stated inclusion (16), thereby concluding the proof of the present Proposition.

□

Let *length* denote the length of an A-module.

Corollary: In the above situation,

(16)

$$length\ \{H^1(\underline{X},W[\alpha])\} = length\ \{H^1(\underline{X},W)\} \ \leq\ length\ \{\Phi\}.$$

§8. Gorenstein rings and congruence elements (minimalist version).

Here we wish to review very briefly a mild modification of the notion of congruence ideal due to Andrew Wiles (exposed in his lectures at the Newton Institute, Cambridge in June 1993; see also the distributed notes of H. Lenstra).

Suppose that our commutative, local, faithfully finite flat $\mathbb{Z}_p$-algebra of scalars, A, is **Gorenstein**. If k is its residue field, we may view A as W(k)-algebra via the canonical homomorphism $W(k) \rightarrow A$ which induces the identity on

residue fields. Let us recall that A is Gorenstein if and only if these equivalent conditions hold:

(a) $\mathrm{Hom}_{\mathbb{Z}_p}(A,\mathbb{Z}_p)$ is a free A-module of rank 1.

(b) $\mathrm{Hom}_{W(k)}(A,W(k))$ is a free A-module of rank 1.

(c) $\mathrm{Hom}_A(\ A\otimes_{\mathbb{Z}_p}A,\ A)$ is a free $A\otimes_{\mathbb{Z}_p}A$-module of rank 1.

(d) $\mathrm{Hom}_A(\ A\otimes_{W(k)}A,\ A)$ is a free $A\otimes_{W(k)}A$-module of rank 1.

Some comments are in order: The "Hom's" mean module-homomorphisms over the coefficient ring which occurs in the subscript. For (c) and (d) we are viewing $A\otimes_{\mathbb{Z}_p}A$ and $A\otimes_{W(k)}A$ as A-modules by letting an element $a\in A$ act on $A\otimes_{\mathbb{Z}_p}A$ via multiplication by $1\otimes a$, and the same for $A\otimes_{W(k)}A$. The module in (c) is given its canonical $A\otimes_{\mathbb{Z}_p}A$-module structure, and the same for (d).

For B any finite flat $\mathbb{Z}_p$-algebra, let us call a **Gorenstein trace**[1] (over B) a homomorphism *tr*: $A\otimes_{\mathbb{Z}_p}B \to B$ of

---

[1] Eventually I would like to replace this section of the notes by some more elaborate discussion of the Gorenstein condition. But for now I must at least warn the reader that to use the word *trace* in the phrase *Gorenstein trace* might be misleading. The reason for possible confusion, of course, is that there is the other, more natural and more standard, trace mapping

$$\mathrm{Trace}_{A/\mathbb{Z}_p}: A \to \mathbb{Z}_p$$

whose value on $a \in A$ is simply the ordinary trace of the matrix with entries in $\mathbb{Z}_p$ obtained by multiplication by a (choosing a $\mathbb{Z}_p$-basis of A which is a free $\mathbb{Z}_p$ -module of finite rank). And these traces can be different. For example, if A is a complete intersection $A = \mathbb{Z}_p[[X_1,X_2,\ldots,X_n]]/\ (f_1,f_2,\ldots,f_n)$, (flat over $\mathbb{Z}_p$) then A possesses a *Gorenstein trace* (over $\mathbb{Z}_p$) *tr* which bears the following relation to $\mathrm{Trace}_{A/\mathbb{Z}_p}$ defined above. $\mathrm{Trace}_{A/\mathbb{Z}_p}$ is equal

B-*modules* which is an $A\otimes_{\mathbb{Z}_p}B$-generator of the (free) $A\otimes_{\mathbb{Z}_p}B$-module $\mathrm{Hom}_B(A\otimes_{\mathbb{Z}_p}B,B)$. Fix such a Gorenstein trace *tr* over A. So *tr* is an A-module homomorphism

$$tr : A\otimes_{\mathbb{Z}_p}A \to A.$$

Let $\pi: A\otimes_{\mathbb{Z}_p}A \to A$ $(a\otimes b \mapsto a\cdot b)$ denote the natural homomorphism of A-algebras.

Consider the composition

$$A \cong \mathrm{Hom}_A(A,A) \xrightarrow{\pi^t} \mathrm{Hom}_A(A\otimes_{\mathbb{Z}_p}A,A) \cong A\otimes_{\mathbb{Z}_p}A \xrightarrow{\pi} A,$$

where the isomorphism in the middle is given by sending $u \in A\otimes_{\mathbb{Z}_p}A$ to $u\cdot tr \in \mathrm{Hom}_A(A\otimes_{\mathbb{Z}_p}A,A)$, and where π^t is the "transpose" of π, i.e., the A-module homomorphism obtained by applying the functor $\mathrm{Hom}_A(-,A)$ to π. The above sequence of homomorphisms are all A-module homomorphisms, and therefore the composition, which is an A-module endomorphism of A, is given by multiplication by a unique scalar $\eta \in A$, called the **congruence element** of A. Although the congruence element η depends upon the choice of Gorenstein trace over A, the ideal that it generates does not and is called the **congruence ideal** of A.

Exercises: 1) If we perform the "identical" construction using $A\otimes_{W(k)}A$ rather than $A\otimes_{\mathbb{Z}_p}A$, we would get the *same* congruence ideal $(\eta) \subset A$.

2) The congruence element η is a non zero-divisor in A if and only if A is reduced, i.e., $A\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ is a

---

to *tr* times the image in $\mathbb{Z}_p$ of the determinant of the jacobian matrix $(\partial f_i/\partial X_j)$.

product of fields.

§9. Cohesive Flach Systems.

Up to now, in our preparatory study of Flach's method, we have formulated the notion of "**Flach System**", which represents a good deal *less* than what the constructions of Flach provide for us in some concrete instances. The point of that exercise in axiomatics, of course, was to invoke the *bare minimum* equipment needed to get the type of annihilation results obtained in the past two §'s.

But as we shall show in Parts II and III, the cohomology classes produced by Flach's construction fit together into a rather "tight structure". Specifically, Flach's construction produces what we will be calling a **Bilateral Flach Derivation** in Chapter 10. But for ease of exposition, it seems natural to pave the way for the axiomatics of Chapter 10, by first introducing an axiomatic structure weaker than the notion of **Bilateral Flach Derivation**, yet stronger than the bare notion of **Flach System**. The existence of this "intermediate structure", which we call **Cohesive Flach Systems**, is already sufficient to yield all the arithmetic applications explicitly given in these course notes.

To review our running hypotheses: The prime p is > 2. We are dealing with H a free A-module of rank two, endowed with a $A[G_{\mathbb{Q},\Sigma}]$-module structure giving rise to a representation

$$\rho: G_{\mathbb{Q},\Sigma} \rightarrow GL_2(A)$$

satisfying the p-cyclotomic determinant condition (1). We suppose that the $\mathrm{Sym}^2(\overline{\rho})$, the symmetric square of the residual representation $\overline{\rho}$ is absolutely irreducible. For

W^* and W as in §3, we have supposed the local ramification conditions at primes $\ell \in \Sigma$ as described in §3.

We now add to our running hypotheses by also assuming from now on that the Δ-vanishing hypothesis holds for all non zero-divisors $\gamma \in A$.

Definition: Let $\alpha \in A$ be a non-zero-divisor, A **Cohesive Flach System (of singular depth α)** for the $A[G_{\mathbb{Q}}]$-module H is a rule which assigns to each prime number ℓ not in Σ a cohomology class $c(\ell) \in H^1(\underline{X}-\{\ell\}, W^*)$ satisfying these properties:

1) The singular depth of $c(\ell)$ at ℓ is divisible by α for all prime numbers $\ell \notin \Sigma$ (cf. Definition 2 of §4)

[Hence, for each prime number $\ell \notin \Sigma$, the image of $c(\ell)$ in $H^1(\underline{X}-\{\ell\}, W^*/\alpha W^*)$ is equal to the image of a unique element, call it $d(\ell)$, in $H^1(\underline{X}, W^*/\alpha W^*)$]

2) For all $\ell \in \mathfrak{L}$, the singular depth of $c(\ell)$ at ℓ is equal to α (cf. Definition 1 of §4)

[Hence restricted to $\ell \in \mathfrak{L}$, $\ell \mapsto c(\ell)$ is a Flach System of singular depth α]

3) There is a unique derivation $\Theta : A \to H^1(\underline{X}, W^*/\alpha W^*)$, from the ring A to the A-module $H^1(\underline{X}, W^*/\alpha W^*)$ with the property that for each prime number $\ell \notin \Sigma$,

$$\Theta(T_\ell) = d(\ell) \in H^1(\underline{X}, W^*/\alpha W^*), \tag{17}$$

where $T_\ell \in A$ is the ℓ-th Hecke operator (cf. §1 above).

If we denote by $D: A \to \Omega_A = \Omega_{A/W(k)}$ the universal

W(k)-derivation of A into the A-module of Kahler differentials[2], then axiom 3) is equivalent to asking that there be a unique homomorphism of A-modules

$$(18) \qquad h : \Omega_A \rightarrow H^1(\underline{X}, W^*/\alpha W^*)$$

such that $h(D(T_\ell)) = d(\ell)$ for all prime numbers $\ell \notin \Sigma$.

Clearly, if we are given a Cohesive Flach System, the A-module $\Phi_{(\alpha)} \subset H^1(\underline{X}, W^*/\alpha W^*)$ (cf. §7 above) generated by the classes $d(\ell)$ for all $\ell \in \mathfrak{L}_{(\alpha)}$ is contained in the image of Ω_A under the homomorphism h. It follows that if we first use Theorem 1 to identify $H^1(\underline{X}, W)$ with $H^1(\underline{X}, W[\alpha])$, and then "pull back" the $\{\alpha,\alpha\}$-Bockstein pairing (via h) to a pairing,

$$(19) \quad H^1(\underline{X}, W) \times \Omega_A \rightarrow \mathbb{Q}_p/\mathbb{Z}_p,$$

we get left-nondegeneracy of (19), and therefore get a natural inclusion of A-modules

$$(20) \quad 0 \rightarrow H^1(\underline{X}, W) \rightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\Omega_A, \mathbb{Q}_p/\mathbb{Z}_p).$$

Corollary: Given a Cohesive Flach System (of any depth), then

$$\textit{length}\ \{H^1(\underline{X}, W)\} \leq \textit{length}\ \{\Omega_A\}.$$

---

[2] Whenever there is a choice we mean *continuous* derivations and Kahler differentials; a good reference for the theory of deriviations and differentials is Grothendieck's EGA IVa 20.3-20.5. Another source is Ch 10 in Matsumura, H. : *Commutative Algebra* W.A. Benjamin Co. New York (1970). A quick compendium, with proofs referred to Matsumura is given in Hartshorne, R.: *Algebraic Geometry* Springer (1977) II §8.

Remark: Beilinson pointed out to me that since we may multiply any Cohesive Flach System (CFS) of depth α by an non-zero-divisor $\beta \in A$, to get a CFS of depth $\alpha\beta$, it might be more natural, given a CFS of depth α, to "divide" the Θ and the h of (17) and (18) by α, i.e., to view the range cohomology group as a submodule in

$$H^1(G_{\mathbb{Q}}, W^* \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

and thereby hope to have (17) and (18) somewhat less "dependent" upon the particular CFS from which it comes.

Chapter four: The deformation theory of rank two Galois representations

§1. Our basic set-up for this Chapter.

We retain all the notation introducted in Chapter 3. Our ring of scalars A is, as usual, (commutative), complete, local, faithfully flat and finite over $\mathbb{Z}_p$ and the prime number p is > 2. We let H be an $A[G_{\mathbb{Q},\Sigma}]$-module which is free of rank two over A; H determines a homomorphism

$$\rho: G_{\mathbb{Q},\Sigma} \rightarrow \mathrm{Aut}_A(H)$$

which gives us an equivalence class of representations which we shall also denote $\rho: G_{\mathbb{Q},\Sigma} \rightarrow GL_2(A)$, and the associated residual representation we denote, as usual $\bar{\rho}$: $G_{\mathbb{Q},\Sigma} \rightarrow GL_2(k)$.

We assume that $\mathrm{Sym}^2(\bar{\rho})$ is **absolutely irreducible**, which implies that $\bar{\rho}$ is absolutely irreducible as well. We assume that the p-***cyclotomic determinant condition*** holds, i.e., that

$$\det_A(\rho) : G_{\mathbb{Q}} \rightarrow \mathbb{Z}_p^* \subset A^*$$

is given by the p-cyclotomic character $\chi: G_{\mathbb{Q}} \rightarrow \mathbb{Z}_p^*$.

Local conditions:

If $\ell \in \Sigma$ and $\ell \neq p$: Assume further that if $\ell \in \Sigma$ and $\ell \neq p$, the restriction of the representation ρ to $G_{\mathbb{Q}_\ell}$ is semi-stable, and that $\bar{\rho}$ *is* ramified.

This means, in down-to-earth terms, that if I_ℓ is an inertia group at ℓ then I_ℓ acts on H through the p-part of its tame quotient $I_\ell \rightarrow \mathbb{Z}_p(1)$, and if γ is a choice of

topological generator of $\mathbb{Z}_p(1)$, then the action of γ is given for a suitable A-basis of H by the matrix:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

In slightly less coordinate-dependent terms, note the following equivalences:

Lemma: Let $\mathcal{G}$ be a commutative noetherian local ring with residue field k. Let $\mathcal{H}$ be a free $\mathcal{G}$-module of rank two over $\mathcal{G}$, and $\gamma: \mathcal{H} \to \mathcal{H}$ an A-linear homomorphism. These conditions are equivalent:

(i) There is an $\mathcal{G}$-basis of $\mathcal{H}$ with respect to which the action of γ is given by the matrix:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

(ii) We have $(\gamma-1)^2=0$, and $\gamma\otimes k$ is *not* the identity in $\mathcal{H}\otimes_{\mathcal{G}}k$.

(iii) The image of $\gamma-1 : \mathcal{H} \to \mathcal{H}$ is equal to the $\ker(\gamma-1)$, and is a free $\mathcal{G}$-module of rank 1, sitting as a direct-summand in $\mathcal{H}$.

Proof: (iii) is equivalent to (i) which clearly implies (ii). Now assume (ii), and let $\nu=\gamma-1$, so that $\nu^2=0$ on $\mathcal{H}$. Consider the mapping

$$\mathcal{H} \to \nu\cdot\mathcal{H} \subset \mathcal{H}[\nu] \subset \mathcal{H}$$

whose composition gives $\nu: \mathcal{H} \to \mathcal{H}$. Since $\nu\otimes_{\mathcal{G}}k$ is nonzero, we have that the inclusion $\mathcal{H}[\nu] \subset \mathcal{H}$ induces a nontrivial homomorphism $\mathcal{H}[\nu]\otimes_{\mathcal{G}}k \to \mathcal{H}\otimes_{\mathcal{G}}k$, and so we can find an

element x in $\mathcal{H}[\nu] \subset \mathcal{H}$ which reduces nontrivially in $\mathcal{H} \otimes_{\mathcal{O}} k$. By Nakayama's lemma (and the fact that $\mathcal{H}$ is free of rank 2 over $\mathcal{O}$) we can find a element y in $\mathcal{H}$ such that x,y is a free $\mathcal{O}$-basis for $\mathcal{H}$. The matrix for ν in terms of the basis x,y is then

$$\begin{bmatrix} 0 & u \\ 0 & v \end{bmatrix},$$

where $u \cdot v = 0$, $v^2 = 0$, and u and v are not both in the maximal ideal of $\mathcal{O}$. It follows that u is a unit, and consequently $v = 0$. Changing x to $u \cdot x$, we have found a basis for which the matrix for γ is:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

□

If $\ell = p$: Assume that the restriction of the representation ρ to $G_{\mathbb{Q}_p}$ is "Barsotti-Tate" in the usual sense that it is isomorphic to a $G_{\mathbb{Q}_p}$-representation (of dimension $2 \cdot [A:\mathbb{Z}_p]$) coming from a Barsotti-Tate group over Spec $\mathbb{Z}_p$.

§2. The deformation theory for $\bar{\rho}$. Let us make a choice of residual representation

(1) $\quad \bar{\rho}: G_{\mathbb{Q},\Sigma} \to GL_2(k),$

(as homomorphism, rather than just conjugacy class of homomorphisms). We wish to make use of a bit of the deformation theory developed last semester. By a **deformation** of $\bar{\rho}$ to a noetherian complete local ring $\mathcal{O}$

with residue field equal to k we mean a lifting of the homomorphism (1) to a **strict equivalence class of homomorphisms**,

(2) $\rho_{\mathcal{O}}: G_{\mathbb{Q},\Sigma} \to GL_2(\mathcal{O})$,

(two homomorphisms being **strictly equivalent** if they can be conjugated one to another by an element in $GL_2(\mathcal{O})$ which reduces to the identity in $GL_2(k)$). It is convenient to "choose" a representative homomorphism $\rho_{\mathcal{O}}$ in each deformation class and to make the minor abuse of language of referring to the homomorphism $\rho_{\mathcal{O}}$ "as the deformation class" but we will try not to allow any confusion to result, and in any event will explicitly signal whether it is the deformation class, or a particular homomorphism in it, that is being discussed.

Let $R^{univ}(\bar{\rho})$ stand for the complete local noetherian ring with residue field k which is the "universal deformation ring" for the residual representation (1). This exists since $\bar{\rho}$ has been assumed to be absolutely irreducible. Let R denote the "somewhat less universal" deformation ring which classifies deformations of $\bar{\rho}$ to complete local noetherian rings $\mathcal{O}$ with residue field k which have the property that

(3) (i) p-**cyclotomic determinant condition.** The determinant $\det_{\mathcal{O}}(\rho_{\mathcal{O}}) : G_{\mathbb{Q}} \to \mathcal{O}^*$ is the composition of the p-cyclotomic character $\chi: G_{\mathbb{Q}} \to \mathbb{Z}_p^*$ with the natural homomorphism from $\mathbb{Z}_p^*$ to $\mathcal{O}^*$,

(ii) **Local conditions away from p.** The representation $\rho_{\mathcal{O}}$ is (unramified outside Σ, and)

semi-stable at primes $\ell \in \Sigma$ with $\ell \neq p$,

(iii) **Local condition at p.** The representation ρ_G is "pro-finite flat" (meaning that for all finite artinian quotients, G_o of G, the induced representations ρ_{G_o} satisfies the finite flat local condition at p).

That this deformation problem is actually representable with the subtle finite flatness condition at p is a result of Ramakrishna ([R])[1].

If G is $\mathbb{Z}_p$-torsion free, condition (iii) is equivalent to asking that ρ_G be "Barsotti-Tate" ( ).

Universality of the ring R means that we have a representation

(4) $\rho_R: G_{\mathbb{Q},\Sigma} \to GL_2(R)$,

satisfying the conditions of (3), determined up to conjugation by an element of $GL_2(R)$ which reduces to the identity in $GL_2(k)$, such that if we are given any deformation (2) of (1) satisfying (3) there is a unique W(k)-homomorphism $R \to G$ such that ρ_G is induced from ρ_R.

Now choose any finite set of primes S and consider the "less restricted" problem of classifying deformations of $\bar{\rho}$ which satisfy the same determinant condition as (3i) above, and which are required to have all of the local behavior required in (3ii) and (3 iii) above for all primes ℓ

[1] This theory was explained last term; cf. e.g. [M] for the general theory related to R^{univ}. The ring R is a quotient of R^{univ} as will be shown in the next Lemma.

which are not in S, but we impose *no conditions* at ℓ, for $\ell \in S$. Call R_S the complete local noetherian ring with residue field k which classifies this problem, and $\rho_{R_S}: G_{\mathbb{Q}} \to GL_2(R_S)$ the "universal deformation" for this problem. So ρ_{R_S} is unramified outside $\Sigma \cup S$; ρ_{R_S} satisfies the local conditions (3ii) and/or (3iii) on the complement of $\Sigma \cap S$ in Σ; and there are no a priori local requirements for ρ_{R_S} on the complement of $\Sigma \cap S$ in S. We have $R = R_{\varnothing}$, and for inclusions $S \subset T$ we have natural mappings $R_T \to R_S$.

Lemma: The mappings $R_T \to R_S$ are surjections.

Proof: Let $S \subset T$ be an inclusion, with T a finite set of prime numbers. Let $\mathcal{R} \subset R_S$ be the image of R_T, and let $\rho_{\mathcal{R}}$ be the deformation of $\bar{\rho}$ to $\mathcal{R}$ induced from the deformation ρ_{R_T} via the surjection $R_T \to \mathcal{R}$. The deformation

$$\rho_{\mathcal{R}}: G_{\mathbb{Q},\, S \cup \Sigma} \to GL_2(\mathcal{R})$$

has the property that extending scalars from $\mathcal{R}$ to R_S the induced deformation is equal to ρ_{R_S}. We wish to show that the representation $\rho_{\mathcal{R}}$ satisfies the local conditions (3ii) and/or (3iii) at prime numbers ℓ in the complement of $\Sigma \cap S$ in Σ. For then, the representation $\rho_{\mathcal{R}}$ would satisfy all the requisite properties for it to be "classified" by the universal deformation ρ_{R_S}, giving us a ring-homomorphism $R_S \to \mathcal{R}$ whose composition with the inclusion $\mathcal{R} \subset R_S$ gives the identity automorphism of R_S; in other words, giving that $\mathcal{R} = R_S$.

For this, first consider the case of a prime number $\ell \neq p$ in the complement of $\Sigma \cap S$ in Σ. Then we must show that if $N = \mathcal{R} \times \mathcal{R}$ is the free $\mathcal{R}$-module of rank two endowed with $G_{\mathbb{Q}}$-action via the homomorphism $\rho_{\mathcal{R}}: G_{\mathbb{Q},\Sigma \cup S} \to GL_2(\mathcal{R})$, and if $\gamma \in \mathbb{Z}_p(1)$ is a topological generator, we must show that $(\gamma-1)$ satisfies any of the three equivalent conditions of the Lemma of §1, for $\mathcal{G}=\mathcal{R}$, and $\mathcal{H}=N=\mathcal{R}\times\mathcal{R}$. But if we extend scalars $M = N \otimes_{\mathcal{R}} R_S$ we do have condition (ii) of the Lemma of §1 for $\mathcal{G}=R_S$, and $\mathcal{H}=M$, i.e., $(\gamma-1)^2=0$ and $(\gamma-1)$ is not the identity after tensoring with k. Since $N \subset M$ and $M \otimes_{R_S} k = N \otimes_{\mathcal{R}} k$, condition (ii) persists for $\mathcal{G}=\mathcal{R}$ and $\mathcal{H}=N$.

□

Next, suppose that p is in the complement of $\Sigma \cap S$ in Σ. We must show that $\rho_{\mathcal{R}}$ satisfies the (pro-) finite flat condition at p. But we know that ρ_{R_S} does. What we want, then, follows from the fact that if $\mathfrak{M}$ is a $G_{\mathbb{Q}_p}$-representation "attached to" a finite flat group scheme $\tilde{\mathfrak{M}}$ over $\mathrm{Spec}(\mathbb{Z}_p)$, and if $\mathfrak{N} \subset \mathfrak{M}$ is a sub-module which is stable under the $G_{\mathbb{Q}_p}$-action, then $\mathfrak{N}$ is "attached to" a finite flat subgroup scheme $\tilde{\mathfrak{N}} \subset \tilde{\mathfrak{M}}$ over $\mathrm{Spec}(\mathbb{Z}_p)$. Here the phrase "attached to" means: is the natural Galois representation on $\bar{\mathbb{Q}}_p$-rational points; e.g., $\mathfrak{M} = \tilde{\mathfrak{M}}(\bar{\mathbb{Q}}_p)$. The subgroup scheme $\tilde{\mathfrak{N}}$ is given be the Zariski closure of $\mathfrak{N}$, viewed as a subgroup scheme of the generic fiber, in $\tilde{\mathfrak{M}}$.

□

Until further notice, the only deformational problems related to $\bar{\rho}$ that we will consider in this course are the problems classified by the rings R_S, and so we will just refer to R_S as the **universal ring (relative to S)**.

Since the deformation $\rho: G_{\mathbb{Q},\Sigma} \to GL_2(A)$ of §1 satisfies all the requirements of the classfication problem solved by the ring R (and a fortiori by the rings R_S) we have a canonical W(k)-homomorphism $\pi: R \to A$ coming from the universal property satisfied by the ring R. This π is the unique W(k)-homomorphism which brings the universal representation ρ_R to ρ. Denote by $\pi_S: R_S \to A$ the composition of π with the natural homomorphism $R_S \to R$. It will be useful at times to view A as R-algebra (and as R_S-algebra) via the structure homomorphism π (and π_S).

§3. The deformation-theoretic interpretation of the cohomology of $\mathrm{End}_A^{\circ}(H) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

In this section it is convenient, but probably not necessary, to assume that A is Gorenstein. By the Corollary of §2 of Chapter 3, it is equivalent to assuming that H have a polarization. Fix, then, a polarization Ψ of H. We get, by Lemma 1 of §3 of Chapter 3, a canonical identification of $A[G_{\mathbb{Q}}]$-modules

$$\iota$$

$$(5) \quad W \cong \mathrm{End}_A^{\circ}(H) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p,$$

where End° refers to endomorphisms of trace zero, and W is the Cartier dual of W^* which is defined to be $\mathrm{Sym}_A^2(H)$ as in Chapter 3.

In view of the local conditions satisfied by H, the $A[G_{\mathbb{Q}}]$-module W is cleanly ramified at each $\ell \neq p$ and is crystalline at p since the functor Sym_A^2 preserves crystalline representations ( ). We impose, at each prime number ℓ, the standard finite/singular structure

on W, as described in Chapter 1.

If $\mathcal{R}$ is a complete noetherian local ring with residue field k denote by $\Omega_{\mathcal{R}} = \Omega_{\mathcal{R}/W(k)}$ the $\mathcal{R}$-module of Kahler differentials. We now turn to a result, which in the generality we state it is due to Wiles :

Theorem 2. Let $S \subset \underline{X}$ be a finite set of primes. There is a canonical isomorphism of A-modules

$$(6)\quad H^1(\underline{X}\text{-}S,\, W) \xrightarrow{\lambda}_{\cong} \mathrm{Hom}_A(\, \Omega_{R_S} \otimes_{R_S} A,\, A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p).$$

Comments . We defer the proof of Theorem 2 to §4, and §5. If S contains Σ, this is a fairly standard deformation-theoretic identification. For variants, see [M-T]. If S contains p, then it is also an essentially elementary exercise; see §4 below. The subtle part of Theorem 2 (due to Wiles) comes in the case when S does not contain p; see §5 below. In this case we are really dealing with the finite flatness condition at p that we have imposed on the deformation problem, i.e., we are using the theory of Ramakrishna **[R]** cited previously, and (for the first time in the course!) we really must come to grips with the imposed *crystalline* finite/singular structure at p.

Changing the polarization Ψ to $a \cdot \Psi$ with $a \in A^*$ changes the isomorphism λ of the Theorem to $a \cdot \lambda$.

Corollary: We have a "canonical" isomorphism of A-modules

$$(7)\quad H^1(\underline{X}\text{-}S,\, W) \xrightarrow{\xi}_{\cong} \mathrm{Hom}_{\mathbb{Z}_p}(\, \Omega_{R_S} \otimes_{R_S} A\, ,\, \mathbb{Q}_p/\mathbb{Z}_p\,).$$

Remark: The quotation marks around the word

"canonical" is just to remind us that ξ will turn out to depend on a choice of polarization, *and* a choice of Gorenstein trace as will be clear in the proof below.

Proof of the Corollary: This turns on the following fact. Fix a Gorenstein trace over $\mathbb{Z}_p$, $tr : A \to \mathbb{Z}_p$, and let tr again denote the induced homomorphism $tr \otimes 1$: $A \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}_p/\mathbb{Z}_p$. Now,

Lemma. Let M be an A-module of finite type. Then the homomorphism

$$\begin{array}{ccccc} \mathrm{Hom}_A(M\ ,\ A\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p\ ) & \to & \mathrm{Hom}_{\mathbb{Z}_p}(M\ ,\mathbb{Q}_p/\mathbb{Z}_p\ ) \\ \varphi & \mapsto & tr\ \circ\ \varphi \end{array}$$

is an isomorphism of A-modules (call it the *trace* isomorphism).

Proof: Resolve M by free A-modules of finite rank,

$$(8) \qquad A^r \xrightarrow{T} A^s \to M \to 0,$$

so that M is finitely presented by the s × r matrix T, with entries in A. Applying $\mathrm{Hom}_A(\ -,\ A\otimes\mathbb{Q}_p/\mathbb{Z}_p)$ to (8) gives us an exact sequence,

$$0\to \mathrm{Hom}_A(M,A\otimes\mathbb{Q}_p/\mathbb{Z}_p)\to \mathrm{Hom}_A(A^s,A\otimes\mathbb{Q}_p/\mathbb{Z}_p)\to \mathrm{Hom}_A(A^r,A\otimes\mathbb{Q}_p/\mathbb{Z}_p)$$

which we can "evaluate" as

$$(9)\ 0 \to \mathrm{Hom}_A(M,A\otimes\mathbb{Q}_p/\mathbb{Z}_p) \to A^s\otimes\mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{T^t\otimes 1} A^r\otimes\mathbb{Q}_p/\mathbb{Z}_p,$$

where T^t is the transpose r × s matrix to T. On the other

hand, applying $\mathrm{Hom}_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(-, \mathbb{Q}_p/\mathbb{Z}_p)$ to (8) gives us an exact sequence of A-modules,

$$0 \to \mathrm{Hom}(M,\mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Hom}(A^s,\mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Hom}(A^r,\mathbb{Q}_p/\mathbb{Z}_p)\ ,$$

which can be identified with

(10)

$$0 \to \mathrm{Hom}(M,\mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Hom}(A,\mathbb{Z}_p)^s \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{T^t \otimes 1} \mathrm{Hom}(A,\mathbb{Z}_p)^r \otimes \mathbb{Q}_p/\mathbb{Z}_p,$$

where T^t is, again, the transpose to T, operating as indicated.

We may now assemble (9) and (10) into a commutative diagram,

$$\begin{array}{ccccc} 0 \to \mathrm{Hom}_A(M, A\otimes\mathbb{Q}_p/\mathbb{Z}_p) & \to & A^s\otimes\mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{T^t\otimes 1} & A^r\otimes\mathbb{Q}_p/\mathbb{Z}_p, \\ \downarrow & & \downarrow & & \downarrow \\ 0 \to \mathrm{Hom}(M,\mathbb{Q}_p/\mathbb{Z}_p) & \to & \mathrm{Hom}(A,\mathbb{Z}_p)^s\otimes\mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{T^t\otimes 1} & \mathrm{Hom}(A,\mathbb{Z}_p)^r\otimes\mathbb{Q}_p/\mathbb{Z}_p \end{array}$$

where the vertical arrows are all induced by the Gorenstein trace *tr* (i.e., the left-most arrow as described in the statement of our Lemma, the middle arrow given by

$$(a_1,a_2,\ldots,a_s) \otimes b \mapsto (a_1 \cdot tr\ , a_2 \cdot tr\ , \ldots, a_s \cdot tr\ ) \otimes b.$$

Since the two right vertical arrows are isomorphisms of A-modules, so is the left-most, giving our Lemma. Composing the mapping λ of the Theorem with the trace isomorphism

of the Lemma gives the isomorphism ξ, and our Corollary. Note that ξ depends on *both* the choice of a polarization and of a Gorenstein trace.
□

§4. Beginning the proof of Theorem 2.

We begin with a standard isomorphism in the deformation theory of Galois representations:

Proposition 1. Let S be a finite set of primes containing Σ, and let $J \subset A$ be an ideal. There is a canonical isomorphism,

$$H^1(G_{\mathbb{Q},S}, \mathrm{End}_A{}^{\circ}(H/J\cdot H)) \xrightarrow{\kappa} \mathrm{Hom}_A(\Omega_{R_S}\otimes_{R_S} A, A/J).$$

Proof: Let $\rho: G_{\mathbb{Q},S} \to \mathrm{Aut}_A(H)$ be our initial representation. Form the A-algebra $\tilde{A} = A \oplus \varepsilon\cdot A/J$, where $\varepsilon^2 = 0$, so that we have the canonically split extension

$$0 \to \varepsilon\cdot A/J \to \tilde{A} \xrightarrow{\upsilon} A \to 0,$$

and form

$$\tilde{H} = H\otimes_A \tilde{A} = H \oplus \varepsilon\cdot H/J\cdot H$$

so that we have an exact sequence

$$1 \to 1 + \varepsilon\cdot\mathrm{End}(H/J\cdot H) \to \mathrm{Aut}_{\tilde{A}}(\tilde{H}) \to \mathrm{Aut}_A(H) \to 1$$

with a canonical splitting,

$$\mathrm{Aut}_{\tilde{A}}(\tilde{H}) = \mathrm{Aut}_A(H) \cdot (1 + \varepsilon \cdot \mathrm{End}(H/J \cdot H)).$$

Given $x \in H^1(G_{\mathbb{Q},S}, \mathrm{End}_A{}^{\circ}(H/J \cdot H))$ we wish to define $\kappa(x)$. Let

$$c: G_{\mathbb{Q},S} \to \mathrm{End}_A{}^{\circ}(H/J \cdot H)$$

be a 1-cocycle representing x.

Define $\rho_c(g) = \rho(g) \cdot (1+\varepsilon \cdot c(g))$, which is a representation lifting ρ, unramified outside S, and such that

$$\det\rho_c(g) = \det\rho(g) \cdot (1+\varepsilon \cdot \mathrm{trace}(c(g))) = \det(\rho(g)),$$

the latter equality since c(g) has trace zero. It follows that ρ_c satisfies the p-cyclotomic determinant condition because ρ does, and therefore ρ_c satisfies all the requirements necessary for it to be "classified " by R_S, i.e., there is a canonical homomorphism, $\pi_c: R_S \to \tilde{A}$ giving rise to ρ_c. The homomorphism π_c, dependent only on the strict equivalence class of ρ_c is therefore *independent of the choice of* 1-cocycle c representing the cohomology class x, for if c' is a 1-cocycle representing the same cohomology class x as c , write $c' = c+\delta(\omega)$ where $\omega \in \mathrm{End}_A{}^{\circ}(H/J \cdot H)$ is viewed as "0-cocycle" and δ is the coboundary. Then $\rho_{c'}$ is directly seen to be equal ρ_c conjugated by the element $1+\varepsilon \cdot \omega$ in the kernel of $\mathrm{Aut}_{\tilde{A}}(\tilde{H}) \to \mathrm{Aut}_A(H)$ } (and conversely: if $\tilde{\rho}$ is the conjugate of ρ_c by such an element $1+\varepsilon \cdot \omega$, then $\tilde{\rho} = \rho_{c'}$ where $c' = c+\delta(\omega)$). With this understanding, we can relabel our homomorphism π_c as $\pi_x: R_S \to \tilde{A}$ since the choice of 1-cocycle c no longer enters into the game.

This discussion yields the commutative diagram below, which will still take some explaining:
(11)

$$
\begin{array}{ccccc}
0 & & & & 0 \\
\downarrow & & & & \downarrow \\
\mathfrak{J} & \to & \mathfrak{J}\,\hat{\otimes}_{R_S}A & \to & \varepsilon\cdot A/J \\
\downarrow & & \downarrow & & \downarrow \\
 & 1\otimes\pi_S & & \pi_x\otimes 1 & \\
R_S\hat{\otimes}_{W(k)}R_S & \to & R_S\hat{\otimes}_{W(k)}A & \to & \tilde{A} \\
\downarrow\ \delta_{R_S} & & \downarrow \delta_A\circ(\pi_S\otimes 1) & & \downarrow \nu \\
R_S & \to & A & = & A \\
\downarrow & \pi_S & \downarrow & & \\
0 & & 0 & &
\end{array}
$$

The $\hat{\otimes}$ are completed tensor products; if $\mathfrak{R}$ is a complete noetherian local W(k)-algebra, the mapping $\delta_{\mathfrak{R}}$: $\mathfrak{R}\hat{\otimes}_{W(k)}\mathfrak{R} \to \mathfrak{R}$ is the natural product homomorphism; the mapping labelled $\pi_x\otimes 1$: $R_S\hat{\otimes}_{W(k)}A \to \tilde{A}$ is viewed as A-algebra homomorphism (where, of course, $R_S\hat{\otimes}_{W(k)}A$ gets its A-algebra structure by the operation on the right).; the ideal $\mathfrak{J}$ is simply the kernel of δ_{R_S}, and we view $\mathfrak{J}$ as R_S-module, via the action on the right; viewing A as R_S-algebra via the structural homomorphism π_S allows us to form the completed tensor product $\mathfrak{J}\,\hat{\otimes}_{R_S}A$. The vertical sequences are exact, and we may view the middle vertical sequence as arising from applying $\hat{\otimes}_{R_S}A$ to the left-most veritical sequence. "Dividing by $\mathfrak{J}^2$" in the

top horizontal line of (11) gives us a diagram

$$
\begin{array}{ccccc}
\mathfrak{I}/\mathfrak{I}^2 & \rightarrow & \mathfrak{I}/\mathfrak{I}^2 \otimes_{R_S} A & \rightarrow & \varepsilon\cdot A/J \\
\downarrow = & & \downarrow = & & \downarrow \cong \\
\Omega_{R_S} & \rightarrow & \Omega_{R_S}\otimes_{R_S} A & \rightarrow & A/J\,. \\
 & & & & \kappa(x)
\end{array}
\tag{12}
$$

The homomorphism of A-modules $\kappa(x)$ that we want to define is then given by the indicated arrow in (12).

To go the other way, begin by noting that any A-module homomorphism κ: $\Omega_{R_S}\otimes_{R_S} A \rightarrow A/J$ defines, threading backwards through diagram (12), a canonical R_S-module homomorphism

$$u_\kappa : \mathfrak{I} \rightarrow \mathfrak{I}/\mathfrak{I}^2 \rightarrow \varepsilon\cdot A/J.$$

Now note that the (right) R_S-algebra $R_S\hat{\otimes}_{W(k)}R_S$ admits a natural splitting,

$$R_S\hat{\otimes}_{W(k)}R_S = R_S \oplus \mathfrak{I}.$$

Using this splitting we can define an R_S-algebra homomorphism $v_\kappa : R_S\hat{\otimes}_{W(k)}R_S \rightarrow \tilde{A}$ (where $R_S\hat{\otimes}_{W(k)}R_S$ is given its right R_S-algebra structure. and $\tilde{A}$ obtains its R_S-algebra structure via the composition of π_S: $R_S \rightarrow A$ with the natural A-algebra structure of $\tilde{A}$) by defining v_κ on $\mathfrak{I}$ to be u_κ and on R_S to be π_S. Restrict v_κ, now, to the (left) $R_S = R_S\otimes 1$ in $R_S\hat{\otimes}_{W(k)}R_S$ to give us a homomorphism, which we will call $\pi_\kappa : R_S \rightarrow$

$\tilde{A}$. This homomorphism induces a deformation ρ_K of ρ to $\tilde{A}$ (induced from the given "universal" deformation to R_S). Taking ρ_K to be represented by a given homomorphism,

$$\rho_K : G_{\mathbb{Q},\Sigma} \to GL(\tilde{H})$$

we can then obtain a 1-cocycle c_K by inverting the procedure of the beginning of this proof, i.e., define c_K by the formula

$$\rho_K(g) = \rho(g)\cdot(1+\varepsilon\cdot c_K(g))$$

and denote its corresponding cohomology class

$$x(\kappa) \in H^1(G_{\mathbb{Q},S}, \mathrm{End}_A{}^{\circ}(H/J\cdot H)).$$

One checks directly that $x \mapsto \kappa(x)$ and $\kappa \mapsto x(\kappa)$ are two-sided inverses.

□

Corollary. Let S be a finite set of primes containing Σ. There is a canonical isomorphism,

$$H^1(\underline{X}\text{-}S, W) \xrightarrow{\lambda_S} \mathrm{Hom}_A(\Omega_{R_S}\otimes_{R_S} A, A\otimes\mathbb{Q}_p/\mathbb{Z}_p),$$
$$\cong$$

(to be given explicitly in the proof below).

Proof. Taking J to be the ideal generated by p^ν (ν=1,2,...) in Proposition 1, gives us isomorphisms

$$H^1(G_{\mathbb{Q},S}, \mathrm{End}_A{}^{\circ}(H/p^\nu H)) \xrightarrow{\kappa_\nu} \mathrm{Hom}_A(\Omega_{R_S}\otimes_{R_S} A, A/p^\nu A)$$
$$\cong$$

and "compiling" these isomorphisms via the natural mappings

$\mathrm{End}_A{}^{\circ}(H/p^{\nu}H) \to \mathrm{End}_A{}^{\circ}(H/p^{\nu+1}H)$ and $A/p^{\nu}A \to A/p^{\nu}A$

both given by multiplication by p, and noting:

$$H^1(G_{\mathbb{Q},S}, \mathrm{End}_A{}^{\circ}(H)\otimes\mathbb{Q}_p/\mathbb{Z}_p) = \text{ind. lim. } H^1(G_{\mathbb{Q},S}, \mathrm{End}_A{}^{\circ}(H/p^{\nu}H))$$
$$\nu \to \infty$$

$$\mathrm{Hom}_A(\Omega_{R_S}\otimes_{R_S}A, A/p^{\nu}A) = \text{ind. lim. } \mathrm{Hom}_A(\Omega_{R_S}\otimes_{R_S}A, A/p^{\nu}A)$$
$$\nu \to \infty$$

gives the isomorphism

$$H^1(G_{\mathbb{Q},S}, \mathrm{End}_A{}^{\circ}(H)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{K} \mathrm{Hom}_A(\Omega_{R_S}\otimes_{R_S}A, A\otimes\mathbb{Q}_p/\mathbb{Z}_p).$$
$$\cong$$

Finally, making the identification (5) gives an isomorphism

$$H^1(\underline{X}\text{-}S, W) \xrightarrow{\lambda_S} \mathrm{Hom}_A(\Omega_{R_S}\otimes_{R_S}A, A\otimes\mathbb{Q}_p/\mathbb{Z}_p).$$
$$\cong$$

□

Theorem 2 will then follow from:

Proposition 2. Let S be any finite set of primes. Let $\tilde{S} = S\cup\Sigma$. There is an isomorphism of A-modules, λ_S, fitting into the commutative diagram,

$$
\begin{array}{ccc}
 & \lambda_S & \\
H^1(\underline{X}\text{-}S,\, W) & \to & \mathrm{Hom}_A(\,\Omega_{R_S}\otimes_{R_S} A,\; A\otimes\mathbb{Q}_p/\mathbb{Z}_p) \\
 & \cong & \\
\downarrow & & \downarrow \\
 & \lambda_{\tilde{S}} & \\
H^1(\underline{X}\text{-}\tilde{S},\, W) & \to & \mathrm{Hom}_A(\,\Omega_{R_{\tilde{S}}}\otimes_{R_{\tilde{S}}} A,\; A\otimes\mathbb{Q}_p/\mathbb{Z}_p), \\
 & \cong &
\end{array}
$$

where the vertical arrows are (the natural) inclusions, and where $\lambda_{\tilde{S}}$ is the isomorphism given to us by the previous Corollary.

Proof: The left-hand vertial mapping is injective as follows directly from our definition of the cohomology groups. The previous Corollary does indeed give us the isomorphism $\lambda_{\tilde{S}}$ since $\tilde{S}$ contains Σ. The right-hand vertical morphism is indeed injective, as follows from the Lemma of §2. What remains be checked is most conveniently expressed using some of the notation from the proof of Proposition 1. Specifically, for any ideal J of finite index in m $\subset$A, and any class,

$$x \in H^1(\underline{X}\text{-}\tilde{S},\; \mathrm{End}_A{}^{\circ}(H/JH))$$

we must show that x lies in $H^1(\underline{X}\text{-}S,\, \mathrm{End}_A{}^{\circ}(H/JH))$ if and only if the representation ρ_c (for one choice of cocycle c representing x, or equivalently, for all choices) satisfies the local conditions (3ii) and/or (3iii) for each $\ell \in S\cap\Sigma$. Considering these conditions, one prime number at a time, this discussion has shown that it suffices to prove:

Lemma: Let S be a finite set of primes, ℓ a prime number not in S, J an ideal of finite index in m $\subset$A, x

an element in the A-module $H^1(\underline{X}\text{-}S\cup\{\ell\}, \mathrm{End}_A{}^{\circ}(H/JH))$, c a 1-cocycle representing x, ρ_c as in the proof of Proposition 1.
Then x lies in the A submodule $H^1(\underline{X}\text{-}S, \mathrm{End}_A{}^{\circ}(H/JH))$ if and only if ρ_c satisfies (3ii) if $\ell \neq p$, and (3iii) if $\ell = p$.

Proof:

Let us first consider the case $\ell \neq p$. By the defining property of 1-dimensional cohomology over X-S, the class x lies in the submodule $H^1(\underline{X}\text{-}S, \mathrm{End}_A{}^{\circ}(H/JH))$ if and only if its restriction to ℓ, $\mathrm{res}_\ell(x)$ goes to zero in the singular quotient,

$H_s{}^1(G_{\mathbb{Q}_\ell}, \mathrm{End}_A{}^{\circ}(H/JH)) = H^1(I_{\mathbb{Q}_\ell}, \mathrm{End}_A{}^{\circ}(H/JH))^{G_{\mathbf{F}_\ell}}$. At this point it is important to specifically fix an imbedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_\ell$ so as to have a fixed imbedding $I_{\mathbb{Q}_\ell} \subset G_{\mathbb{Q}_\ell} \subset G_{\mathbb{Q}}$ in mind. Having done this, then we can find a representative 1-cocycle c for x which, when restricted to $I_{\mathbb{Q}_\ell}$ vanishes. Then the representation $\rho_c(g) = \rho(g)\cdot(1+\varepsilon\cdot c(g))$ is evidently semi-stable at ℓ, since ρ is. Going the other way, we choose $\gamma \in I_{\mathbb{Q}_\ell}$ mapping to a topological generator of $\mathbb{Z}_p(1)$ (cf. notation as in Chapter 1), and fix a basis for H so that $\rho(\gamma)$ is given by the matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Writing $c(\gamma)$ as a matrix (entries in A/J)

$$\begin{bmatrix} r & s \\ u & v \end{bmatrix},$$

with r+v =0, we now consider what conditions the entries of the matrix $c(\gamma)$ must satisfy in order for

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1+\varepsilon\cdot r & \varepsilon\cdot s\\ \varepsilon\cdot u & 1+\varepsilon\cdot v\end{bmatrix} = \begin{bmatrix}1+\varepsilon\cdot(r+u) & 1+\varepsilon\cdot(v+s)\\ \varepsilon\cdot u & 1+\varepsilon\cdot v\end{bmatrix}$$

to be unipotent. Since the trace must be 2, we have $u=0$, and therefore, since the eigenvalues must "both" be 1, we get $r=v=0$
as well, leaving us with a matrix for $c(\gamma)$ of the form

$$\begin{bmatrix}0 & s\\ 0 & 0\end{bmatrix},$$

but letting c_o denote the coboundary of the "0-cocycle"

$$\begin{bmatrix}0 & 0\\ 0 & s\end{bmatrix},$$

we have $c_o(\gamma) = c(\gamma)$, i.e., $res_\ell(c)$ projects to zero in

$$H_s^1(G_{\mathbb{Q}_\ell}, End_A{}^o(H/JH)) = H^1(I_{\mathbb{Q}_\ell}, End_A{}^o(H/JH))^{G_{\mathbf{F}_\ell}}$$ as was to be shown.

§5. **The case $\ell=p$.** We now consider the case $\ell=p$, this being the first time that we must consider, in its particularities, the finite/singular structure at p.....

****** (to be written)**********

Chapter five. Deformation-theoretic implications of the existence of Flach Systems, and of Cohesive Flach Systems

§1. Our basic set-up for this Chapter.

Let A, ρ, $\bar{\rho}$, H, W^*, W, etc. be as in §1. Fix a polarization Ψ of H. Assume that A is Gorenstein, and fix $tr : A \to \mathbb{Z}_p$, a Gorenstein trace. Let η be the associated congruence element of A. Assume that η is a non-zero-divisor of A (equivalently, $A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a product of fields). Assume the Δ-hypothesis for all non-zero-divisors $\gamma \in A$.

Let R be the universal ring for $\bar{\rho}$, as in §2 above (relative to S= the empty set of primes). We have the homomorphism of rings π: R $\to$ A. **Assume that π is surjective**. This would be the case, for example, if A were generated as $\mathbb{Z}_p$-algebra by the Hecke operators T_ℓ for all $\ell \notin \Sigma$.

§2. Consequences of the existence of a Flach System.

Now assume that **we have a Flach System $\ell \mapsto c(\ell)$ of depth α** for W as in Chapter 2, where ℓ ranges through prime numbers in $\mathcal{L}$, and where the notation is from §4, §5 of Chapter 2. For $\ell \in \mathcal{L}$, we have denoted $d(\ell) \in H^1(\underline{X}, W^*/\alpha W^*)$ to be the "image" of the class $c(\ell)$, and $\Phi \subset H^1(\underline{X}, W^*/\alpha W^*)$ the A-submodule generated by the $d(\ell)$'s for $\ell \in \mathcal{L}$. Applying Proposition 1 of §7 of Chapter 2, we have that the (α,α)-Bockstein pairing restricted on the right to $\Phi_{(\alpha)}$,

$$H^1(\underline{X}, W[\alpha]) \times \Phi_{(\alpha)} \to \mathbb{Q}_p/\mathbb{Z}_p$$

is left-nondegenerate, and by Theorem 1 of Chapter 3, §6, we have that

$$H^1(\underline{X}, W[\alpha]) = H^1(\underline{X}, W).$$

Putting this together with the Corollary to Theorem 2 of §3 in Chapter 4, applied in the case when S is empty, we have that the $\{\alpha,\alpha\}$ Bockstein pairing restricted on the right to $\Phi_{(\alpha)}$ can be viewed as giving a pairing,

$$(1) \quad \mathrm{Hom}_{\mathbb{Z}_p}(\Omega_R \otimes_R A, \mathbb{Q}_p/\mathbb{Z}_p) \times \Phi_{(\alpha)} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

which is nondegenerate on the left, and with respect to which A is Hermitian.

Thus, given a Flach system of depth α, we have (by left-nondegeneracy of (1)) a natural injection

(2)

$$0 \rightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\Omega_R \otimes_R A, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\Phi_{(\alpha)}, \mathbb{Q}_p/\mathbb{Z}_p),$$

and, passing to Pontrjagin duals, a natural surjection,

$$(3) \quad \Phi_{(\alpha)} \rightarrow \Omega_R \otimes_R A \rightarrow 0$$

of A-modules.

Corllary 1: The length of $\Omega_R \otimes_R A$ is finite, and less than or equal to the length of $\Phi_{(\alpha)}$.

Corollary 2: If the depth α of the Flach system is a unit in A, then $R = A = W(k)$.

Proof: For then $\Omega_R \otimes_R A$ vanishes and therefore so does Ω_R and therefore the Zariski tangent space of R vanishes

as well. Nakayama's lemma gives surjectivity of $W(k) \to R$; but the injection $W(k) \to A$ factors through the surjection $R \to A$; in a word, we have the equalities of the Corollary.

□

Corollary 3 : Spec $(A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ is open in Spec $(R \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$.

Proof: Let $\mathcal{K} = W(k) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, the field of fractions of $W(k)$; let $\mathcal{G} = A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, which, by our assumptions is a product of (finite) field extensions of $\mathcal{K}$. Let $\mathcal{R} = R \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We have the surjection of $\mathcal{K}$-algebras induced by π, $\Pi: \mathcal{R} \to \mathcal{G}$. Let $\hat{\mathcal{G}}$ denote the semi-local $\mathcal{K}$-algebra which is the completion of $\mathcal{R}$ with respect to the ideal $\ker(\Pi)$. Since $\Omega_R \otimes_R A$ is of finite length over $W(k)$, the $\mathcal{K}$-vector space $\Omega_R \otimes_R A \otimes_{W(k)} \mathcal{K}$ vanishes, and since

$$\Omega_{\hat{\mathcal{G}}/\mathcal{K}} \otimes_{\mathcal{R}} \mathcal{G} = \Omega_{\mathcal{R}/\mathcal{K}} \otimes_{\mathcal{R}} \mathcal{G} = \Omega_R \otimes_R A \otimes_{W(k)} \mathcal{K},$$

we have that $\Omega_{\hat{\mathcal{G}}/\mathcal{K}} \otimes_{\mathcal{R}} \mathcal{G}$ vanishes and hence (by a application of Nakayama's lemma to the semi-local complete ring $\hat{\mathcal{G}}$) we have that $\Omega_{\hat{\mathcal{G}}/\mathcal{K}}$ vanishes as well, giving that $\hat{\mathcal{G}} = \mathcal{G}$ and giving, therefore, the conclusion of our Corollary.

□

§3. Preliminary consequences of the existence of a Cohesive Flach System.

Suppose that the hypotheses of §5 are in force, and beyond that let us (suppose that there exists, and) fix a

Cohesive Flach System for the $A[G_{\mathbb{Q}}]$-module H, as in §9 of Chapter 3, of depth $\alpha = \eta$, where η is a congruence element for the Gorenstein ring A.

Combining the injective homomorphism (20) of §9 of Chapter three (dependent, of course, on the Cohesive Flach System):

$$(4)\quad 0 \to H^1(\underline{X},W) \to \mathrm{Hom}_{\mathbb{Z}_p}(\Omega_A, \mathbb{Q}_p/\mathbb{Z}_p),$$

and the identification

$$(5)\quad \mathrm{Hom}_{\mathbb{Z}_p}(\Omega_R \otimes_R A, \mathbb{Q}_p/\mathbb{Z}_p) \cong H^1(X,W)$$

of the Corollary to Theorem 2 of §3 of Chapter four (dependent upon a choice of principal polarization of H and of Gorenstein trace for A) we get, after passing to Pontrjagin duals, a natural surjection of A-modules:

$$(6)\quad \Omega_A \to \Omega_R \otimes_R A \to 0,$$

this surjection being dependent upon the hypothesized Cohesive Flach System, and the choices enumerated above.

Let us also recall the surjection (3) (but here with $\alpha = \eta$):

$$(7)\quad \Phi_{(\eta)} \to \Omega_R \otimes_R A \to 0,$$

and the natural surjection

$$(8)\quad \Omega_R \otimes_R A \to \Omega_A \to 0$$

(stemming from our hypothesis that $\pi: R \to A$ be surjective).

Combining, now,

(**a**) the three surjections (6), (7), (8), and

(**b**) the inclusions $\Phi_{(\alpha)} \subset h(\Omega_A) \subset H^1(\underline{X}, W^*/\eta W^*)$,

we deduce that all three surjections in (**a**) above are isomorphisms of A-modules, and that the homomorphism $h: \Omega_A \to H^1(\underline{X}, W^*/\eta W^*)$ is an isomorphism of Ω_A onto the submodule $\Phi_{(\eta)}$. To record some of this:

Corollary 1: The (surjective) homomorphism $\pi: R \to A$ induces an isomorphism of A-modules

$$\Omega_R \otimes_R A \xrightarrow{\cong} \Omega_A.$$

□

Definition: Given a surjective homomorphism of noetherian local rings, $f: B \to A$, with the property that the induced mapping of A-modules $\Omega_B \otimes_B A \to \Omega_A$ is an isomorphism, we shall say that f (or B) is an **evolution**[1] of A.

So Corollary 1 can be rephrased as saying that the universal deformation ring R is an "evolution" of A. For an analysis of this notion of "evolution", see §4 below.

Corollary 2: In the above situation, the homomorphism

$$h : \Omega_A \to H^1(\underline{X}, W^*/\alpha W^*)$$

is injective.

---

[1] The motivation for the term is just that, thinking of Spec A as a closed subscheme of Spec B, the larger scheme Spec B possesses no new infinitesimal directions that can be seen from the vantage-point of Spec A, i.e., whatever "growth" occurs, going from the smaller scheme to the larger, follows in already set-down directions: it is an "evolution". I am thankful to David Eisenbud for pointing out that this notion occurs in the papers of (See [ ], for example) where the property in question is called "differentially basic".

□

In a certain context, below, where A is Gorenstein we will construct Flach Systems of depth α equal to η, a congruence element of A. Given such a Cohesive Flach System, some questions come to mind:

1) Is the homomorphism $h : \Omega_A \rightarrow H^1(\underline{X}, W^*/\alpha W^*)$ an isomorphism?

2) Composing the isomorphisms (6) and (8) we get A-module isomorphism $U: \Omega_A \rightarrow \Omega_A$. It doesn't quite (yet) make sense to ask: What is U? This is because the pairing $\langle\ ,\ \rangle$ depends upon a choice of polarization, a choice of Gorenstein trace, to say nothing of a choice of Cohesive Flach System. Any change of the first two choices entails modification by multiplication by a unit of A. Also, since the depth of a Cohesive Flach System is fixed to be η, one can still modify the System by multiplication by any unit in A. Nevertheless it still makes sense to ask: Is U given by multiplication by a unit in A?

§4. Evolutions (minimalist version)

Let A be a (commutative, faithfully finite, flat, local) W(k)-algebra such that $A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a product of fields, where k is the residue field of A. Recall from §3 above that an **evolution** $f: B \rightarrow A$ is a surjective homomorphism of complete (noetherian) local rings with the property that the induced homomorphism of A-modules, $df: \Omega_B \otimes_B A \rightarrow \Omega_A$, is an isomorphism.

I am thankful to Hendrik Lenstra for enlightening discussions on the topic of evolutions (and on other topics), and for conveying to me the Lemma below which provides a necessary and sufficient condition for the ring

A to admit no nontrivial evolutions:

Let $P = W(k)[[X_1,...,X_n]]$ be a power series ring in n variables over W(k); let $(*)\ 0 \to I \to P \to A \to 0$ be a presentation of A; and let U denote the kernel of the induced homomorphism $\Omega_P \otimes_P A \to \Omega_A$. We have a natural surjection of A-modules $v: I/I^2 \to U$.

Lemma (Lenstra): These are equivalent:

1) A admits no nontrivial evolutions.

2) The induced homomorphism $v \otimes k: (I/I^2) \otimes_A k \to U \otimes_A k$ is an isomorphism (for one, and equivalently for all presentations $(*)$)

3) the dimension of the k-vector space $(I/I^2) \otimes_A k$ is less than or equal to the dimension of $U \otimes_A k$ (for one, and equivalently for all presentations $(*)$).

Definition: If the ring A possesses the (equivalent) properties above, we will say that A is **evolutionarily stable**.

Proof of the Lemma: 3) $\Leftrightarrow$ 2): For $v \otimes k$ is surjective.

2) $\Rightarrow$ 1): Let $B \to A$ be an evolution, and we can suppose that B is presented by P as well, giving a diagram:

$$\begin{array}{ccccccccc} 0 & \to & J & \to & P & \to & B & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & I & \to & P & \to & A & \to & 0 \end{array}$$

and

$$\begin{array}{ccccc} J/J^2 & \to & \Omega_P \otimes_P A & \to & \Omega_B \otimes_B A \to 0 \\ \downarrow & & \downarrow = & & \downarrow = \\ I/I^2 & \to & \Omega_P \otimes_P A & \to & \Omega_A \to 0, \end{array}$$

so that the composition $J/J^2 \to I/I^2 \to U$ is surjective. Tensoring with k, we deduce, from 2), that

$$(J/J^2) \otimes_A k \to (I/I^2) \otimes_A k$$

is surjective, and therefore, by Nakayama, so is $J \to I$.

1) $\Rightarrow$ 2): Let $\mathfrak{N} \subset (I/I^2) \otimes_A k$ be a k-subspace complementary to the kernel of $\nu \otimes k$: $(I/I^2) \otimes_A k \to U \otimes_A k$, and let $\overline{\varphi}_1, \ldots, \overline{\varphi}_r \in \mathfrak{N}$ be a k-basis. Lift the $\overline{\varphi}_j$'s to elements φ_j in I, and letting $J = (\varphi_1, \ldots, \varphi_r)$ be the sub-ideal in I of P that they generate, I guess it is clear that B=P/J is a nontrivial evolution of A. □

Corollary: If the W(k)-algebra A, satisfying the properties above, is a complete intersection, then A is evolutionarily stable.

Remark: In a forthcoming article written jointly with David Eisenbud, the following result will be shown :

Proposition: Let A be local with residue field equal to k, which is reduced, Gorenstein, finite flat over W(k), *and* which has imbedding dimension ≤ 3 over W(k) (i.e., the relative Zariski tangent space of A is of dimension ≤ 3 over k, or equivalently, the W(k)-algebra A admits a surjective W(k)-algebra homomorphism from the power series ring in three variables over W(k)).

Then A is evolutionarily stable.

□

A corollary of the above Proposition is

Corollary: Let A be local with residue field equal to k, which is reduced, Gorenstein, finite flat over W(k), *and* which has W(k)-rank ≤ 4.
Then A is evolutionarily stable.

□

Problem: Find any example of a local ring A which is reduced and finite flat over W(k)-- and which is either Gorenstein or not-- which admits a nontrivial evolution.

We still lack any such example!

Side comments concerning the cotangent complex: It is natural to try to gain some perspective on the notion of *evolutions* by appealing to the theory of the cotangent complex (**[I]** Illusie, L.: Complexe Cotangent et Déformations I Lecture Notes in Mathematics 239 Springer-Verlag (1971)). In **[I]** a functor $B \mapsto L_{B/C}$ is constructed from (commutative) C-algebras B to simplicial B-modules $L_{B/C}$ (this simplicial B-module being taken only up to quasi-isomorphism, and called the **cotangent complex attached to** B/C). There is a canonical isomorphism of B-modules $H_0(L_{B/C}) \cong \Omega_{B/C}$. Given a homomorphism of W(k)-algebras $R \to A$, one gets from the functorial construction of the cotangent complex an induced homomorphism of simplical A-modules,

$$(9) \qquad L_{R/W(k)} \otimes_R A \to L_{A/W(k)}$$

such that the induced homomorphism on *homology in degree zero* gives the functorial homomorphism of A-modules,

$$(10) \qquad \Omega_R \otimes_R A \to \Omega_A.$$

If the homomorphism (9) of simplicial A-modules is a *quasi-isomorphism*, then it follows from **[I]** III 1.2.5.1

and III 3.1) that $R \to A$ would be étale, and in our situation ($R \to A$ a surjective homomorphism of complete noetherian local rings) $R \to A$ would then be an isomorphism. What axiomatics, if any, would refine the homomorphism (6) to produce a homomorphism of simplicial A-modules $L_{A/W(k)} \to L_{R/W(k)} \otimes_R A$ whose induced homomorphism on homology in degree zero yields (6)?

§5. Criteria for universality.

In this § we give some sufficient conditions for the representation ρ to be a "universal" deformation of $\bar{\rho}$ in the sense of §2 above (i.e., satisfying the conditions (3) there). Actually, as Kazhdan mentioned, one would prefer to have *necessary and* sufficient conditions...

For clarity of the statement of the "criterion" below, we include explicit mention in its text of *all* of our "running hypotheses" along with the specific hypotheses we need for this particular Proposition.

Proposition: (a criterion for a representation to be "universal")

1) The context. Let $p > 2$. Let

$$\bar{\rho}: G_{\mathbb{Q},\Sigma} \to GL_2(k)$$

be a residual representation such that $\mathrm{Sym}^2(\bar{\rho})$ is absolutely irreducible, and which is (unramified for prime numbers $\ell \notin \Sigma$, and) semi-stably ramified, but *actually ramified* , for all $\ell \in \Sigma$ such that $\ell \neq p$, and which is finite flat at p. Suppose that ρ is a deformation of $\bar{\rho}$ to a local ring A with residue field equal to k, and which is a reduced finite flat W(k)-algebra. Let H (=A×A) denote the free rank two $A[G_{\mathbb{Q}}]$-module given by the representation

ρ, and suppose H is endowed with a (principal) polarization (and therefore A is Gorenstein). We shall make use of the notation W^*, W with their usual definitions. Suppose that ρ, W, A have the following properties:

2) Conditions on ρ: The deformation ρ satisfies the p-cyclotomic determinant condition; it is (unramified for $\ell \notin \Sigma$, and) semi-stably ramified for $\ell \in \Sigma$, $\ell \neq p$; and it is Barsotti-Tate at p.

3) Conditions on W: The Δ-vanishing hypothesis holds for all non-zero-divisors of A.

4) Conditions on the deformation of ρ **to** A: We suppose that A is generated by all the Hecke operators T_ℓ for $\ell \notin \Sigma$, and that a Cohesive Flach System exists for the $A[G_{\mathbb{Q}}]$-module H.

5) Conditions on A: We suppose that A admits no nontrivial evolutions, i.e., that A is "evolutionarily stable".

Conclusion: The deformation ρ of $\bar{\rho}$ to A is the *universal deformation of* $\bar{\rho}$ ("universal" in the sense of §2). Equivalently: The mapping $\pi: R \to A$ determined by the deformation ρ is an isomorphism.

Proof: Since A is generated by the Hecke operators T_ℓ for $\ell \notin \Sigma$, the mapping $\pi: R \to A$ is surjective. Our other hypotheses then allow us to apply Corollary 1 of §3, giving that $\pi: R \to A$ is an evolution, and therefore an isomorphism by virtue of the condition we imposed on A.

□

Let us signal the conclusion above by the simple phrase : "**ρ is universal**". Assume that we are given a ρ as in the

context **1)** above and assume that conditions **2), 3), 4),** are satisfied but not (yet) that the mysterious condition **5)** holds.

Corollary 1 (Wiles[2]): Under the above assumptions **1) -4),** if A is a complete intersection, then "ρ is universal".

Proof: Using the Corollary of §4, we have condition **5)** when A is a complete intersection.

□

Corollary 2: Under the above assumptions 1) -4), if the W(k)-algebra A has imbedding dimension ≤ 3 (or if A has W(k) rank ≤ 4) then "ρ is universal".

Proof: This follows from the result with Eisenbud quoted in §4.

□

But, this Chapter and our axiomatic study has gone on, perhaps, too long! In the second half of the course we will study Flach's construction (of "Flach Systems").

---

[2] This result (in its essence, with minor differences, perhaps, in language and setting) is a consequence of one of the results Andrew Wiles covered in his Princeton course (Spring, 94): Under the hypothesis that A be a complete intersection, Wiles **also** discussed universality of ρ for cases of "raised level" when $\bar{\rho}$ can no longer be assumed to be "cleanly ramified".

Appendix A. Schur's lemma for complete local noetherian rings.

Let Π be a profinite group and $\rho: \Pi \to GL_N(R)$ any continuous homomorphism where R is a complete local ring with residue field k. Let $C(\rho) \subset GL_N(R)$ be the subgroup of matrices in $GL_N(R)$ commuting with the image of ρ. Then if the residual representation $\bar{\rho}: \Pi \to GL_N(k)$ obtained from ρ is absolutely irreducible, the group $C(\rho)$ is the subgroup of scalar matrices in $GL_N(R)$.

Proof: It suffices to prove this for artinian local rings A, for one then gets the full result by passage to a projective limit. So let R = A be an artinian local ring with residue field k. Our proof will go by induction on the length of A, noting that when A=k, this is indeed one of the classical versions of Schur's lemma. We therefore are led to consider a small extension,

$$0 \to I \to A \to A_0 \to 0$$

where I is a principal ideal (τ) annihilated by m_A and assume we are given $\rho: \Pi \to GL_N(A)$, a continuous homomorphism which is residually absolutely irreducible, and denoting by $\rho_0: \Pi \to GL_N(A_0)$ the representation induced from ρ we may assume, by induction, that $C(\rho_0) \subset GL_N(A_0)$ consists of scalar matrices. Now take an element $c \in GL_n(A)$ which commutes with $\rho(\Pi)$. By our inductive assumption, c projects to a scalar matrix in $GL_N(A_0)$. Modifying c by an appropriate scalar matrix in $GL_N(A)$ we may assume that it reduces to the identity matrix in $GL_N(A_0)$. Since the kernel of $GL_N(A) \to GL_N(A_0)$ consists of matrices of the form $I + \tau \cdot M_N(A)$ and since τ is annihilated by m_A, c may be written as $I+\tau \cdot S$ for a matrix $S \in M_N(A)$, and the image $\bar{S} \in M_N(k)$ is uniquely determined by c. Moreover, we may write $c = I+\tau \cdot S'$ for any S'

ϵ $M_N(A)$ with $\overline{S}' = \overline{S}$. Since c commutes with $\rho(\Pi)$, the matrix $\overline{S}$ commutes with $\overline{\rho}(\Pi)$, and therefore, by the classical Schur's lemma again, $\overline{S}$ is a scalar matrix in $M_N(k)$, hence so is c.

□

Part II : Constructions

Chapter six. Cohomological Preliminaries

Reference text: **[Milne 2]** Milne, J.S.: Étale cohomology Princteon Univ. Press (1980)

§1. Cohomological purity and its immediate consequences.

In this section let S denote an irreducible base scheme, which will eventually restricted to being the spectrum of a field or a discrete valuation ring. Let V be an irreducible smooth S-scheme. Let $Z \subset V$ be a smooth S-subscheme closed in V of codimension c. In the terminology we used on Monday, (Z,V) is a **smooth** pair over S. By a **morphism of smooth pairs** over S we mean a morphism $\varphi: (Z',V') \to (Z,V)$ such that (both (Z',V') and (Z,V) are smooth pairs, and) Z' is the *scheme-theoretic* fiber product $Z' = Z \times_V V'$. Let (Z,V) be a smooth pair over S, and set U = V-Z, giving us a diagram:

$$\begin{array}{ccccc} & \overset{i}{} & & \overset{j}{} & \\ Z & \hookrightarrow & V & \hookleftarrow & U \\ & \searrow & \downarrow & \swarrow & \\ & & S\,. & & \end{array}$$

Let F be a locally constant torsion sheaf for the étale topology on V annihilated by an integer n which is relatively prime to all the characteristics of the closed points of S. [From Monday's lecture, we have the theorem of cohomological purity-- cf. **[Milne** 2: Ch. VI §5 Thm 5.1; §6 Thm 6.1] --namely we can "evaluate" the

sheaves $\underline{H}^r_Z(V,F)$ for the étale topology on Z as follows:]

Theorem:

$$\underline{H}^r_Z(V,F) = 0 \text{ if } r \neq 2c, \quad \text{and}$$

$$\underline{H}^{2c}_Z(V,F) \cong i_*F(-c),$$

the isomorphism being canonical.

Consequences:

1) (Global cohomology with support) Since we have, "in general", a Spectral sequence:

$$H^r(Z, \underline{H}^s_Z(V,F)) \Rightarrow H^{r+s}_Z(V,F),$$

we get for our smooth pair (Z,V):

Corollary 1: There is a canonical isomorphism

$$H^r(Z,F(-c)) \cong H^{r+2c}_Z(V,F)$$

(called the "Gysin isomorphism", and given by cupping with the fundamental class).

□

Corollary 2: $H^r_Z(V,F) = 0$ if $r < 2c$.

□

Corollary 3: If S is the Spectrum of a field K and $Z = z$ is the Spectrum of a field extension L/K, then

$$H^r{}_z(V,F) \cong H^{r-2c}(G_L,F(-c)).$$

□

Let us also record that, in the above context, if $\hat{V}$ denotes the completion of V at z, we have

$$H^r_Z(V,F) \cong H^r_Z(\hat{V},F) \cong H^{r-2c}(G_L,F(-c)).$$

Applying the functor $Ext^r_V(-,F)$ to the exact sequence of sheaves on V

$$0 \to j_!j^*\mathbb{Z} \to \mathbb{Z} \to i_*i^*\mathbb{Z} \to 0$$

gives us a long exact sequence:

$$(1) \ldots \to H^r_Z(V,F) \to H^r(V,F) \to H^r(U,F) \to H^{r+1}_Z(V,F) \to \ldots$$

and replacing the term $H^r_Z(V,F)$ by its image under the Gysin isomorphism gives us (the "Gysin" sequence)

Corollary 4: In the above context we have a natural long exact sequence

$$\ldots \to H^{r-2c}(Z,F(-c)) \to H^r(V,F) \to H^r(U,F) \to H^{r+1-2c}(Z,F(-c)) \to \ldots$$

§2. The fundamental class.

The theory of the "canonical class" goes hand-in-hand with the isomorphism of sheaves given in the statement of the purity theorem of §1. Specifically, let Λ denote $\mathbb{Z}_p$ for p a prime not equal to any of the residual characteristics of the residue fields of S, and when we want specifically to emphasize that we are viewing Λ as constant sheaf on any of the schemes involved we may denote it $\underline{\Lambda}$.

At the risk of proceeding backwards relative to the logical development of the theory; cf. **[Milne 2]**, a direct consequence of Corollary 1 of the Theorem of §1 is the following:

Corollary: Let $Z \subset V$ be a smooth, irreducible, S-subscheme closed in V of codimension c. There is a canonical isomorphism of sheaves on Z:

$$\Delta \cong \underline{H}_Z^{2c}(V,\Lambda(c)).$$

By the **fundamental class**

$$s(Z/V) \in H_Z^{2c}(V,\Lambda(c)) = \Gamma(Z, \underline{H}_Z^{2c}(V,\Lambda(c))),$$

we mean the section of image of $1 \in \Lambda$ under the above isomorphism (cf. **[Milne 2]** VI, §6) and if Z is not necessarily connected, i.e., $Z = \cup Z_j$ where Z_j are the connected components of Z, then define

$$s(Z/V) \in H_Z^{2c}(V,\Lambda(c)) = \oplus H_{Z_j}^{2c}(V,\Lambda(c))$$

to be the sum $\Sigma_j s(Z_j/V)$. The rule:

$$Z/V \dashrightarrow s(Z/V) \in H_Z^{2c}(V,\Lambda(c))$$

enjoys these properties:

1) (**functoriality**) If $\varphi : (Z'/V') \to (Z/V)$ is a morphism of smooth pairs of codimension c, then

$$\varphi^*(s(Z/V)) = s(Z'/V').$$

2) (**a generating section**) Multiplication by s(Z/V) induces an isomorphism of sheaves

$$\cong$$

$$\underline{\Delta} \qquad \to \qquad \underline{H}_Z^{2c}(V,\Lambda(c)).$$

$$s(Z/V)$$

3) (**in codimension 1**) Let c=1, so that Z is a smooth *irreducible* divisor in V. We have a commutative diagram

(2)

$$\begin{array}{ccccccc} H^0(U,\mathbb{G}_m) & \to & H_Z^1(V,\mathbb{G}_m) & \to & H^1(V,\mathbb{G}_m) & \to & H^1(U,\mathbb{G}_m) \\ \cong\downarrow & & \cong\downarrow & & \cong\downarrow & & \cong\downarrow \\ \Gamma(U,\mathcal{O}_U^*) & \xrightarrow{ord_Z} & \mathbb{Z} & \to & Pic(V) & \to & Pic(U) \end{array}$$

and the standard Kummer sequences

$$0 \to (\Lambda/p^n\Lambda)(1) \to \mathbb{G}_m \xrightarrow{p^n} \mathbb{G}_m \to 0$$

compile (as $n \mapsto \infty$) to yield a homomorphism

$$\Lambda = \Lambda \otimes H_Z^1(V,\mathbb{G}_m) \to H_Z^2(V,\Lambda(1)) .$$

The image of $1 \in \Lambda$ under this homomorphism is s(Z/V).

4) (**transitivity**). Suppose now that we have a triple of smooth varieties over S $Z \subset Y \subset V$, where Z and Y are closed subschemes of V, Z is of codimension a in Y, Y is of codimension b in V (and therefore Z is of codimension c=a+b in V). In this situation, the Spectral Sequence

$$H_Z^r(Y, \underline{H}_Y^s(V,\Lambda(c))) \Rightarrow H_Z^{r+s}(V, \Lambda(c))$$

degenerates, by purity, to an isomorphism

$$H_Z^{2a}(Y, \underline{H}_Y^{2b}(V,\Lambda(c))) \cong H_Z^{2c}(V, \Lambda(c)),$$

and since the domain of this isomorphism can be written as

$$H_Z^{2a}(Y, \underline{H}_Y^{2b}(V,\Lambda(c))) = H_Z^{2a}(Y, \Lambda(a) \otimes H_Y^{2b}(V,\Lambda(b)))$$

$$= H_Z^{2a}(Y,\Lambda(a)) \otimes H_Y^{2b}(V,\Lambda(b),$$

we get a natural isomorphism

$$H_Z^{2a}(Y,\Lambda(a)) \otimes H_Y^{2b}(V,\Lambda(b)) \cong H_Z^{2c}(V,\Lambda(c)).$$

Then the tensor product of the fundamental classes $s(Z/Y) \otimes s(Y/V)$ maps, under this isomorphism, to $s(Z/V)$.

One easily sees that a functor $(Z/V) \dashrightarrow s(Z/V)$ satisfying 1)-4) is necessarily unique. For a proof of existence, see [Milne 2] VI §6.

§3. "Extension obstructions" for the three-dimensional cohomology of smooth surfaces.

Let V be a smooth S-surface. For the moment, let $Z \subset V$ be of codimension $c=2$, and $U = V-Z$. Thus Z is zero-dimensional and smooth over S, i.e., Z is an étale extension of S. If $r= 3$, Corollary 4 gives the exact sequence

$$(3) \quad 0 \rightarrow H^3(V,F) \rightarrow H^3(U,F) \rightarrow H^0(Z,F(-2))$$

i.e., if a three-dimensional cohomology class on U "extends" to a class on V, it does so uniquely, and the

obstruction to its doing so is measured by a canonical homomorphism to $H^0(Z,F(-2))$.

Letting $F = \mathbb{Z}/p^n\mathbb{Z}(2)$ we have that the group $H^0(Z,F(-2))$ is canonically $\mathbb{Z}/p^n\mathbb{Z}$-- and then, more conveniently, passing to the limit and letting $F = \mathbb{Z}_p(2)$-- we get a natural exact sequence

$$\gamma_Z$$

$$(4) \quad 0 \to H^3(V,\mathbb{Z}_p(2)) \to H^3(U,\mathbb{Z}_p(2)) \to H^0(Z,\mathbb{Z}_p).$$

Call the image $\gamma_Z(c) \in H^0(Z,\mathbb{Z}_p)$ of a class $c \in H^3(U,\mathbb{Z}_p(2))$ the **extension obstruction** of c (**across** Z): we may think of the exact sequence (4) as saying that a class c in $H^3(U,\mathbb{Z}_p(2))$ "extends" to V if and only if its "extension obstruction" vanishes, and if it does extend, it does so uniquely. Of particular interest to us will be the following situation: S = Spec K, V is smooth *and proper* over S, and U is the complement of a finite set of closed points z_j $(j=1,\ldots,\nu)$ in V. Then a class c in $H^3(U,\mathbb{Z}_p(2))$ extends to the compactification V of U if and only if the ν-tuple of p-adic integers given by the obstruction invariants

$$(\gamma_{z_1}(c), \gamma_{z_2}(c), \ldots, \gamma_{z_\nu}(c))$$

vanishes, and its extension is unique.

§4. Three-dimensional cohomology of proper smooth surfaces over fields.

Here let S = Spec K, $\overline{S}$= Spec $\overline{K}$, for $\overline{K}$ an algebraic closure of K. and let V be proper. Denote by $\overline{V}$ the base change $V \otimes_S \overline{S}$. We have the Spectral Sequence

(5) $\quad H^r(G_K, H^s(\bar{V}, \mathbb{Z}_p(2)) \Rightarrow H^{r+s}(V, \mathbb{Z}_p(2))$

from which let us consider the edge-homomorphism

$$e: \quad H^3(V, \mathbb{Z}_p(2)) \rightarrow H^0(G_K, H^3(\bar{V}, \mathbb{Z}_p(2)))$$

Lemma: If $H^3(\bar{V}, \mathbb{Z}_p(2))$ is torsion-free and K is either a Global number field or a local number field of residual characteristic different from p, or a finite field of characteristic different from p, then $e=0$.

A consequence of the above lemma is that the Spectral Sequence (5), under the hypotheses of the Lemma, determines a canonical mapping

(5) $\quad H^3(V, \mathbb{Z}_p(2)) \rightarrow H^1(G_K, H^2(\bar{V}, \mathbb{Z}_p(2)))$

$$c \quad \mapsto \quad \tilde{c}\,.$$

§5. Smooth curves in surfaces.

Now we wish to consider smooth surfaces over S again, but no longer assume them to be proper as was assumed in §4. *So let us call our ambient, not necessarily proper, surface* U. Let $Z \subset U$ be closed subscheme of codimension c= 1, smooth over S; in particular, Z is a smooth curve over S. The local-to-global Spectral Sequence for cohomology with supports on Z gives the isomorphism:

$$H^1(Z, \mathbb{Z}_p(1) \otimes \underline{H}_Z^2(U, \mathbb{Z}_p(1))) \cong H_Z^3(U, \mathbb{Z}_p(2)),$$

and, identifying the domain with

$H^1(Z, \mathbb{Z}_p(1)) \otimes H_Z^2(U, \mathbb{Z}_p(1))$, we get a canonical isomorphism

(7) $H^1(Z, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H_Z^2(U,\mathbb{Z}_p(1)) \cong H_Z^3(U,\mathbb{Z}_p(2))$,

or, more concisely, an isomorphism

(8) $H^1(Z, \mathbb{Z}_p(1)) \cong H_Z^3(U,\mathbb{Z}_p(2))$

obtained by "cupping with" the canonical class s(Z/U).

The cohomology group $H^1(Z, \mathbb{Z}_p(1))$ can be computed using the Kummer sequence, giving:

(9)
$$0 \to \mathcal{O}^*(Z)\otimes_{\mathbb{Z}}\mathbb{Z}_p \to H^1(Z, \mathbb{Z}_p(1)) \to \mathrm{Tate}_p(\mathrm{Pic}(Z)) \to 0.$$

Composing the isomorphism (8) on the right with the natural mapping $H_Z^3(U,\mathbb{Z}_p(2)) \to H^3(U,\mathbb{Z}_p(2))$, and on the left with the natural injection $\mathcal{O}^*(Z)\otimes_{\mathbb{Z}}\mathbb{Z}_p \to H^1(Z, \mathbb{Z}_p(1))$ of (9) we get a canonical homomorphism

(10) $\sigma : \mathcal{O}^*(Z)\otimes_{\mathbb{Z}}\mathbb{Z}_p \to H^3(U,\mathbb{Z}_p(2))$.

For $f \in \mathcal{O}^*(Z)\otimes_{\mathbb{Z}}\mathbb{Z}_p$ denote by $\sigma(f;Z/U) \in H^3(U,\mathbb{Z}_p(2))$ the cohomology class $\sigma(f)$. If, further, the surface U satisfies the hypotheses required of V in the Lemma of §4 above, then the Hochschild-Serre Spectral sequence yields a homomorphism $H^3(U,\mathbb{Z}_p(2)) \to H^1(G_K,H^2(\bar{U},\mathbb{Z}_p(2)))$ and we shall, most often, be dealing with the image

$\sigma'(f;Z/U) \in H^1(G_K,H^2(\bar{U},\mathbb{Z}_p(2)))$

of $\sigma(f;Z/U)$ under that homomorphism.

Note: Let us give ourselves an element $f \in \mathcal{O}^*(C)\otimes_{\mathbb{Z}}\mathbb{Z}_p$, and *assume* :

(a) S = Spec K is a Global number field,

(b) U is "almost proper", i.e., it possesses a smooth compatification V such that V-U is a finite union of closed points $z_1, \ldots, z_\nu$,

(c) $H^3(V,\mathbb{Z}_p(2))$ has no p-torsion.

Then we have the following three natural questions:

The questions:

1) What are the "extension obstructions" for the cohomology class $\sigma(f) = \sigma(f;Z/V)$ across the points z_i? Assume these obstructions vanish, so that $\sigma(f)$ extends (uniquely) to $H^3(V,\mathbb{Z}_p(2))$ and then the previous discussion (in particular, thanks to our hypotheses **a)**, **b)**, **c)**, the Lemma of §3) gives us a class $\tilde{\sigma}(f) \in H^1(G_K,H^2(\bar{V},\mathbb{Z}_p(2)))$.

2) At which primes λ of K is the class $\tilde{\sigma}(f)$ ramified?

3) When the class $\tilde{\sigma}(f)$ is not ramified at λ, how can one pin down its image in $H^1(G_{k_\lambda},H^2(\bar{V},\mathbb{Z}_p(2)))$?

§6. Properties of $\sigma(f;Z/U)$.

1) (**functoriality**) If $\varphi : (Z',U') \to (Z,U)$ is a morphism of smooth pairs over S-schemes of codimension 1, then:

$$\varphi^*(\sigma(f;\, Z/U)) = \sigma(f\circ\varphi;\, Z'/U').$$

2) (**linearity**)

$$\sigma(\lambda_1 f_1+\lambda_2 f_2\,;\, Z/U) = \lambda_1\sigma(f_1\,;\, Z/U) + \lambda_2\sigma(f_2\,;\, Z/U).$$

§7. Calculating the extension obstruction.

Let C denote a closed curve in a smooth surface V over S= Spec K with K a perfect field. Let $z \in C(K)$ be a (closed) K-valued point of C, such that Z = C-z is smooth, so that if U = V-z, then (Z,U) is a smooth S-pair. Let $\tilde{C} \to C$ denote the normalization of C, so that Z = C-z is naturally contained in $\tilde{C}$ as an open subscheme. Let $\tilde{z}_1,\ldots,\tilde{z}_r$ denote the closed points of $\tilde{C}$ in the complement of Z, i.e., lying over z. Let d_i denote the degree of the residue field extension $\tilde{z}_i/z$. If f is a rational function on $\tilde{C}$ which is regular on Z, define $\mathrm{ord}_z(f)$ by:

$$\mathrm{ord}_z(f) = \sum_{j=1}^{r} d_j\cdot \mathrm{ord}_{\tilde{z}_j}(f).$$

Theorem: In the above situation, if γ_z denotes the "extension obstruction" over the point z (as defined in §3 above) and if the base field K is of characteristic 0, then

$$\gamma_z(\,\sigma(f\,;\, Z/U)) = \mathrm{ord}_z(f).$$

Proof: The extension obstruction is insensitive to change of base field K, so we may (and do) assume that K is algebraically closed: all the points $\tilde{z}_j$ are defined over K, and therefore all the d_j's are equal to 1. The extension obstruction at z also being unchanged by completion at z we assume that V is the spectrum of a complete regular

local ring (K-algebra) of dimension 2 with residue field equal to K, i.e., V = Spec K[[x,y]], and U = V-z. The formula of our Theorem is "additive on components" in the sense that if Z breaks up as the disjoint union of components Z_j for j=1,...,s and if f_j denotes the restriction of f to the j-th component Z_j, then $\Sigma\ ord_Z(f_j) = ord_Z(f)$, and $\Sigma\ \gamma_Z(\sigma(f_j ; Z_j/U)) = \gamma_Z(\sigma(f ; Z/U))$ so that we may also (and we do) reduce attention to the case where $C \subset V$ is irreducible.

We now consider the special case where C is **smooth** in V. After suitable change of coordinates, we may take C to be the closed subscheme of V given by the equation y=0.

For this, we need the following commutative diagram:

(11)
$$\begin{array}{ccccc} & & \overset{ord_Z}{} & & \\ & \mathcal{O}^*(Z) & \to & H_z^1(C,\mathbb{G}_m) & \cong\ \mathbb{Z} \\ \kappa & \downarrow & & \downarrow\ \kappa & \\ & & \overset{\partial}{} & & \\ & H^1(Z,\mathbb{Z}_p(1)) & \to & H_z^2(C,\mathbb{Z}_p(1)) & \cong\ \mathbb{Z}_p \\ \cup s(Z/U) & \downarrow & & \downarrow\ \cup s(C/V) & \\ & H_Z^3(U,\mathbb{Z}_p(2)) & \to & H_z^4(V,\mathbb{Z}_p(2)) & \cong\ \mathbb{Z}_p \\ & & \overset{\partial\circ i}{} & & \end{array}$$

where the mappings κ are the natural mappings coming from Kummer Theory, the mappings ∂ come from coboundary mappings of the evident long exact sequences for cohomology, and the mapping i is the natural mapping $H_Z^3(U,\mathbb{Z}_p(2)) \to H^3(U,\mathbb{Z}_p(2))$.

(**Check this commutativity!**) Granted commutativity

of (11) our Theorem follows in this case (C smooth) because if you make the circuit

$$\mathcal{O}^*(C) \to H_z^4(V,\mathbb{Z}_p(2)) \cong \mathbb{Z}_p$$

by the right-hand route you get $ord_z(f) \in \mathbb{Z}_p$, while making it via the left-hand route gives $\gamma_z(\sigma(f;Z/U))$.

To reduce to the case where C is smooth, let C now be an arbitrary but irreducible curve in V, let C_o = Spec K[[t]], and let $V \to C_o$ be a projection for which the composition $C \to C_o$ is not constant, i.e., is of finite degree. Judicious change of the coordinates x,y will allow us to take this projection to be given by t = x, so that $V = C_o \hat{\times} D$ where D = Spec K [[y]]. The mapping $V \to C$ is formally smooth. Let $\nu:\tilde{C} \to C$ be the normalization of C, and since we are in a completed situation, we have that there is a unique point $\tilde{z}$ in $\tilde{C}$ lying above z. Let μ denote the degree of the mapping $\tilde{C} \to C_o$. Since K is algebraically closed of characteristic 0, : $\tilde{C} \to C_o$ is Galois, cyclic of order μ (a "model" being given by $K[[t]] \subset K[[t^{1/\mu}]]$). Let $g:t^{1/\mu} \mapsto \zeta_\mu \cdot t^{1/\mu}$ be a generator of the Galois group, for ζ_μ a primitive μ-th root of 1 in K. Put

$$\tilde{V} = \tilde{C} \times_{C_o} V = \tilde{C} \hat{\times} D,$$

so that the natural projection $\tilde{V} \to V$ is cyclic Galois of degree μ, and is merely the product of the cyclic Galois mapping of degree μ $\tilde{C} \to C_o$ with the identity on D .

Our $\tilde{V}$ is (formally) smooth over $\tilde{C}$ which is also (formally) smooth. There are μ distinct sections $\tilde{\eta}_j : \tilde{C} \to \tilde{V}$ ($j=1,\ldots,\mu$) given by $\tilde{\eta}_j = (g^j, \nu)$. Let $\tilde{Z}_j = \tilde{\eta}_j(\tilde{C}) - \tilde{z}$ and let $\tilde{f}_j$ denote the unique function on $\tilde{Z}_j$ such that $\tilde{f}_j \circ \tilde{\eta}_j = f \cdot \nu$ on $\tilde{C}$, for $j= 1,\ldots,\mu$. Put $\tilde{U} = \tilde{V} - \tilde{z}$. If $\tilde{Z}$ denotes the

pullback, $\tilde{Z} = \tilde{U} \times_U Z$, then $\tilde{Z}$ is the disjoint union of the $\tilde{Z}_j$ and we have a morphism of smooth S-pairs, $\varphi:(\tilde{Z},\tilde{U}) \to (Z,U)$. Moreover, $f\circ\varphi$ on $\tilde{Z}$ restricts to $\tilde{f}_j$ on the component $\tilde{Z}_j$.

Since $\tilde{C}_j$ is smooth in $\tilde{V}$, we know that

$$\gamma_{\tilde{Z}}(\sigma(\tilde{f}_j\ ;\ \tilde{Z}_j/\tilde{U}\ )) = \mathrm{ord}_{\tilde{Z}}(\tilde{f}_j) = \mathrm{ord}_Z(f).$$

Moreover, we have a commutative diagram,

(12)

$$\begin{array}{ccc} & \varphi^* & \\ H_Z^3(U,\mathbb{Z}_p(2)) & \to & H_{\tilde{Z}}^3(\tilde{U},\mathbb{Z}_p(2)) \\ \downarrow i & & \downarrow i \\ H^3(U,\mathbb{Z}_p(2)) & \to & H^3(\tilde{U},\mathbb{Z}_p(2)) \\ \downarrow \partial & & \downarrow \partial \\ H_Z^4(V,\mathbb{Z}_p(2)) & \to & H_{\tilde{Z}}^4(\tilde{V},\mathbb{Z}_p(2)) \\ \downarrow \cong & & \downarrow \cong \\ \mathbb{Z}_p & \to & \mathbb{Z}_p\ . \\ & \mu & \end{array}$$

and since $\varphi^*: H_Z^3(U,\mathbb{Z}_p(2)) \to H_{\tilde{Z}}^3(\tilde{U},\mathbb{Z}_p(2))$ brings the class $\sigma(f\ ;\ Z/U)$ to

$$\sigma(f\circ\varphi\ ;\ \tilde{Z}/\tilde{U}) = \sum_{j=1}^{\mu} \sigma(\tilde{f}_j\ ;\ \tilde{Z}_j/\tilde{U}\ ),$$

we compute that

$$\mu\cdot\gamma_Z(\ \sigma(f\ ;\ Z/U)) = \sum_{j=1}^{\mu} \gamma_{\tilde{Z}}(\sigma(\tilde{f}_j\ ;\ \tilde{Z}_j/\tilde{U}\ )) = \mu\cdot\mathrm{ord}_Z(f),$$

which gives what we want.

□

§8. Measuring ramification.

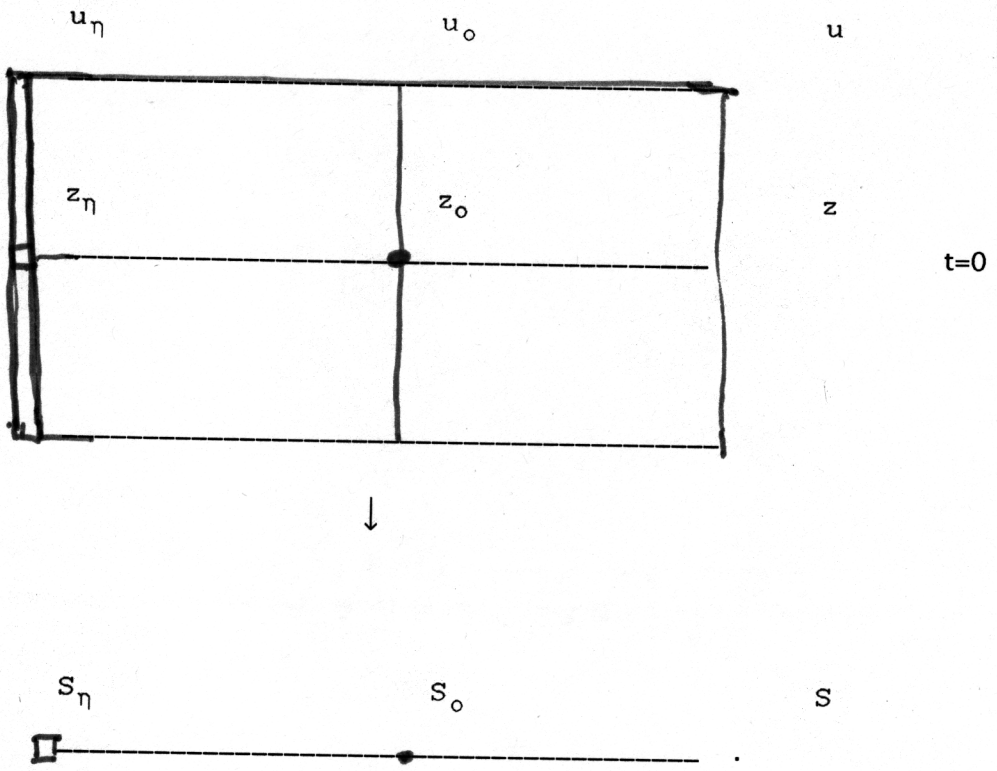
We begin with a review of two basic compatibilities which are preliminary "exercises" in preparation for the eventual Proposition of this section.

Let K be a finite extension of $\mathbb{Q}_\ell$, with $\ell \neq p$. The following diagram is commutative:

(13)
$$\begin{array}{ccccc} & & \kappa & & \\ K^* & \to & H^1(G_K, \mathbb{Z}_p(1)) & \to & H^1(I_K, \mathbb{Z}_p(1))^{G_k} \\ \text{ord}\ \downarrow & & & & \delta \downarrow\ \cong \\ \mathbb{Z} & \subset & \text{Hom}(\mathbb{Z}_p, \mathbb{Z}_p) & = & \text{Hom}_{G_k}(\mathbb{Z}_p(1), \mathbb{Z}_p(1)) \end{array}$$

where κ comes from Kummer Theory, the horizontal arrow comes from restricting cocycles on G_K to $I_K \subset G_K$, and the vertical isomorphism comes from the natural isomorphism δ (cf. §7 of Ch. 1 of Part I) which identifies the maximal pro-p quotient of I_K with $\mathbb{Z}_p(1)$.

Next, let $S = \text{Spec}(\mathcal{O}_K)$, $S_o = \text{Spec}(k)$, and $S_\eta = \text{Spec } K$, and $u = \text{Spec}(\mathcal{O}_K[[t]])$, $u_o = \text{Spec}(k[[t]])$, and $u_\eta = \text{Spec } K[[t]]$. Define the sections $z \subset u$, $z_o \subset u_o$, and $z_\eta \subset u_\eta$ by $t=0$, giving the following picture:



Let f be in K^*. Then the following diagram is commutative.

(14)

$$
\begin{array}{ccccc}
K^* & \xrightarrow{e} & H^1(z_\eta,\mathbb{Z}_p(1))\otimes H_{z_\eta}{}^2(u_\eta,\mathbb{Z}_p(1)) & \xrightarrow{c} & H_{z_\eta}{}^3(u_\eta,\mathbb{Z}_p(2)) \\
\downarrow \text{ord} & & & & \downarrow \\
\mathbb{Z} & & & & H^1 G_K,\ H_{z_{\overline{\eta}}}{}^2(u_{\overline{\eta}},\mathbb{Z}_p(2))) \\
\downarrow & & & & \downarrow \\
\mathbb{Z}_p & & & & H^1(G_K,\mathbb{Z}_p(1)) \\
\downarrow & & & \cong & \downarrow \\
\mathrm{Hom}(\mathbb{Z}_p(1),\mathbb{Z}_p(1))=\mathrm{Hom}_{G_k}(\mathbb{Z}_p(1),\mathbb{Z}_p(1)) & & \xrightarrow{\delta^{-1}} & & H^1(I_K,\mathbb{Z}_p(1))^{G_k}
\end{array}
$$

Here the mapping labelled e is given by our "basic construction", i.e., tensoring with the image of f under Kummer Theory with the fundamental class,

$$f \mapsto \kappa(f) \otimes s(z_\eta/u_\eta).$$

The mapping labelled c is given by cup-product, and the right-hand vertical mappings are given, reading from bottom to top, as follows.

The bottom arrow comes from the Hochschild-Serre Spectral Sequence, the middle arrow comes by the identification of the G_K-modules

$$\begin{array}{ccc} & & \otimes s(\, z_{\overline{\eta}}/u_{\overline{\eta}}\,) \\ \mathbb{Z}_p(1) & \to & H_{z_{\overline{\eta}}}{}^2(u_{\overline{\eta}}, \mathbb{Z}_p(2)), \\ & \cong & \end{array}$$

while the top arrow also comes from the appropriate Hochschild-Serre Spectral Sequence, in view of the fact that $H_{z_{\overline{\eta}}}{}^3(u_{\overline{\eta}}, \mathbb{Z}_p(2))$ vanishes.

Now let U be proper and smooth over S. Let Z be a subscheme of U. Suppose Z to be regular, and proper over S. Let, as above, the subscripts "η" and "o" refer to generic and special fibers, respectively. Suppose further that $Z_\eta \subset U_\eta$ is a smooth pair over S_η, and the special fiber Z_o is reduced. Let f be a rational function on Z_η (not identically zero) satisfying the "ord-condition". We may view f as a rational function on the regular scheme Z, and if (f) denotes its associated Cartier divisor of zeroes-and-poles on Z, let $(f)_{vert}$ denote that part of the divisor (f) supported on Z_o; equivalently, the difference of the

two divisors, $(f)-(f)_{vert}$, is a "horizontal" Cartier divisor, i.e., contains no irreducible component of the fibers of $Z \to S$ in its support.

We can form the cohomology class $\kappa(f) \otimes s(Z_\eta/U_\eta)$, which lies in $H_{Z_\eta}^3(U_\eta, \mathbb{Z}_p(2))$, and which maps to the cohomology class we have called $\tilde{\sigma}(f; Z_\eta/U_\eta)$ in $H^1(G_K, H^2(U_{\bar{\eta}}, \mathbb{Z}_p(2))$.

We wish to **describe the ramification** of the class $\tilde{\sigma}(f; Z_\eta/U_\eta)$ in the sense that we want to know its image under the natural mapping

$$(15) \quad H^1(G_K, H^2(U_{\bar{\eta}}, \mathbb{Z}_p(2)) \to H^1(I_K, H^2(U_{\bar{\eta}}, \mathbb{Z}_p(2))^{G_k}.$$

Of course, the class $\tilde{\sigma}(f; Z_\eta/U_\eta)$ is unramified if and only if its image under (15) is zero. We can think of the mapping (15) as having the following domain and range:

$$H^1(G_K, H^2(U_{\bar{\eta}}, \mathbb{Z}_p(1)) \otimes \mathbb{Z}_p(1)) \to H^1(I_K, H^2(U_{\bar{\eta}}, \mathbb{Z}_p(1)) \otimes \mathbb{Z}_p(1))^{G_k}.$$

Since U is smooth over S and since we are assuming that $\ell \neq p$, the action of the inertia group I_K on the module $H^2(U_{\bar{\eta}}, \mathbb{Z}_p(1)) \otimes \mathbb{Z}_p(1)$ is trivial. Therefore the range above can be identified with

$$\begin{aligned} &\mathrm{Hom}(I_K, H^2(U_{\bar{\eta}}, \mathbb{Z}_p(1)) \otimes \mathbb{Z}_p(1))^{G_k} = \\ &\mathrm{Hom}_{G_k}(\mathbb{Z}_p(1), H^2(U_{\bar{\eta}}, \mathbb{Z}_p(1)) \otimes \mathbb{Z}_p(1)) = \\ &\quad H^2(U_{\bar{\eta}}, \mathbb{Z}_p(1))^{G_k} = \\ &\quad H^2(U_o \otimes_k \bar{k}, \mathbb{Z}_p(1))^{G_k}, \end{aligned}$$

the last identification being given by the comparison

theorem for the étale cohomology of the generic and special fibers of the the smooth proper scheme U over S.

The isomorphism (15), after the identification of its range with $H^2(U_o \otimes_k \bar{k}, \mathbb{Z}_p(1))^{G_k}$ as above, yields the mapping:

$$(16)\quad H^1(G_K, H^2(U_{\bar{\eta}}, \mathbb{Z}_p(2)) \to H^2(U_o \otimes_k \bar{k}, \mathbb{Z}_p(1))^{G_k}.$$

Definition: Let ξ be a cohomology class in $H^1(G_K, H^2(U_{\bar{\eta}}, \mathbb{Z}_p(2))$ and let D denote a Cartier divisor in U_o. We will say that **the ramification of ξ is given by** D (in notation: $ram(\xi) = D$) if the image of ξ under (4) is equal to the Chern class of D in $H^2(U_o, \mathbb{Z}_p(1))^{G_k}$.

Proposition: The ramification of the class $\tilde{\sigma}(f; Z_\eta / U_\eta)$ is given by the Cartier divisor $(f)_{vert}$.

Proof: The key, here, is to prove a stronger statement. We shall use our rational function f on Z_η to produce a class $\tilde{\sigma}(f; Z_\eta / U - Z_o)$ in $H_{Z_\eta}{}^3(U - Z_o, \mathbb{Z}_p(2))$ which maps to $\tilde{\sigma}(f; Z_\eta / U_\eta)$ under the natural mapping $H_{Z_\eta}{}^3(U - Z_o, \mathbb{Z}_p(2)) \to H_{Z_\eta}{}^3(U_\eta, \mathbb{Z}_p(2))$. We then compute the image of $\tilde{\sigma}(f; Z_\eta / U - Z_o)$ under the composition

$$(17)\quad H_{Z_\eta}{}^3(U - Z_o, \mathbb{Z}_p(2)) \to H^3(U - Z_o, \mathbb{Z}_p(2)) \to H_{Z_o}{}^4(U, \mathbb{Z}_p(2)).$$

If Π denotes the G_k-set (i.e., set, with given G_k-action) of irreducible components of the scheme $Z_o \otimes_{Spec\ k} Spec\bar{k}$, we may

(a) identify the range of (3) with the $\mathbb{Z}_p$-module $\mathbb{Z}_p[\Pi]^{G_k}$,

and

(b) view $(f)_{vert} = \Sigma\, m_j \cdot C_j$ $(m_j \in \mathbb{Z},\ C_j \in \Pi)$ as being an element in $\mathbb{Z}[\Pi]^{G_k}$.

We shall prove that the image of $\tilde{\sigma}(f; Z_\eta / U - Z_o)$ in $\mathbb{Z}_p[\Pi]^{G_k}$ is equal to $(f)_{vert} = \Sigma\, m_j \cdot C_j$. This suffices to establish our proposition, as can be seen by consulting the following commutative diagram:

(18)

$$\begin{array}{ccccc} H_{Z_\eta}{}^3(U-Z_o, \mathbb{Z}_p(2)) & \rightarrow & H^3(U-Z_o, \mathbb{Z}_p(2)) & \rightarrow & H_{Z_o}{}^4(U, \mathbb{Z}_p(2)) \\ \downarrow & & & & \downarrow \\ H_{Z_\eta}{}^3(U_\eta, \mathbb{Z}_p(2)) & \rightarrow & H^1(G_K, H^2(U_{\bar{\eta}}, \mathbb{Z}_p(2)) & \rightarrow & H^2(U_o \otimes_k \bar{k}, \mathbb{Z}_p(1))^{G_k}. \end{array}$$

where the right-hand vertical mapping is given by sending an element $\Sigma\, m_j \cdot C_j$ in $H_{Z_o}{}^4(U, \mathbb{Z}_p(2)) = \mathbb{Z}[\Pi]^{G_k}$ to its "Chern class", $\Sigma\, m_j \cdot \text{Chern}(C_j)$ in $H^2(U_o \otimes_k \bar{k}, \mathbb{Z}_p(1))^{G_k}$.

Returning to the proof of the Proposition, let C_o be any component of Z_o, and let m_o denote the multiplicity of that component in (f), or equivalently, in $(f)_{vert}$. We wish to show that the multiplicity of C_o in the image of $\tilde{\sigma}(f; Z_\eta / U - Z_o)$ in $\mathbb{Z}_p[\Pi]^{G_k}$ is also equal to m_o. But, to

check this equality of integers, we may restrict our entire picture to a formal neighborhood $\mathcal{U}$ in U of a (smooth) affine open in $C_o \subset U_o$; let $\mathcal{Z}$ denote the "scheme-theoretic" intersection of $\mathcal{U}$ with Z, i.e., the formal scheme cut out in $\mathcal{U}$ by the ideal of definition of the scheme Z. We may reduce our picture even further and still be able to check the desired equality of integers. Namely, after making, if necessary, a finite base change of k find a "transverse slice" u to C_o in $\mathcal{U}$. If we let "z" denote the (formal) scheme-theoretic intersection of u with Z, we have that $z \cong \mathrm{Spf}(\mathcal{O}_L)$ and $u \cong \mathrm{Spf}(\mathcal{O}_L[[t]])$ for L an appropriate finite extension of K, and t a uniformizer. The equality we are required to check then follows directly from commutativity of the diagram (14).

□

§9. Commentary about the resolutions of Gersten, and of Bloch-Ogus.

The "Gersten resolution" , and its cohomological reformulation studied by Bloch and Ogus, are systematic machines which produce elements in the K-theory of schemes U, and in various cohomology theories of U, respectively. See [G], [B-O]. Our treatment of the cohomological classes $\sigma(f; Z/U)$ may be viewed as a somewhat ad hoc reconstruction of a tiny piece of this machinery in the simplest case. We shall not need an more of this than we have already made explicit, but let us recall that the full Gersten resolution of the sheaf $\underline{K}_n$ on a smooth scheme U over a field (conjectured by Gersten, and proved in this context by Quillen; cf. [B]) is a chain complex of sheaves for the Zariski topology on U,

(19)

$$\coprod_{u \in U^0} i_u K_n(k(u)) \to \coprod_{u \in U^1} i_u K_{n-1}(k(u)) \to \dots \to \coprod_{u \in U^n} i_u K_0(k(u)) \to 0,$$

where U^j refers to the set of points u of codimension j in U, k(u) is the residue field of u, and $i_u F$, for F a commutative group, is the direct image to U of the constant sheaf F on the Zariski closure of u in U. The analogous (Bloch-Ogus) resolution for the sheaf $\underline{H}^n(\mathbb{Z}_p(n))$ for the Zariski topology on U associated to the pre-sheaf $\mathcal{U} \mapsto H^n(\mathcal{U}, \mathbb{Z}_p(n))$ (H^* = étale cohomology, and U smooth over a field of characteristic different from p; cf. [B]) is given by the complex

(20)

$$\coprod_{u\in U^0} i_u H^n(k(u), \mathbb{Z}_p(n)) \to \coprod_{u\in U^1} i_u H^{n-1}(k(u), \mathbb{Z}_p(n-1)) \to \dots$$

$$\to \coprod_{u\in U^n} i_u H^0(k(u), \mathbb{Z}_p(0)) \to 0,$$

The previous paragraphs of this Chapter have been dealing, in effect, with $H^1(U, \underline{K}_2)$ and with $H^1(U, \underline{H}^2(\mathbb{Z}_p(2)))$ as computed via the complexes (19) and (20) for n=2. Moreover, $H^1(U, \underline{H}^2(\mathbb{Z}_p(2)))$ is related to $H^3(U, \mathbb{Z}_p(2))$ via the Spectral Sequence

$$H^r(U, \underline{H}^s(\mathbb{Z}_p(2))) \Rightarrow H^{r+s}(U, \mathbb{Z}_p(2)).$$

To formalize what we have done, let GC(U) denote the "Gersten" 1-cocycles of the complex (19), i.e.:

$$GC(U) := \ker \{ \bigoplus_{\substack{u_1 \in U \\ \operatorname{cod} u_1 = 1}} k(u_1)^* \xrightarrow{\text{"ord"}} \bigoplus_{\substack{u_2 \in U \\ \operatorname{cod} u_2 = 2}} \mathbb{Z} \}.$$

The formation of GC is both covariantly and contravariantly functorial in U for finite faithfully flat morphisms: if $\varphi: U \to V$ is a finite faithfully flat morphism, we have the commutative diagram

$$\begin{array}{ccc} k(v_1)^* & \to & \bigoplus_{u_1 \mapsto v_1} k(u_1)^* \\ \text{ord} \downarrow & & \downarrow \text{ord} \\ \mathbb{Z} & \to & \bigoplus_{u_1 \mapsto v_1} \mathbb{Z} \end{array} \tag{21}$$

where $v_1 \in V$ is a point of codimension 1, and $u_1 \in U$ ranges through the full inverse image of v_1. The top horizontal mapping is the natural one, and the bottom horizontal mapping sends $1 \in \mathbb{Z}$ to the vector

$$(\ldots, e_{u_1}, \ldots) \in \bigoplus_{u_1 \mapsto v_1} \mathbb{Z}$$

whose u_1-component (for each $u_1 \mapsto v_1$) is the ramification index of the localization of U at u_1 over the localization of V at v_1. The "direct sum" of the diagrams (19) for all points $v_1 \in V$ of codimension 1 induces the (contravariant) functorial homomorphism

$$\varphi^*: GC(V) \to GC(U).$$

The covariant functor is obtained from the norm mapping. Explicitly, we have the commutative diagram

$$\begin{array}{ccc} & & \text{Norm} \\ \bigoplus_{u_1 \mapsto v_1} & k(u_1)^* & \to \quad k(v_1)^* \\ \text{ord} \downarrow & & \downarrow \text{ord} \\ \bigoplus_{u_1 \mapsto v_1} & \mathbb{Z} & \to \quad \mathbb{Z} \end{array} \tag{22}$$

where the botttom horizontal arrow sends $(\ldots,a_{u_1},\ldots)$ to

$$\sum_{u_1 \mapsto v_1} [k(u_1):k(v_1)] \cdot a_{u_1}$$

and where the brackets [,] means degree of the field extension. The "direct sum" of the diagrams (20) for all points $v_1 \in V$ of codimension 1 induces the (covariant) functorial homomorphism $\varphi_*: GC(U) \to GC(V)$.

We have a natural homomorphism

$$GC(U) \xrightarrow{\sigma} H^3(U,\mathbb{Z}_p(2))$$

which commutes with φ^* and φ_* and which is constructed as in the previous paragraphs. Specifically, if $c \in GC(U)$ and if we write

$$c = \oplus c_{u_1} \quad \in \quad \bigoplus_{\substack{u_1 \in U \\ \operatorname{cod} u_1 = 1}} k(u_1)^* ,$$

let Z be the (closed reduced) scheme which is the closure of the finite set of points $u_1 \in U$ of codimension 1, such that the component c_{u_1} of c in $k(u_1)^*$ is not equal to 1, and let f denote the rational function on Z which on the component of Z given by the closure of u_1 is equal to c_{u_1}.

Then, since c is a Gersten cycle, we have that "ord f" = 0 on Z , and $\sigma(c)$ is defined to be the class $\sigma(f;Z/U)$ in $H^3(U,\mathbb{Z}_p(2))$.

Chapter seven. Correspondences

§1. "Marked curves" and "marked correspondences".

Let S = Spec K, with K perfect. For an integer w, a w-**marked curve** over S will mean a reduced curve X over S, marked with a nontrivial rational section, call it f_X, of the w-th tensor power of the line bundle $\Omega^1_{X_{sm}/S}$ where X_{sm} is the smooth locus of X.

The integer w we will call the **degree** of the marking f_X.

Let X,Y be irreducible curves over S. By a (reduced; resp.: irreducible) **correspondence** Γ "from" X "to" Y we mean a reduced (resp.: reduced and irreducible) closed one-dimensional subscheme $\Gamma \subset X \times Y$, and we will assume that every irreducible component of Γ maps nontrivially to X and to Y, under the natural projection maps π_X and π_Y. A "**general**" correspondence is a formal sum (rational integer coefficients) of irreducible correspondences.

If X, Y are proper and smooth over S, and if $\Gamma \subset X \times Y$ is an irreducible correspondence ("from X to Y ") the projections π_X and π_Y are both finite and faithfully flat. Consequently π_X and π_Y induce both covariant and contravariant mappings on cohomology. The correspondence Γ itself induces a homomorphism denoted $\Gamma_* := \pi_{Y*} \circ \pi_X^*$ from the étale cohomology of X to that of Y, and a homomorphism $\Gamma^* := \pi_{X*} \circ \pi_Y^*$ from the étale cohomology of Y to that of X. We extend the formation of Γ_* and Γ^* from irreducible correspondences to all correspondences, by linearity. More explicit description of

this, and use of it, will be made in §2 below.

If X is w-marked and Y is v-marked, we may view a reduced correspondence Γ as (w-v)-marked by setting f_Γ to be the rational section of the (w-v)-th tensor power of $\Omega^1_{\Gamma_{sm}/S}$ given as the image of

$$\pi_X^*(f_X) \otimes \pi_Y^*(f_Y)^{-1}$$

(restricted to the smooth locus Γ_{sm}).

Remark: Saying that the correspondence is "from" X and "to" Y is perhaps arbitrary since the notion of correspondence makes no distinction between the first or second factors in X×Y, but it is useful to make this (non)-distinction anyway. First, one gets convenient notation for the two induced mappings on cohomology (Γ_* and Γ^*). Secondly, the marking given to Γ clearly does depend upon the ordering of X and Y.

We take X, Y irreducible and smooth over S, but our correspondences Γ may (and generally will) have singularities and many components. If X and Y are both w-marked for some $w \in \mathbb{Z}$, then any correspondence Γ from X to Y is "0-marked", i.e., is endowed with a chosen rational function f_Γ. The "hook-up" of this situation with the constructions of Chapter 6 is that we have a smooth surface V = X×Y over S, a reduced curve Γ on that surface, and a rational function f_Γ on Γ. Recall the definition of "ord_Z" as in §3, Chapter 6, and define the bad **set** $\mathcal{Y}$ (**for** Γ **in** X×Y) to be the (finite) set of points at which "$ord_Z(f_\Gamma)$" $\neq 0$.

For any prime number $p \neq char(K)$, we have constructed, in §5, Chapter 6, the cohomology class

$$\sigma_\Gamma = \sigma(f_\Gamma ; \Gamma / X\times Y) \in H^3(X\times Y - \mathcal{Z}; \mathbb{Z}_p(2)).$$

In the special case where the "bad set" is empty, i.e., "$\mathrm{ord}_z(f_\Gamma)$" = 0 for all $z \in \Gamma$, we have

$$\sigma_\Gamma \in H^3(X\times Y; \mathbb{Z}_p(2)).$$

We can extend the construction $\Gamma \mapsto \sigma_\Gamma$ by linearity to apply to formal sums of reduced Γ's, i.e., to general correspondences.

§2. Composition of correspondences

Let X, Y, Z be irreducible smooth curves over S. Let F be a correspondence from X to Y, and G a correspondence from Y to Z. There are various equivalent ways to express the composition correspondence $\Gamma = G\circ F$. Here is one.

Consider the three projections

$$\pi_Z: X\times Y\times Z \to X\times Y$$
$$\pi_Y: X\times Y\times Z \to X\times Z$$
$$\pi_X: X\times Y\times Z \to Y\times Z.$$

Let π_* and π^* denote the usual mappings of cycles, so that (for example) if C is a 1-cycle in $X\times Z$, then $\pi_Y{}^*(C)$ is the cycle $C\times Y$ in $X\times Y\times Z$, and if C is an irreducible 1-cycle (i.e., closed irreducible curve) in $X\times Y\times Z$ then $\pi_{Y*}(C) = 0$ if C is a fiber of π_Y and is $d\cdot\tilde{C}$ if $\pi_Y(C)$ is a curve $\tilde{C}$ in $X\times Z$, where d = the degree of the (finite) mapping

$$\pi_Y: C \to \tilde{C}.$$

Lemma:

1) The two (reduced, effective) divisors $\pi_X^*(G)$ and $\pi_Z^*(F)$ in $X \times Y \times Z$ intersect properly (i.e., have no irreducible components in common).

2) If K is of characteristic 0, the intersection of any irreducible component of $\pi_X^*(G)$ and any irreducible component $\pi_Z^*(F)$ is generically transversal.

3) More generally, we have the conclusion of **2)** under the assumption that at least one of the projection mappings

$$G \to Y \quad \text{or} \quad F \to Y$$

is generically étale on each irreducible component of their respective domains.

Proof: As for the first assertion, note that any component of $\pi_X^*(G)$ is a union of fibers of π_X and any irreducible component of $\pi_Z^*(F)$ is a union of fibers of π_Z, and therefore if they had an irreducible component in common, this common irreducible component would be a (single) fiber of the mapping

$$\pi_{X,Z} : X \times Y \times Z \to Y,$$

contradicting the assumption that every irreducible component of F and G maps nontrivially to each factor.

As for **3)**, let us begin by considering any closed point ξ in the intersection of the smooth locus of an irreducible component Q of $\pi_X^*(G)$ and that of an

irreducible component R of $\pi_Z^*(F)$. We may write ξ as $x\times\gamma = \varphi\times y$ for points $\gamma \in G$, $\varphi \in F$, $x \in X$, and $y \in Y$. In the tangent space $\mathcal{T}$ of the point ξ in $X\times Y\times Z$ we have the lines $\mathcal{T}_X$, $\mathcal{T}_Y$, $\mathcal{T}_Z$ determined by the coordinate axes, and the tangent planes $\mathcal{T}_Q$, $\mathcal{T}_R$ to the surfaces Q and R (both assumed to be smooth at ξ). By construction, $\mathcal{T}_X \subset \mathcal{T}_Q$, and $\mathcal{T}_Z \subset \mathcal{T}_R$. If we had a nontransversal intersection of $\mathcal{T}_Q$ and $\mathcal{T}_R$ at ξ, we would have equality $\mathcal{T}_Q = \mathcal{T}_R$ and consequently, $\mathcal{T}_Q = \mathcal{T}_R = \mathcal{T}_X\times\mathcal{T}_Z$. In a word, the projections $Q\to Y$ and $R\to Y$ would have vanishing differential at γ and φ, respectively. By the hypothesis of **3)**, one of these projections, say $Q\to Y$, is generically étale, and therefore by choosing γ sufficently general we get a contradiction to nontransversality at ξ, proving **3)**.

Since these projections (being nontrivial) are generically étale if the characteristic of K is 0, we get **2)**.

□

Let then $C = \pi_X^*(G) \cap \pi_Z^*(F)$, meaning the (scheme-theoretic) intersection. By **1)** we have that $\dim(C) \leq 1$. So as not to have to worry *too much* let us define the notion of **composition of correspondences** G and F *only* under the hypothesis that

(*) The **scheme C is generically reduced**[1].

Under this hypothesis, we use the same letter C now to denote the (reduced) 1-cycle in $X\times Y\times Z$ given as the "sum" of the irreducible components of the scheme C.

Definition: Given a pair of correspondences F from X to Y and G from Y to Z satisfying **(*)**, the **composition of**

[1] In what follows we will only be considering the construction of the composition of correspondences for base fields of characteristic 0, in which case, by **3)** our hypothesis (*) is automatically satisfied

correspondences G and F, denoted G∘F, is $\Gamma = \pi_{Y*}(C)$ viewed as a correspondence from X to Z.

Note: It is sometimes helpful to "think of" G∘F as "$(1\times G)_*(F)$" or as "$(F\times 1)^*(G)$", which is what it would be if G (or F) were actual functions.

§3. The Liebniz property.

Let us now hypothesize that X, Y, Z are irreducible smooth w-marked curves over S (all for the same w), and that F is a correspondence from X to Y, and G a correspondence from Y to Z. Let $\Gamma = G\circ F$. We suppose further that the "bad sets" for all three (0-marked) correspondences F,G,Γ are empty. This gives three cohomology classes,

$$\sigma_F \in H^3(X\times Y, \mathbb{Z}_p(2))$$

$$\sigma_G \in H^3(Y\times Z, \mathbb{Z}_p(2))$$

$$\sigma_\Gamma \in H^3(X\times Z, \mathbb{Z}_p(2)).$$

What is the relationship between them?

Proposition:

$$(1) \qquad \sigma_\Gamma = (F\times 1)^*\cdot\sigma_G + (1\times G)_*\cdot\sigma_F,$$

where we view $F\times 1$ as giving a correspondence from $X\times Z$ to $Y\times Z$, and $1\times G$ as giving a cohomological correspondence from $X\times Y$ to $X\times Z$.

Proof: I am very grateful to Beilinson for giving me the following elegant proof of this Proposition: It is sufficient to establish the above formula on the level of "Gersten Cycles" using the terminology of §9 of Chapter 6. It is also sufficient to do this after replacing X and Z by finite étale coverings of their generic points. After a suitable such

replacement we may assume that the projections $F \to X$, $G \to Z$ are isomorphisms on each irreducible component of F, G, respectively. By bilinearity, we may assume that $F \to X$ and $G \to Z$ are isomorphisms; now (1) is clear.

□

§4. Galois cohomology classes coming from correspondences.

Let X, Y be smooth proper irreducible w-marked curves over K, a number field or a finite extension of $\mathbb{Q}_\ell$ for $\ell \neq p$. .Let Γ be a correspondence from X to Y, with empty "bad set". Let

$$\tau_\Gamma \in H^1(G_K, H^2(\overline{X} \times \overline{Y}; \mathbb{Z}_p(2))$$

be the image of the class σ_Γ constructed in the previous sections where $\bar{}$ means passage to $\overline{K}$. Since $\mathbb{Z}_p(2)$ has no p-torsion, and the cohomology of curves over algebraically closed fields have no p-torsion we may project to Künneth components, and we let

$$\eta_\Gamma \in H^1(G_K, H^1(\overline{X}; \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\overline{Y}; \mathbb{Z}_p(1)))$$

be the class induced from τ_Γ under the canonical projection

$$H^2(\overline{X} \times \overline{Y}; \mathbb{Z}_p(2) \to H^1(\overline{X}; \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} H^1(\overline{Y}; \mathbb{Z}_p(1)).$$

Using the Proposition of §3, if we have three smooth w-marked curves X,Y,Z and correspondences F, G as in §3 with composition equal to Γ, then

$$\eta_\Gamma \in H^1(G_K,\, H^1(\overline{X};\, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\overline{Z};\, \mathbb{Z}_p(1)))$$

is given by the formula

$$(2) \qquad \eta_\Gamma = (F^* \otimes 1)\cdot\eta_G + (1 \otimes G_*)\cdot\eta_F$$

where

$$(3) \qquad F^* : H^1(\overline{Y};\, \mathbb{Z}_p(1)) \to H^1(\overline{X};\, \mathbb{Z}_p(1)) \text{ and}$$
$$G_* : H^1(\overline{Y};\, \mathbb{Z}_p(1)) \to H^1(\overline{Z};\, \mathbb{Z}_p(1))$$

are the inverse and direct image mappings on the cohomology groups cited induced from the respective correspondences, and the "parentheses" ( ) occurring in (2) means the natural mappings induced from these on 1-dimensional G_K cohomology.

§5. Bilateral derivations: first visit.

For use in subsequent paragraphs, let us quickly introduce a bit of algebra somewhat separately from the context in which it will arise. We will revisit this topic in significantly greater detail in Chapter 9, below.

Let $\mathcal{G}$ be a $\mathbb{Z}_p$-algebra not necessarily commutative, or noetherian.

Definition: A **bilateral derivation** from a $\mathbb{Z}_p$-algebra $\mathcal{G}$ to an $\mathcal{G}\otimes_{\mathbb{Z}_p}\mathcal{G}$-module N is a $\mathbb{Z}_p$-linear mapping

$$\mathbb{D}: \mathcal{G} \to N$$

such that $\mathbb{D}(x\cdot y) = (x\otimes 1)\cdot\mathbb{D}y + (1\otimes y)\cdot\mathbb{D}x$ for all x,y in $\mathcal{G}$.

Example: The $\mathbb{Z}_p$-linear homomorphism

$$\delta: \mathcal{G} \to N = \mathcal{G} \otimes_{\mathbb{Z}_p} \mathcal{G}$$

given by $\delta(\alpha) = \alpha \otimes 1 - 1 \otimes \alpha$, for $\alpha \in \mathcal{G}$ is a bilateral driviation.

If $\mathbb{D}: \mathcal{G} \to N$ is a bilateral derivation, and if x and y are commuting elements in $\mathcal{G}$, then we have

(4) $$\delta(x) \cdot \mathbb{D}(y) = \delta(y) \cdot \mathbb{D}x.$$

Suppose, now, that $\mathcal{G}$ is a commutative $\mathbb{Z}_p$-algebra. Given an $\mathcal{G} \otimes_{\mathbb{Z}_p} \mathcal{G}$-module N, let $N_\delta \subset N$ denote the intersection of the kernels of multiplication by the elements $\delta(\alpha) = \alpha \otimes 1 - 1 \otimes \alpha$ acting on N, for all $\alpha \in \mathcal{G}$.

Note that N_δ is naturally an $\mathcal{G}$-module, for its $\mathcal{G} \otimes_{\mathbb{Z}_p} \mathcal{G}$-module action factors through the natural homomorphism $\mu: \mathcal{G} \otimes_{\mathbb{Z}_p} \mathcal{G} \to \mathcal{G}$.

Lemma: If $\mathcal{G}$ is a commutative $\mathbb{Z}_p$-algebra, N an $\mathcal{G} \otimes_{\mathbb{Z}_p} \mathcal{G}$-module, $\mathbb{D}: \mathcal{G} \to N$ a bilateral derivation, and $I \subset \mathcal{G}$ an ideal such that $1 \otimes I$ and $I \otimes 1$ annihilate N, then the restriction of $\mathbb{D}$ to $I \subset \mathcal{G}$, induces an $\mathcal{G}$-module homomorphism

(5) $$\tilde{\mathbb{D}}: I / I^2 \to N_\delta$$

Proof: If $\beta \in I$, then $(\alpha \otimes 1) \cdot \mathbb{D}\beta = \mathbb{D}(\alpha \cdot \beta) = \mathbb{D}(\beta \cdot \alpha) = (1 \otimes \alpha)\mathbb{D}\beta$ for all $\alpha \in \mathcal{G}$. If both α and β are in I, then the above gives $\mathbb{D}(\alpha \cdot \beta) = 0$.

□

§6. Self-correspondences.

Let X be a smooth proper irreducible w-marked curve over K, a number field or a finite extension of $\mathbb{Q}_\ell$ for $\ell \neq p$. A correspondence F from X to X is **self-adjoint** if the two induced mappings

$$F^* : H^1(\bar{X}; \mathbb{Z}_p(1)) \to H^1(\bar{X}; \mathbb{Z}_p(1))$$

and

$$F_* : H^1(\bar{X}; \mathbb{Z}_p(1)) \to H^1(\bar{X}; \mathbb{Z}_p(1))$$

agree.

We view $H^1(\bar{X}; \mathbb{Z}_p(1))$ as $\mathbb{Z}_p[G_K]$-module.

Let $\mathcal{G}_o$ denote an algebra (possibly infinitely generated) of commuting, self-adjoint correspondences from X to X, the multiplicative structure being given by composition. Let $\mathcal{G} = \mathcal{G}_o \otimes \mathbb{Z}_p$. Then $H^1(\bar{X}; \mathbb{Z}_p(1))$ is an $\mathcal{G}$-module, its $\mathcal{G}$-action commuting with the action of G_K, and the action of $\Gamma \in \mathcal{G}_o$ being given either as Γ^* or Γ_*, these being the same since Γ is assumed self-adjoint. Let B denote the image of $\mathcal{G}$ in $\mathrm{End}_{\mathbb{Z}_p}(H^1(\bar{X}; \mathbb{Z}_p(1)))$, so that B is a finite flat $\mathbb{Z}_p$-algebra.

At this point we wish to **choose** a maximal ideal $\underline{m} \subset B$ and let A denote the completion of B at $\underline{m}$, so that A occurs as a factor algebra of the semi-local algebra B Let H:= the completion of the B-module $H^1(\bar{X}; \mathbb{Z}_p(1))$ with respect to $\underline{m}$, or equivalently, $H = H^1(\bar{X}; \mathbb{Z}_p(1)) \otimes_B A$. We

have that H is an $A[G_K]$-module.

Let I denote the kernel of the projection of $\mathcal{G}$ to A:

$$0 \to I \to \mathcal{G} \to A \to 0.$$

The $\mathbb{Z}_p$-module $H \otimes_{\mathbb{Z}_p} H$ has a natural $A \otimes_{\mathbb{Z}_p} A$ module structure which commutes with its natural $G_K \times G_K$ action. So, the cohomology group $H^1(G_K, H \otimes_{\mathbb{Z}_p} H)$ is endowed with an $A \otimes_{\mathbb{Z}_p} A$-module structure.

The discussion up to this point has given us the

Proposition. There is a bilateral derivation

$$\mathbb{D} : \mathcal{G} \to H^1(G_K, H \otimes_{\mathbb{Z}_p} H) \tag{6}$$

uniquely determined by the requirement that the image of $\mathbb{D}(\Gamma)$ in $H^1(G_K, H \otimes_{\mathbb{Z}_p} H)$ be equal to η_Γ. Let $I = \ker(\mathcal{G} \to A)$. Then the restriction of $\mathbb{D}$ to I induces (see (5) above) an A-module homomorphism,

$$\tilde{\mathbb{D}} : I/I^2 \to H^1(G_K, H \otimes_{\mathbb{Z}_p} H)_\delta \,. \tag{7}$$

Proof: The proof of this Proposition follows directly from formula (2) of §4, the fact that our correspondences are self-adjoint, the definition of bilateral derivation, and the lemma of §5.

□

Define the derivation $\mathcal{D}$ of $\mathcal{G}$ as follows: The natural projection $H \otimes_{\mathbb{Z}_p} H \to H \otimes_A H$ induces a homomorphism on cohomology

$$H^1(G_K, H \otimes_{\mathbb{Z}_p} H) \to H^1(G_K, H \otimes_A H)$$

which when composed with (6) gives a (plain old!) derivation

(8) $\mathfrak{D}: \mathfrak{G} \to H^1(G_K, H \otimes_A H)$

where $H^1(G_K, H \otimes_A H)$ is viewed as $\mathfrak{G}$-module. Note that $\mathfrak{D}$ annihilates I^2 and when restricted to I factors through an A-homomorphism

(9) $\tilde{\mathfrak{D}} : I/I^2 \to H^1(G_K, H \otimes_A H).$

§7. Divisibility of $\tilde{\mathfrak{D}}$ by η.

To prepare for the "Divisibility Proposition" below we need two elementary lemmas in commutative algebra. For the first, let B be a commutative reduced ring, finite flat over $\mathbb{Z}_p$ and Gorenstein. Since B is reduced, if η is a congruence element for B, we have that η is a non-zero-divisor of B.

Let M,N be free B-modules of finite rank. Consider the composition of $B \otimes_{\mathbb{Z}_p} B$ -module homomorphisms

(10) $j: (M \otimes_{\mathbb{Z}_p} N)_\delta \subset M \otimes_{\mathbb{Z}_p} N \to M \otimes_B N,$

where we recall the notation "subscript δ" of §5: The B-module $(M \otimes_{\mathbb{Z}_p} N)_\delta$ is, by definition, the intersection of the kernels of multiplication by $\delta(x) = x \otimes 1 - 1 \otimes x$ (all $x \in B$) in the $B \otimes_{\mathbb{Z}_p} B$-module $M \otimes_{\mathbb{Z}_p} N$. We can (and do) view j as B-module homomorphism since the first and last modules in (10) are canonically B-modules.

Lemma 1. The B-module homomorphism j identifies the

B-module $(M\otimes_{\mathbb{Z}_p}N)_\delta$ with the submodule $\eta\cdot(M\otimes_B N) \subset M\otimes_B N$.

Proof: The statement being "bilinear" in M and N (e.g., $((M_1\oplus M_2)\otimes_{\mathbb{Z}_p}N)_\delta$ is canonically isomorphic to

$$(M_1\otimes_{\mathbb{Z}_p}N)_\delta \oplus (M_2\otimes_{\mathbb{Z}_p}N)_\delta,$$

etc.) we may suppose that M and N are both free of rank 1. So let us rewrite (10) for this case:

$$(11) \qquad j:\ (B\otimes_{\mathbb{Z}_p}B)_\delta \to B\otimes_{\mathbb{Z}_p}B \xrightarrow{\mu} B,$$

where the modules involved are viewed as $B\otimes_{\mathbb{Z}_p}B$-modules, the morphisms being $B\otimes_{\mathbb{Z}_p}B$-linear. Now "dualize" (11), to get

$$(12) \qquad \mathrm{Hom}_{\mathbb{Z}_p}(B,\mathbb{Z}_p) \to \mathrm{Hom}_{\mathbb{Z}_p}(B\otimes_{\mathbb{Z}_p}B, \mathbb{Z}_p) \to \mathrm{Hom}_{\mathbb{Z}_p}((B\otimes_{\mathbb{Z}_p}B)_\delta, \mathbb{Z}_p),$$

which we identify with the diagram of $B\otimes_{\mathbb{Z}_p}B$-modules

$$B \xrightarrow{\hat{\mu}} B\otimes_{\mathbb{Z}_p}B \xrightarrow{\mu} B\otimes_B B = B.$$

But the composition $\mu\circ\hat{\mu}$ is simply multiplication by η (by definition of congruence element).

□

Now assume that H is free over A (in which case A is then Gorenstein, since H has a principal polarization and A acts in a self-adjoint way) , **and that A is reduced**. Let

η be a (fixed) congruence element for A. By Lemma 1 we have that there is a "canonical" isomorphism β of A-modules making the following square commutative:

$$
\begin{array}{ccccc}
(H\otimes_{\mathbb{Z}_p}H)_\delta & \subset & H\otimes_{\mathbb{Z}_p}H & \to & H\otimes_A H \\
\beta\downarrow\cong & & & & \downarrow = \\
H\otimes_A H & & \xrightarrow[\eta]{} & & H\otimes_A H\,.
\end{array} \tag{13}
$$

Of course, β is dependent upon the choice of congruence element η.

Lemma 2: If for every Jordan-Holder constituent M of the $\mathbb{Z}_p[G_K]$-module $H\otimes_{\mathbb{Z}_p}H$ we have $M^{G_K}=0$, then

$$H^1(G_K, H\otimes_{\mathbb{Z}_p}H)_\delta = H^1(G_K, (H\otimes_{\mathbb{Z}_p}H)_\delta).$$

Proof: This is quite general: Let N be a $\mathbb{Z}_p[G_K]$-module such that every one of its Jordan-Holder constituents M has $M^{G_K}=0$ (equivalently, this is true for every subquotient $\mathbb{Z}_p[G_K]$-module attached to N) and let Ψ denote a set of $\mathbb{Z}_p[G_K]$-endomorphisms of N (say a finite set, $\Psi=\{\psi_1,\ldots,\psi_\nu\}$ but finiteness is not really necessary). Then

$$H^1(G_K, N[\Psi]) = H^1(G_K, N)\,[\Psi],$$

where $[\Psi]$ means the intersection of the kernels of the endomorphisms $\psi\in\Psi$.

This we prove by induction on ν, using the fact that the hypothesis made for N is also valid for any of its $\mathbb{Z}_p[G_K]$-

submodules, and so we are reduced to showing our lemma for $v=1$. For this, let us consider the exact sequences

$$\begin{array}{ccccccccc} & & & & \tilde{\psi} & & & & \\ 0 & \to & N[\psi] & \to & N & \to & \psi N & \to & 0 \\ & & & & \tilde{\psi}\downarrow & & \downarrow i & & \\ & & & & & & & & \\ & & 0 & \to & \psi N & \to & N & \to & N/\psi N \to 0. \\ & & & & & i & & & \end{array}$$

to distinguish the endomorphism ψ from the homomorphism $N \to \psi N$ we call the latter $\tilde{\psi}$, so that $\psi = i \cdot \tilde{\psi}$. By virtue of our hypothesis, we have that $H^0(G_K, N/\psi N)=0$, and therefore (by the exact sequence induced from the lower line of our diagram)

$$i_*: H^1(G_K, \psi N) \to H^1(G_K, N)$$

is injective, and consequently,

$$\begin{aligned} H^1(G_K, N)[\psi] &= \ker\{ \psi: H^1(G_K, N) \to H^1(G_K, N)\} = \\ &= \ker\{ \tilde{\psi}: H^1(G_K, N) \to H^1(G_K, \psi N)\}. \end{aligned}$$

But $H^0(G_K, \psi N)$ also vanishes by our hypothesis, and therefore the exact sequence induced from the upper line in the diagram gives

$$H^1(G_K, N[\psi]) = \ker\{ \tilde{\psi}: H^1(G_K, N) \to H^1(G_K, \psi N)\} = H^1(G_K, N)[\psi] .$$

□

Assume, from now on, the hypothesis of the above lemma.

The restriction to $I \subset \mathcal{G}$ of the bilateral derivation $\mathbb{D}: \mathcal{G} \to H^1(G_K, H \otimes_{\mathbb{Z}_p} H)$ has given us an A-homomorphism which we called $\tilde{\mathbb{D}}: I/I^2 \to H^1(G_K, H \otimes_{\mathbb{Z}_p} H)_\delta$. By the above lemma, and by (13) we may make the identifications

$$(14)\quad H^1(G_K, H \otimes_{\mathbb{Z}_p} H)_\delta = H^1(G_K, (H \otimes_{\mathbb{Z}_p} H)_\delta) \overset{\beta}{\cong} H^1(G_K, H \otimes_A H).$$

Composing $\tilde{\mathbb{D}}$ with the isomorphism of A-modules given in (14) we obtain an A-homomorphism which we denote

$$(15)\quad \Delta: I/I^2 \to H^1(G_K, H \otimes_A H).$$

The above constructions and discussion give us the following simple relationship between $\tilde{\mathcal{D}}$ of (9) and Δ of (15):

Divisibility Proposition: $\eta \cdot \Delta = \tilde{\mathcal{D}}$,

(i.e., $\tilde{\mathcal{D}}$ is "divisible" by η).

Corollary: There is a unique derivation of A,

$$(16)\quad \Theta: A \to H^1(G_K, H \otimes_A H/\eta \cdot H \otimes_A H),$$

fitting into the commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & I & \to & \mathcal{G} & \to & A & \to & 0 \\ & & \Delta \downarrow & & \mathcal{D} \downarrow & & \Theta \downarrow & & \\ 0 & \to & H^1(G_K, H \otimes_A H) & \xrightarrow{\eta} & H^1(G_K, H \otimes_A H) & \to & H^1(G_K, H \otimes_A H/\eta \cdot H \otimes_A H), & & \end{array} \tag{17}$$

where the lower line is a piece of the long exact sequence on cohomology coming from the exact sequence

$$0 \to H \otimes_A H \to H \otimes_A H \to H \otimes_A H/\eta \cdot H \otimes_A H \to 0.$$

□

Chapter eight. Hecke axiomatics

§1. Hecke Curves.

In attempting to clarifying the logical structure of some of the arguments to follow I found it useful for myself, and I hope also for the reader, to simply "axiomatize" the constellation of geometric properties of the modular curves (for the modular groups $\Gamma_0(N)$, N square-free) that seem particularly critical to us. What follows, then, is an exposition of an axiomatic set-up of which I know only one example: namely the tower of modular curves $X_0(N)$ for N squarefree (cf. Chapter 8.5 below).

Let $\mathfrak{N}$ denote the set of square-free positive integers.

Definition 1. A **Hecke Tower** $\mathcal{X}$ is a collection of smooth projective, geometrically irreducible curves X_n over Spec $\mathbb{Q}$, for $n \in \mathfrak{N}$, with the following extra structure.

Data:

(a) For each pair $m,n \in \mathfrak{N}$, with m dividing n, we are given a nonconstant morphism defined over Spec $\mathbb{Q}$,

$$j_{n,m}: X_n \to X_m ,$$

(b) For each pair $m,n \in \mathfrak{N}$, with m dividing n, we are given an involution defined over Spec $\mathbb{Q}$,

$$w_m: X_n \to X_n .$$

This data is required to satisfy the following list of

Hypotheses:

(i) Transitivity of the j's:

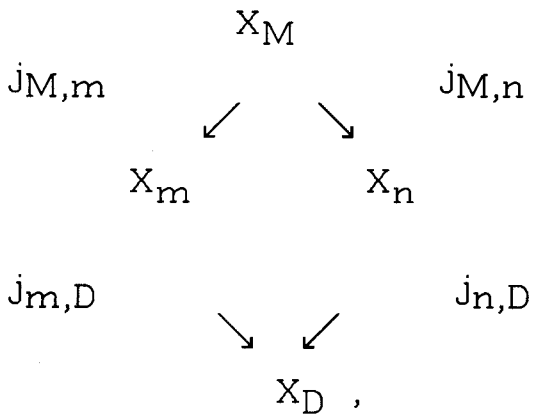
Given m, n, r in $\mathfrak{N}$ each dividing the next, we have that the composition

$$X_r \xrightarrow{j_{r,n}} X_n \xrightarrow{j_{n,m}} X_m$$

is equal to $j_{r,m}$ (i.e, we have a "tower of curves" indexed multiplicatively by $\mathfrak{N}$).

(ii) The multiplicative nature of the j's:

Let $m,n \in \mathfrak{N}$, and put M = the least common multiple of m and n, and D = the greatest common divisor of m and n. We have (by (i) above) a commutative diagram



which gives us a mapping of the curve X_M to the fiber product of curves $X_m \times_{X_D} X_n$. We hypothesize that this mapping is a birational isomorphism. In particular, this implies that the fiber products $X_m \times_{X_D} X_n$ are geometrically irreducible.

(iii) The multiplicative nature of the w's:

If m_1 and m_2 are relatively prime positive divisors of $n \in \mathfrak{N}$ then the involutions w_{m_1} and w_{m_2} of X_n commute and their composition is equal to $w_{m_1 \cdot m_2}$.

(iv) The relationship between the j's and the w's:

Given m, n, r in $\mathfrak{N}$, each dividing the next, then w_m commutes with $j_{r,n}$, i.e., we have a commutative diagram

$$\begin{array}{ccc} & \overset{w_m}{} & \\ X_r & \rightarrow & X_r \\ {\scriptstyle j_{r,n}}\downarrow & & \downarrow{\scriptstyle j_{r,n}} \\ X_n & \rightarrow & X_n \\ & {\scriptstyle w_m} & \end{array} .$$

(v) Models over Spec $\mathbb{Z}$. We hypothesize further that each curve $X_{n/\mathrm{Spec}\ \mathbb{Q}}$ ($n \in \mathfrak{N}$) of the Hecke Tower be given a proper, regular, semi-stable model over Spec $\mathbb{Z}$, denoted $X_{n/\mathrm{Spec}\ \mathbb{Z}}$. The model $X_{n/\mathrm{Spec}\ \mathbb{Z}}$ is hypothesized to be smooth over Spec $\mathbb{Z}[1/n]$.

(vi) The mappings w and j over Spec $\mathbb{Z}$. For all m,n $\in \mathfrak{N}$ with m dividing n, we require the involutions w_m extend to involutions $w_{m/\mathrm{Spec}\ \mathbb{Z}}$ of these models. We require the morphisms $j_{n,m}$ extend to morphisms

$$j_{n,m/\mathrm{Spec}\ \mathbb{Z}} : X_{n/\mathrm{Spec}\ \mathbb{Z}} \rightarrow X_{m/\mathrm{Spec}\ \mathbb{Z}}.$$

Moreover, if r is any prime number not dividing n, we

want the restriction, $j_{n,m/\text{Spec } \mathbf{F}_r}$, of the morphism $j_{n,m/\text{Spec } \mathbb{Z}}$ to characteristic r to be a generically étale mapping of the curve $X_{n/\text{Spec } \mathbf{F}_r}$ onto $X_{m/\text{Spec } \mathbf{F}_r}$.

(vii) The "Eichler -Shimura" relation and Hecke Correspondences: For square-free positive integers n, m which are relatively prime, let $\Gamma_{n,m} \subset X_m \times X_m$ denote the image of the mapping

$$j_{n\cdot m,m} \times (j_{n\cdot m,m} \circ w_n) : X_{n\cdot m} \to X_n \times X_n$$

which we view as being an irreducible geometric correspondence from $X_{n/\mathbb{Q}}$ to $X_{n/\mathbb{Q}}$. We will refer to $\Gamma_{n,m/\mathbb{Q}}$ as the n-th **Hecke Correspondence** and sometimes abbreviate this notation to just Γ_n if the curve X_m on which we are operating is "understood". Let ℓ be a prime number not dividing $m \in \mathfrak{N}$ and let

$$\Gamma_{\ell/\mathbb{Z}} = \Gamma_{\ell,m/\mathbb{Z}} \subset X_m \times X_{m/\text{Spec } \mathbb{Z}}$$

denote the Zariski closure of $\Gamma_{\ell,m/\mathbb{Q}}$ in the model of $X_m \times X_m$ over Spec $\mathbb{Z}$ given to us by **(v)**. We hypothesize that the fiber, $\Gamma_{\ell/\mathbf{F}_\ell}$, of $\Gamma_{\ell/\mathbb{Z}}$ over Spec $\mathbf{F}_\ell$ is the reduced divisor in the regular surface $X_m \times X_{m/\mathbf{F}_\ell}$ consisting of two irreducible components: $\text{Frob}_\ell \subset X_m \times X_{m/\mathbf{F}_\ell}$, the graph of the Frobenius mapping, and $\text{Frob}_\ell^{\#} \subset X_m \times X_{m/\mathbf{F}_\ell}$, its transpose (i.e., $\text{Frob}_\ell^{\#}$ is the image of Frob_ℓ under the symmetry of $X_m \times X_m$ wich permutes the two factor X_m's).

Lemma 1.

(a) The subvarieties $\Gamma_n = \Gamma_{n,m} \subset X_m \times X_m$ are invariant under the involution of $X_m \times X_m$ which interchanges factors.

(b) The correspondences Γ_n are self-adjoint.

(c) If n,m are mutually relatively prime square-free positive integers, then we have $\Gamma_n \circ \Gamma_m = \Gamma_{n \cdot m}$ where $\circ$ denotes composition of correspondences.

(d) The correspondences Γ_n ($n \in \mathfrak{N}$) all commute (under "composition of correspondences").

(e) Let p and ℓ be distinct prime numbers not dividing $m \in \mathfrak{N}$. The action $\Gamma_{\ell *}: H^1(\bar{X}_m; \mathbb{Q}_p) \to H^1(\bar{X}_m; \mathbb{Q}_p)$ of the Hecke correspondence Γ_ℓ on one-dimensional étale cohomology of $\bar{X}_m = X_m \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$ with coefficients in $\mathbb{Q}_p$ is given by

(The "Eichler Shimura" relation)

$$\Gamma_{\ell *} = \mathrm{Frob}_{\ell *} + \mathrm{Frob}_\ell{}^*.$$

Proof: (a) Since w_n is an involution, the subvariety $\Gamma_n = \Gamma_{n,m} \subset X_m \times X_m$ can also be viewed as the image of the mapping

$$(j_{n \cdot m, m} \circ w_n) \times j_{n \cdot m, m} : X_{n \cdot m} \to X_m \times X_m,$$

i.e., $\Gamma_n \subset X_m \times X_m$ is invariant under the involution of $X_m \times X_m$ which interchanges the factors. Assertion **(b)**, that the correspondences Γ_n are Hermitian follows

immediately from **(a)**. As for **(c)**, we must show that $\pi_{Y*}\{\pi_X^*(\Gamma_m) \cap \pi_Z^*(\Gamma_n)\} = \Gamma_{n\cdot m}$ (cf. §2 of Chapter 7) and this is straightforward from the definition of the Γ's, using that $w_n \cdot w_m = w_{n\cdot m}$. Assertion **(d)** then immediately follows. Assertion **(e)** comes directly from the hypothesis **(vii)** above and the comparison theorem for étale cohomology of smooth proper schemes.

□

Definition: Let N be a square-free positive integer. A **Hecke curve of level** N is a curve X over Spec $\mathbb{Q}$ given along with a Hecke Tower $\mathcal{X}$ and an isomorphism $X \cong X_N$ over $\mathbb{Q}$, where the curve X_N is the N-th curve of the tower $\mathcal{X}$.

§2. Admissible w-markings on Hecke Curves. Let N be a square-free positive integer. Let us be given a Hecke curve X of level N as in §1, i.e., $X \cong X_N$, the N-th curve in a Hecke Tower $\mathcal{X} = \{X_n\}_{n\in\mathfrak{N}}$. Let w be an integer, and f_X a w-marking on $X_{/\mathbb{Q}}$ (as defined in Chapter 7 §1). Thus f_X is a rational section of the line bundle $(\Omega_{X_{/\mathbb{Q}}})^{\otimes w}$ on X. Let $\mathrm{Div}(f_X)$ denote the divisor of zeroes and poles of the rational section f_X of the pluricanonical sheaf $(\Omega_{X^{sm}/\mathrm{Spec}\ \mathbb{Z}})^{\otimes w}$ on the smooth locus of the stable model $X_{/\mathrm{Spec}\ \mathbb{Z}}$.

Notation: For each $n\in\mathfrak{N}$ relatively prime to N, denote by $f_{X,n}$, or f_n for short, the 0-marking (alias: *nontrivial rational function*) on Γ_n induced, as in Chapter 7 §1, by the w-marking f_X on each of the two factors in $X\times X$.

Note that multiplying the w-marking f_X by a non-zero

rational number does not change the rational functions $f_{X,n}$, $n \in \mathfrak{N}$, and the mapping $f_X \mapsto f_{X,n}$ is multiplicative in the w-marking f_X, for each $n \in \mathfrak{N}$.

Now fix a w-marking f_X, and for $n \in \mathfrak{N}$, we let f_n denote $f_{X,n}$.

Lemma 1: If ℓ is a prime number not dividing N, then the vertical part, $(f_\ell)_{vert}$, of the divisor of zeroes and poles of the rational function f_ℓ on $\Gamma_{\ell}/\mathrm{Spec}\ \mathbb{Z}$ is supported entirely in characteristics dividing $\ell \cdot N$. In characteristic ℓ this divisor, $(f_\ell)_{vert/\mathbf{F}_\ell}$ when viewed as a Cartier divisor on the smooth surface $X \times X_{/\mathbf{F}_\ell}$ is given by the formula

$$(f_\ell)_{vert/\mathbf{F}_\ell} = w \cdot (\mathrm{Frob}_\ell{}^{\#} - \mathrm{Frob}_\ell).$$

(Recall that Frob_ℓ is the graph of ℓ-Frobenius and $\mathrm{Frob}_\ell{}^{\#}$ is its transpose).

Proof: Let r be a prime number not dividing N. Since $X_{N/\mathbf{F}_r}$ is geometrically irreducible for any prime number r not dividing N (and since $\mathbb{Z}$ is a PID) we may "force" the vertical part of the divisor $\mathrm{Div}(f_X)$ in all such characteristics r to vanish, by multipling f_X by a suitable nonzero rational number. Recalling that the functions f_n are left unchanged by multiplying f_X by any nonzero rational number, we may (and do) suppose that we are in the case where the divisor $\mathrm{Div}(f_X)$ has no vertical component in characteristics r not dividing N.

Now let r be a prime number not dividing $\ell \cdot N$. Noting

that $j_{\ell\cdot N,N/\mathrm{Spec}\ \mathbf{F}_r}$ has been hypothesized to be a generically étale mapping of the curve $X_{\ell\cdot N/\mathrm{Spec}\ \mathbf{F}_r}$ onto $X_{N/\mathrm{Spec}\ \mathbf{F}_r}$ (in Definition 1, **(vi)**, in §1 above) it follows that the projection of Γ_ℓ to each factor of $X_N \times X_N$ is generically étale in characteristic r, and therefore $(f_\ell)_{vert}$ has no support in characteristic r.

It remains to consider the case when $r=\ell$. Hypothesis **(vii)** of Definition 1 allows us to explicitly compute the support of $(f_\ell)_{vert}$ in characteristic ℓ and this computation gives us the formula displayed in our Lemma. Namely, the pullback of f_X to Frob_ℓ under $j_{\ell\cdot N,N}$ in characteristic ℓ contributes nothing to the vertical component of (f_ℓ) since the projection of Frob_ℓ, the graph of ℓ-Frobenius, to the first factor of $X_N \times X_{N/\mathrm{Spec}\ \mathbf{F}_\ell}$ is étale. The pullback, however, of f_X to $\mathrm{Frob}_\ell\#$ under $j_{\ell\cdot N,N}$ in characteristic ℓ "picks up a factor of ℓ^w" since $j_{\ell\cdot N,N}$ is purely inseparable on $\mathrm{Frob}_\ell\#$ and looks locally like " $z \mapsto z^\ell$", and since we are working in the sheaf $(\Omega_{X_N})^{\otimes w}$. Thus the vertical component of the divisor of zeroes and poles of $(j_{\ell\cdot N,N})^*(f_X)$ in characteristic ℓ is given by $w\cdot\mathrm{Frob}_\ell\#$. The roles of Frob_ℓ and of $\mathrm{Frob}_\ell\#$ get reversed when we consider the contribution to f_n of $(j_{\ell\cdot N,N}\circ w_\ell)^*(f_X)$, and this accounts for the formula displayed in our Lemma. □

Definition 2. A w-**marking** f_X on $X_{/\mathbb{Q}}$ will be said to be **admissible** if for all $n\in\mathfrak{N}$ (n relatively prime to N) and for all closed points z of $\Gamma_{n/\mathbb{Q}}$,

$$\text{"ord}_z(f_n)\text{"}=0.$$

Notation: Denote by $\mathcal{GM}(X)$ the set of all admissible markings of X.

Then $\mathcal{GM}(X)$ forms a (commutative) group under multiplication, and the mapping which associates to a marking $f_X \in \mathcal{GM}(X)$ its degree w is a homomorphism

$$\text{(1)} \qquad \mathcal{GM}(X) \xrightarrow{\text{degree}} \mathbb{Z}.$$

§3. The Hecke rings: If X is a Hecke curve of level N, as defined in §1 above, for n any square-free positive integer not dividing N, let $\Gamma_n \subset X \times X$ denote the geometric self-correspondence of X isomorphic to the n-th Hecke correspondence $\Gamma_{n,N} \subset X_N \times X_N$ of the Hecke Tower $\mathcal{X}$ "attached to" X, the isomorphism induced by the isomorphism given between X and X_N. We refer to Γ_n as the n-th Hecke correspondence for X. Let $\mathcal{G}_o = \mathcal{G}_{o,X}$ denote the (commutative) $\mathbb{Z}$-algebra of self-correspondences of X generated by the Hecke correspondences Γ_n ($n \in \mathfrak{N}$, n relatively prime to N) where the multiplication is given by composition of correspondences. From Lemma 1 **(c)**, $\mathcal{G}_o$ is generated by the Γ_ℓ's where ℓ runs through all prime numbers not dividing N. Let $\mathcal{G} = \mathcal{G}_o \otimes_{\mathbb{Z}} \mathbb{Z}_p$ be the $\mathbb{Z}_p$-algebra obtained by tensor product. Then the rule which associates to each $\Gamma_n \in \mathcal{G}_o$ the endomorphism Γ_{n*} of $H^1(X_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))$ extends to define a unique action of the $\mathbb{Z}_p$-algebra $\mathcal{G}$ on $H^1(X_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))$. Let B the $\mathbb{Z}_p$-algebra quotient of $\mathcal{G}$ operating faithfully on $H^1(X_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))$ (notation here as in Chapter 7). We have that B is a finite flat $\mathbb{Z}_p$-algebra, hence semi-local. Fixing one of the (finitely many) maximal ideals $\underline{m} \subset B$, put $A := B_{\underline{m}}$, i.e., the completion of B at the maximal ideal $\underline{m}$, and

$$H := H^1(\bar{X},\mathbb{Z}_p(1))\otimes_B B_{\underline{m}},$$

viewed now as $A[G_{\mathbb{Q},\Sigma}]$-module. Here Σ is the set of prime divisors of $p\cdot N$.

Definition 3: The maximal ideal $\underline{m} \subset B$ will be said to be **admissible** if its residual characteristic, p, is odd, and the following four hypotheses hold.

(1) The ring A is reduced.

(2) The A-module H is free of rank 2.

(3) As usual, let $\rho : G_{\mathbb{Q},\Sigma} \to \mathrm{Aut}_A(H) \cong GL_2(A)$ denote the representation coming from the $G_{\mathbb{Q}}$ action on H, where Σ is as above, and the $\cong$ is given by the choice of an A-basis of H assuming **(2)**, and let $\bar{\rho} : G_{\mathbb{Q},\Sigma} \to GL_2(k)$ denote the residual representation associated to ρ, where k is the residue field of A. We hypothesize that $\bar{\rho}$ is ramified, and cleanly ramified, at each prime divisor of N. We hypothesize further that $\mathrm{Sym}_k{}^2\bar{\rho}$ is absolutely irreducible.

Note: The "Weil pairing" for 1-dimensional cohomology of the curve $X/\bar{\mathbb{Q}}$ induces a principal polarization on H, and by Lemma 1 of §1, the action of A is Hermitian with respect to this pairing. It follows from our hypotheses up to this point and from the Lemma of §2 of Chapter 3 that A is Gorenstein.

(4) Let $W^* := \mathrm{Sym}_A{}^2(H)$ and $W = \mathrm{Hom}_{\mathbb{Z}_p}(W^*,\mu)$ these both being considered as $A[G_{\mathbb{Q}}]$-modules. We assume the "Δ-hypothesis" for $\alpha \in A$, for all non-zero-divisors $\alpha \in \Gamma$, as in §5 of Chapter 2.

§4. The Flach Classes.

Let us give ourselves now a Hecke Curve X of level N together with an admissible w-marking f_X and an admissible maximal ideal $\underline{m}$, keeping the notation of the previous §'s.

Then for each prime number ℓ not dividing p·N we obtain (using hypothesis **(1)** of §2 above, and the constructions of Chapter 6) a cohomology class,

$$\sigma_\ell = \sigma(f_\ell; \Gamma_\ell / X\times X) \in H^3(X\times X_{/\mathbb{Q}}, \mathbb{Z}_p(2)).$$

Put $V = X\times X$ and $\bar{V} = V\otimes_{\mathbb{Q}}\bar{\mathbb{Q}}$. Since, by the Lemma of §4 of Chapter 6, the edge-homomorphism $e: H^3(V,\mathbb{Z}_p(2)) \to H^0(G_K,H^3(\bar{V},\mathbb{Z}_p(2)))$ vanishes (because K is a number field and $H^3(\bar{X}\times\bar{X},\mathbb{Z}_p(2))$ is torsionfree), it follows, as in §4, §5 of Chapter 6, that the Hochschild-Serrre Spectral Sequence yields a natural homomorphism,

$$H^3(V,\mathbb{Z}_p(2)) \to H^1(G_K,H^2(\bar{V},\mathbb{Z}_p(2)))$$

and, conforming to prior notational conventions, we denote by $\sigma'_\ell = \sigma'(f_\ell; \Gamma_\ell / X\times X) \in H^1(G_K,H^2(\bar{X}\times\bar{X},\mathbb{Z}_p(2)))$ the image of $\sigma(f_\ell; \Gamma_\ell / X\times X)$ under this homomorphism.

Now let

$$(2) \qquad \tilde{\sigma}_\ell \in H^1(G_{\mathbb{Q}}, H^1(\bar{X},\mathbb{Z}_p(1))\otimes_{\mathbb{Z}_p} H^1(\bar{X},\mathbb{Z}_p(1)))$$

denote the image of σ'_ℓ under the natural mapping induced on cohomology from Künneth projection

$$H^2(\bar{X}\times\bar{X},\mathbb{Z}_p(2)) \to H^1(\bar{X},\mathbb{Z}_p(1))\otimes_{\mathbb{Z}_p} H^1(\bar{X},\mathbb{Z}_p(1)).$$

Let us consider the "ramification" of the classes σ'_ℓ and $\tilde{\sigma}_\ell$.

As for the behavior of $\tilde{\sigma}_\ell$ restricted to the decomposition groups at primes dividing $N \cdot p$, we defer this to § below. As for its behavior at primes r not dividing $N \cdot p$, we have, from Chapter 7, that the "ramification" of σ'_ℓ is measured by the divisor $\mathrm{Ram}_r(\sigma_\ell) \in \mathrm{Div}(X_{/\mathbf{F}_r} \times X_{/\mathbf{F}_r})$ given by the "part" of the Cartier divisor (f_ℓ) which is *vertically supported in characteristic* r. By the hypothesis **(2)** of §2 above, we have then that σ_ℓ is *unramified* except possibly in characteristics dividing $\ell \cdot N \cdot p$. In characteristic ℓ, we have, by the hypothesis **(3)** of §2 above, the formula:

$$(3) \qquad \mathrm{Ram}_\ell(\sigma_\ell) = w \cdot (\mathrm{Frob}_\ell - \mathrm{Frob}_\ell^*).$$

Definition 4: Let $(X, f_X, \underline{m})$ be a triple, where X is a Hecke Curve, f_X an admissible w-marking on X, and $\underline{m}$ an admissible maximal ideal (we also use the same notation, $\underline{m}$, for the maximal ideal of the ring $A = B_{\underline{m}}$; cf. Definitions 2,3 above).

For each prime number ℓ not dividing N the ℓ-th **Flach Class**

$$c(\ell) \in H^1(G_{\mathbb{Q}, \Sigma \cup \{\ell\}}, W^*)$$

is defined to be the image of the class $\tilde{\sigma}_\ell$ under the natural projection

$$H^1(G_{\mathbb{Q}}, H^1(\bar{X}, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\bar{X}, \mathbb{Z}_p(1))) \to H^1(G_{\mathbb{Q}}, W^*).$$

§5. Cohesive Flach Systems attached to Hecke

curves.

Theorem: Let X be a Hecke curve endowed with an admissible w-marking f_X, and an admissible maximal ideal $\underline{m} \subset A$ (cf. above, for the definition of A, which is Gorenstein in this situation). Let $p > 2$ be the residual characteristic of $\underline{m}$. The rule $\ell \mapsto c(\ell)$ assigning to each prime number ℓ not dividing $p \cdot N$ the Flach class $c(\ell)$ is a Cohesive Flach System for the representation

$$\rho: G_{\mathbb{Q},\Sigma} \to GL_2(A)$$

(of depth $w \cdot \eta$, where η is a congruence element for A).

Proof: We defer the proof of the following Proposition to the next §:

Proposition ("finiteness of the Flach classes"): For all prime numbers ℓ not dividing $p \cdot N$, the Flach class $c(\ell)$ lies in $H^1(\underline{X}-\{\ell],W^*) \subset H^1(G_{\mathbb{Q},\Sigma\cup\{\ell\}},W^*)$.

Proof of the Theorem, assuming the Proposition:

We shall check the three properties in the definition of Cohesive Flach System (cf. Chapter 3, §9 above).

Property 1: In fact, we shall show:

Lemma 1: For all primes ℓ not dividing $p \cdot N$, the Chern class of the divisor Frob-Frob$^{\#} \in \mathrm{Div}(X_{\mathbf{F}_\ell} \times X_{\mathbf{F}_\ell})$ under the composition of homomorphisms

$$(4) \qquad H^2(X_{\overline{\mathbf{F}}_\ell} \times X_{\overline{\mathbf{F}}_\ell}, \mathbb{Z}_p(1))^{G_{\mathbf{F}_\ell}} =$$

$$H_s^1(G_{\mathbb{Q}_\ell}, H^2(X_{\overline{\mathbb{Q}}_\ell} \times X_{\overline{\mathbb{Q}}_\ell}, \mathbb{Z}_p(2))) \to$$

$$H_s^1(G_{\mathbb{Q}_\ell}, H^1(X_{\overline{\mathbb{Q}}_\ell}\mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(X_{\overline{\mathbb{Q}}_\ell}\mathbb{Z}_p(1))) \rightarrow$$

$$H_s^1(G_{\mathbb{Q}_\ell}, H \otimes_{\mathbb{Z}_p} H) \rightarrow H_s^1(G_{\mathbb{Q}_\ell}, H \otimes_A H) \rightarrow H_s^1(G_{\mathbb{Q}_\ell}, W^*),$$

is divisible by η, where the subscript "s" refers to the *singular part* as in §5 of Chapter 1.

Proof: Since the Frobenius endomorphism and its transpose commute with the action of A, the image of the Chern class of $(\text{Frob}-\text{Frob}^{\#})$ in $H_s^1(G_{\mathbb{Q}_\ell}, H \otimes_{\mathbb{Z}_p} H) =$

$\text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H \otimes_{\mathbb{Z}_p} H)$ under the chain of homomorphisms in (4) above lies in the submodule

$$(5)\quad \text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), (H \otimes_{\mathbb{Z}_p} H)_\delta) \subset \text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H \otimes_{\mathbb{Z}_p} H).$$

Using Lemma 1 of §7 of Chapter 7, and the diagram (13) we get the commutative diagram

$$\begin{array}{ccc} \text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), (H \otimes_{\mathbb{Z}_p} H)_\delta) & \subset & \text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H \otimes_{\mathbb{Z}_p} H) \\ (6) \qquad \beta \downarrow \cong & & \downarrow \\ \text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H \otimes_A H) & \xrightarrow{\eta} & \text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H \otimes_A H), \end{array}$$

giving us that the image of Chern $(\text{Frob}-\text{Frob}^{\#})$ is divisible by η, thereby establishing our Lemma and property 1).

□

Property 2: We will now be making intensive use of

the notation and theory of §4 of Chapter 3. For $\ell \in \mathcal{L}$, let us call $\varphi_\ell \in H_s^1(G_{\mathbb{Q}_\ell}, W^*)$ the image of the class

$$\text{Chern (Frob-Frob}^{\#}) \in H^2(X_{\overline{\mathbf{F}}_\ell} \times X_{\overline{\mathbf{F}}_\ell}, \mathbb{Z}_p(1))^{G_{\mathbf{F}_\ell}}$$

under the composition of homomorphisms of (4) above. Property 2) follows from:

Lemma 2: For $\ell \in \mathcal{L}$, the class $\varphi_\ell \in H_s^1(G_{\mathbb{Q}_\ell}, W^*)$ is of depth η (i.e., is equal to η times a generator).

Proof: Fix $\ell \in \mathcal{L}$. Consider the image, κ_ℓ, of the class Chern(Frob-Frob$^{\#}$) under the composition of the first three morphisms of (4); namely:

$$\begin{aligned}
(7)\quad \text{Chern(Frob-Frob}^{\#}) \in H^2(X_{\overline{\mathbf{F}}_\ell} \times X_{\overline{\mathbf{F}}_\ell}, \mathbb{Z}_p(1))^{G_{\mathbf{F}_\ell}} = \\
H_s^1(G_{\mathbb{Q}_\ell}, H^2(X_{\overline{\mathbb{Q}}_\ell} \times X_{\overline{\mathbb{Q}}_\ell}, \mathbb{Z}_p(2))) \to \\
\downarrow \\
H_s^1(G_{\mathbb{Q}_\ell}, H^1(X_{\overline{\mathbb{Q}}_\ell} \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(X_{\overline{\mathbb{Q}}_\ell} \mathbb{Z}_p(1))) \to \\
\kappa_\ell \qquad\qquad \in \qquad H_s^1(G_{\mathbb{Q}_\ell}, H \otimes_{\mathbb{Z}_p} H).
\end{aligned}$$

As discussed above, since the correspondence Frob commutes with the action of A, it follows that κ_ℓ lies in the submodule $\text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), (H \otimes_{\mathbb{Z}_p} H)_\delta) \subset$ $\text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H \otimes_{\mathbb{Z}_p} H) = H_s^1(G_{\mathbb{Q}_\ell}, H \otimes_{\mathbb{Z}_p} H)$. Consider the image of $\kappa_\ell \in \text{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H \otimes_{\mathbb{Z}_p} H)$ under the homomorphism,

β: $\mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H\otimes_{\mathbb{Z}_p} H) \to \mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H\otimes_A H)$

of diagram (7) above.

If u and v are the two eigenvalues of the Hecke operator T_ℓ on H we write $H = H_u \oplus H_v$ for the two eigenspaces. Make the choice of a $\mathbb{Z}_p$-generator γ of $\mathbb{Z}_p(1)$ and an A-generator x of H_u. Having made these choices find an A-generator y for H_v such that $x \wedge y = \gamma$ under the Hermitian pairing $\wedge: H_u \otimes H_v \to \mathbb{Z}_p(1)$ determined by the polarization on H (cf. §4 of Chapter 3) In terms of these bases of H_u and H_v, we get an A-basis of $\mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H\otimes_A H)$ which, by Chapter 3, §4, (7) is identified with

(8) $\mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H_u\otimes_A H_v) \oplus \mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H_v\otimes_A H_u)$;

namely, the homomorphism $\{\gamma \mapsto x\otimes y\}$ is an A-basis of $\mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H_u\otimes_A H_v)$ and $\{\gamma \mapsto y\otimes x\}$ is an A-basis of $\mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H_v\otimes_A H_u)$. The image of the Chern class of Frob in $\mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H\otimes_A H)$ is then given by

$$\{\gamma \mapsto u\cdot x\otimes y \oplus v\cdot y\otimes x\},$$

while that of the transpose of Frob is given by

$$\{\gamma \mapsto v\cdot x\otimes y \oplus u\cdot y\otimes x\},$$

so that κ_ℓ is $(u-v)\cdot\{\gamma \mapsto x\otimes y+y\otimes x\}$. Since, for $\ell \in \mathfrak{L}$, u-v is congruent to 2 modulo the maximal ideal m of A, and since $p > 2$, this gives that for $\ell \in \mathfrak{L}$, κ_ℓ is a generator of the subspace of $\mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H\otimes_A H)$ which is fixed under the involution that permutes the two factors H in

$H \otimes_A H$. Since φ_ℓ is the projection to $H_s^1(G_{\mathbb{Q}_\ell}, W^*)$ of $\eta \cdot \beta(\kappa_\ell)$, it follows that φ_ℓ is η times an A-generator of $H_s^1(G_{\mathbb{Q}_\ell}, W^*)$. It follows that $c(\ell)$ has singular depth η at ℓ.

□

Property 3: We shall be checking what is, in essence, a stronger form of the "derivation property" **3)**; namely:

Lemma 3: The rule

$$\Gamma_\ell \mapsto \tilde{\sigma}_\ell \in H^1(G_{\mathbb{Q}}, H^1(\bar{X}, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\bar{X}, \mathbb{Z}_p(1)))$$

which, for each prime number ℓ not dividing $p \cdot N$, assigns to the ℓ-th Hecke correspondence Γ_ℓ the class $\tilde{\sigma}_\ell$ (as defined in §4 above) extends to a bilateral $\mathbb{Z}_p$-derivation of the algebra $\mathcal{Q} = \mathcal{Q}_o \otimes_{\mathbb{Z}} \mathbb{Z}_p$ to the $\mathcal{Q} \otimes_{\mathbb{Z}_p} \mathcal{Q}$-module

$$H^1(G_{\mathbb{Q}}, H^1(\bar{X}, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\bar{X}, \mathbb{Z}_p(1))).$$

Proof: The hypotheses that we have made in our present situation give us all the hypotheses required in the Proposition of §6 of Chapter 7; the conclusion, then, of that Proposition gives us our Lemma. Conforming to our notation there, let us denote the bilateral derivation

$$(9) \qquad \mathbb{D}: \mathcal{Q} \to H^1(G_{\mathbb{Q}}, H^1(\bar{X}, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\bar{X}, \mathbb{Z}_p(1))).$$

□

It then follows from the Corollary to the Divisibility Proposition of §7 of Chapter 7 that the bilateral derivation $\mathbb{D}$ "gives rise to" a unique derivation

(10) Θ: $A \to H^1(G_{\mathbb{Q}}, H \otimes_A H)$

which fits into the commutative diagram (17) of §7 of Chapter 7. This derivation Θ has the required properties to give us **3)**.

□

§6. "Finiteness" of the Flach classes.

The Proposition of §5 requires that we check that, for all prime numbers $r \neq \ell$, the restrictions of the Flach classes land in the "finite parts" of $\mathbb{Q}_r$ - Galois cohomology. These classes are unramified for primes r not dividing $p \cdot N \cdot \ell$, and so it only remains to check the primes r dividing N, and the prime r=p. We separate these two statements as distinct lemmas, and also take the opportunity to record a statement somewhat more precise than is needed above, but which will be needed later. Recall the class

(11) $\tilde{\sigma}_\ell \in H^1(G_{\mathbb{Q},\Sigma\cup\{\ell\}}, H^1(\bar{X},\mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\bar{X},\mathbb{Z}_p(1)))$

constructed in (2) of §4 above. For use in Chapter 11 we want to deal with this "finer" class $\tilde{\sigma}_\ell$ rather than the Flach class $c(\ell) \in H^1(G_{\mathbb{Q},\Sigma\cup\{\ell\}}, W^*)$. Note that the statements of the Lemmas below explicitly make use of the natural finite/singular structure on the $G_{\mathbb{Q}}$-module $H^1(\bar{X},\mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\bar{X},\mathbb{Z}_p(1))$.

Lemma 1: For all prime numbers ℓ not dividing $p \cdot N$, and all prime number q dividing N, the restriction $\mathrm{res}_q \tilde{\sigma}_\ell$ of the class $\tilde{\sigma}_\ell$ to $G_{\mathbb{Q}_\ell}$ lies in the finite part,

$$H_f^1(G_{\mathbb{Q}_q}, H^1(\bar{X},\mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\bar{X},\mathbb{Z}_p(1))),$$

in $H^1(G_{\mathbb{Q}_q}, H^1(\bar{X},\mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} H^1(\bar{X},\mathbb{Z}_p(1)))$.

Lemma 2: For all prime numbers ℓ not dividing $p\cdot N$, the restriction $\mathrm{res}_p\tilde{\sigma}_\ell$ of the class $\tilde{\sigma}_\ell$ to $G_{\mathbb{Q}_\ell}$ lies in the finite part, $H_f^1(G_{\mathbb{Q}_p}, H^1(\bar{X},\mathbb{Z}_p(1))\otimes_{\mathbb{Z}_p}H^1(\bar{X},\mathbb{Z}_p(1)))$, in $H^1(G_{\mathbb{Q}_p}, H^1(\bar{X},\mathbb{Z}_p(1))\otimes_{\mathbb{Z}_p}H^1(\bar{X},\mathbb{Z}_p(1)))$.

What we need, at present, of these two lemmas are the following:

Corollary 1: For all prime numbers ℓ not dividing $p\cdot N$, and all prime number q dividing N, the restriction $\mathrm{res}_q c(\ell)$ of the Flach class $c(\ell) \in H^1(G_{\mathbb{Q},\Sigma\cup\{\ell\}},W^*)$ to $H^1(G_{\mathbb{Q}_q},W^*)$ lies in the finite part, $H_f^1(G_{\mathbb{Q}_q},W^*) \subset H^1(G_{\mathbb{Q}_q},W^*)$.

Corollary 2: For all prime numbers ℓ not dividing $p\cdot N$, the restriction $\mathrm{res}_p c(\ell)$ of the Flach class $c(\ell) \in H^1(G_{\mathbb{Q},\Sigma\cup\{\ell\}},W^*)$ to $H^1(G_{\mathbb{Q}_p},W^*)$ lies in the finite part, $H_f^1(G_{\mathbb{Q}_p},W^*) \subset H^1(G_{\mathbb{Q}_p},W^*)$.

Proofs of Lemma 1 and Lemma 2: Not yet done!!

... In §8 of Chapter 6 we "measured" the ramification of cohomology classes (denoted there $\tilde{\sigma}(f;Z_\eta/U_\eta)$) constructed from "Gersten cycles" (f, Z/U) at primes ℓ of *good reduction* for the ambient surface U. To deal with Lemma 1, we must now extend this theory to measure ramification at primes ℓ of semistable reduction. At least we must do this in the particular context that we find ourselves, namely where our surface U is X×X, for X a curve of semistable reduction at ℓ.

****

Chapter 9. Modular Curves.

§1. A quick review of the basic geometry of modular curves of square-free level.

References: [S], [L],....

Let M be a square-free positive integer. The modular curve $X_0(M)_{/\mathbb{Q}}$ is a projective smooth geometrically irreducible curve over $\mathbb{Q}$ containing an affine open usually denoted $Y_0(M)$, which is the "coarse moduli space" classifying isomorphism classes of pairs (E,C_M) where E is an elliptic curve, and $C_M \subset E$ is a cyclic subgroups in E of order M. The complement of $Y_0(M)$ in $X_0(M)$ consists in the finite set, $\mathcal{C}_0(M)$, of "cusps" which can also be given a "modular interpretation" as classifying isomorphism classes of pairs $(\mathcal{E},\mathcal{C}_M)$ where $\mathcal{E}$ is isomorphic to $\mathbf{G}_m \times \mathbb{Z}/M\cdot\mathbb{Z}$ (a "degenerate elliptic curve"), and $\mathcal{C}_M \subset \mathcal{E}$ is again a cyclic subgroup of order M. The points of $\mathcal{C}_0(M)$ are all $\mathbb{Q}$-rational and are in natural one:one correspondence with the set, D(M), of positive divisors of M, by the rule that a pair $(\mathcal{E},\mathcal{C}_M)$ corresponds to the integer d = the order of $\mathbf{G}_m \cap \mathcal{C}_M$. There is a commutative group of involutions acting on $X_0(M)_{/\mathbb{Q}}$, usually referred to as "the Atkin-Lehner involutions", or "the w-operators", the elements of which are in one:one correspondence with D(M); let us call this group $\mathfrak{W}_0(M)$. The involution w_d which "corresponds" to $d \in D(M)$ under the one:one correspondence $D(M) \longleftrightarrow \mathfrak{W}_0(M)$ is defined by the rule that associates to the pair (E,C_M) the pair (E',C'_M) where E' is the quotient of E by the (unique) cyclic subgroup of

order d in C_M, and C'_M is the image in E' of the subgroup in E generated by C_M and the kernel of multiplication by d.

If N is a positive divisor of M, there is a surjective mapping defined over $\mathbb{Q}$, denoted $j_{M,N}$: $X_0(M) \to X_0(N)$ given by the rule which associates to the pair (E, C_M) the pair (E,C_N) where $C_N \subset C_M$ is the (unique) subgroup of order N.

There are regular semi-stable (projective) models over Spec$\mathbb{Z}$, for the curves $X_0(M)_{/\mathbb{Q}}$ which are smooth over Spec $\mathbb{Z}[1/M]$ (all square-free $M \geq 1$). These semistable models have the further properties that the action of the groups of involutions $\mathfrak{W}_0(M)$ extend to the model of $X_0(M)$ (all square-free $M \geq 1$) and the morphisms $j_{M,N}$ extend to yield morphisms of the semistable model of $X_0(M)$ to that of $X_0(N)$ (all square-free $M \geq 1$, and positive divisors N of M). One has:

Proposition: Let $\mathfrak{N}$ denote the set of positive square-free integers The association $n \mapsto X_n := X_0(n)$ for $n \in \mathfrak{N}$, with the j's and w's given as above constitute a *Hecke Tower*, in the sense of Chapter 8.

□

In fact, as confessed previously, this is the only example I know of a Hecke Tower.

§2. The j's and w's acting on the set of cusps.

Let M be a multiple of N and both M,N square-free positive integers. The Atkin-Lehner involutions and the mappings $j_{M,N}$ preserve cusps. The set $\mathfrak{C}_0(M)$ is a principle homogeneous set under the action of Atkin-Lehner involutions $\mathfrak{W}_0(M)$. If we use the identifications of the sets $\mathfrak{C}_0(M)$ and $\mathfrak{W}_0(M)$ with D(M) as described in §1,

and compose one of these identifications with the inverse of the other to make an identification of sets $\mathcal{C}_0(M) \cong \mathfrak{W}_0(M)$, the action of $\mathfrak{W}_0(M)$ on $\mathcal{C}_0(M)$ is then given by the multiplication law of $\mathfrak{W}_0(M)$. We have a commutative diagram

$$\begin{array}{ccc} & j_{M,N} & \\ \mathcal{C}_0(M) & \rightarrow & \mathcal{C}_0(N) \\ \cong \downarrow & & \downarrow \cong \\ D(M) & \rightarrow & D(N) \end{array}$$

$$d \quad \mapsto \quad gcd\,(d,N).$$

Lemma: The degree of the mapping $j_{M,N}$: $X_0(M) \rightarrow X_0(N)$ at the cusp c_d in $\mathcal{C}_0(M)$ identified with the divisor $d \in D(M)$ is equal to

$$d/gcd\,(d,N).$$

Proof: .....

□

For purposes of the next §, let us draw the local picture of the mapping $j_{M,N}$ on cusps. Fix $c \in \mathcal{C}_0(N)$, and let $\mathcal{C}_0(M;c) \subset \mathcal{C}_0(N)$ denote the full inverse image, $j_{M,N}^{-1}(c)$. From the previous discussion, we have an identification of $\mathcal{C}_0(M;c)$ with the set $D(M/N)$ of positive divisors of M/N, and the degree of the mapping $j_{M,N}$ at the cusp c_δ in $\mathcal{C}_0(M;c)$ corresponding to the divisor $\delta \in D(M/N)$ is, by the previous Lemma, equal to δ. Let δ^* denote the integer such that $\delta \cdot \delta^* = M/N$. Then, also by the Lemma, the degree of the mapping $j_{M,N} \circ w_{M/N}$ at the cusp c_δ is equal to δ^*.

Now let us focus on the mapping of eventual interest to us,

(1) $j_{M,N} \times j_{M,N} \circ w_{M/N} : X_0(M) \to \Gamma_{M/N} \subset X \times X,$

where we fix $X = X_0(N)$. As a summary of the above discussion, we have that the image of the set of cusps $\mathcal{C}_0(M)$ under the above mapping consists of the "diagonal" in $\mathcal{C}_0(N) \times \mathcal{C}_0(N)$; given a diagonal cusp $(c,c) \in \mathcal{C}_0(N) \times \mathcal{C}_0(N) \subset X \times X$, the inverse image of (c,c) in $X_0(M)$ is precisely the set $\mathcal{C}_0(M;c) \cong D(M/N)$, the local degree of the projection of $X_0(M)$ to the first factor X at the cusp $c_\delta \in \mathcal{C}_0(M;c)$ corresponding to the divisor $\delta \in D(M/N)$ being equal to δ, and the local degree of the projection to the second factor being δ^*.

§3. Modular units.

The term "modular unit" denotes a rational function f on a modular curve (e.g., on $X_0(N)$) such that the divisor (f) of zeroes and poles of f is supported at cusps. For a systematic treatment of modular units, see **[K-L]**.

Now let us fix our sights on the Hecke Tower $\mathcal{X}$ described in §1 above; i.e., for $n \in \mathfrak{N}$, the curve X_n is equal to $X_0(n)_{/\mathbb{Q}}$. Fix $N \in \mathfrak{N}$, and put $X = X_N$ $(= X_0(N))$ for short. Let $w \in \mathbb{Z}$, and let f_X be a w-marking of the curve X (equivalently, f_X is a rational section of the pluricanonical sheaf $(\Omega_{X_0(N)_{/\mathbb{Q}}})^{\otimes w}$). Recall the construction of the functions f_n on $\Gamma_n = \Gamma_{n,N} \subset X \times X$ for all $n \in \mathfrak{N}$ relatively prime to N, given in §2 of Chapter 8 (see, in particular, the paragraph labelled **Notation** there). Let us view the rational function f_n as being a rational function on $X_{n \cdot N} = X_0(n \cdot N)$, the normalization of

$\Gamma_n = \Gamma_{n,N}$.

Definition: Say that f_X is a **modular unit generator** (of level N and *of weight* $k = 2w$ for $w \in \mathbb{Z}$) if for all $n \in \mathfrak{N}$ which are relatively prime to N, the rational function f_n on $X_0(n \cdot N)$ is a modular unit.

Example: The classical modular form $\Delta = q \cdot \Pi(1-q^n)^{24}$ of level 1 and weight 12, which we view as a rational section of the sheaf $\{\Omega^1_{X_0(1)}\}^{\otimes 6}$ is a "modular unit generator" of level 1.
Proof: .....

Proposition: If f_X is a "modular unit generator", then f_X is admissible, in the sense of Definition 2 of §2 of Chapter 8, i.e.,

(2) $\quad$ "$\mathrm{ord}_z(f_n)$" = 0

for all $n \in \mathfrak{N}$ be relatively prime to N, and z closed points of Γ_n.

Proof: Let $n \in \mathfrak{N}$ be relatively prime to N, and note that since our hypothesis gives us that the divisor of zeroes and poles of f_n on $X_0(n \cdot N)$ is supported on cusps, to check the proposition it suffices to check (2) for points $z \in \Gamma_n$ which are images of cusps. But this comes "for free" in view of the lengthy "summary" given at the end of §2 above. Here is the argument, in which we make use of the notational conventions of §2. Recall, in particular, that c is a cusp of $X = X_0(N)$ and, for $\delta \in D(M/N)$ we let $c_\delta \in \mathcal{C}_0(M;c)$ denote the cusp projecting to c under $j_{M,N}$ which corresponds to δ under the identification $D(M/N) \cong \mathcal{C}_0(M;c)$.

Suppose that we choose Z a local uniformizer of

$X_0(M)_{/\mathbb{Q}}$ about c_δ, so that $z = Z^\delta$ is a local uniformizer of $X = X_0(N)_{/\mathbb{Q}}$ about c. Consider some local meromorphic section $\varphi = z^r \cdot (dz)^{\otimes w}$ of $(\Omega_{X_{/\mathbb{Q}}})^{\otimes w}$ about c, with $r, w \in \mathbb{Z}$. Putting $\Phi_\delta := j_{M,N}{}^*(\varphi)$ and $\Psi_\delta := (j_{M,N} \circ w_{M/N})^*(\varphi)$ both restricted to a suitable neighborhood of c_δ, we use the discussion of §2 to compute ords at c_δ:

(3) $\quad \mathrm{ord}_Z(\Phi_\delta) = r\cdot\delta + w\cdot(\delta - 1)$

$\quad\quad \mathrm{ord}_Z(\Psi_\delta) = r\cdot\delta^* + w\cdot(\delta^* - 1).$

Returning to the mapping (1) of §2, and summing (3) over all $c_\delta \in \mathcal{C}_0(M;c)$, we compute

(4) $\quad$ "$\mathrm{ord}_{(c,c)}\{j_{M,N}{}^*(\varphi) \otimes (j_{M,N} \circ w_{M/N})^*(\varphi)^{-1}\}$" =

$$\sum_{\delta \in D(M/N)} r\cdot\delta + w\cdot(\delta - 1) \; - \; r\cdot\delta^* + w\cdot(\delta^* - 1),$$

and we note that the sum is zero (for any r and w). Applying this local analysis to $\varphi = f_X$ restricted to each cusp $c \in \mathcal{C}_0(N)$ gives (2).

□

To summarize the above, for $X = X_0(N)$ we may identify $\mathcal{GM}(X)$, the group of admissible markings on X (cf. Chapter 8, §1), with the group of "modular unit generators" on X. The image of the degree mapping

$$\mathcal{GM}(X) \to \mathbb{Z}$$

(cf. (1) of Chapter 8, §1) contains $6\cdot\mathbb{Z}$ (since Δ is an admissible 6-marking).

Part III Bilateral axiomatics

Chapter ten. Bilateral algebra.

§1. **Bilateral derivations.** All the rings and algebras we will consider in this section are assumed to be commutative.
Let, then, Λ be a noetherian (commutative) ring (with unity).

Notation: For B a (commutative) Λ-algebra, consider the Λ-algebra

$$B_2 = B \otimes_\Lambda B.$$

We view B_2 as equipped with its two natural B-algebra structures, its "left B-algebra structure" via the ring homomorphism $b \mapsto b \otimes 1$ and its "right B-algebra structure" via the ring homomorphism $b \mapsto 1 \otimes b$. The natural "diagonal" homomorphism $\mu: B \otimes_\Lambda B \to B$, which is a homomorphism of B-algebras (when B_2 is given either its left or its right B-algebra structure) gives B a natural B_2-algebra structure.

Let B be a Λ-algebra, and M a B_2-module.

Definition: A **bilateral Λ-derivation of** B **to** M to be a Λ-homomorphism

$$\partial : B \to M$$

satisfying the relation $\partial(x \cdot y) = (1 \otimes x) \cdot \partial y + (y \otimes 1) \cdot \partial x$ for all x,y
in B.

Example: For any (commutative) Λ-algebra B the **canonical bilateral derivation** $\delta : B \to B_2$ is defined

by the rule $\delta(x) = 1\otimes x - x\otimes 1$.

Remark: This notion occurs in .....

Lemma: Let $\partial: B \to M$ be a bilateral Λ-derivation. Then for any two elements $x, y \in B$, $\delta(x)\cdot\partial(y) = \delta(y)\cdot\partial(x)$.

Proof: This comes from comparing the two sides of the equation $\partial(x\cdot y) = \partial(y\cdot x)$, using the definition of bilateral derivation.

□

Notation:

Let $\Gamma_B \subset B_2$ denote the kernel of the homomorphism

$$\mu: B_2 \to B \qquad (\mu: b\otimes_\Lambda b' \mapsto b\cdot b').$$

The sub B_2-module Γ_B is generated by the image $\delta(B)$. The canonical bilateral derivation δ takes its values in $\Gamma_B \subset B_2$.

If M is any B_2-module let

$$M_\delta := \{ m \in M \mid \delta(x)\cdot m = 0, \text{ for all } x \in B\};$$

i.e., M_δ is the intersection of the kernels of the B_2-endomorphisms $\delta(x)$ of M where x runs through all elements of B. Equivalently, $M_\delta = M[\Gamma_B]$. Since the ideal Γ_B annihilates M_δ, and since $\Gamma_B = \ker(\mu)$, we see that the B_2-action on the B_2-submodule $M_\delta \subset M$ factors through B. Therefore M_δ may be (and will be) viewed as a B-module.

§2. "Counter-algebras" and congruence ideals:

Let B be a Λ-algebra, and consider $M = B_2$ viewed as B_2-module. What geometric significance does the ideal $B_{2,\delta} \subset B_2$ have, and what is the significance of the image $\mu(B_{2,\delta}) \subset B$?

Definitions: If Λ is any commutative ring, and B any (commutative) Λ-algebra, define the Λ-**counter-algebra** $B^{\perp}$ **of** B to be the quotient $B_2/B_{2,\delta}$. Also (following H. Lenstra **[L]**) let us call the ideal $\mu(B_{2,\delta})$ in B the **congruence ideal** of the Λ-algebra B. Call the quotient Λ-algebra $\overline{B} = B/\mu(B_{2,\delta})$ the **congruence quotient algebra** of B.

For any Λ-algebra B, then, we have the natural commutative diagram, where "lines are exact" and where the lower right square is a Cartesian square (of Λ-algebras with surjective homomorphisms) ,

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & 0 & \to & B_{2,\delta}\cap\Gamma_B & \to & \Gamma_B & & & \\
 & & & \downarrow & & \downarrow & & & \\
(1) & 0 & \to & B_{2,\delta} & \to & B_2 & \to & B^{\perp} & \to 0 \\
 & & & \downarrow & & \downarrow & & \downarrow & \\
 & 0 & \to & \mu(B_{2,\delta}) & \to & B & \to & \overline{B} & \to 0 \\
 & & & \downarrow & & \downarrow & & \downarrow & \\
 & & & 0 & & 0 & & 0\,. &
\end{array}
$$

Carrying over some of this notation to the corresponding affine schemes, if $S = \operatorname{Spec} \Lambda$ and $X = \operatorname{Spec} B$, the "Spec" of the Cartesian square above gives us a Cartesian diagram of S-schemes (morphisms being closed immersions) which can be denoted

$$
\begin{array}{ccc}
X\times_S X & \leftarrow & X^{\perp} \\
\uparrow & & \uparrow \\
X & \leftarrow & \overline{X},
\end{array}
\tag{2}
$$

where $X \to X\times_S X$ is the diagonal morphism, and $\overline{X}$ is the scheme-theoretic intersection of X and $X^{\perp}$ in $X\times_S X$. The formation of the diagrams $(1)_{B/\Lambda}$ and $(2)_{X/S}$ are "functorial" (in an evident sense) in B/Λ and X/S, respectively, and commute with base change of Λ and of S, respectively [in the sense that tensoring the diagram $(1)_{B/\Lambda}$ term-by-term with Λ' over Λ yields $(1)_{B'/\Lambda'}$ where $B' = B\otimes_{\Lambda}\Lambda'$, and similarly for $(2)_{X/S}$].

Examples: 1) In the special case where B is a finite étale Λ-algebra (equivalently, X is finite étale over S) the diagonal subscheme is open and closed in $X\times_S X$, and $X^{\perp}$ can easily be seen to be the *complement of the diagonal* in $X\times_S X$. In this case $\overline{X}$ is empty, and diagram (2) boils down to the assertion that there is a decomposition of $X\times_S X$ as the disjoint union:

$$X\times_S X = X \amalg X^{\perp}.$$

We can also state this in terms of diagram (1): we have

$$B_{2,\delta}\cap\Gamma_B = \{0\},\ B_{2,\delta} \cong \mu(B_{2,\delta}) = B, \text{ and}$$

$$B_2 \cong B \times \Gamma_B .$$

2) Next, consider the case where Λ is an integral domain and B is a finite flat and generically étale Λ-

algebra. Let K denote the fraction field of Λ, and put $\mathcal{S}$= Spec)K) and $\mathcal{X}$ = Spec($B\otimes_{\Lambda}K$). Then, as in **1)**, we have

$$\mathcal{X}\times_{\mathcal{S}}\mathcal{X} = \mathcal{X} \amalg \mathcal{X}^{\perp},$$

where $\mathcal{X}$ imbeds in $\mathcal{X}\times_{\mathcal{S}}\mathcal{X}$ as the diagonal, and $\mathcal{X}^{\perp}$ is the complement to the diagonal.

We also have that the diagonal $X \subset X\times_S X$ is the Zariski-closure of $\mathcal{X}$ in $X\times_S X$, and that $X^{\perp} \subset X\times_S X$ is the Zariski-closure in $X\times_S X$ of the complement-to-the-diagonal $\mathcal{X}^{\perp} \subset \mathcal{X}\times_{\mathcal{S}}\mathcal{X}$. So the "congruence quotient scheme" $\overline{X}$ is, in this case, the scheme-theoretic intersection of the Zariski-closures over all of S of *diagonal* and *complement-to-diagonal* schemes at the generic point of S. Diagram (1) simplifies in this case, for we have:

Lemma : $B_{2,\delta}\cap\Gamma_B = \{0\}$.

(**Proof:** Since Λ is an integral domain, and $B_{2,\delta}\cap\Gamma_B \subset B_2$ which is finite and flat over Λ, $B_{2,\delta}\cap\Gamma_B$ is contained in $K\otimes_{\Lambda}(B_{2,\delta}\cap\Gamma_B)$ which vanishes)

giving us the commutative diagram (with exact straight lines):

$$
\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & = & \downarrow & & \\
 & & & & \Gamma_B & \to & \Gamma_B & & \\
 & & & & \downarrow & & \downarrow & & \\
(3)\quad 0 \to & B_{2,\delta} & \to & B_2 & & \to & B^{\perp} & \to & 0 \\
 & \cong\downarrow & & \downarrow & & & \downarrow & & \\
0 \to & \mu(B_{2,\delta}) & \to & B & & \to & \overline{B} & \to & 0 \\
 & & & \downarrow & & & \downarrow & & \\
 & & & 0 & & & 0\,. & &
\end{array}
$$

3) When B is Gorenstein. Making the assumptions of **2)**, i.e., that Λ is a (noetherian, commutative) integral domain and B is a finite flat and generically étale Λ-algebra, and making the further assumption that B is Gorenstein, we have that $\mu(B_{2,\delta}) \subset B$ is a principal ideal generated by a (by any) congruence element η of B, i.e., $\overline{B} = B/\mu \cdot B$. We also have that η is a non-zero divisor in B. It follows from diagram (3) above (since $B_{2,\delta} \to \mu(B_{2,\delta})$ is an isomorphism of B-modules) that $B_{2,\delta}$ is a principal ideal of B_2, generated by any lifting $\tilde{\eta} \in B_{2,\delta}$ of η. Let us refer to such a lifting $\tilde{\eta}$ as a **bilateral congruence element** (in B_2). Diagram (3) then reads:

$$
\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & = & \downarrow & & \\
 & & & & \Gamma_B & \to & \Gamma_B & & \\
 & & & & \downarrow & & \downarrow & & \\
(4)\quad 0 \to & (\tilde{\eta}) & \to & B_2 & & \to & B^{\perp} & \to & 0 \\
 & \cong\downarrow & & \downarrow & & & \downarrow & & \\
0 \to & (\eta) & \to & B & & \to & B/(\eta) & \to & 0 \\
 & & & \downarrow & & & \downarrow & & \\
 & & & 0 & & & 0\,. & &
\end{array}
$$

§3. Annihilating ideals.

Let $\pi: B \to A$ be a surjective Λ-homomorphism of (commutative, as always) Λ-algebras, with kernel given by the ideal $I \subset B$. Then the kernel of the induced Λ-homomorphism $B_2 \to A_2$ is the ideal $I \otimes B + B \otimes I \subset B_2$.

Let M be an A_2-module, viewed as B_2-module via π; equivalently, M is a B_2-module annihilated by $I \otimes 1$ and $1 \otimes I$. Let $\partial: B \to M$ be a bilateral Λ-derivation of B to M. Then, as proved in Part II,

Lemma: The restriction of ∂ to I induces a homomorphism $\tilde{\partial}$ of A-modules,

$$\begin{array}{ccc} & \overset{\tilde{\partial}}{} & \\ I/I^2 & \to & M_\delta \\ \uparrow & & \downarrow \subset \\ I \subset B & \to & M. \\ & \overset{\partial}{} & \end{array} \tag{5}$$

□

§4. The module of bilateral differentials.

For B a Λ-algebra, consider the category of bilateral Λ-derivation on B, and let $d: B \to \tilde{\Omega}_{B/\Lambda}$ denote a *universal* bilateral Λ-derivation (as will be constructed in the Proposition below). Equivalently, $d: B \to \tilde{\Omega}_{B/\Lambda}$ is an initial object of the category of bilateral Λ-derivations on B. This simply means that $\tilde{\Omega}_{B/\Lambda}$ is a B_2-module, and d is a bilateral derivation from B to $\tilde{\Omega}_{B/\Lambda}$ with the property that given any B_2-module M and bilateral derivation $\partial: B \to M$, there is a unique B_2-homomorphism $h: \tilde{\Omega}_{B/\Lambda} \to M$ such that $\partial = d \circ h$. We will refer to $\tilde{\Omega}_{B/\Lambda}$ as the B_2-**module of bilateral differentials (relative to Λ)**. In § below we shall, in fact, show that for any Λ-algebra B, the canonical bilateral Λ-derivation $\delta: B \to \Gamma_B$ is

universal. But for the time being let us content ourselves with the assertion of existence:

Proposition 1: For any Λ-algebra B, there exists a universal bilateral Λ-derivation $d: B \to \tilde{\Omega}_{B/\Lambda}$.

Proof: One could simply dispose of this proposition by making the evident construction; i.e., form the the free B_2-module generated (freely) by elements db as b runs through all the elements of B, and then take the quotient B_2-module of that free module obtained by imposing all the relations necessary for $b \mapsto db$ to be a bilateral Λ-derivation. Nevertheless, here is a somewhat more economical construction of $\tilde{\Omega}_{B/\Lambda}$ which may be slightly more revealing.

Construction:

Step 1: Let $\mathfrak{X}$ be any set, and let P denote the (free, commutative) polynomial algebra over Λ generated by the set $\mathfrak{X}$. Define $F_{\mathfrak{X}}$ to be the free P_2-module generated by the set of symbols dx for $x \in \mathfrak{X}$. Let $\mathfrak{W}_{\mathfrak{X}}$ be the quotient P_2-module of $F_{\mathfrak{X}}$ obtained by imposing the relations $\delta(x)\cdot dy = \delta(y)\cdot dx$ for all $x,y \in \mathfrak{X}$.

Lemma 1: There is a unique bilateral derivation $d: P \to \mathfrak{W}_{\mathfrak{X}}$ which sends each $x \in \mathfrak{X}$ to $dx \in \mathfrak{W}_{\mathfrak{X}}$.

Proof: We define d on the set $\mathfrak{M}_n$ of monomials of degree $\leq n$ in the elements of $\mathfrak{X}$ comprising a basis of P as Λ-module proceeding inductively in n. Our inductive hypothesis is that we have defined d on $\mathfrak{M}_n$ in such a way so that

(6) $d(\alpha\cdot\beta) = (1\otimes\alpha)d\beta + (\beta\otimes 1)d\alpha$

for any monomials α,β with $\alpha\cdot\beta \in \mathfrak{M}_n$. It follows that we

also have $\delta(\alpha)\cdot d\beta = \delta(\beta)\cdot d\alpha$ for such pairs α,β. The definition of d on $\mathfrak{M}_1$ is forced by the prescription given in the lemma, and visibly satisfies (6) so we may assume that d has been defined satisfying (6) on $\mathfrak{M}_n$ for some $n\geq 1$, and we must inductively define d on $\mathfrak{M}_{n+1}$ showing that it is "well-defined", and also that it satisfies (6) on its extended domain. Given a monomial $m \in \mathfrak{M}_{n+1}$ writing m as $m = x\cdot r$ for some $x \in \mathcal{X}$ and $r \in \mathfrak{M}_n$ the definition of dm is forced on us: $dm = (x\otimes 1)\cdot dr + (1\otimes r)\cdot dx$. To see that this prescription is well-defined, imagine a different factorization of m, $m = y\cdot s$, and we must compare

(7) $(x\otimes 1)\cdot dr + (1\otimes r)\cdot dx$

with

(8) $(y\otimes 1)\cdot ds + (1\otimes s)\cdot dy$.

Assuming that the two factorizations are distinct, i.e., that $x\neq y$, we may write $m=x\cdot y\cdot t$ with $r=y\cdot t$ and $s = x\cdot t$, both in $\mathfrak{M}_n$. By induction we have

$$dr = (y\otimes 1)\cdot dt+(1\otimes t)\cdot dy, \quad ds = (x\otimes 1)\cdot dt+(1\otimes t)\cdot dx,$$

and therefore (7)-(8) is given by

(9) $(x\otimes t)\cdot dy + (1\otimes yt)\cdot dx - (y\otimes t)\cdot dx - (1\otimes xt)\cdot dy =$

$(1\otimes t)\{\delta(x)\cdot dy - \delta(y)\cdot dx\}$

and this vanishes since the term in brackets is one of our relations. What we have done so far is to define d on $\mathfrak{M}_{n+1}$ and to check, in fact, that (6) holds if α or β is of degree 1.

To check that (6) holds for α,β of general degree with $\alpha\cdot\beta \in \mathfrak{M}_{n+1}$, write $\alpha = x\cdot a$ for x of degree 1 and a of

degree ≥ 1, giving us, from what we have done so far, that $d(\alpha\cdot\beta) = (x\otimes 1)\cdot d(a\cdot\beta) + (1\otimes a\cdot\beta)\cdot dx$ and $d\alpha = (x\otimes 1)\cdot da + (1\otimes a)\cdot dx$. By induction applied to $a\cdot\beta \in \mathfrak{M}_n$ we also have

$$d(a\cdot\beta) = (1\otimes a)d\beta + (\beta\otimes 1)da,$$

so we are in reasonable shape to compute the difference,

$$d(\alpha\cdot\beta) - \{(1\otimes\alpha)d\beta + (\beta\otimes 1)d\alpha\}$$

as being equal to

(10) $(1\otimes a)\{\delta x\cdot d\beta - \delta\beta\cdot dx\}$

which vanishes since the term in the brackets vanishes by the inductive assumption, $x\cdot\beta$ being in $\mathfrak{M}_n$.

□

Corollary: The bilateral Λ-derivation $d: P \to \mathfrak{W}_{\mathcal{X}}$ is universal for the Λ-algebra P.

Proof: If $\partial: P \to M$ is any bilateral Λ-derivation, then define the P_2-homomorphism $h: F_{\mathcal{X}} \to M$ by the rule that $dx \mapsto \partial(x)$. Since $\delta(\alpha)\cdot\partial\beta = \delta(\beta)\cdot\partial\alpha$ for any two elements $\alpha,\beta \in P$, the relations $\delta(x)\cdot dy - \delta(y)\cdot dx$ in $F_{\mathcal{X}}$ are sent to zero under h, and therefore h induces a homomorphism $h: \mathfrak{W}_{\mathcal{X}} \to M$ such that $\partial = h\circ d$, and clearly h is uniquely determined by this equation.

□

Having established that $d: P \to \mathfrak{W}_{\mathcal{X}}$ is universal for bilateral Λ-derivations of P, let us rename it $d: P \to \tilde{\Omega}_{P/\Lambda}$ noting that in view of its universality property it is canonically defined, independent of the basis $\mathcal{X}$ chosen, and uniquely so up to canonical isomorphism.

Step 2: Now let B be any Λ-algebra, and $\mathcal{X} \subset B$ any set

of generating elements for the Λ-algebra B. Let P denote the (free, commutative) polynomial algebra over Λ generated by the set $\mathcal{X}$. Let $I \subset P$ denote the kernel of the natural surjection of Λ-algebras $P \to B$. By the lemma of §3, the composition of mappings

$$P \to \tilde{\Omega}_{P/\Lambda} \to \tilde{\Omega}_{P/\Lambda} \otimes_{P_2} B_2 = \tilde{\Omega}_{P/\Lambda} / (I \otimes_\Lambda P + P \otimes_\Lambda I) \cdot \tilde{\Omega}_{P/\Lambda}$$
$$\alpha \qquad \mapsto \qquad d\alpha \otimes 1$$

induces a homomorphism of B_2 -modules

$$\tilde{d}: I/I^2 \to \tilde{\Omega}_{P/\Lambda} \otimes_{P_2} B_2$$

(in fact, of B-modules, if we restrict the range to the submodule $(\tilde{\Omega}_{P/\Lambda} \otimes_{P_2} B_2)_\delta$).

Define $\tilde{\Omega}_{B/\Lambda}$ to be the quotient B_2-module of $\tilde{\Omega}_{P/\Lambda} \otimes_{P_2} B_2$ which fits into the exact sequence of B_2-modules,

$$(11) \qquad I/I^2 \to \tilde{\Omega}_{P/\Lambda} \otimes_{P_2} B_2 \to \tilde{\Omega}_{B/\Lambda} \to 0.$$

An equivalent description of the B_2-module $\tilde{\Omega}_{B/\Lambda}$ is given as follows. Consider the *subset* $\mathcal{J} = dI + (I \otimes_\Lambda P + P \otimes_\Lambda I) \cdot \tilde{\Omega}_{P/\Lambda}$ in $\tilde{\Omega}_{P/\Lambda}$, i.e., the subset of elements of the form $d\alpha + \nu$ where $\alpha \in I$, and $\nu \in (I \otimes_\Lambda P + P \otimes_\Lambda I) \cdot \tilde{\Omega}_{P/\Lambda}$. Then this subset $\mathcal{J}$ forms a sub P_2-module of $\tilde{\Omega}_{P/\Lambda}$ and $\tilde{\Omega}_{B/\Lambda}$ is the quotient P_2-module $\tilde{\Omega}_{P/\Lambda} / \mathcal{J}$ with its inherited B_2-module structure.

Define $d_B: B \to \tilde{\Omega}_{B/\Lambda}$ to be the universal bilateral Λ-derivation on P, $d: P \to \tilde{\Omega}_{P/\Lambda}$ taken modulo $\mathcal{J}$.

Lemma 2: The mapping $d_B: B \to \tilde{\Omega}_{B/\Lambda}$ is a universal bilateral Λ-derivation on B.

Proof: The mapping $d_B: B \to \tilde{\Omega}_{B/\Lambda}$ is indeed well-defined on B, i.e. $d_B I = 0$ since $dI \in \mathfrak{J}$, and d_B is a bilateral Λ-derivation on B. Given any bilateral Λ-derivation on B, $\partial: B \to M$ where M is a B_2-module, we may view ∂ as giving a bilateral Λ-derivation on P with values in M, viewed as P_2-module. By universality of $\tilde{\Omega}_{P/\Lambda}$ we have a unique P_2-homomorphism $h: \tilde{\Omega}_{P/\Lambda} \to M$ such that $\partial = h \circ d$. It is immediate that $h(\mathfrak{J}) = 0$, giving our lemma, and therefore our Proposition.

□

Corollary: Let $\pi: C \to B$ be a surjection of Λ-algebra with kernel equal to $J \subset C$. Then π induces a surjective homomorphism $\tilde{\Omega}_{C/\Lambda} \otimes_{C_2} B_2 \to \tilde{\Omega}_{B/\Lambda}$ of B_2-modules fitting into an exact sequence:

$$(12) \qquad J/J^2 \to \tilde{\Omega}_{C/\Lambda} \otimes_{C_2} B_2 \to \tilde{\Omega}_{B/\Lambda} \to 0.$$

□

Remark: We will often be dealing with complete (noetherian) local rings Λ and complete (noetherian) local Λ-algebras B viewed as topological rings, and for these it is more appropriate to deal with "continuous" bilateral derivations and differentials. When working in this category we let B_2 denote the *completed* tensor square $B \hat{\otimes}_\Lambda B$ and we consider only *continuous* bilateral derivations from B to B_2-modules. The initial object in this category (of continuous bilateral derivations from B to B_2-modules) we will call the **module of continuous bilateral differentials** $\tilde{\Omega}_{B/\Lambda,\text{cont}}$. If $m \subset B$ is the maximal ideal then $\tilde{\Omega}_{B/\Lambda,\text{cont}}$ is isomorphic to the projective limit

$$\tilde{\Omega}_{B/\Lambda,\mathrm{cont}} = \lim_{\nu\to\infty}\text{proj. } \tilde{\Omega}_{(B/m^{\nu})/\Lambda}.$$

If $\mathcal{X}$ is a set, and P the power series ring in the variables $\mathcal{X}$ with coefficients in Λ, then $\tilde{\Omega}_{P/\Lambda,\mathrm{cont}}$ is the P_2-module generated by $\mathcal{X}$ with relations $\delta x\cdot dy = \delta y\cdot dx$ for all $x,y \in \mathcal{X}$.

The previous Corollary has a direct analogue for continuous bilateral differentials; namely: Let Λ be a complete noetherian local ring, and $\pi: C\to B$ a surjection of complete noetherian local Λ-algebras with kernel equal to $J \subset C$. Then π induces a surjective homomorphism $\tilde{\Omega}_{C/\Lambda,\mathrm{cont}} \otimes_{C_2} B_2 \to \tilde{\Omega}_{B/\Lambda,\mathrm{cont}}$ of B_2-modules fitting into an exact sequence:

$$(13)\qquad J/J^2 \to \tilde{\Omega}_{C/\Lambda,\mathrm{cont}}\otimes_{C_2} B_2 \to \tilde{\Omega}_{B/\Lambda,\mathrm{cont}} \to 0.$$

Remark: When we are clearly working in this category of complete noetherian local rings and continuous bilateral derivations and differentials (as will almost always be the case from §6 on!), and when no confusion can result, we will drop the subscript "cont" from the notation.

§5. The projection to "plain old" differentials.

Composing any bilateral Λ-derivation $\partial: B \to M$ with the natural projection $\iota: M \to M\otimes_{B_2} B$ yields a Λ-derivation $\Theta = \iota\circ\partial: B\to M\otimes_{B_2} B$ (that is, a derivation in the more usual sense, which we might call here "unilateral" derivations) Let us say then that the bilateral Λ-derivation ∂ **covers** the "unilateral" Λ-derivation Θ. From the universal property of $\Omega_{B/\Lambda}$ we get a canonical

homomorphism of B-modules,

$$c: \quad \Omega_{B/\Lambda} \rightarrow \tilde{\Omega}_{B/\Lambda} \otimes_{B_2} B.$$

Proposition: The homomorphism c is an isomorphism.

Proof: Using the universality property of the B_2-module $\tilde{\Omega}_{B/\Lambda}$ (for bilateral Λ-derivations on B) one checks that the B-module $\tilde{\Omega}_{B/\Lambda} \otimes_{B_2} B$ is universal for (unilateral) Λ-derivations on B.

□

§6. The canonical homomorphism ε.

Since the "canonical" bilateral Λ-derivation

$$\delta: B \rightarrow \Gamma_B$$

(of §1) is a bilateral Λ-derivation, there is a unique homomorphism of B_2-modules

$$\varepsilon: \tilde{\Omega}_{B/\Lambda} \rightarrow \Gamma_B \subset B_2$$

such that $\varepsilon \circ d = \delta$.

(we will call ε **the canonical homomorphism**). The following is a Corollary of the mere existence of the canonical homomorphism ε.

Corollary: Let $\alpha \in B$. The annihilator ideal (in B_2) of the element $d\alpha$ in $\tilde{\Omega}_{B/\Lambda}$ is contained in the annihilator ideal of the element $\delta\alpha$ in B_2. If $\delta\alpha$ is a nonzero-divisor, then the annihilator ideal of $d\alpha$ in $\tilde{\Omega}_{B/\Lambda}$ is trivial.

Proof: If $\gamma \cdot d\alpha = 0$, then applying ε to this we get $\gamma \cdot \delta\alpha = 0$.

□

Proposition 2: Let B be any (commutative) Λ-algebra. The canonical homomorphism $\varepsilon: \tilde{\Omega}_{B/\Lambda} \to \Gamma_B$ is an isomorphism.[1] The canonical bilateral Λ-derivation $\delta: B \to \Gamma_B$ is universal.

Corollary 1: We have a commutative square of B_2-modules

$$\begin{array}{ccc} \tilde{\Omega}_{B/\Lambda} & \to & \Omega_{B/\Lambda} \\ \cong \downarrow \varepsilon & & \cong \downarrow \\ \Gamma_B & \to & \Gamma_B/\Gamma_B{}^2 \end{array}$$

where the upper horizontal homomorphism is the homomorphism coming from the Proposition of §5, and the lower one is the natural projection.

Proof of Corollary 1: The unlabelled vertical arrow in the diagram which can be identified with $\varepsilon \otimes_{B_2} 1_B$ is directly seen to be the standard isomorphism $\Omega_{B/\Lambda} \cong \Gamma_B/\Gamma_B{}^2$ in the theory of derivations.

□

Corollary 2: For B any (commutative) Λ-algebra, the module of bilateral differentials $\tilde{\Omega}_{B/\Lambda}$ is annihilated by $B_{2,\delta}$ and inherits a canonical $B^{\perp}$-module structure induced from its B_2-module structure.

Proof of Corollary 2: Since $B_{2,\delta}$ is the annihilator ideal

[1] It would be embarrassing to me if anyone knew how many weeks I walked this planet covering blackboards and yellowpads with scribblings about bilateral differentials before I realized that this isomorphism exists.

in B_2 of Γ_B the statements in the Corollary hold for the B_2-module Γ_B.

□

Proof of Proposition 2:

Of course it is only the first assertion of the Proposition that needs proof, for the second then follows. I am thankful to Beilinson for providing me with the following short proof of this Proposition.

For M a B_2-module, let X(M) denote the set of isomorphism classes of pairs $(\mathcal{E}, e)$ consisting of extensions

$$(\mathcal{E}) \qquad 0 \to M \to E \to B \to 0$$

in the category of B_2-modules, and liftings $e \in E$ of the identity $1 \in B$. Note that given an $(\mathcal{E},e) \in X(M)$ we have a "$B\otimes 1$-linear" section $s: B \to E$ given by $s(b) = (b\otimes 1)e$, allowing us to write E (viewed as "$B\otimes 1$ -module") canonically as $E = B \oplus M$; explicitly:

$$(14) \qquad E = s(B) \oplus M \quad (= \text{"}(B\otimes 1)\cdot e \quad \oplus M\text{"}).$$

The essential structure, then, of the isomorphism class $(\mathcal{E},e) \in X(M)$ is given by the $1\otimes B$-module structure on (14). The $1\otimes B$-module structure on E, being determined on $0 \oplus M$ by the B_2-module structure of M, and being also determined on the projection to the first summand B, is entirely captured by the following data: form the bilateral derivation $d:B\to M$ given by $d(b') = \delta(b')\cdot e$ viewed as an element of M, where $b' \in B$. We may reconstruct $(\mathcal{E},e)$ from d, the prescription being

$$(15) \qquad (1\otimes b')\cdot(b \oplus m) = b'\cdot b \oplus \{(1\otimes b')\cdot m + (b\otimes 1)\cdot d(b')\}$$

where the direct sum $\oplus$ refers to the decomposition of 14) above.

Moreover, given any bilateral Λ-derivation $d:B\to M$ (15) determines a B_2-module structure on (14) which defines an isomorphism class $(\mathcal{E},e) \in X(M)$. This gives us a canonical bijection

$$(16) \qquad X(M) \cong \mathrm{Hom}_{B_2}(\tilde{\Omega}_{B/\Lambda},M).$$

We also have a mapping $X(M) \to \mathrm{Hom}_{B_2}(\Gamma_B,M)$ by sending $(\mathcal{E},e)$ to the B_2-homomorphism $f: \Gamma_B \to M$ given by $f(\gamma)=\gamma\cdot e$ viewed as element of M. We can reconstruct $(\mathcal{E},e)$ from such an f by taking the image under f of the class $(\mathcal{E}_o,e_o)$

in $X(\Gamma_B)$ where $\mathcal{E}_o$ is the exact sequence of B_2-modules $\{0\to\Gamma_B\to B_2\to B\to 0\}$ and e_o is taken to be the identity element $1_{B_2} \in B_2$. Thus we have a bijection

$$(17) \qquad X(M) \cong \mathrm{Hom}_{B_2}(\Gamma_B,M).$$

Composing the two bijections (16) and (17) gives us a bijection

$$\mathrm{Hom}_{B_2}(\Gamma_B,M) \cong \mathrm{Hom}_{B_2}(\tilde{\Omega}_{B/\Lambda},M)$$

which is directly seen to be an isomorphism of B_2-modules,
giving Proposition 2.

□

Remark about continuous bilateral differentials: Working in the category of complete noetherian local rings we have the analogous isomorphism $\tilde{\Omega}_{B/\Lambda,\mathrm{cont}} \cong \Gamma_B$ where Γ_B is the kernel of $B\hat{\otimes}_\Lambda B \to B$. Again, if we are working squarely in this category and no confusion can result, we will suppress the subscript "cont" and the $\hat{}$ from the notation.

§6. Bilateral evolution.

Definition: Say that a surjective homomorphism of Λ-algebras, $\pi: C \to B$ is a **bilateral evolution** if the induced homomorphism $\tilde{\Omega}_{C/\Lambda} \otimes_{C_2} B_2 \to \tilde{\Omega}_{B/\Lambda}$ of B_2-modules is an isomorphism:

$$\tilde{\Omega}_{C/\Lambda} \otimes_{C_2} B_2 \xrightarrow{\cong} \tilde{\Omega}_{B/\Lambda} .$$

Let Λ be a complete noetherian local ring with residue field k, and let us now work exclusively in the category of complete noetherian local Λ-algebras with residue field k. Thus if B, C are objects of this category then $B \otimes_\Lambda C$ will mean *completed* tensor product, B_2 will mean $B \hat{\otimes}_\Lambda B$, and we will drop the "cont" from the subscript in the notation for the module $\tilde{\Omega}_{B/\Lambda,cont}$ of continuous bilateral differentials.

Proposition: If Λ is a complete local noetherian ring with residue field k, and $\pi: C \to B$ is a surjective bilateral evolution of complete local noetherian Λ-algebras with residue field k and such that B is flat over Λ, then π is an isomorphism.

Proof: I am thankful, again, to Beilinson for providing me with the following simple proof of this. First, using Proposition 2 of §5, one can check directly that a surjective homomorphism $\pi: C \to B$ is a bilateral evolution if and only if $\mathrm{Tor}^{C_2}_1(B_2,C)$ vanishes. Secondly, for C-modules M, N that are flat over Λ one also directly checks that there is a natural isomorphism of Λ-modules, $\mathrm{Tor}^{C}_1(M,N) \cong \mathrm{Tor}^{C_2}_1(M \otimes_\Lambda N, C)$. Taking $M=N=B$ the above facts mean that we are merely required to show the vanishing of $\mathrm{Tor}^{C}_1(B,B)$, which follows from

(surjectivity of π, and) Nakayama's lemma.

□

Chapter eleven. Bilateral Flach Derivations

§1. The basic set-up for this Chapter.

In part II we showed (subject to the clearing up a list of "loose ends") that Flach's construction yields a "Cohesive Flach System" in the terminology of Chapter 5. In fact, a reader of that Chapter will notice that, to obtain this result, we did not really make the maximal use of the cohomology classes of Flach's construction. We now wish to provide a system of axioms that sharpens the notion of "cohesive Flach system" and that records a bit less profligately the type of information given to us by Flach's construction.

Let p be a prime number > 2. Let A be a local, finite flat reduced $\mathbb{Z}_p$-algebra and H a free A-module of rank two endowed with an A-linear $G_{\mathbb{Q},\Sigma}$-action (for Σ a finite set of primes containing p). We assume that H satisfies the running hypotheses of §1 of Chapter 5. In particular, it satisfies the p-cyclotomic determinant condition. Denoting by $\rho: G_{\mathbb{Q},\Sigma} \to \mathrm{Aut}_A(H) \cong GL_2(A)$ the representation determined by this action, and $\bar{\rho}$ the associated residual representation, we assume that $\mathrm{Sym}^2(\bar{\rho})$ is absolutely irreducible and that $\bar{\rho}$ is cleanly ramified at all primes of Σ different from p, that ρ is semi-stably ramified at these primes, and that ρ is Barsotti-Tate at p. For prime numbers ℓ not in Σ, let $T_\ell \in A$ denote the "ℓ-th Hecke operator" as defined in Part I, i.e., T_ℓ is the A-Trace of the element $\rho(\mathrm{Frob}_\ell) \in GL_2(A)$ where Frob_ℓ is any choice of ℓ-Frobenius element. Let $\mathcal{G}$ denote the free $\mathbb{Z}_p$-algebra on the generating set $\{T_\ell\}_{\ell \notin \Sigma}$ and let $\mathcal{G} \to A$ denote the natural homomorphism of $\mathbb{Z}_p$-algebras. Make the **hypothesis** that $\mathcal{G} \to A$ is surjective.

[Remark: Looking ahead, one may want to define,

in certain contexts, an element $T_p \in A$ and include a "corresponding generator" T_p in the algebra $\mathbb{G}$, but let's not bother to do that now.]

We also assume that the H possesses a principal polarization with respect to which the action of A is Hermitian. In particular, A is a Gorenstein ring (Corollary 2 of §2 of Chapter 3). Let η be a congruence element for A.

§2. The $A \otimes_{\mathbb{Z}_p} A$-module $H \otimes_{\mathbb{Z}_p} H$ and its cohomology.

Using the notation $A_2 = A \otimes_{\mathbb{Z}_p} A$ of Chapter 10, we have that $H \otimes_{\mathbb{Z}_p} H$ is a free A_2-module of rank 4. Although this may seem a bit strained, let us give the following *new* notation for the $A_2[G_{\mathbb{Q},\Sigma}]$-module $H \otimes_{\mathbb{Z}_p} H$.

New notation: Put $\tilde{W}^* := H \otimes_{\mathbb{Z}_p} H$, and let $\tilde{W}$ denote the $A_2[G_{\mathbb{Q},\Sigma}]$-module which is Cartier dual to $\tilde{W}^*$, i.e.,

$$\tilde{W} := \mathrm{Hom}_{\mathbb{Z}_p}(H \otimes_{\mathbb{Z}_p} H, \mu).$$

We want to think of $\tilde{W}^*$ and $\tilde{W}$ as *refinements* of the Cartier dual $A[G_{\mathbb{Q},\Sigma}]$-modules W^* and W of Part I of these notes. We have natural surjections

$$(1) \quad \tilde{W}^* \to \tilde{W}^* \otimes_{A_2} A \to W^*,$$

and natural injections,

$$(2) \quad W \to \mathrm{Hom}_{\mathbb{Z}_p}(H \otimes_A H, \mu) \to \tilde{W}^*.$$

From diagram (4) of §2 of Chapter 10, we have the exact sequence of A_2-modules,

$$0 \to (\tilde{\eta}) \to A_2 \to A^{\perp} \to 0,$$

which, when tensored with $H \otimes_{\mathbb{Z}_p} H$, yields an exact sequence

$$\begin{array}{ccccccccc} & 0 & \to & (H\otimes_{\mathbb{Z}_p}H)_{\delta} & \to & H\otimes_{\mathbb{Z}_p}H & \to & (H\otimes_{\mathbb{Z}_p}H)\otimes_{A_2}A^{\perp} & \to 0 \\ (3) & & & = \downarrow & & = \downarrow & & = \downarrow & \\ & 0 & \to & \tilde{\eta}\cdot\tilde{W}^* & \to & W^* & \to & W^*/\tilde{\eta}\cdot\tilde{W}^* & \to 0. \end{array}$$

The $A^{\perp}[G_{\mathbb{Q},\Sigma}]$-module $W^*/\tilde{\eta}\cdot\tilde{W}^* = (H\otimes_{\mathbb{Z}_p}H)\otimes_{A_2}A^{\perp}$ is, of course, free of rank 4. [**Recall, though, that $\tilde{\eta}$ is usually not a non-zero-divisor in A_2**]

Notation: Given any bilateral $\mathbb{Z}_p$-derivation,

$$\mathbb{D} : \mathcal{G} \to H^1(G_{\mathbb{Q}}, \tilde{W}^*),$$

we denote by

$$\mathbf{S}\mathbb{D}: \mathcal{G} \to H^1(G_{\mathbb{Q}}, W^*)$$

the "unilateral" $\mathbb{Z}_p$-derivation of $\mathcal{G}$ obtained by composing the bilateral $\mathbb{Z}_p$-derivation $\mathbb{D} : \mathcal{G} \to H^1(G_{\mathbb{Q}}, \tilde{W}^*)$, with the homomorphism on cohomology induced by the surjection $\tilde{W}^* \to W^*$ of (1).

§3. (Bilateral) Flach Derivations connected to Galois representations.

Fix a prime number $p > 2$ and a square-free positive integer N. Let $\mathfrak{B}$ denote the (non-noetherian) $\mathbb{Z}_p$-algebra of polynomials in a countable number of variables, these variables being denoted by the symbols t_ℓ where ℓ runs through all prime numbers not dividing $p \cdot N$.

$$\mathfrak{B} = \mathbb{Z}_p[\ldots, t_\ell, \ldots].$$

Let

$$\rho: G_{\mathbb{Q},\Sigma} \to GL_2(A) \cong \mathrm{Aut}_A(H)$$

be a Galois representation satisfying the hypotheses of §1. We may view A as a $\mathfrak{B}$-algebra, via the mapping $\mathfrak{B} \to A$ of $\mathbb{Z}_p$-algebras which sends t_ℓ to the "Hecke operator" $T_\ell \in A$. In particular, we have a natural $\mathfrak{B}$-module structure on H induced from its A-module structure, and we have a natural $\mathfrak{B}_2 = \mathfrak{B} \otimes_{\mathbb{Z}_p} \mathfrak{B}$-module structure on $H \otimes_{\mathbb{Z}_p} H$.

We shall make two definitions. The point of the first definition is to formulate a relatively loose catch-all notion. The point of the second is to capture the precise structures we have already constructed.

Definition 1: A **(Bilateral) Flach Derivation** for ρ is a bilateral $\mathbb{Z}_p$-derivation

$$\mathbb{D} : \mathfrak{B} \to H^1(G_{\mathbb{Q}}, \tilde{W}^*) = H^1(G_{\mathbb{Q}}, H \otimes_{\mathbb{Z}_p} H)$$

with the following two properties.

1) For prime numbers $r \neq \ell$ the restriction of the

cohomology class $\tau_\ell := \mathbb{D}(t_\ell)$ to the decomposition group at r, $G_{\mathbb{Q}_r}$, is "finite", i.e., lies in $H_f^1(G_{\mathbb{Q}_r}, H\otimes_{\mathbb{Z}_p}H)$.

2) For all $\ell \notin \Sigma$ the restriction of the class $\tau_\ell = \mathbb{D}(t_\ell) \in H^1(G_{\mathbb{Q}}, H\otimes_{\mathbb{Z}_p}H)$ to the decomposition group at ℓ, $\mathrm{res}_\ell \tau_\ell \in H^1(G_{\mathbb{Q}_\ell}, H\otimes_{\mathbb{Z}_p}H) = \mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H\otimes_{\mathbb{Z}_p}H)$, lies in the submodule

$$\mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), (H\otimes_{\mathbb{Z}_p}H)^\delta) \subset \mathrm{Hom}_{G_{\mathbf{F}_\ell}}(\mathbb{Z}_p(1), H\otimes_{\mathbb{Z}_p}H).$$

Proposition: To give a Bilateral Flach Derivation for ρ, it is equivalent to give, for each prime number ℓ different from p, a class τ_ℓ in the $\mathfrak{B}_2 = \mathfrak{B}\otimes_{\mathbb{Z}_p}\mathfrak{B}$ -module $H^1(G_{\mathbb{Q}}, \tilde{W}^*) = H^1(G_{\mathbb{Q}}, H\otimes_{\mathbb{Z}_p}H)$ such that the classes τ_ℓ ($\ell \neq p$) satisfy properties **1)** and **2)** of Definition 1, and such that, we have the further relation

3) $$\delta t_{\ell_1}\cdot\tau_{\ell_2} = \delta t_{\ell_2}\cdot\tau_{\ell_1}$$

for any pair ℓ_1, ℓ_2 of prime numbers different from p.

Proof: The connection between the classes τ_ℓ described in our Proposition and Bilateral Flach Derivations is, of course, as follows: Given a Bilateral Flach Derivation $\mathbb{D}$, the classes $\tau_\ell = \mathbb{D}(t_\ell)$ satisfy the Properties of our Proposition, where **3)** follows from the Lemma of §1 of Chapter 10. Given a system of classes τ_ℓ as in the statement of the Proposition, that there is a unique Bilateral Flach Derivation $\mathbb{D}$ such that $\mathbb{D}(t_\ell) = \tau_\ell$ for all $\ell \neq p$ follows from Lemma 1 of §4 of Chapter 10.

□

Any finite linear combination of Bilateral Flach Derivations attached to ρ with coefficents in $A_2 = A \otimes_{\mathbb{Z}_p} A$ is again a Bilateral Flach Derivation attached to ρ.

Notation: Denote by $BFD(\rho)$ the A_2-module of all Bilateral Flach Derivations attached to ρ.

Definition 2: Let $\alpha \in A$ be a nonzero-divisor. A (Bilateral) Flach Derivation,

$$\mathbb{D} : \mathcal{G} \rightarrow H^1(G_{\mathbb{Q}}, \tilde{W}^*)$$

for the representation ρ will be said to have **singular depth α** if the rule assigning to each ℓ not in Σ the class $\mathbf{S}\mathbb{D}(t_\ell) \in H^1(G_{\mathbb{Q}}, W^*)$ is a Cohesive Flach System of depth α for ρ.

Pedantic Remark: In discussing *singular depth* it is convenient to be able to talk, as well, of the degenerate case of "**Bilateral Flach Derivations of singular depth 0**", these being Bilateral Flach Derivations such that for *all* prime numbers r (i.e., *including* $r=\ell$) the restriction of the cohomology class $\mathbf{S}\mathbb{D}(t_\ell)$ to the decomposition group at r lies in $H_f^1(G_{\mathbb{Q}_r}, W^*)$.

The proof of the Theorem of §5 in Chapter 8 actually constructs (given a w-marking f_X) a Bilateral Flach Derivation of singular depth $\alpha = w \cdot \eta$ (in the sense just axiomatized) attached to the representations ρ dealt with in that §. To be more explicit at the expense of being redundant, Let $\mathcal{G}$ denote the $\mathbb{Z}_p$-algebra of geometric self-correspondences of X as defined in §6 of Chapter 7. We

view $\mathcal{G}$ as $\mathcal{B}$-algebra by sending $t_\ell \in \mathcal{B}$ to $\Gamma_\ell \in \mathcal{G}$, for all prime numbers $\ell \neq p$.

Theorem: Let N be a square-free positive integer. Let $X = X_0(N)$, and let f_X be a modular unit generator on X of degree $w \in \mathbb{Z}$. Let $\underline{m}$ be an admissible maximal ideal and A its associated Gorenstein ring as discussed in Chapter 8, Let η be a congruence element of A. Let

$$\rho: G_{\mathbb{Q},\Sigma} \rightarrow GL_2(A)$$

be the associated Galois representation. The construction given by formula (9) of §5 of Chapter 8 projects to a Bilateral Flach Derivation of singular depth $w \cdot \eta$ attached to the Galois representation ρ, which factors through the $\mathcal{B}$-algebra $\mathcal{G}$,

$$\mathbb{D} : \mathcal{B} \rightarrow \mathcal{G} \rightarrow H^1(G_{\mathbb{Q}}, \tilde{W}^*)$$

□

§4. Are the Bilateral Flach Derivations that we have constructed "canonical" ?

Fixing $X = X_0(N)$ and an admissible maximal ideal $\underline{m}$, the construction of the Theorem above gives us a rule, call it $\beta = \beta_{N,\underline{m}}$, which assigns to any modular unit generator f_X of degree w a Bilateral Flach Derivation attached to the Galois representation ρ associated to $\underline{m}$. The mapping β is a homomorphism of the group of modular unit generators of level N (equivalently: of "admissible markings" on X) to the underlying additive group of the A_2-module of Bilateral Flach Derivations for ρ,

$$\beta_{N,\underline{m}} : \mathcal{GM}(X) \rightarrow BFD(\rho),$$

and recall that the singular depth of $\beta(f_X)$ is equal to $w \cdot \eta$.

It follows from the last phrase above that the kernel of β is contained in the kernel of the degree mapping,

$$\text{degree: } \mathcal{GM}(X) \rightarrow \mathbb{Z}.$$

Question: Is the kernel of β equal to the kernel of the degree mapping?

An affirmative answer to this question would be equivalent to the statement that the Bilateral Flach Derivations constructed here are "essentially" independent of the modular unit generator f_X: they are dependent only upon the degree w of f_X. If the answer to this question is "yes", one would be tempted, given ρ and a suitable "degree" $w \in \mathbb{Z}$, to look for a more direct definition of, or perhaps a characterization of, the Bilateral Flach Derivation of depth $w \cdot \eta$ we have constructed for ρ?

§5. The bilateral derivation of A associated to a Bilateral Flach Derivation.

Remaining in the context of §1, let

$$\mathbb{D} : \mathcal{B} \rightarrow H^1(G_{\mathbb{Q}}, \tilde{W}^*)$$

be a Bilateral Flach Derivation attached to the representation ρ. Letting I denote the kernel of $\mathcal{B} \rightarrow A$, we have, from Chapter 10, that the restriction $\tilde{\mathbb{D}}$ of $\mathbb{D}$ to I/I^2 is an A-homomorphism,

$$(4) \qquad \tilde{\mathbb{D}} : I/I^2 \rightarrow H^1(G_{\mathbb{Q}}, H \otimes_{\mathbb{Z}_p} H)_{\delta}.$$

We now **make the hypothesis** that no subquotient $A \otimes_{\mathbb{Z}_p} A$-module of $H \otimes_{\mathbb{Z}_p} H$ has nontrivial $G_{\mathbb{Q}}$-invariant elements, and therefore we have an associated exact

sequence of cohomology,

(5) $0 \to H^1(G_{\mathbb{Q}}, (H \otimes_{\mathbb{Z}_p} H)_\delta) \to H^1(G_{\mathbb{Q}}, H \otimes_{\mathbb{Z}_p} H) \to H^1(G_{\mathbb{Q}}, \tilde{W}^*/\tilde{\eta}\cdot\tilde{W}^*)$,

and also, by the Lemma of §7 of Chapter 7, we have the isomorphism

$$H^1(G_{\mathbb{Q}}, H \otimes_{\mathbb{Z}_p} H)_\delta \cong H^1(G_{\mathbb{Q}}, (H \otimes_{\mathbb{Z}_p} H)_\delta),$$

so we may view (4) as giving us an $A \otimes_{\mathbb{Z}_p} A$-homomorphism

(6) $\tilde{\mathbb{D}} : I/I^2 \to H^1(G_{\mathbb{Q}}, (H \otimes_{\mathbb{Z}_p} H)_\delta)$.

From (5) and (6) we see that $\mathbb{D}$ induces a bilateral $\mathbb{Z}_p$-derivation from A to the $A^\perp$-module $H^1(G_{\mathbb{Q},\Sigma}, \tilde{W}^*/\tilde{\eta}\cdot\tilde{W}^*)$; this bilateral $\mathbb{Z}_p$-derivation we will call

(7) $\mathbb{D}^\perp : A \to H^1(G_{\mathbb{Q},\Sigma}, \tilde{W}^*/\tilde{\eta}\cdot\tilde{W}^*) = H^1(\underline{X}\text{-}S, \tilde{W}^*/\tilde{\eta}\cdot\tilde{W}^*)$,

where the "$\underline{X}$" that appears in (7) is Spec $\mathbb{Z}$, following the conventions of Part I of these notes.

Proposition: The image of $\mathbb{D}^\perp$ lies in the submodule

$$H^1(\underline{X}, \tilde{W}^*/\tilde{\eta}\cdot\tilde{W}^*) \subset H^1(\underline{X}\text{-}S, \tilde{W}^*/\tilde{\eta}\cdot\tilde{W}^*).$$

Proof: This uses Lemmas 1 and 2 of §6 of Chapter 8.

[But recall that proofs for these have not yet been written down]

Specifically,.....

****

Corollary: The bilateral derivation $\mathbb{D}^{\perp}$ induces an $A^{\perp}$ homomorphism $\tilde{h}$ which fits into the commutative diagram

$$
\begin{array}{ccc}
 & \tilde{h} & \\
\tilde{\Omega}_{A/\mathbb{Z}_p} & \rightarrow & H^1(\underline{X}-\Sigma, \tilde{W}^*/\tilde{\eta}\cdot\tilde{W}^*) \\
\downarrow & & \downarrow \\
 & h & \\
\Omega_{A/\mathbb{Z}_p} & \rightarrow & H^1(\underline{X}-\Sigma, W^*/\eta\cdot W^*)
\end{array}
\qquad (8)
$$

where the $\tilde{A}$-homomorphism h is the one associated to the derivation $\Theta : A \rightarrow H^1(\underline{X}, W^*/\eta\cdot W^*)$ coming from the Cohesive Flach System $\ell \mapsto d(T_\ell)$, and where the vertical arrows are given by the natural mappings.

□