Some Contemporary Problems with Origins in the Jugendtraum

R.P. Langlands

The twelfth problem of Hilbert reminds us, although the reminder should be unnecessary, of the blood relationship of three subjects which have since undergone often separate developments. The first of these, the theory of class fields or of abelian extensions of number fields, attained what was pretty much its final form early in this century. The second, the algebraic theory of elliptic curves and, more generally, of abelian varieties, has been for fifty years a topic of research whose vigor and quality shows as yet no sign of abatement. The third, the theory of automorphic functions, has been slower to mature and is still inextricably entangled with the study of abelian varieties, especially of their moduli.

Of course at the time of Hilbert these subjects had only begun to set themselves off from the general mathematical landscape as separate theories and at the time of Kronecker existed only as part of the theories of elliptic modular functions and of cyclotomic fields. It is in a letter from Kronecker to Dedekind of 1880,[1] in which he explains his work on the relation between abelian extensions of imaginary quadratic fields and elliptic curves with complex multiplication, that the word *Jugendtraum* appears. Because these subjects were so interwoven it seems to have been impossible to disintangle the different kinds of mathematics which were involved in the Jugendtraum, especially to separate the algebraic aspects from the analytic or number theoretic. Hilbert in particular may have been led to mistake an accident, or perhaps necessity, of historical development for an "*innigste gegenseitige Berührung*." We may be able to judge this better if we attempt to view the mathematical content of the *Jugendtraum* with the eyes of a sophisticated contemporary mathematician.

An elliptic curve over a field k is a curve A in some projective space $\mathbf{P}^n$ defined, say, by equations

$$g_i(x_0, \dots, x_n) = 0$$

together with a rational map

$$z_j = f_j(x_0, \dots, x_n; y_0, \dots, y_n)$$

from $A \times A$ to A which turns the set of points on A into a group. Roughly speaking — the adverb is to be taken seriously — an elliptic curve over an arbitrary commutative ring R, which we always take to be noetherian, is defined in the same way except that the coefficients of f_j and g_i are to lie in R. If one has an elliptic curve over B_1 and a homomorphism $\varphi : B_1 \to B_2$ then replacing the coefficients of f_j and g_i by their images under φ we obtain an elliptic curve over B_2. In this way the sets $\mathcal{A}(B)$ of isomorphism classes of elliptic curves over a commutative noetherian ring B become a covariant functor on the category of such rings.

In the theory of complex multiplication one introduces a subfunctor. Take E to be an imaginary quadratic field and let O be the ring of integers in E. We are now interested only in rings B together with a homomorphism $\psi : O \to B$ and maps $B_1 \to B_2$ for which

$$\begin{array}{ccc} & O & \\ \psi_1 \swarrow & & \searrow \psi_2 \\ B_1 & \longrightarrow & B_2 \end{array}$$

is commutative. The tangent space $T(A)$ to an elliptic curve over B at the zero is a B-module. We are interested in abelian varieties A over B together with an action of the elements of O as endomorphisms of A such that the associated action of $x \in O$ on $T(A)$ is just multiplication by $\psi(x) \in B$. This gives us a new functor $B \to \mathcal{A}^O(B)$. If n is a positive integer and if we consider only rings B in which n is invertible, we can introduce a refinement. We can let $A_n(B)$ be the points of A with coefficients from B whose order divides n and introduce as additional datum an isomorphism of O-modules

$$\lambda : O/nO \to A_n(B).$$

This defines a new function $B \to \mathcal{A}^0_n(B)$.

[1] Gesammelte Werke, Bd V.

The methods of contemporary algebraic geometry, with which the present author is as yet only superficially acquainted, allow one to prove the existence of a universal object for this functor. This is a ring B_n, a homomorphism $O \to B_n$, an abelian variety A' over B_n, an action of O on A', and an isomorphism

$$\lambda' : O/nO \to A'_n(B_n)$$

such that the conditions imposed above are satisfied and such that for any B any element of $\mathcal{A}_n^O(B)$ is obtained by functoriality from A', λ' and a uniquely determined homomorphism $B_n \to B$. This is not quite true for small n but the difficulty can be obviated by some technical considerations and is not worth stressing here.

The methods not only establish the existence but also allow one to read off properties of the ring B_n from properties of the functor $\mathcal{A}_n^O$, that is, of elliptic curves over rings. For example, the notion of smoothness or, in the language of algebraic number theory, lack of ramification, is translated into a notion of deformability. The deformation theory of elliptic curves, and of abelian varieties, is well understood, and one can show that $F_n = B_n \otimes_O E$ is a finite direct sum $\oplus E_i$ of finite algebraic extensions of E unramified away from the primes dividing n and that if O_i is the ring of integers in E_i then B_n, a subring of F_n, is equal to

$$\oplus O_i[\frac{1}{n}].$$

Here $O_i\frac{1}{n}]$ is the subring of E generated by O_i and $\frac{1}{n}$.

If we imbed E into $\bar{\mathbf{Q}} \subseteq \mathbf{C}$ then the algebra F_n is determined by the action of $\mathfrak{G}(\bar{\mathbf{Q}}/E)$ on the set of its E-homomorphisms into $\mathbf{C}$, which is also $\mathcal{A}_n^O(\bar{\mathbf{Q}}) = \mathcal{A}_n^O(\mathbf{C})$. If the action is transitive the algebra is a field. Before investigating it we introduce some automorphisms of F_n. These are defined by automorphisms of the functor restricted for the moment to rings in which every positive integer is invertible. This means that B_n is to be replaced by F_n.

Let I_f be those ideles of E whose component at infinity is 1. We may imbed $E^\times$ in I_f. We are going to define an action of I_f on the functor $\mathcal{A}_n^O$. Let O_f be the ring of adeles which are integral everywhere and have component 1 at infinity. Suppose first that $g \in I_f \cap O_f$. There is a positive integer m and an $h \in I_f \cap O_f$ such that $gh = m$. Suppose $\{A, \lambda\}$ in $\mathcal{A}_n^O(B)$ is given. There is an extension B' of B and an isomorphism (of sheaves!)

$$\lambda' : O/n'O \longrightarrow A_{n'}(B')$$

such that

$$m\lambda'(x) = \lambda(x).$$

g acts on $O/n'O$ and we define a new elliptic curve A_1 by dividing by

$$\{\lambda'(gx) \mid x \in nO\}.$$

There is then an isogeny $\psi : A \to A_1$ with this kernel and we define λ_1 by

$$\lambda_1(x) = \psi(\lambda'(gx)).$$

The pair $\{A_1, \lambda_1\}$ actually defines an element of $\mathcal{A}_n^O(B)$. The action of g takes A, λ to A_1, λ_1. Since elements of O are easily seen to act trivially we can extend the action to all of I_f by letting that of ℓg, with ℓ a positive integer, be the same as that of g.

The action on $\mathcal{A}_n^O(\mathbf{C})$ can easily be made explicit. If $g \in I_f$ let gO be the ideal $gO_f \cap E$. We have imbedded E in $\mathbf{C}$, and the quotient of $\mathbf{C}$ by the lattice gO is an elliptic curve A^g on which O acts. Moreover

$$A_n^g(\mathbb{C}) = \frac{gO}{n}/gO.$$

If we regard O/nO as O_f/nO_f we may define λ^g as

$$x \to \frac{gx}{n}.$$

If

$$K^n = \{k \in I_f \mid k \equiv k^{-1} \equiv 1(\text{mod } n)\}$$

then A^g, λ^g and A^h, λ^h are isomorphic if and only if

$$h \in E^\times g k^n$$

so that as a set $\mathcal{A}_n^O(\mathbb{C})$ is just the quotient space $E^\times \backslash I_f / K^n$. The action of I_f is the obvious action on the quotient space.

By functoriality the action of $\mathfrak{G}(\bar{\mathbf{Q}}/E)$ on $\mathcal{A}_n^O(\bar{\mathbf{Q}}) = \mathcal{A}_n^O(\mathbf{C})$ commutes with that of I_f. Therefore there is a unique homomorphism $\sigma \to \varphi(\sigma)$ of $\mathfrak{G}(\bar{\mathbf{Q}}/E)$ into $E^\times \backslash I_f / K^n$ such that the actions of σ and $\varphi(\sigma)$ are the same. It follows in particular that $\mathfrak{G}(\bar{\mathbf{Q}}/E)$ acts through an abelian quotient. To understand the homomorphism $\sigma \to \varphi(\sigma)$ we have only to identify $\varphi(\sigma)$ when σ is the Frobenius at a prime $\mathfrak{p}$ of E which does not divide n.

Let $E_\mathfrak{p}$ be the completion of E at $\mathfrak{p}$, $\bar{E}_\mathfrak{p}$ an algebraic closure of $E_\mathfrak{p}$, and $\bar{O}_\mathfrak{p}$ the ring of integers in $\bar{E}_\mathfrak{p}$. Fix an imbedding $\bar{\mathbf{Q}} \hookrightarrow \bar{E}_\mathfrak{p}$.

$$\mathcal{A}_n^O(\bar{\mathbf{Q}}) \xrightarrow{\sim} \mathcal{A}_n^O(\bar{E}_\mathfrak{p}) = \mathrm{Hom}_O(B_n, \bar{E}_\mathfrak{p}) = \mathrm{Hom}_O(B_n, \bar{O}_\mathfrak{p}).$$

Since B_n is unramified at $\mathfrak{p}$, we may use the map $\bar{O}_\mathfrak{p} \to \bar{\kappa}_\mathfrak{p}$, the algebraic closure of the residue field $\kappa_\mathfrak{p}$ of O at $\mathfrak{p}$, to obtain

$$\mathrm{Hom}_O(B_n, \bar{O}_\mathfrak{p}) \simeq \mathrm{Hom}_O(B_n, \bar{\kappa}_\mathfrak{p}) = \mathcal{A}_n^O(\bar{\kappa}_\mathfrak{p}).$$

All these isomorphisms do not affect the action of the Frobenius. Because p is not invertible in $\bar{\kappa}_\mathfrak{p}$, the group I_f no longer operates, at least not quite as before. However I_f^p, consisting of those ideles which are 1 at infinity and at p, continues to operate, because for these ideles we can take the auxiliary integer m prime to p, and the difficulties attendant upon the anomalous behavior of p-division points in characteristic p do not appear. Actually because of the simplicity of the present situation, it is rather easy to define an action of the missing part of I_f, namely I_p, the multiplicative group of $O \otimes \mathbf{Q}_p$. However, we want to avoid all *ad hoc* techniques. What is needed is an understanding of the finite subgroups, in the scheme-theoretic sense, of an elliptic curve over a field of characteristic p with order a power of p. The general method is the theory of the Dieudonné module. I do not want to give its definition here. It is a module $D(A)$ functorially associated to A. The action of I_p is replaced by the action of the O-automorphisms of $D(A) \otimes \mathbf{Q}$. This group turns out however, because of the special situation with which we are dealing, to be I_p so that I_f does operate once again. Moreover $E^\times$ and K^n still act trivially. Since I_f is generated by $E^\times, I_f^p$, and K^n its action is compatible with the isomorphisms of sets introduced above.

If ϖ is a generator of the maximal ideal of $O_\mathfrak{p}$ then $\varpi \in E_\mathfrak{p}^\times \subseteq I_p$. The theory of Dieudonné modules acquired, it is immediate that the action of ϖ on $\mathcal{A}_n^O(\bar{\kappa}_\mathfrak{p})$ is the same as that of the Frobenius. It follows that F_n is a field and is the abelian extension of E associated to $E^\times I_\infty K^n \subseteq I$ by class field theory. Moreover the homomorphism

$$\mathfrak{G}(\bar{\mathbf{Q}}/E) \longrightarrow \mathfrak{G}(F_n/E) \simeq I/E^\times I_\infty K^n \simeq I_f/E^\times K^n$$

given by class-field theory is just $\sigma \to \varphi(\sigma)$. So far we have gotten by without any real arithmetic; only the arithmetic of finite fields has played a role. However, it is an essential part of the *Jugendtraum* that every abelian extension of E is contained in some F_n. For this we appeal to class-field theory.

But no elliptic modular functions have yet appeared. Let $V(\mathbf{Z})$ be the module of column vectors of length two over $\mathbf{Z}$. We can consider the functor which associates to B the isomorphism

$$\lambda : V(\mathbf{Z}/n\mathbf{Z}) \longrightarrow A_n(B).$$

This functor is also represented by a universal object over a ring J_n. The morphism $\mathcal{A}_n^O \to \mathcal{A}_n$ obtained by fixing an isomorphism

$$O \simeq V(\mathbf{Z})$$

and then forgetting the action of O yields a homomorphism $\eta : J_n \longrightarrow B_n$. If we imbed $B_n \longrightarrow \mathbf{C}$ over E then of course the image generates a class-field, as described above. Composing the imbedding with η yields a homomorphism of J_n or of $J_n \otimes \mathbf{C}$ into $\mathbf{C}$.

$J_n \otimes \mathbf{C}$ is the ring of rational functions on an algebraic variety S_n over $\mathbf{C}$ whose points give the homomorphisms of J_n into $\mathbf{C}$, that is, the elements of $\mathcal{A}_n(\mathbf{C})$. In particular, to obtain ψ we have to evaluate the elements of J_n at some point of $S_n(\mathbf{C})$. There is, at least from the analytic standpoint, a more concrete way of viewing $S_n(\mathbf{C})$ and hence $J_n \otimes \mathbf{C}$. Let G be the group $GL(2)$. Let J_0 be the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

If $g = (g_\infty, g_f)$ belongs to $G(\mathbf{A})$ with $g_\infty \in G(\mathbf{R}), g_f \in G(\mathbf{A}_f)$ we set

$$g_f V(\mathbf{Z}) = g_f V(\mathbf{Z}_f) \cap V(\mathbf{Q}).$$

Here $\mathbf{Z}_f$ is the closure of $\mathbf{Z}$ in $\mathbf{A}_f$ and $V(\mathbf{Z}_f) = V(\mathbf{Z}) \otimes \mathbf{Z}_f$. Then $g_f V(\mathbf{Z})$ is a lattice in $V(\mathbf{R})$. Let $J = g_\infty J_0 g_\infty^{-1}$. We turn $V(\mathbf{R})$ into a one-dimensional space over $\mathbf{C}$ by defining multiplication by $\sqrt{-1}$ to be J. Then

$$V(\mathbf{R})/g_f V(\mathbf{Z})$$

is an elliptic curve A^g over $\mathbf{C}$. Also

$$A_n^g(\mathbf{C}) = \frac{g_f V(\mathbf{Z})}{n} \Big/ g_f V(\mathbf{Z})$$

so we may take λ^g to be

$$x \rightarrow \frac{g_f x}{n}.$$

The isomorphism class of $\{A^g, \lambda^g\}$ is determined solely by the image of g in the double coset space

$$G(\mathbf{Q})\backslash G(\mathbf{A})/K_\infty K^n$$

if K_∞ is the centralizer of J_0 in $G(\mathbf{R})$ and K^n is

$$\{k \in G(\mathbf{Z}_f) \mid k \equiv 1 (\mathrm{mod}\ n)\}.$$

This double coset space has a natural complex structure and may now be identified with $S_n(\mathbf{C}) = \mathcal{A}_n(\mathbf{C})$.

Analyzing the double cosets more carefully one sees that $S_n(\mathbf{C})$ consists of finitely many connected pieces each of which is the quotient of the Poincaré half-plane by a congruence subgroup. The elements of $J_n \otimes \mathbf{C}$, in particular the elements of J_n, are functions on these pieces and are in fact just the elliptic modular functions of level n. The points of $S_n(\mathbf{C})$ corresponding to the homomorphism ψ introduced above are easily found explicitly. Summing up, we conclude that the class field F_n is generated by the values of the elliptic modular functions in J_n at a certain easily found point of

$$G(\mathbf{Q})\backslash G(\mathbf{A})/K_\infty K^n.$$

As we said, any connected piece of this space is a quotient of the Poincaré half-plane by a discrete group. If we lift the functions in J_n to the half-plane they become transcendental.

This aspect, the generation of class fields by the values of transcendental functions, has been emphasized by Hilbert who suggests, in the twelfth problem, that it may be possible to find for an arbitrary number field transcendental functions with a similar property. Whether justly or not, the twelfth problem has received very little attention. Any progress made on it has been an incidental result of research with quite different ends, although it too has its origins in the Jugendtraum. The bulk of this research is due to Shimura.

A characteristic of the number theory of the twentieth century has been the dominant role played by zeta-functions and L-functions, especially at a conjectural level. The analytic properties of the L-functions associated to an algebraic variety over a number field have been particularly difficult, usually impossible, to determine. But Shimura has studied very deeply certain varieties, which, like the varieties defined by elliptic modular functions, are closely related to algebraic groups. For various reasons it is to be expected that the L-functions associated to these Shimura varieties can be expressed in terms of the L-functions associated to automorphic forms on the group defining the variety and on certain related groups. This in itself is not enough to establish the analytic properties but it is a first step. Shimura, inspired by earlier work of Eichler, has been able to confirm the expectation for some of his varieties, basically those which are curves.

But many problems remain. I want to discuss one of them, rather casually, in the remainder of the lecture. There are various notions of a reciprocity law, all of them implicit in the laws of class-field theory. For example, one can view a theorem asserting that an L-function defined by diophantine data, that is, by an algebraic variety over a number field, is equal to an L-function defined by analytic data, that is, by an automorphic form, as a reciprocity law. There is good reason for this, for the Artin reciprocity law is such an assertion. The results of Eichler and Shimura are also of this form. There is nonetheless a more concrete notion available.

Suppose one has an algebraic variety S defined over a number field E. Suppose in fact that equations defining S have been chosen whose coefficients are integral outside of some finite set of primes Q. If $\mathfrak{p} \notin Q$ and $\kappa_{\mathfrak{p}}$ is the residue field of E at $\mathfrak{p}$ we can reduce the equations modulo $\mathfrak{p}$ and then speak of the set $S(\bar{\kappa}_{\mathfrak{p}})$ of points of S with coefficients in $\bar{\kappa}_{\mathfrak{p}}$. $S(\bar{\kappa}_{\mathfrak{p}})$ is given together with an action on it, that of the Frobenius $\Phi_{\mathfrak{p}}$. An explicit description of the sets $S(\bar{\kappa}_{\mathfrak{p}})$ and of the actions of $\Phi_{\mathfrak{p}}$ for all $\mathfrak{p} \notin Q$ could also be viewed as a reciprocity law. For example, if $E = Q$ and S is defined by the equation

$$x^2 + 1 = 0$$

then $S(\bar{\kappa}_p)$ for $p \neq 2$ is a set with two elements and Φ_p acts trivially or not according as $p \equiv 1$ or $p \equiv 3$ modulo 4. This is the first supplement to the law of quadratic reciprocity.

It is very likely that Shimura varieties admit a reciprocity law in this sense. I want to describe explicitly the form the law will most probably take. The description is speculative, but I have verified its correctness, in so far as my limited command of the necessary techniques allows, for those varieties which arise as solutions of moduli problems for abelian varieties.

To know the zeta-function of a variety, at least in the sense of knowing the factors of its Euler product expansion for almost all $\mathfrak{p}$, one just has to know the number of points in $S(\kappa_{\mathfrak{p}}^n)$ for all positive n, if $\kappa_{\mathfrak{p}}$ is the extension of $\kappa_{\mathfrak{p}}$ of degree n. This is just the number of fixed points of $\Phi_{\mathfrak{p}}^n$ in $S(\bar{\kappa}_{\mathfrak{p}})$. One might expect that this could be determined from the explicit description of $S(\bar{\kappa}_{\mathfrak{p}})$ and of the action of $\Phi_{\mathfrak{p}}$; so that from a reciprocity law in the second sense for the Shimura variety S one could obtain one in the first sense, at least for its zeta-function. However, difficult combinatorial problems arise which have not yet been seriously broached. But I have been able to make the transition in a limited number of cases, among which are included varieties of arbitrary large dimension.

The work of Shimura has been expounded in a remarkably clear fashion by Deligne,[2] who also added improvements of his own. One begins with a reductive algebraic group G over $\mathbf{Q}$ and a homomorphism $H_0 : GL(1) \to G$ defined over $\mathbf{C}$. The pair (G, h_0) is subject to some simple formal conditions. If R is the torus over $\mathbf{R}$ obtained from $GL(1)$ over $\mathbf{C}$ by restriction of scalars so that over $\mathbf{C}$

$$R \simeq GL(1) \times GL(1)$$

then the composition

$$h : R \xrightarrow{\sim} GL(1) \times GL(1) \to G,$$

where the second map is $(x, y) \to h_0(x)^\rho h_0(y)$ with ρ the complex conjugation, is to be a homomorphism defined over $\mathbf{R}$. The centralizer of $h(\mathbf{R})$ in $G_{\mathrm{der}}(\mathbf{R})$ is to be maximal compact subgroup of $G_{\mathrm{der}}(\mathbf{R})$ and if K_∞ is the centralizer of $h(\mathbf{R})$ in $G_{\mathrm{der}}(\mathbf{R})$ then the quotient $G(\mathbf{R})/K_\infty$ is to carry an invariant complex structure, specified by h_0.

It is in fact not h_0 which is significant but the collection of ad $g \circ h_0, g \in G(\mathbf{R})$. If T is a Cartan subgroup of G defined over $\mathbf{Q}$ with $T(\mathbf{R}) \cap G_{\mathrm{der}}(\mathbf{R})$ compact we may choose $h_0' = \mathrm{ad} g \circ h_0$ so that it factors through T. We then denote $h_0' : GL(1) \to T$ by $\hat{\mu}$; it is a coweight of T. If E is defined to be the fixed field of the set of all $\sigma \in \mathfrak{G}(\bar{\mathbf{Q}}/\mathbf{Q})$ for which $\sigma\hat{\mu} = \omega\hat{\mu}$ with ω in the Weyl group of T then E, which is a finite extension of $\mathbf{Q}$ in $\mathbf{C}$, plays an important role in the study of Shimura varieties.

[2] Séminaire Bourbaki, 1970/71.

If K is an open compact subgroup of $G(\mathbf{A}_f)$ then the complex manifold

$$S_K(\mathbf{C}) = G(\mathbf{Q})\backslash G(\mathbf{A})/K_\infty K$$

is the set of complex points of an algebraic variety of $\mathbf{C}$. It has been conjectured, hesitantly by Shimura, openly by Deligne, that this family of algebraic varieties should have models S_K over E. The precise conjecture actually demands certain further properties of the S_K, which serve to characterize them uniquely. These properties are patterned on the Jugendtraum; so that implicit in any proof of the existence of these canonical models S_K is a partial solution to the twelfth problem. The conjecture, colloquially referred to as the Shimura conjecture, has been solved for many groups but by no means all. My suggestions will only make sense for those groups for which the Shimura conjecture is acquired.

The group $G(\mathbf{A}_f)$ operates on

$$\lim_{\substack{\leftarrow \\ K}} S_K(\mathbf{C}).$$

It is demanded that this be reflected in an action of $G(\mathbf{A}_f)$ on

$$\lim_{\substack{\leftarrow \\ K}} S_K$$

defined over E.

Fix a prime $\mathfrak{p}$ of E and let p be the prime of $\mathbf{Q}$ it divides. I shall suppose that the group G is quasi-split over $\mathbf{Q}_p$ and split over an unramified extension. Recall that if G_{sc} is the simply-connected form of the derived group G_{der} then Bruhat and Tits have associated a building to $G_{sc}(\mathbf{Q}_p)$ on which $G(\mathbf{Q}_p)$ acts. A special maximal compact subgroup of $G(\mathbf{Q}_p)$ is the intersection of the stabilizer in $G(\mathbf{Q}_p)$ of a special vertex of the Bruhat-Tits building with

$$\{g \in G(\mathbf{Q}_p) \;\Big|\; |\chi(g)| = 1 \text{ for all rational characters of } G \text{ defined over } \mathbf{Q}_p\}.$$

We shall only be interested in K of the form

$$K = K^p K_p$$

where $K^p \subset G(\mathbf{A}_f^p)$ and K_p is a special maximal compact of $G(\mathbf{Q}_p)$.

The varieties S_K are defined over E and hence over $E_\mathfrak{p}$. Suppose $O_\mathfrak{p}$ is the ring of integers of $E_\mathfrak{p}$. To speak of $S_K(\bar\kappa_\mathfrak{p})$ we need models over $O_\mathfrak{p}$. At the moment I do not know how they should be characterized. Presumably if S_K/E is proper and smooth then $S_K/O_\mathfrak{p}$ should also be proper and smooth. But if S_K/E is not proper, some attention will have to be paid to the behavior at infinity. I simply ignore the difficulty for now and go on to describe the expected structure of $S_K(\bar\kappa_\mathfrak{p})$. It is enough to consider that of

$$\lim_{\substack{\leftarrow \\ K^p}} S_K(\bar\kappa_\mathfrak{p}) = S_{K_p}(\bar\kappa_\mathfrak{p})$$

provided that we know how $G(\mathbf{A}_f^p)$ acts on the right-hand side, for

$$S_K(\bar\kappa_\mathfrak{p}) = S_{K_p}(\bar\kappa_\mathfrak{p})/K^p.$$

The set $S_{K_p}(\bar\kappa_\mathfrak{p})$ should be the union of certain subsets invariant under $G(\mathbf{A}_f^p)$ and $\Phi = \Phi_\mathfrak{p}$. Each of them is constructed from the following data:

(i) a group H over $\mathbf{Q}$ and an imbedding $H(\mathbf{A}_f^p) \hookrightarrow G(\mathbf{A}_f^p)$;

(ii) a group $\bar G$ over $\mathbf{Q}_p$ and an imbedding $H(\mathbf{Q}_p) \hookrightarrow \bar G(\mathbf{Q}_p)$;

(iii) a space X on which $\bar G(\mathbf{Q}_p)$ and Φ act, the two actions commuting with each other.

The imbeddings $H(\mathbf{A}_f^p) \hookrightarrow G(\mathbf{A}_f^p), H(\mathbf{Q}_p) \hookrightarrow \bar G(\mathbf{Q}_p)$ when combined with the diagonal imbedding $H(\mathbf{Q}) \hookrightarrow H(\mathbf{A}_f)$ yield an action of $H(\mathbf{Q})$ on $G(\mathbf{A}_f^p) \times X$. The subsets to which I referred have the form

$$Y = H(\mathbf{Q})\backslash G(\mathbf{A}_f^p) \times X.$$

$G(\mathbf{A}_f^p)$ acts in the obvious way to the right and Φ acts through its action on X.

Before venturing a general prescription for H, G, and X we should orient ourselves with a brief glance at $G = GL(2)$ with h given by

$$(a+ib, a-ib) \longrightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \qquad a, b \in \mathbf{C}, a^2+b^2 \neq 0.$$

For mnemonic reasons, I adhere to a slightly different convention than Deligne, so that my h is the inverse of his. For this pair G, h there is one subset for each imaginary quadratic extension F of $\mathbf{Q}$. H is the group F^* over $\mathbf{Q}$ associated in the usual way to F so that $H(\mathbf{Q}) = F^\times, \bar{G}$ is also H, and X is the quotient of $H(\mathbf{Q}_\mathfrak{p}) = (E \otimes \mathbf{Q}_p)^\times \simeq \mathbf{Q}_p^\times \times Q_p^\times$ by $H(\mathbf{Z}_p)$, the group of units, $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$. If $\mathfrak{g}$ is one of the prime divisors of p in E and ϖ the corresponding uniformizing parameter then Φ is multiplication by $\varpi \in (E \otimes \mathbf{Q}_p)^\times$. There is one additional subset. For it, H is the multiplicative group of the quaternion algebra over $\mathbf{Q}$ split everywhere except at infinity and p and $\bar{G}$ is H. X is the quotient $\bar{G}(\mathbf{Q}_p)/\bar{G}(\mathbf{Z}_p)$, if $\bar{G}(\mathbf{Z}_p)$ is the multiplicative group of the maximal order in the completion of the algebra at p. Φ is multiplication by any ϖ in this order which generates the maximal ideal.

There is an alternative description of the X for the final subset which yields more insight into the general situation. Let $\mathfrak{k}$ be the completion of the maximal unramified extension of $\mathbf{Q}_p$ and $\mathfrak{o}$ its ring of integers. Denote by $a \to {}^\sigma a$ the action of the Frobenius. Let $\mathcal{H}$ be the set of $\mathfrak{o}$-lattices in the space of column vectors of length 2 over $\mathfrak{k}$. $\mathcal{H}$ is the set of vertices in the Bruhat-Tits building of $G(\mathfrak{k})$. Set

$$b = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}.$$

Define an action of Φ on $\mathcal{H}$ by

$$\Phi\mathfrak{k} = b^\sigma\mathfrak{k}.$$

Then

$$\bar{G}(\mathbf{Q}_p) = \{g \in G(\mathfrak{k}) \mid b^\sigma g b^{-1} = g\}$$

and X is the set of all $\mathfrak{x}$ in $\mathcal{H}$ for which

$$p\mathfrak{x} \underset{\neq}{\subset} \Phi\mathfrak{x} \underset{\neq}{\subset} \mathfrak{x}.$$

Geometrically this means that the images of $\mathfrak{x}$ and $\Phi\mathfrak{x}$ in the Bruhat-Tits building of $G_{sc}(\mathfrak{k}) = SL(2, \mathfrak{k})$ are joined by an edge. To verify that the two descriptions of X are not essentially different, one uses the fact that the Bruhat-Tits building is a tree. It is an amusing exercise.

To define $H, \bar{G}$, and X in general we fix $\bar{\mathbf{Q}} \hookrightarrow \mathbf{C}$ and then choose, once and for all, an imbedding $\bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$ so that the prime of E it defines is $\mathfrak{p}$. Suppose γ belongs to $G(\mathbf{Q})$ and is semi-simple. Suppose moreover that all the eigenvalues of γ have absolute value 1 away from infinity and p. Let

$$H^o = \{g \in G \mid g\gamma^m = \gamma^m g \text{ for some } m \neq 0 \text{ in } \mathbf{Z}\}.$$

H^o is connected and of course defined over $\mathbf{Q}$. Suppose $h^o : R \to H^o$ and the composition

$$R \xrightarrow{h^o} H^O \hookrightarrow G$$

is conjugate under $G(\mathbf{R})$ to h. If T is a Cartan subgroup of H^o defined over $\mathbf{Q}$ with $T(\mathbf{R}) \cap G_{\mathrm{der}}(\mathbf{R})$ compact, then, as before, replacing h^o by ad $g \circ h^o, g \in H^o(\mathbf{R})$ if necessary, we may suppose h^o factors through T. The associated

$$h_0^o : GL(1) \to T$$

is a coweight $\hat{\mu}$ of T. $\hat{\mu}$ is not uniquely determined by h^o, but its orbit under the Weyl group of T in H^o is; and that suffices for the following.

If $L(T)$ is the $\mathbf{Z}$-module

$$\mathrm{Hom}(T, GL(1))$$

and

$$\hat{L}(T) = \mathrm{Hom}(GL(1), T)$$

then $\hat{L}(T)$ is also

$$\mathrm{Hom}(L(T), \mathbf{Z}).$$

Define $\hat{\lambda}(\gamma) \in \hat{L}(\mathbf{R})$ by

$$|\lambda(\gamma)|_p = p^{-\langle \lambda, \hat{\lambda}(\gamma)\rangle}, \qquad \lambda \in L(T).$$

Let M be the lattice of rational characters of H^o defined over $\mathbf{Q}_p$. We say that the pair (γ, h^o) is of Frobenius type if there is an $r > 0$ in $\mathbf{Q}$ such that $\hat{\lambda}(\gamma) - r\hat{\mu}$ is orthogonal to M.

Later an equivalence relation will be introduced on pairs of Frobenius type. To each equivalence class will be associated $H, \bar{G}$, and X, as well as

$$Y = H(\mathbf{Q})\backslash G(\mathbf{A}_f^p) \times X.$$

For each equivalence class we will also define a multiplicity d. If dY is the disjoint union of d copies of Y then, as a set on which Φ and $G(\mathbf{A}_f^p)$ act, $S_{K_p}(\bar{\kappa}_{\mathfrak{p}})$ should be isomorphic to the disjoint union over equivalence classes of pairs of Frobenius type of the sets dY.

For the moment fix γ and h^o. H will be obtained from H^o by an inner twisting. Since the Hasse principle is valid for the adjoint group H^o_{ad}, it is enough to specify the twisting locally! Of course it has also to be verified that there is a global twisting with the specified local behavior; but this turns out to be a matter of standard techniques. The twisting is trivial except at infinity and p. At infinity it is so arranged that $H_{\mathrm{der}}(\mathbf{R})$ is compact. Before describing the twisting at p, we introduce a subgroup $\bar{G}^o$ of G defined over $\mathbf{Q}_p$. It is the connected subgroup whose Lie algebra is spanned by those elements V in the Lie algebra of G satisfying

$$\mathrm{Ad}\gamma(V) = \epsilon V$$

with $\epsilon \in \bar{\mathbf{Q}}_p$ and $|\epsilon|_p = 1$. $\bar{G}$ will be a twisted form of $\bar{G}^o$.

We shall in fact twist $\bar{G}^o$ and H^o simultaneously. If T is as above, let T_{ad} be its image in H^o_{ad} and $\bar{T}_{\mathrm{ad}}$ its image in $\bar{G}^o_{\mathrm{ad}}$. We choose T so that T_{ad} is anisotropic over $\mathbf{Q}_p$. Choose a finite Galois extension k of $\mathbf{Q}$ in $\bar{\mathbf{Q}}$ over which T splits. Suppose $a_{\sigma,\tau}$ is a fundamental 2-cocycle for $k_p/\mathbf{Q}_p$. Since

$$T(k_p) = \hat{L}(T) \otimes k_p^\times$$

we may introduce the 1-cochain

$$\sigma \to a_\sigma = \sum_{\tau \in \mathfrak{G}(k_p/\mathbf{Q}_p)} \sigma\tau\hat{\mu} \otimes a_{\sigma,\tau}.$$

It takes values in $T(k_p)$ but is not a 1-cocycle. However its image in $T_{\mathrm{ad}}(k_p)$ or $\bar{T}_{\mathrm{ad}}(k_p)$ is. Composing with the maps

$$H^1(\mathfrak{G}(k_p/\mathbf{Q}_p), T_{\mathrm{ad}}(k_p)) \to H^1(\bar{\mathbf{Q}}_p, H^o)$$
$$H^1(\mathfrak{G}(k_p/\mathbf{Q}_p), \bar{T}_{\mathrm{ad}}(k_p)) \to H^1(\bar{\mathbf{Q}}_p, \bar{G}^o)$$

we obtain the twisting cocycles for H^o and $\bar{G}^o$ at p. One must of course verify that the twistings are independent of all auxiliary data.

The homomorphism $H^o \to G_{\mathrm{der}}\backslash G$ yields $H \to G_{\mathrm{der}}\backslash G$. The multiplicity d is the number of elements in $H^1(\bar{\mathbf{Q}}, H)$ which are trivial at every place except p, including infinity, and which lie in the kernel of

$$H^1(\bar{\mathbf{Q}}, H) \to H^1(\bar{\mathbf{Q}}, G_{\mathrm{der}}\backslash G).$$

It may be, however, a little rash to predict d on the basis of the examples studied, for the groups involved have special cohomological properties.

The set X is the object must complicated to define. Set

$$\hat{\nu} = \sum_{\tau \in \mathfrak{G}(k_p/\mathbf{Q}_p)} \tau\hat{\mu}$$

and denote

$$\hat{\nu} \otimes x \in \hat{L}(T) \otimes k_p^\times = T(k_p)$$

by $x^{\hat{\nu}}$. We define the Weil group, $W_{k_p/\mathbf{Q}_p}$, by means of the cocycle $a_{\sigma,\tau}$. If $w = (x, \sigma) \in W_{k_p/\mathbf{Q}_p}$, with $x \in k_p^\times, \sigma \in \mathfrak{G}(k_p/\mathbf{Q}_p)$, set

$$b_w = x^{\hat{\nu}} a_\sigma.$$

Then $w \to b_w$ is a 1-cocycle. Let D be the maximal torus in the centre of H^o split over $\mathbf{Q}_p$. Let $\mathfrak{k}$ be the maximal unramified extension of $\mathbf{Q}_p$. It turns out that if we enlarge k_p to some k'_p and inflate b_w to $W_{k'_p/\mathbf{Q}_p}$ then we may represent its class by a cocycle $\{\bar{b}_w\}$ such that

$$\bar{b}_w = \bar{b}'_w \bar{b}''_w$$

where $\bar{b}'_w \in T(\mathfrak{k}), \bar{b}''_w \in D(\bar{\mathbf{Q}}_p)$ and

$$|\lambda(\bar{b}''_w)|_p = 1$$

for all rational characters of D. Moreover if W^o is the kernel of $W_{k_p}/\mathbf{Q}_p \to \mathfrak{G}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ then we may take $\bar{b}'_w = 1$ for $w \in W^o$. If w is any element of $W_{k'_p}/\mathbf{Q}_p$ which maps to the Frobenius in $\mathfrak{G}(\bar{\kappa}_\mathfrak{p}/\kappa_\mathfrak{p})$ set

$$b = \bar{b}'_w.$$

We regard b as an element of $G(\mathfrak{k})$. Any other choice of the auxiliary data replaces b by $cb^\sigma c^{-1}$ if σ is the Frobenius on $\mathfrak{k}$. Such a change is irrelevant for our purposes. Observe that we may realize $\bar{G}(\mathbf{Q}_p)$ as

$$\{g \in G(\mathfrak{k}) \mid b^\sigma g b^{-1} = g\}.$$

The group K_p determines a special vertex in the Bruhat-Tits building of $G_{sc}(\mathbf{Q}_p)$ and hence of $G_{sc}(\mathfrak{k})$ which in turn determines a parahoric subgroup of $K_p(\mathfrak{k})$ of $G(\mathfrak{k})$. Set

$$\mathcal{H} = G(\mathfrak{k})/K_p(\mathfrak{k}).$$

Let F be the map $\mathcal{H} \to \mathcal{H}$ which takes the point represented by g to the point represented by $b^\sigma g$.

There is a bijection between conjugacy classes of parabolic subgroups of G and conjugacy classes of parahoric subgroups with a representative in $K_p(\mathfrak{k})$. Let $\mathfrak{I}$ be the class determined by the parabolic subgroup generated by T and the family of one-parameter subgroups corresponding to roots α with $\langle\alpha, \hat{\mu}\rangle \leq 0$. Any point $\mathfrak{x}$ of $\mathcal{H}$ determines a special spoint $\mathfrak{x}_i$ in the Bruhat-Tits building of each simple factor $G_i(\mathfrak{k})$ of $G_{sc}(\mathfrak{k})$. We consider only those $\mathfrak{x}$ such that if $\mathfrak{y} = F\mathfrak{x}$ then, for each $i, \mathfrak{x}_i$ and $\mathfrak{y}_i$ are either the same or are joined by an edge. Then $\mathfrak{x}_i$ and $\mathfrak{y}_i$ determine a parahoric subgroup of $G_i(\mathfrak{k})$ and, as a consequence, $\mathfrak{x}$ and $\mathfrak{y}$ determine a parahoric subgroup of $G(\mathfrak{k})$. X consists of those $\mathfrak{x}$ for which this parahoric subgroup lies in the class $\mathfrak{I}$. $G(\mathbf{Q}_p)$ acts on X. If $r = [E_\mathfrak{k} : \mathbf{Q}_p]$ we define the action of $\Phi_\mathfrak{k}$ to be F^r.

The correct conditions defining the equivalence of two pairs $(\gamma_1, h_1^o), (\gamma_2, h_2^o)$ seem to be local, one condition at each finite place, but none at the infinite place. There should be positive integers m and n and a δ in the centre of $G(\mathbf{Q})$ with every eigenvalue a unit such that, first of all, γ_1^m and $\delta\gamma_2^n$ are conjugate in $G(\mathbf{Q}_\ell)$ for each $\ell \neq p$. They should also be conjugate in $G(\mathfrak{k})$. Let

$$\delta\gamma_2^n = g\gamma_1^m g^{-1}, \qquad g \in G(\mathfrak{k}).$$

Suppose b_1 and b_2 in $H_1^o(\mathfrak{R})$ and $H_2^o(\mathfrak{R})$ are associated to (γ_1, h_1^o) and (γ_2, h_2^o) as above. Then $gb_1^\sigma g^{-1} \in H_2^o(\mathfrak{k})$. The final condition for equivalence is that there be a c in $H_2^o(\mathfrak{k})$ such that

$$cgb_1{}^\sigma g^{-1}\,{}^\sigma c^{-1} = b_2.$$

In order to define the Γ-factors that should appear in the functional equation of the zeta-function of a Shimura variety one must also know something about their behavior at the infinite places of E. Two problems arise. If τ is an automorphism of $\bar{\mathbf{Q}}$ over $\mathbf{Q}$ we may apply τ to the family S_K over E to obtain a family of varieties ${}^{\tau}S_K$ over ${}^{\tau}E$. This new family should be again just the canonical models for the Shimura varieties defined by some new pair $({}^{\tau}G, {}^{\tau}h_0)$. There is an obvious guess. ${}^{\tau}G$ should be obtained from G by an inner twisting which is trivial at every finite place. If ρ is the complex conjugation and T is chosen as above then the twisting cocycle at infinity should be $\rho \to t_\rho$ with

$$\lambda(t_\rho) = (-1)^{\langle \lambda, \tau\hat{\mu} - \hat{\mu} \rangle}, \qquad \lambda \in L(T).$$

Then T may also be regarded as a Cartan subgroup of ${}^{\tau}G$ over $\mathbf{R}$. The homomorphism ${}^{\tau}h_0$ should just be the composition

$$GL(1) \xrightarrow{\tau\hat{\mu}} T \hookrightarrow {}^{I}\tau G.$$

If the field E is real then the complex involution acts on $S_K(\mathbf{C})$ which as a complex manifold is isomorphic to

$$G(\mathbf{Q})\backslash G(\mathbf{A})/K_\infty K.$$

It should be possible to define the resulting involution on the double coset space explicitly. E can be real only if $\rho\hat{\mu} = \omega\hat{\mu}$ with ω in the Weyl group of T in G. If this is so then ω can be realized by an element w in the normalizer of T in $G(\mathbf{R})$. The element w will normalize K_∞ so that the map $g \to gw$ may be transferred to the quotient. This should give the involution.

Shimura and Shih are working on these two problems, which are deeper than they appear at first glance.