On Katz Modular Forms

Gabor Wiese*

November 9, 2003

Abstract

These are slightly revised notes of a series of four talks given at the local geometry seminar in Leiden in December 2002 and January 2003. The subtitle "preliminary version" has vanished in this update, not because this text is in any form finished or complete, but because I do not intend to change it any further. For, since I learned some things since the first version, I feel that these notes actually ought to be completely reworked. However, since I got some positive feed-back on them, I decided to put them back on the web with only minor changes and corrections.

In the notes I take a very naive point of view on Katz modular forms, which is certainly at some points too naive. So certainly there are still some incorrect statements to be found.

In the first talk, the definition of Katz modular forms was given and motivated by showing that over the complex numbers they coincide with the well-known modular forms.

The second talk, consisting of two parts, presented a theorem due to Bas Edixhoven, which provides a method for the calculation of the space of cuspidal Katz modular forms of weight 1 over finite fields.

In the final talk, the so-called Serre conjecture in an extended form was presented, which - among other things - predicts the existence of a Katz eigenform of weight 1 in characteristic p belonging to a given irreducible odd representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$, which is unramified at p. Moreover, the results of some calculations of weight 1 modular forms over $\overline{\mathbb{F}_2}$ (originally performed by Mestre) were presented.

These notes owe even their mere existence to long explanations by Bas Edixhoven.

The attentive reader will, however, most likely find many inaccuracies and even mistakes, very probably due to the author, who would be grateful to be informed about them.

*gabor@math.leidenuniv.nl

Contents

1 Definition of Katz modular forms

This talk was given on 10 December 2002.

My principal aim is to motivate and explain the *idea* behind the definition of *Katz modular forms*. We start with the classical theory and try to make the algebraisation appear naturally. Due to time limitations, I shall not be able to present but the most elementary properties of the Katz forms.

We will always consider the non-compactified version of the moduli spaces appearing and deal with the cusps separately. For to my mind the ideas then become more easily accessible. We shall thus naturally find functions transforming like modular forms, but that can even have essential singularities in the cusps. In this talk I will call them *M-forms*.

Since I have not (yet) read the original articles by Katz, I shall be careful always to speak of Katz modular forms and not of modular forms as defined by Katz. The reader should be aware that there might be differences.

The exposition is based on lecture notes and explanations by Bas Edixhoven.

1.1 The level structure diagram

In this section we will introduce a commutative diagram, which on the one hand encodes *level structures*, and on the other hand gives rise to M-forms as invariant holomorphic sections resp. differentials. The latter points will be dealt with in the following two sections.

By the *level structure diagram* I mean the following commutative diagram

$$\begin{tikzcd} \mathbb{Z}^2 \times \mathbb{H} \arrow[r, hook, "(x,\tau)\mapsto(\phi_\tau(x),\tau)"] \arrow[dr, two heads, "\pi"'] & \mathbb{C} \times \mathbb{H} \arrow[r, two heads] \arrow[d, two heads, "\pi"] & \mathbb{E} \arrow[dl, two heads, "\pi"] \\ & \mathbb{H}, & \end{tikzcd}$$

where the map ϕ_τ is defined by $\begin{pmatrix} n \\ m \end{pmatrix} \mapsto \begin{pmatrix} n \\ m \end{pmatrix}^T \begin{pmatrix} \tau \\ 1 \end{pmatrix} = n\tau + m$ and π denotes the obvious projection maps. We shall consider this diagram in the category of complex manifolds.

Let us look at the fibre of a point $\tau \in \mathbb{H}$ under π, it is

$$0 \to \mathbb{Z}^2 \xrightarrow{\phi_\tau} \mathbb{C} \to E_\tau \to 0,$$

where $E_\tau = \mathbb{C}/\Lambda_\tau$ with $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$. I.e. the fibre is an elliptic curve over $\mathbb{C}$, and we have kept track of the lattice, in a standard form, that gives rise to the curve.

Next we bring natural actions of the group $\mathrm{SL}_2(\mathbb{Z})$ into play. First of all, it (actually even the group $\mathrm{SL}_2(\mathbb{R})$) acts on the upper half plane $\mathbb{H}$ by homographies, that is to say

$$\gamma.\tau = \frac{a\tau + b}{c\tau + d}, \quad \text{with } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We want to relate this action to the standard one on $\mathbb{Z}^2$. First we note the obvious formula

$$(c\tau + d) \begin{pmatrix} \gamma.\tau \\ 1 \end{pmatrix} = \gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix}.$$

Furthermore, one immediately finds the commutative diagram

$$\begin{tikzcd}
\mathbb{Z}^2 \arrow[d, "\phi_\tau"'] & \mathbb{Z}^2 \arrow[l, "\gamma^T"'] \arrow[d, "\phi_{\gamma\tau}"] \\
\Lambda_\tau & \Lambda_{\gamma\tau}. \arrow[l, "\cdot(c\tau+d)"']
\end{tikzcd}$$

We will put these relations to two different uses. First, we define actions by the group $\mathrm{SL}_2(\mathbb{Z})$ on the level structure diagram. So let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $\mathrm{SL}_2(\mathbb{Z})$. We make γ act on $\mathbb{Z}^2 \times \mathbb{H}$ by $\gamma.(\begin{pmatrix} n \\ m \end{pmatrix}, \tau) := (\gamma^{-1,T} \begin{pmatrix} n \\ m \end{pmatrix}, \gamma.\tau)$ and on $\mathbb{C} \times \mathbb{H}$ by $\gamma.(z, \tau) := (\frac{z}{c\tau+d}, \gamma.\tau)$.

It is immediate to check, e.g. using the relations exhibitied above, that the left hand side of the level structure diagram is $\mathrm{SL}_2(\mathbb{Z})$-equivariant. We transport the action to the right hand side, and could consequently pass to the quotient for any subgroup $\Gamma < \mathrm{SL}_2(\mathbb{Z})$. The quotient maps would also be analytic again. However, we avoid the use of quotients at this stage. Instead of speaking of a fibre of $\Gamma\tau$ for the quotients, we can look at the family of exact sequences

$$0 \to \mathbb{Z}^2 \xrightarrow{\phi_{\gamma\tau}} \mathbb{C} \to E_{\gamma\tau} \to 0 \qquad \text{for } \gamma \in \Gamma.$$

We will now define subgroups of $\mathrm{SL}_2(\mathbb{Z})$ giving rise to families of elliptic curves having some common property related to their torsion groups.

For that it is convenient to consider such an exact sequence as a pair (E_τ, ϕ_τ) (here, of course, the second component determines the first one). We interpret ϕ_τ as the choice of a lattice basis.

Let $N > 0$ be an integer. The N-torsion group $E_\tau[N]$ of the elliptic curve E_τ is defined as the first term in the exact sequence

$$0 \to \frac{1}{N}\Lambda_\tau/\Lambda_\tau \to E_\tau \xrightarrow{\cdot N} E_\tau.$$

The "choice of basis" isomorphism ϕ_τ descends to give the isomorphism

$$\overline{\phi_\tau} : (\mathbb{Z}/N)^2 \to E_\tau[N], \quad x \mapsto \frac{1}{N}\phi_\tau(x),$$

which should also be interpreted as a choice of basis of the torsion group. $\overline{\phi_\tau}$ is called a *level structure*.

Let us now compare the exact sequence of τ with the one of $\gamma\tau$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ as above, i.e. we want to relate the pair (E_τ, ϕ_τ) to $(E_{\gamma\tau}, \phi_{\gamma\tau})$. From one of the diagrams above, we immediately obtain the commutative diagram of isomorphisms

$$\begin{tikzcd} (\mathbb{Z}/N)^2 \arrow[d, "\overline{\phi_\tau}"'] & (\mathbb{Z}/N)^2 \arrow[l, "\overline{\gamma^T}"'] \arrow[d, "\overline{\phi_{\gamma\tau}}"] \\ E_\tau[N] & E_{\gamma\tau}[N]. \arrow[l, "\cdot(c\tau+d)"'] \end{tikzcd}$$

We now consider three different families. We fix a $\tau \in \mathbb{H}$.

- Let us define the group

  $$\Gamma(N) := \operatorname{Ker}\big(\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N)\big).$$

  Thus $\Gamma(N)$ is the normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of those matrices, the reduction modulo N of which is the unit matrix.

  $\Gamma(N)$ gives rise to the family of the exact sequences represented by the pairs $(E_{\gamma\tau}, \phi_{\gamma\tau})$ for $\gamma \in \Gamma(N)$, which precisely have in common that the choice of basis of their torsion groups are the same (for the natural ismorphism between E_τ and $E_{\gamma\tau}$).

  Hence the family $\Gamma(N)\tau$ corresponds to the isomorphism class of a pair $(E_\tau, \overline{\phi_\tau})$. By isomorphism of pairs we mean an isomorphism between the curves respecting the level structure, i.e. sitting in the commutative diagram

  $$\begin{tikzcd} & (\mathbb{Z}/N)^2 \arrow[dl, "\overline{\phi_\tau}"'] \arrow[dr, "\overline{\phi_{\gamma\tau}}"] & \\ E_\tau[N] & & E_{\gamma\tau}[N]. \arrow[ll, "\cdot(c\tau+d)"'] \end{tikzcd}$$

- Next consider the group $\Gamma_1(N)$ sitting in the cartesian diagram

  $$\begin{tikzcd} \Gamma(N) \arrow[r, hook] \arrow[d, equal] & \mathrm{SL}_2(\mathbb{Z}) \arrow[r, two heads] \arrow[dr, phantom, "\square"] & \mathrm{SL}_2(\mathbb{Z}/N) \\ \Gamma(N) \arrow[r, hook] & \Gamma_1(N) \arrow[r, two heads] \arrow[u, hook] & \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z}/N)}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right). \arrow[u, hook] \end{tikzcd}$$

  Thus, $\Gamma_1(N)$ consists precisely of those matrices, the reduction modulo N of which is upper triangular with 1's on the diagonal.

Consequently, $\Gamma_1(N)$ gives rise to the family, where $\overline{\phi_\tau}(\begin{pmatrix} 0 \\ 1 \end{pmatrix}) = \overline{\phi_{\gamma\tau}}(\begin{pmatrix} 0 \\ 1 \end{pmatrix})$. That means that the natural isomorphism maps the point $\frac{1}{N}$ of E_τ to the point $\frac{1}{N}$ of $E_{\gamma\tau}$.

We can also express that by introducing the injection

$$\psi_\tau : \mathbb{Z}/N \xrightarrow{1 \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}} (\mathbb{Z}/N)^2 \xrightarrow{\overline{\phi_\tau}} E_\tau[N].$$

Then this family corresponds to the isomorphism class of the pair $(E_\tau, \psi_\tau) = (E_\tau, 1/N)$.

- Finally, we consider the group $\Gamma_0(N)$ in the cartesian diagram

$$\begin{tikzcd}
\Gamma(N) \arrow[r, hook] \arrow[d, equal] & \mathrm{SL}_2(\mathbb{Z}) \arrow[r, two heads] \arrow[dr, phantom, "\square"] & \mathrm{SL}_2(\mathbb{Z}/N) \\
\Gamma(N) \arrow[r, hook] & \Gamma_0(N) \arrow[r, two heads] \arrow[u, hook] & \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z}/N)}(\overline{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}), \arrow[u, hook]
\end{tikzcd}$$

where we consider $\overline{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}$ as an element of the projective space $\mathbb{P}^1(\mathbb{Z}/N)$ over $\mathbb{Z}/N$, on which $\mathrm{SL}_2(\mathbb{Z})$ acts naturally. Hence, $\Gamma_0(N)$ is the set of matrices in $\mathrm{SL}_2(\mathbb{Z})$ that reduce modulo N to an upper triangular matrix.

The family corresponding to it can be characterised by saying that the subgroup of $E_\tau[N]$ generated by $\frac{1}{N}$ is mapped isomorphically into the corresponding one of $E_{\gamma\tau}[N]$.

We also have the interpretation as the isomorphism class of a pair $(E_\tau, < 1/N >)$.

I ought to remark that we have been quite restrictive considering only elliptic curves of the form E_τ. More generally one ought to regard pairs (E, ϕ), where E is an elliptic curve over $\mathbb{C}$ and $\phi : \mathbb{Z}^2 \to H_1(E(\mathbb{C}), \mathbb{Z})$ is a group isomorphism, in which case $E = H_1(E(\mathbb{C}), \mathbb{R})/H_1(E(\mathbb{C}), \mathbb{Z})$. Since, however, scaling the lattice by a non-zero complex number results in an isomorphic elliptic curve, the isomorphism class of (E, ϕ) always contains an element of the form (E_τ, ϕ_τ). In particular, there is an obvious way to broaden the definition of the pairs in the three points above, while the isomorphism classes stay the same.

1.2 Classical M-forms as invariant holomorphic sections

Given some $k \in \mathbb{Z}$, let us consider a global holomorphic section F of the line bundle $\mathbb{C}\times\mathbb{H} \xrightarrow{\pi} \mathbb{H}$, defined by the central vertical arrow in the level structure diagram. We shall - in this section - change the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{C}\times\mathbb{H}$ to be $\gamma(z,\tau) = ((c\tau+d)^k z, \gamma\tau)$. (Earlier we had $k = -1$.)

By a global holomorphic section we mean a holomorphic function $F : \mathbb{H} \to \mathbb{C} \times \mathbb{H}$ such that $\pi \circ F = \mathrm{id}_{\mathbb{H}}$. Hence $F(\tau) = (f(\tau), \tau)$, where $f : \mathbb{H} \to \mathbb{C}$ is holomorphic (it is F composed with the projection of $\mathbb{C} \times \mathbb{H}$ onto its first factor). Let us further assume that F is Γ-invariant, for a subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, i.e. $F(\gamma\tau) = \gamma F(\tau)$. We now make this equation more explicit for $\gamma \in \Gamma$ as above:

$$\begin{array}{rrcl} & F(\gamma\tau) & = & (f(\gamma\tau), \gamma\tau) \\ = & \gamma F(\tau) & = & (f(\tau)(c\tau+d)^k, \gamma\tau). \end{array}$$

We find that

(i) $f : \mathbb{H} \to \mathbb{C}$ is a holomorphic function and

(ii) $f(\gamma\tau) = f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau)$ for all $\gamma \in \Gamma$.

As we mentioned in the introduction, we shall call such a function f an *M-form* of weight k for Γ. We must impose some conditions on the cusps in order to obtain modular forms, which we shall postpone until later, since the decisive generalization can be done without them. We point out that f can have essential singularities at the cusps.

1.3 Classical M-forms as invariant holomorphic differentials

We shall now start with the algebraisation. That is, we are intending to express M-forms as sections of a sheaf (also) existing in algebraic geometry. It will be the pull-back of a sheaf of relative differentials.

To start with, we will introduce the sheaf of relative holomorphic differentials (i.e. differentials of the first kind) by the exact sequence

$$\begin{tikzcd} \pi^*{\Omega^1}_{\mathbb{H}} \arrow[r, hook] \arrow[d, equal] & {\Omega^1}_{\mathbb{C}\times\mathbb{H}} \arrow[r, two heads] \arrow[d, equal] & {\Omega^1}_{\mathbb{C}\times\mathbb{H}/\mathbb{H}} \arrow[d, equal] \\ \mathcal{O}_{\mathbb{C}\times\mathbb{H}} d\tau \arrow[r, hook] & \mathcal{O}_{\mathbb{C}\times\mathbb{H}} dz + \mathcal{O}_{\mathbb{C}\times\mathbb{H}} d\tau \arrow[r, two heads] & \mathcal{O}_{\mathbb{C}\times\mathbb{H}} dz, \end{tikzcd}$$

where z and τ are the standard coordinates on $\mathbb{C}$ resp. $\mathbb{H}$. In the same way one finds ${\Omega^1}_{\mathbb{E}/\mathbb{H}} \cong \mathcal{O}_{\mathbb{E}} dz$. Let us denote by 0 the sections in the level structure diagram mapping τ to

$(0,\tau)$. Then we can pull back the sheaf of relative differentials to obtain a first version of the object playing the main role in this setting:

$$\underline{\omega}_{\mathbb{E}/\mathbb{H}} := 0^*\Omega^1{}_{\mathbb{E}/\mathbb{H}} = 0^*\mathcal{O}_{\mathbb{E}}dz = \mathcal{O}_{\mathbb{H}}dz.$$

For a Γ-invariant open subset $U \subseteq \mathbb{H}$ the action of $\mathrm{SL}_2(\mathbb{Z})$ on the standard coordinates, coming from the action in the level structure diagram, gives rise to an action on $\underline{\omega}_{\mathbb{E}/\mathbb{H}}^{\otimes k}(U)$ in the following way

$$\gamma(f(\tau)(dz)^{\otimes k}) = f(\gamma\tau)(d\gamma z)^{\otimes k} = f(\gamma\tau)\frac{1}{(c\tau+d)^k}(dz)^{\otimes k}.$$

We consequently see that f is an M-form of weight k for Γ if and only if $f(\tau)(dz)^{\otimes k}$ is a Γ-invariant global section of $\underline{\omega}_{\mathbb{E}/\mathbb{H}}^{\otimes k}$.

Appendix: the complex Kodaira-Spencer isomorphism

This seems to be an appropriate point to mention a first version of the Kodaira-Spencer isomorphism. We have the following two sheaves on $\mathbb{H}$

$$\underline{\omega}_{\mathbb{E}/\mathbb{H}}^{\otimes k} = \mathcal{O}_{\mathbb{H}}(dz)^{\otimes k} \quad \text{and} \quad \Omega_{\mathbb{H}}^{\otimes l} = \mathcal{O}_{\mathbb{H}}(d\tau)^{\otimes l}.$$

Let us calculate the transformation of $d\tau^{\otimes l}$ under an element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Using the quotient rule we find

$$(d\gamma\tau)^{\otimes l} = (d\frac{a\tau+b}{c\tau+d})^{\otimes l} = \frac{1}{(c\tau+d)^{2l}}(d\tau)^{\otimes l}.$$

Consequently, we obtain an isomorphism respecting the $\mathrm{SL}_2(\mathbb{Z})$-action

$$\underline{\omega}_{\mathbb{E}/\mathbb{H}}^{\otimes k} \cong \Omega_{\mathbb{H}}^{\otimes l}$$

with $k = 2l$. Thus M-forms of *even weight* can be defined as the f in the invariant sections of the holomorphic differentials on $\mathbb{H}$.

1.4 The case of Γ acting freely

We have seen that M-forms arise naturally as the elements of $(\underline{\omega}_{\mathbb{E}/\mathbb{H}}^{\otimes k}(\mathbb{H}))^{\Gamma}$, which is defined using analytic objects. In this section we assume that $\underline{\Gamma \text{ acts freely on } \mathbb{H}}$, since we will then be able to give an algebraic analogue.

Proposition 1.4.1 *Denote by p the quotient morphism $\mathbb{H} \to \Gamma\backslash\mathbb{H}$. Then we have*

$$(p_*\underline{\omega}_{\mathbb{E}/\mathbb{H}})^{\Gamma} \cong \underline{\omega}_{(\Gamma\backslash\mathbb{E})/(\Gamma\backslash\mathbb{H})}.$$

Proof. I do not want to prove that in detail and just say that the freeness of the action of Γ on $\mathbb{H}$ implies the freeness on $\mathbb{E}$. Hence the quotient maps $p : \mathbb{H} \to \Gamma\backslash\mathbb{H}$ and $q : \mathbb{E} \to \Gamma\backslash\mathbb{E}$ are unramified coverings. For an open cover $\bigcup U_i$ of $\Gamma\backslash\mathbb{H}$ with U_i small enough, one consequently has canonical isomorphisms

$$(q_*{\Omega^1}_{\mathbb{E}})^\Gamma(\pi^{-1}(U_i)) \to {\Omega^1}_{\Gamma\backslash\mathbb{E}}(\pi^{-1}(U_i))$$

and similarly for ${\Omega^1}_{\mathbb{H}}$. Therefore, one has to check that the defining exact sequences for the relative differential modules and the 0-sections are respected. $\square$

One can find algebraic curves over $\mathrm{Spec}(\mathbb{C})$, the complex points of which are precisely those curves. Hence, one can define an algebraic analogue of the sheaf $\underline{\omega}_{(\Gamma\backslash\mathbb{E})/(\Gamma\backslash\mathbb{H})}$. Of course, that is the point, where we will use the moduli spaces of elliptic curves defined in Bas' talks. We will be more precise on that in the following section.

1.5 Towards an algebraic definition

If Γ does not act freely, then $(\Gamma\backslash\mathbb{E})/(\Gamma\backslash\mathbb{H})$ is not an elliptic curve. To make up for that, one instead looks at all (suitable) elliptic curves in order to recover the same information as in the preceding section. We will make that precise below.

Let us start by a calculation, which we will need several times in this section.

Lemma 1.5.1 *Let E, E', S and S' be schemes fitting in the cartesian diagram*

$$\begin{tikzcd} E' \arrow[r, "h"] \arrow[d] \arrow[dr, phantom, "\Box"] & E \arrow[d] \\ S' \arrow[r, "g"] & S, \end{tikzcd}$$

and assume that there are sections for the vertical arrows, both called 0, which also make the diagram commutative, i.e. $h \circ 0 = 0 \circ g$. Then

$$g^* \underline{\omega}_{E/S}^{\otimes k} \cong \underline{\omega}_{E'/S'}^{\otimes k}.$$

Proof. It is a well-known fact (Hartshorne, II.8.10) that the sheaf of relative differentials is stable under base change: $h^*{\Omega^1}_{E/S} \cong {\Omega^1}_{E'/S'}$. We get $g^*\underline{\omega}_{E/S}^{\otimes k} = (g^* \circ 0^*)\Omega_{E/S}^{1\otimes k} = (0 \circ g)^*\Omega_{E/S}^{1\otimes k} = (h \circ 0)^*\Omega_{E/S}^{1\otimes k} \cong 0^*\Omega_{E'/S'}^{1\otimes k} = \underline{\omega}_{E'/S'}^{\otimes k}$. $\square$

In the setting of the lemma we have the commutative diagram

$$\begin{tikzcd}
{\Omega^1}_{E/S}(E) \arrow[r, "h^*"] \arrow[d, "0^*"] & h^*{\Omega^1}_{E/S}(E') \arrow[r, "\sim"] \arrow[d, "0^*"] & {\Omega^1}_{E'/S'}(E') \arrow[d, "0^*"] \\
\underline{\omega}_{E/S}(S) \arrow[r] & h^*\underline{\omega}_{E/S}(S') \arrow[r, "\sim"] & \underline{\omega}_{E'/S'}(S').
\end{tikzcd}$$

Due to the section relation $0^* \circ \pi^* = \mathrm{id}_{\underline{\omega}_{E/S}(S)}$, the left bottom arrow can be defined as $0^* \circ h^* \circ \pi^*$. Composing it with the isomorphism on the right, we obtain a homomorphism

$$(h/g)^* : \underline{\omega}_{E/S}(S) \to \underline{\omega}_{E'/S'}(S').$$

Let us now look at a special case. We have the cartesian diagram

$$\begin{tikzcd}
E_{\gamma\tau} \arrow[r, "\cdot(c\tau+d)"] \arrow[d] \arrow[dr, phantom, "\square"] & E_\tau \arrow[d] \\
\mathrm{Spec}(\mathbb{C}) \arrow[r, equal] & \mathrm{Spec}(\mathbb{C}).
\end{tikzcd}$$

Considering the differential modules again analytically, one finds that the homomorphism of abelian groups

$$\begin{gathered}
((c\tau+d)/\mathrm{id})^* : \underline{\omega}^{\otimes k}_{E_\tau/\operatorname{Spec}(\mathbb{C})}(\mathrm{Spec}(\mathbb{C})) \to \underline{\omega}^{\otimes k}_{E_{\gamma\tau}/\operatorname{Spec}(\mathbb{C})}(\mathrm{Spec}(\mathbb{C})), \\
r(ds)^{\otimes k} \overset{\pi^*}{\mapsto} r(dz)^{\otimes k} \overset{h^*}{\mapsto} (c\tau+d)^k r(dz)^{\otimes k} \overset{0^*}{\mapsto} (c\tau+d)^k r(ds)^{\otimes k}
\end{gathered}$$

is given by multiplication by $(c\tau+d)^k$. Here r is an element of $\mathbb{C}$, considered as a function on $\mathrm{Spec}(\mathbb{C})$, the standard coordinate of which we call s.

Now let F be a rule assigning to each $E_\tau/\operatorname{Spec}(\mathbb{C})$ an element in $\underline{\omega}^{\otimes k}_{E_\tau/\operatorname{Spec}(\mathbb{C})}(\mathrm{Spec}(\mathbb{C}))$, subject to the condition that, whenever two such elements fit in a cartesian diagram as above, then the pull-back $(h/g)^*$ has to be respected, i.e. in general

$$(h/g)^* F(E/S) = F(E'/S')$$

In the case treated right before, this condition comes down to

$$f(\gamma\tau) = (c\tau+d)^k f(\tau),$$

if we put $F(E_\tau/\operatorname{Spec}(\mathbb{C})) = f(\tau)ds$. We thus find another characterisation of the transformation rule of M-forms for Γ, if we precisely allow the cartesian diagrams for E_τ and $E_{\gamma\tau}$ with $\gamma \in \Gamma$. This condition is naturally expressed by saying that the level structures in question must be respected.

Defining F only on the E_τ's does, however, not imply the holomorphicity of f. In the case, where Γ acts freely, we can impose the additional condition that F must also take a value at the elliptic curve $(\Gamma\backslash\mathbb{E})/(\Gamma\backslash\mathbb{H})$. If F also respects the cartesian diagram (in the sense as above)

$$\begin{tikzcd} E_\tau \arrow[r, "h"] \arrow[d] \arrow[dr, phantom, "\square"] & \Gamma\backslash\mathbb{E} \arrow[d] \\ \operatorname{Spec}(\mathbb{C}) \arrow[r, "g"] & \Gamma\backslash\mathbb{H}, \end{tikzcd}$$

then $F(E_\tau/\mathbb{C})$ is uniquely determined by $F((\Gamma\backslash\mathbb{E})/(\Gamma\backslash\mathbb{H}))$ and f is holomorphic.

We cannot carry this last remark over word for word to the case, where Γ does not act freely, since then the object $(\Gamma\backslash\mathbb{E})/(\Gamma\backslash\mathbb{H})$ is not an elliptic curve, which we would like. However, the way we got the modular forms in this section does generalize. We give the definition in the following section in detail.

1.6 Definition of Katz M-forms

We will now restrict the generality and deal only with the congruence subgroup $\Gamma_1(N)$ for $N > 0$. It is, however, not difficult to replace the category defined below by the corresponding one for $\Gamma_0(N)$ for instance.

We introduce the category $[\Gamma_1(N)]_R$ of *elliptic curves with a given torsion point* for a ring R.

- Objects: Pairs $(E/S/R, \phi)$. $E/S/R$ is an elliptic curve, i.e. E/S a proper smooth scheme over $\operatorname{Spec}(R)$, whose geometric fibres are connected smooth curves of genus 1, and there is an S-valued point 0 of E. And $\phi : (\mathbb{Z}/N)_S \hookrightarrow E[N]$ is an embedding of group schemes. We briefly recall that $E[N]$ is the S-group scheme obtained from the cartesian diagram

$$\begin{tikzcd} E \arrow[r, "\cdot N"] \arrow[dr, phantom, "\square"] & E \\ E[N] \arrow[u] \arrow[r] & S, \arrow[u, "0"'] \end{tikzcd}$$

i.e. it is the kernel of the multiplication by N map, which results from E/S being an abelian group scheme.

- Morphisms: Cartesian diagrams

$$\begin{tikzcd} E' \arrow[r, "h"] \arrow[d] \arrow[dr, phantom, "\square"] & E \arrow[d] \\ S' \arrow[r, "g"] & S, \end{tikzcd}$$

  such that the diagram

$$\begin{tikzcd} E' \arrow[r, "h"] & E \\ S' \arrow[u, "0"] \arrow[r, "g"] & S \arrow[u, "0"'] \end{tikzcd}$$

  is commutative, and the embedding

$$\phi' : (\mathbb{Z}/N)_{S'} \hookrightarrow E'[N]$$

  is obtained by base change from

$$\phi : (\mathbb{Z}/N)_S \hookrightarrow E[N].$$

Next we describe the object $H^0([\Gamma_1(N)]_R, \underline{\omega}^{\otimes k})$. I think it is an example of the cohomology of stacks (= champs). There is a down to earth way to describe it. I shall, however, amuse myself by introducing this object slightly more categorially first, and then writing down what it comes down to.

Let $\mathcal{C}$ be a category and $H^0(\cdot, \underline{\omega})$ a functor from $\mathcal{C}$ to another category $\mathcal{D}$. Let us moreover assume that there exists a forgetful functor $\text{forget} : \mathcal{D} \to (\text{Sets})$. Now the set (class?, probably need some assumption on the categories) $H^0(\mathcal{C}, \underline{\omega})$ is defined as the set of morphisms of functors from $(\text{trivial} : \mathcal{C} \to (\text{Sets}), C \mapsto \{0\})$ to $(\text{forget} \circ H^0(\cdot, \underline{\omega}))$. This means that $f \in H^0(\mathcal{C}, \underline{\omega})$ is a rule assigning to each $C \in \mathcal{C}$ an element in the set $(\text{forget} \circ H^0(\cdot, \underline{\omega}))(C)$ compatible with the morphisms in the category $\mathcal{C}$.

We shall now apply this to our situation. The category $\mathcal{C}$ will, of course, be replaced by $[\Gamma_1(N)]_R$. The functor $H^0(\cdot, \underline{\omega})$ is taken to be

$$(E/S/R, \phi) \mapsto H^0(S, \underline{\omega}_{E/S}^{\otimes k}) = \underline{\omega}_{E/S}^{\otimes k}(S).$$

Here we have set

$$\underline{\omega}_{E/S}^{\otimes k} = 0^* \Omega_{E/S}^{1 \otimes k},$$

which is a sheaf on S.

We repeat ourselves by pointing out that an element $F \in H^0([\Gamma_1(N)]_R, \underline{\omega}^{\otimes k})$ is the choice of elements $F(E/S/R, \phi) \in H^0(S, \underline{\omega}_{E/S}^{\otimes k})$, subject to the rule

$$(h/g)^* F(E/S/R, \phi) = F(E'/S'/R, \phi')$$

for any cartesian diagram as above.

Definition 1.6.1 Let R be a ring and k and N integers with $N > 0$. The space of *Katz M-forms of weight k for the group* $\Gamma_1(N)$ is defined as

$$\mathcal{M}(\Gamma_1(N), k)_R = H^0([\Gamma_1(N)]_R, \underline{\omega}^{\otimes k}).$$

We point out that if the category has a final object $(E_{\Gamma_1(N)}/Y_{\Gamma_1(N)}/R, \phi_{\Gamma_1(N)})$, then

$$H^0([\Gamma_1(N)]_R, \underline{\omega}^{\otimes k}) = H^0(Y_{\Gamma_1(N)}, \underline{\omega}_{E_{\Gamma_1(N)}/Y_{\Gamma_1(N)}}^{\otimes k}).$$

Let us now describe briefly, why the Katz M-forms coincide with the classical M-forms, which have no essential singularities at the boundary, if the ring R is $\mathbb{C}$.

Assume first that $\Gamma = \Gamma_1(N)$ acts freely. Then Bas proved in his second talk of this series that there exists a final object $(E_{\Gamma_1(N)}/Y_{\Gamma_1(N)}/R, \phi_{\Gamma_1(N)})$ in the category $[\Gamma_1(N)]_R$ if $N > 4$ and N is invertible in R. If $R = \mathbb{C}$ then by the universality, the complex points of $Y_{\Gamma_1(N)}$ correspond to pairs $(E_\tau/\operatorname{Spec}(\mathbb{C}), 1/N)$. One actually finds (for that, some compatibilities ought to be checked) that $E_{\Gamma_1(N)}(\mathbb{C}) \cong \Gamma\backslash\mathbb{E}$ and $Y_{\Gamma_1(N)}(\mathbb{C}) \cong \Gamma\backslash\mathbb{H}$ and that these isomorphisms respect the structural morphisms. Thus the difference between the analytically defined group $\underline{\omega}_{(\Gamma\backslash\mathbb{E})/(\Gamma\backslash\mathbb{H})}(\Gamma\backslash\mathbb{E})$ and its algebraic counterpart $\underline{\omega}_{E_{\Gamma_1(N)}/Y_{\Gamma_1(N)}}(Y_{\Gamma_1(N)})$ lies on the boundary. Consequently, for freely acting Γ the Katz M-forms over $\mathbb{C}$ coincide with the classical ones, which do not have essential singularities in the cusps.

If $\Gamma_1(N)$ does not act freely, we do not dispose of such an easy description. Instead, we pass to a subgroup $\Gamma_1(Nm)$, which acts freely on $\mathbb{H}$ ($Nm > 4$). We will also assume that m is invertible in R. We then have an injection (of sets)

$$H^0([\Gamma_1(N)]_R, \underline{\omega}^{\otimes k}) \hookrightarrow H^0([\Gamma_1(Nm)]_R, \underline{\omega}^{\otimes k}), \qquad f \mapsto f \circ \psi,$$

coming from the (surjective) functor

$$\psi : [\Gamma_1(Nm)]_R \to [\Gamma_1(N)]_R, \qquad (E/S/R, \phi) \mapsto (E/S/R, \phi \circ i),$$

where i is natural embedding of group schemes $(\mathbb{Z}/N)_S \to (\mathbb{Z}/Nm)_S$ defined by sending 1 to m.

Applying this with $R = \mathbb{C}$, we obtain that also Katz M-forms for $\Gamma_1(N)$ are holomorphic. More precisely, they can be characterized as the subspace of Katz M-forms for $\Gamma_1(Nm)$ satisfying the transformation rule for $\Gamma_1(N)$.

Appendix: the Kodaira-Spencer isomorphism

In this section we mention that the Kodaira-Spencer morphism

$$\underline{\omega}_{E/S}^{\otimes 2} \to \Omega^1{}_{S/T}$$

for E/S an elliptic curve and $S \to T$ any morphism can be defined in general (in the algebraic setting), and not only over $\mathbb{C}$, as we did before. It actually is an isomorphism if we take $(E/S/T)$ to be $E_\Gamma/Y_\Gamma/\mathbb{Z}[1/N]$ with $\Gamma = \Gamma_1(N)$ and $N > 4$. This, of course, allows us to consider M-forms of even weight for this group to be global differentials, just as we had in the complex case.

1.7 q-expansions and Katz modular forms

In this section we let $N > 2$ and $\Gamma = \Gamma_1(N)$, since we do not want to be troubled with irregular cusps. This is not a conceptual restriction, it just saves a bit of work here.

We start by recalling the classical notion of q-expansions, which we will, of course, recover later in the Katz setting.

As $\gamma := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is in Γ, every M-form f satisfies

$$f(\gamma\tau) = f(\tau + 1) = f(\tau).$$

So f is periodic with period 1, whence we can write

$$f(\tau) = g(q) = \sum_{n \geq -\infty} a_n q^n$$

with $q = e^{2\pi i \tau}$, where the last equality is the expansion around 0, which is called the q-expansion of f at the standard cusp ∞ (because $\tau \to i\infty \Leftrightarrow q \to 0$).

We want to extend this notion to other cusps as well. Let $x = \sigma\infty$ for $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ be another cusp and let Γ_x be its stabilizer in the group Γ. We get

$$\sigma^{-1}\Gamma_x\sigma \leq \Gamma_\infty = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\mathbb{Z}}, \quad \text{hence} \quad \sigma^{-1}\Gamma_x\sigma = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^{\mathbb{Z}}$$

for some $h|N$. Let us now consider the function

$$f|_k(\sigma)(\tau) = (c\tau + d)^{-k} f(\sigma\tau), \quad \text{for} \quad \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

($|_k$ is called the *Petersson (slash-)operator*.) We point out that f satisfies the transformation rule for σ if and only if $f|_k(\sigma) = f$. An easy calculation gives

$$f|_k(\gamma)|_k(\gamma') = f|_k(\gamma\gamma').$$

Using this with $\sigma^{-1}\gamma\sigma = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ for some $\gamma \in \Gamma_x$, one gets

$$f|_k(\sigma)(\tau) = f|_k(\sigma)(\tau + h).$$

This allows us again to develop $f|_k(\sigma)$ into a Laurent series in the variable $q^{1/h}$. That is called the *q-expansion at the cusp x.*

In order to find a translation into the language of Katz forms, we consider the following cartesian diagram

$$\begin{tikzcd} (E_\tau, \frac{-b\ (\mathrm{mod}\ N)}{N}\tau + \frac{a\ (\mathrm{mod}\ N)}{N}) \arrow[rr, "\cdot(c\tau+d)^{-1}"] \arrow[d] \arrow[drr, phantom, "\square"] & & (E_{\sigma\tau}, \frac{1}{N}) \arrow[d] \\ \mathrm{Spec}(\mathbb{C}) \arrow[rr, equal] & & \mathrm{Spec}(\mathbb{C}). \end{tikzcd}$$

If F is now a Katz M-form with the usual identification $f(\tau)(ds)^{\otimes k} = F(E_\tau/\mathbb{C}, 1/N)$, then we find from the transformation rule

$$\begin{aligned} f|_k(\sigma)(\tau)(ds)^{\otimes k} &= (c\tau + d)^{-k} f(\sigma\tau)(ds)^{\otimes k} = (c\tau + d)^{-k} F(E_{\sigma\tau}, 1/N) \\ &= F(E_\tau, \frac{-b\ (\mathrm{mod}\ N)}{N}\tau + \frac{a\ (\mathrm{mod}\ N)}{N}). \end{aligned}$$

That means that the function $f|_k(\sigma)$ corresponds to the evaluation of F at the usual elliptic curves E_τ, but now with the torsion point $\frac{-b\ (\mathrm{mod}\ N)}{N}\tau + \frac{a\ (\mathrm{mod}\ N)}{N}$.

We bring the Tate curve into the business and consider the isomorphism

$$(\mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}, \frac{-b\ (\mathrm{mod}\ N)}{N}\tau + \frac{a\ (\mathrm{mod}\ N)}{N}) \xrightarrow{e^{2\pi i}} (\mathbb{C}^*/q^{\mathbb{Z}}, \zeta_N^a q^{-b/N}),$$

where $\zeta_N = e^{2\pi i/N}$.

Let us recall briefly some properties of the Tate curve (it is $\mathbb{G}_m/q^{\mathbb{Z}}$):

- The Tate curve $\mathrm{Tate}(q)_{\mathbb{Z}((q))}$ is an elliptic curve over $\mathbb{Z}((q))$.
- $\underline{\omega}^{\otimes k}_{\mathrm{Tate}(q)_{\mathbb{Z}((q))}/\mathbb{Z}((q))}(\mathbb{Z}((q))) = \mathbb{Z}((q))(\frac{dt}{t})^{\otimes k}$.
- The N-torsion group of $\mathrm{Tate}(q)_{\mathbb{Z}((q))[q^{1/N},\zeta_N]}$ is given by $\zeta_N^a q^{b/N}$ for all pairs a, b, which generate $\mathbb{Z}/N$.

Now we show that the Tate curve $\mathrm{Tate}(q)_{\mathbb{C}((q))[q^{1/N}]}$ provides us with a q-expansion. We use that its $\mathbb{C}$-points are precisely the elliptic curves of the form $\mathbb{C}^*/q^{\mathbb{Z}}$. We look at the big cartesian diagram

$$\begin{tikzcd}
(E_\tau, \frac{-b \pmod N}{N}\tau + \frac{a \pmod N}{N}) \arrow[r, "e^{2\pi i}", "\sim"'] \arrow[d] \arrow[dr, phantom, "\square"] & (\mathbb{C}^*/q^{\mathbb{Z}}, \zeta_N^a q^{-b/N}) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & (\mathrm{Tate}(q)_{\mathbb{C}((q))[q^{1/N}]}, \zeta_N^a q^{-b/N}) \arrow[d] \\
\mathrm{Spec}(\mathbb{C}) \arrow[r, equal] & \mathrm{Spec}(\mathbb{C}) \arrow[r] & \mathrm{Spec}(\mathbb{C}((q))[q^{1/N}]).
\end{tikzcd}$$

We note that the left column describes $f|_k(\sigma)(\tau)$. We use that $\underline{\omega}^{\otimes k}_{\mathrm{Tate}(q)_{\mathbb{C}((q))[q^{1/N}]}/\mathbb{C}((q))[q^{1/N}]}(\mathbb{C}((q))[q^{1/N}])$ is of the form $\mathbb{C}((q))[q^{1/N}](\frac{dt}{t})^{\otimes k}$, whence

$$f|_k(\sigma)(\tau)(ds)^{\otimes k} = g(q^{1/N})(\frac{dt}{t})^{\otimes k},$$

where g is a Laurent series in q. $f|_k(\sigma)$ is also classically expressed in a q-expansion, as we have seen. These two q-expansions coincide because they both describe the same holomorphic function on a pointed disc. Now it is clear, how one should define q-expansions for Katz M-forms also when the ring is not $\mathbb{C}$.

The q expansion at the cusp $\sigma\infty$ of a Katz M-form F of weight k for the group $\Gamma_1(N)$ over a $\mathbb{Z}[1/N]$-algebra R is defined as the Laurent series $g \in R[\zeta_N]((q^{1/N}))$ such that

$$F(\mathrm{Tate}(q)_{R((q))[q^{1/N},\zeta_N]}/R((q))[q^{1/N},\zeta_N]/R, \zeta_N^a q^{-b/N}) = g(q^{1/N})(\frac{dt}{t})^{\otimes k}.$$

We point out that for the cusp ∞ we have that $h = 1$, and hence the q-expansion is in the variable q (instead of $q^{1/N}$). At the cusp 0 one finds $h = N$, so $q^{1/N}$ is really needed (in general), but on the other hand the adjoining of a primitive N-th root of unity is not.

Definition 1.7.1 A Katz M-form F of weight k for the group $\Gamma_1(N)$ over a $\mathbb{Z}[1/N]$-algebra R is called a

- *Katz modular form* (an element of $\mathcal{M}_k(\Gamma_1(N), R)$) if the q-expansions are power series at all cusps, resp. a

- *Katz cusp form* (an element of $\mathcal{S}_k(\Gamma_1(N), R)$) if the q-expansions are power series without constant term at all cusps.

If $R = \mathbb{C}$, we can conclude from what we developped above that the Katz modular forms are precisely the classical ones.

1.8 First properties of Katz modular forms

- Let $R' \to R$ be a flat ring homomorphism and $(E/S/R, \phi)$ and elliptic curve with a level structure. Denote by $(E'/S'/R', \phi')$ the curve obtained by base change. Since exactness is preserved, one finds

  $$\mathcal{M}_k(\Gamma_1(N), R') \otimes_{R'} R \cong \mathcal{M}_k(\Gamma_1(N), R)$$

  and the same for the space of Katz cusp forms. For a general $R'' \to R$ one still has a homomorphism of R-algebras.

- Let now $R = k$ be a field. Then the space of Katz modular forms is a k-vector space of finite dimension. One can actually calculate this dimension using Riemann-Roch, if one consideres the compactified moduli space.

- Let A be a subring of $\mathbb{C}$, in which N is invertible, and f a classical modular form for $\Gamma_1(N)$ of weight k, the coefficients of the standard q-expansion of which are all in A. Then f is also a Katz modular form for the ring A of weight k for $\Gamma_1(N)$.

- There are no Katz modular forms of negative weight.

2 Calculating characteristic p Katz modular forms of weight 1, after Bas Edixhoven

This talk was given in two parts on 15 and 22 January 2003.

The aim of this talk is to present a theorem by Bas Edixhoven ([E]), which describes the space of cuspidal Katz modular forms of weight 1 with a given character over a finite field just in terms of the Hecke algebra of classical modular forms (over the complex numbers, for the group $\Gamma_1(N)$, without a character). Moreover, effective bounds on the number of Hecke operators needed are given. Using standard software tools, the calculations can be performed using only linear algebra methods.

We shall also present a variant of the theorem (valid in certain cases) for the calculation of cuspidal Katz modular forms of weight 1 with trivial character, where one uses the classical Hecke algebra for modular forms for $\Gamma_0(N)$.

Along the way we introduce Hecke operators, parabolic cohomology and also a way to calculate classical modular forms of weight $k \geq 2$.

2.1 Different definitions of Katz modular forms and comparison with the classical theory

In the introduction to the first talk I warned the reader that our definition of Katz forms might differ from Katz' original one. Since we need to work with different notions of modular forms, we present them in this section and also give relations between them.

Let us fix a $\mathbb{Z}[1/N]$-algebra R, where $N \geq 5$ is an integer (most works for arbitrary N). Katz worked in [K] in the more general setting of the category of elliptic curves with a full level N-structure, i.e. a fixed isomorphism of group schemes

$$\alpha : (\mathbb{Z}/N)_S^2 \cong E[N].$$

This is a more general case of our situation, where we consider the category $[\Gamma_1(N)]_R$ of elliptic curves $E/S/R$ together with embeddings of group schemes

$$\beta : (\mathbb{Z}/N)_S \hookrightarrow E[N],$$

which correspond to fixing an N-torsion point (i.e. the image of 1 in $E[N]$). The Katz modular forms (resp. cusp forms) will, as previously, be denoted by $\mathcal{M}_k(\Gamma_1(N), R)$ (resp. $\mathcal{S}_k(\Gamma_1(N), R)$).

In Gross' article [G] a different notion is presented. Namely, he considers the category $[\Gamma_1(N)]'_R$ of elliptic curves $E/S/R$ as before, but now with an embedding of group schemes

$$\gamma : (\mu_N)_S \hookrightarrow E[N].$$

The theory of modular forms can be developped precisely as we presented it in the first talk. The (Katz) modular forms (resp. cusp forms) obtained in this setting will be denoted by $\mathcal{M}_k(\Gamma_1(N), R)'$ (resp. $\mathcal{S}_k(\Gamma_1(N), R)'$).

The advantage of the new setting is that one does not need to adjoin a primitive N-th root of unity to the ring in order to obtain the q-expansion at infinity. In the previously developped setting this becomes necessary just because we want to evaluate a modular form at the Tate curve $\mathbb{G}_{m,R}/q^{\mathbb{Z}}$ together with the torsion point ζ_N (see the remark below, why we need to choose precisely that one). The $[\Gamma_1(N)]'_R$-setting is hence an elegant way to avoid this trouble! And it is clear that the two settings coincide if R contains the N-th roots of unity.

Let us now compare the two settings by quoting the (also for the sequel) very important

Theorem 2.1.1 *Let S be an R-algebra with R an $\mathbb{Z}[1/N]$-algebra for some integer $N \geq 5$. Let $k \in \mathbb{N}$ and suppose one of the following holds:*

(i) $k \geq 2$

(ii) $R \to S$ *is flat.*

Then the following natural maps are isomorphisms:

$$\begin{aligned} \mathcal{M}_k(\Gamma_1(N), R) \otimes_R S &\cong \mathcal{M}_k(\Gamma_1(N), S), \\ \mathcal{M}_k(\Gamma_1(N), R)' \otimes_R S &\cong \mathcal{M}_k(\Gamma_1(N), S)', \\ \mathcal{S}_k(\Gamma_1(N), R) \otimes_R S &\cong \mathcal{S}_k(\Gamma_1(N), S) \quad \textit{and} \\ \mathcal{S}_k(\Gamma_1(N), R)' \otimes_R S &\cong \mathcal{S}_k(\Gamma_1(N), S)'. \end{aligned}$$

Proof. For the "undashed" version we refer to [DI], Theorem 12.3.2, and for the other one to [G], Proposition 2.5, for $k \geq 2$. The flat case works for both settings in the same way. □

From this we can conclude the

Proposition 2.1.2 *The Hecke and diamond operators T_n and $< a >$ for $n \in \mathbb{N}$ and $a \in (\mathbb{Z}/N)^*$ generate the same ring of endomorphisms $\mathbb{T}$ in $\mathcal{S}_k(\Gamma_1(N), \mathbb{Z}[1/N])$ and $\mathcal{S}_k(\Gamma_1(N), \mathbb{Z}[1/N])'$, and these two $\mathbb{T}$-modules are isomorphic.*

Proof. Edixhoven proves this proposition in [E] (Proposition 4.11) without reference to the above theorem. Here we give a different proof.

Both spaces are free $\mathbb{Z}[1/N]$-modules. Since $\mathbb{Z}[1/N] \hookrightarrow \mathbb{Z}[1/N, \zeta_N]$ is flat, it follows from the theorem and the remarks preceding it that

$$\begin{aligned} &\mathcal{S}_k(\Gamma_1(N), \mathbb{Z}[1/N]) \otimes \mathbb{Z}[1/N, \zeta_N] \cong \mathcal{S}_k(\Gamma_1(N), \mathbb{Z}[1/N, \zeta_N]) \\ = &\mathcal{S}_k(\Gamma_1(N), \mathbb{Z}[1/N, \zeta_N])' \cong \mathcal{S}_k(\Gamma_1(N), \mathbb{Z}[1/N])' \otimes \mathbb{Z}[1/N, \zeta_N]. \end{aligned}$$

This isomorphism gives rise to an isomorphism (by conjugation)

$$\phi : \mathrm{End}_{\mathbb{Z}[1/N,\zeta_N]}(\mathcal{S}_k(\Gamma_1(N), \mathbb{Z}[1/N, \zeta_N])) \cong \mathrm{End}_{\mathbb{Z}[1/N,\zeta_N]}(\mathcal{S}_k(\Gamma_1(N), \mathbb{Z}[1/N, \zeta_N])'),$$

under which the T_n and $< a >$ correspond on both sides. This implies the assertion. □

In the previous talk/section we have seen that the classical space of modular forms coincides with the Katz space over $\mathbb{C}$:

$$\mathcal{M}_k(\Gamma_1(N), \mathbb{C}) \cong M_k(\Gamma_1(N), \mathbb{C}).$$

It is customary to define the classical subspace of modular forms of weight k with coefficients in $\mathbb{Z}[1/N]$ as

$$M_k(\Gamma_1(N), \mathbb{Z}[1/N]) = \{\ f \in M_k(\Gamma_1(N), \mathbb{C}) \mid q-\text{expansion at } \infty \text{ has coefficients in } \mathbb{Z}[1/N]\ \}.$$

Furthermore, one sets

$$M_k(\Gamma_1(N), A) = M_k(\Gamma_1(N), \mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} A$$

for any $\mathbb{Z}[1/N]$-algebra A. We now use that our q-expansion coincides with the classical one in both cases (over $\mathbb{C}$). As we have pointed out, in $[\Gamma_1(N)]'_R$ (with $R = \mathbb{Z}[1/N]$) the coefficients of the q-expansions are in $\mathbb{Z}[1/N]$. From this we immediately obtain for all k:

$$M_k(\Gamma_1(N), \mathbb{Z}[1/N]) = \mathcal{M}_k(\Gamma_1(N), \mathbb{Z}[1/N])'.$$

For $k \geq 2$ the theorem above implies by comparison with the Katz theory that

$$M_k(\Gamma_1(N), \mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} \mathbb{C} = M_k(\Gamma_1(N), \mathbb{C}),$$

which is a weak version of the theorem by Shimura (I think) that says that the classical space of modular forms (i.e. over $\mathbb{C}$) has a basis of forms with Fourier coefficients in $\mathbb{Z}$.

Remark 2.1.3 The natural isomorphism

$$\mathbb{C}/\mathbb{Z}\sigma\tau + \mathbb{Z} \xrightarrow{\cdot(c\tau+d)} \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$$

for a matrix $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)(\mathbb{Z})$ fixes precisely the N-torsion points $\frac{r}{N}$ for $r \in (\mathbb{Z}/N)^*$ (as an immediate calculation shows).

So the only possible correspondences between Katz forms (in both settings) and classical modular forms over $\mathbb{C}$ are given by

$$F(\mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}, \frac{r}{N}) = f(\tau)(ds)^k,$$

where ds is a basis of the $\mathbb{C}$-vector space of global sections of $\underline{\omega}^{\otimes k}_{\mathbb{C}/\mathbb{Z}\tau+\mathbb{Z}}$. These correspondences differ precisely by the diamond operators.

In other words, if one wants the Katz forms to coincide with the classical forms, one has to choose any of the N-torsion points r/N and not $r\tau/N$.

Remark 2.1.4 A different approach to solving the trouble of having to adjoin a primitive N-th root of unity in order to obtain a q-expansion (by the above remark one does not have the choice of an essentially different torsion point) could be to consider q-expansions at the cusp 0. Then an easy calculation shows that one gets an expansion in the variable $q^{1/N}$ instead of q, not involving N-th roots of unity. The Hecke operators do, however, not fix the cusp 0. That means that the q-expansion of the transformed function involves q-expansions at some other cusps. At those cusps the adjoining of an N-th root of unity is also not necessary.

The elegant solution to use $[\Gamma_1(N)]'_R$ presented in Gross' paper seems preferable.

2.2 Parabolic cohomology

In the case of classical modular forms of weight $k \geq 2$ for $\Gamma_1(N)$ with $N \geq 5$, one can describe the Hecke algebra by an action on a faithful module that is completely described in terms of group cohomology.

More precisely, one can identify (via an isomorphism of $\mathbb{C}$-vector spaces) the space $S_k(\Gamma_1(N), \mathbb{C}) \oplus \overline{S_k(\Gamma_1(N), \mathbb{C})}$ with the vector space $H^1_{\text{par}}(\Gamma_1(N), M_k(\mathbb{C}))$, where $M_k(\mathbb{C}) = \text{Sym}^{k-2}(\mathbb{C} \times \mathbb{C})$. This vector space has a natural $\mathbb{Z}$-lattice, namely $H^1_{\text{par}}(\Gamma_1(N), M_k(\mathbb{Z}))$. As we will see in the next section, one gets a natural action of Hecke operators on this space. Since the isomorphisms, which we will explain here below, respect the Hecke action, we obtain a faithful Hecke module (in simple terms!), which allows us to calculate the Hecke algebra (for classical modular forms). See also the propositions in the section on calculating classical modular forms.

2.3 Operators on modular forms

We describe a general setting, which allows us to treat Hecke and diamond operators at the same time.

Let $\alpha \in \text{GL}_2(\mathbb{Q})^+$ and set for abbreviation $\Gamma := \Gamma_1(N)$, where we again impose that N be greater equal 5. Then the groups

$$\Gamma_\alpha := \alpha^{-1}\Gamma\alpha \cap \Gamma \quad \text{and} \quad \Gamma^\alpha := \alpha\Gamma\alpha^{-1} \cap \Gamma$$

have finite index in Γ. We consider the commutative diagram

$$\begin{tikzcd}
\Gamma_\alpha\backslash\mathbb{H} \arrow[r, "\alpha", "\sim"'] \arrow[d, "\pi"] & \Gamma^\alpha\backslash\mathbb{H} \arrow[d, "\pi"] \\
\Gamma\backslash\mathbb{H} & \Gamma\backslash\mathbb{H},
\end{tikzcd}$$

where π denotes the natural projections. For the covering groups we obtain (recall the assumption $N \geq 5$) the commutative diagram

$$\begin{tikzcd}
\Gamma_\alpha \arrow[r, "\gamma\mapsto\alpha\gamma\alpha^{-1}", "\sim"'] \arrow[d, hook, "\iota"] & \Gamma^\alpha \arrow[d, hook, "\iota"] \\
\Gamma & \Gamma,
\end{tikzcd}$$

where ι denotes the natural inclusions.

We can now define operators T_α on modular forms and compatibly on group cohomology.

(i) For a modular form F (over $\mathbb{C}$) set

$$(T_\alpha F)(\tau) = (\det(\alpha)^{-1}) \sum_{x\in(\pi\alpha)^{-1}(\tau)} F(\pi(x)).$$

It has to be checked (in fact it is obvious on the q-expansions as we will see) that a modular form is transformed into a modular form and a cusp form into a cusp form.

(ii) On the group cohomology we define the homomorphism T_α by the commutative diagram:

$$\begin{tikzcd}
H^1(\Gamma_\alpha, M) \arrow[r, "\text{conj. by }\alpha", "\sim"'] \arrow[d, "\text{cores}"] & H^1(\Gamma^\alpha, M) \\
H^1(\Gamma, M) & H^1(\Gamma, M), \arrow[l, "T_\alpha"'] \arrow[u, "\text{res}"']
\end{tikzcd}$$

where M is a Γ-module. One should also calculate at this point that the morphism T_α fixes the parabolic subspace, and that the isomorphism of the preceding chapter between parabolic cohomology (over $\mathbb{C}$) and the space of holomorphic and antiholomorphic cusp forms respects the operators T_α.

Now we apply this abstract situation to two cases, in both of which we will give an equivalent description on the moduli spaces, which allows us to extend the operators in a natural way to Katz modular forms.

Diamond operators:

Let a be an integer coprime to N. Then there exists a matrix $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. As $\Gamma_1(N)$ is a normal subgroup of $\Gamma_1(N)$ the groups Γ_α and Γ^α are equal to Γ and the maps π are the identity. The operator corresponding to α is called the *diamond operator* and denoted $< a >$. It will become apparent that it indeed only depends on a and not on the choice of α.

Under α, the elliptic curve with given torsion point $(\mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}, 1/N)$ is mapped to $(\mathbb{C}/\mathbb{Z}\alpha\tau + \mathbb{Z}, 1/N)$, which is isomorphic to $(\mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}, a/N)$.

This suggests the extension of the definition of the diamond operator to Katz modular forms as follows:

$$\begin{aligned} < a >: \mathcal{M}_k(\Gamma_1(N), R) \to \mathcal{M}_k(\Gamma_1(N), R) \quad & \text{such that} \\ (< a > F)(E/S/R, P) = F(E/S/R, aP). & \end{aligned}$$

If we are working with embeddings $\mu_N \hookrightarrow E[N]$ instead of torsion points, we must, of course, just compose with the a-th power map $\mu_N \to \mu_N$.

In all cases, one thus gets an action of the group $(\mathbb{Z}/N)^* \cong \Gamma_0(N)/\Gamma_1(N)$ on the space of modular forms (cusp forms). Let $\epsilon : (\mathbb{Z}/N)^* \to R^*$ be a character. Then we set

$$\mathcal{M}_k(\Gamma_1(N), \epsilon, R) = \{ f \in \mathcal{M}_k(\Gamma_1(N), R) \mid < a > f = \epsilon(a) f \ \forall a \in (\mathbb{Z}/N)^* \}$$

and for the other spaces in question similarly.

If $R = K$ is a field of characteristic not 2, one finds by considering $< -1 >$ that there are no non-trivial (Katz) modular forms if $\epsilon(-1) \neq (-1)^k$.

Furthermore, one finds

$$\mathcal{M}_k(\Gamma_1(N), 1, R) = \mathcal{M}_k(\Gamma_0(N), R).$$

In fact, I have not defined the space on the right (although a definition suggests itself), so we can also work with this as a definition.

Hecke operators:

For simplicity, we give the definition of Hecke operators only for primes l and define the operators for composite numbers by the formulae that one usually obtains by calculation.

So let l be a prime. The l-th Hecke operator T_l is defined by the matrix $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}$. We must point out that we divide by l in the definition of the operator. As we will see on q-expansions, the factor $1/l$ vanishes from the description. So one must take the action on the

q-expansion as a definition in case of characteristic l. This requires some additional work, that we do not perform here (in fact we shall just overlook this problem). The reader is referred to [G], proposition 4.1.

Straightforward calculations yield (whether l divides N or not)

$$\Gamma_\alpha = \Gamma_1(N) \cap \Gamma_0(l) \text{ and } \Gamma^\alpha = \Gamma_1(N) \cap (\Gamma_0(l))^T,$$

where the superscript T stands for transpose. By identifying $\tau \mapsto (\mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}, 1/N, < \tau/l >)$, one gets a one-to-one correspondence between $\Gamma^\alpha \backslash \mathbb{H}$ and triples (E, P, H), where E is an elliptic curve with N-torsion point P and $H \leq E$ a (cyclic) subgroup of order l that does not contain the point P. For Γ_α one can proceed similarly (the third component must be replaced by $< 1/l >$). Direct inspection shows that on the moduli spaces the map α corresponds to

$$(E, P, H) \mapsto (E/H, P \bmod H, E[l]/H).$$

Of course, the maps π just mean dropping the third component.

Now it should be obvious how to extend the definition of T_l to Katz modular forms (in both settings, since the embedding of μ_N is not affected), namely by setting

$$T_l : \mathcal{M}_k(\Gamma_1(N), R) \to \mathcal{M}_k(\Gamma_1(N), R) \quad \text{such that}$$
$$(T_l F)(E/S/R, P) = \sum_H F((E/H)/S/R, P \bmod H),$$

where the sum runs over all (cyclic) subgroups H of E of order l, which do not contain the point P.

The Hecke operators T_n with n composite are defined by the formulae:

(i) $T_{l^{r+1}} = T_l \circ T_{l^r} - l^{k-1} < l > \circ T_{l^{r-1}}$ if $l \nmid N$,

(ii) $T_{l^{r+1}} = T_l \circ T_{l^r}$ if $l \mid N$ and

(iii) $T_{nm} = T_n \circ T_m$ if n and m are coprime.

It is easy to determine all order l subgroups H of the Tate curve. Consequently, a simple calculation yields the formula for the action of the Hecke operator on the q-expansions. Here I just give the result (for $l \nmid N$, otherwise the second summand must be dropped):

$$a_n(T_l f) = a_{ln}(f) + l^{k-1} a_{n/l}(< l > f),$$

where $a_{n/l}$ has to be interpreted as 0 if $l \nmid n$. From this one also obtains the for the sequel very important formula

$$a_1(T_n f) = a_n(f).$$

2.4 Calculation of classical modular forms of weight $k \geq 2$ from the Hecke algebra

In this section we present a well known method for calculating a basis of eigenforms for the Hecke algebra (in the classical setting). We shall restrict to the case $k \geq 2$ in all of this section because of the practical fact that using parabolic cohomology (resp. modular symbols) only gives the Hecke algebra in this case. As far as we have developped the theory here, we can also not conclude (at least I do not know how) that there is also a $\mathbb{Z}[1/N]$-basis in weight 1. It should, however, be possible to prove that by extending theorem 2.1.1 to include $k = 1$ for rings contained in $\overline{\mathbb{Q}}$.

In the sequel of this section we commit a slight inconsistency with the previous and the following settings: we shall use $\mathbb{Z}$ instead of $\mathbb{Z}[1/N]$ in several places. This is justified since we do not treat Katz modular forms here. See also the discussion of classical modular forms in the beginning of this talk/chapter.

Definition 2.4.1 By the *Hecke algebra* of weight k for the group $\Gamma_1(N)$ (for classical modular forms) we understand the subring $\mathbb{T} < \mathrm{End}_{\mathbb{C}}(S_k(\Gamma_1(N), \mathbb{C}))$ generated by the operators T_n $n \in \mathbb{N}$.

Proposition 2.4.2 *Under the isomorphism between cusp forms and parabolic cohomology*

$$H^1_{\mathit{par}}(\Gamma_1(N), M_k(\mathbb{Z})) \otimes \mathbb{C} \cong S_k(\Gamma_1(N), \mathbb{C}) \oplus \overline{S_k(\Gamma_1(N), \mathbb{C})},$$

the Hecke operators T_n on parabolic cohomology corresponds to the operator $T_n \oplus \overline{T_n}$. Moreover, the Hecke algebra $\mathbb{T}$ generated by the T_n as a subring of $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_1(N), \mathbb{C}))$ is isomorphic with the algebra generated by the T_n as a subring of $\mathrm{End}_{\mathbb{C}}(H^1_{\mathit{par}}(\Gamma_1(N), M_k(\mathbb{Z})) \otimes \mathbb{C})$.

Proof. The second statement is an immediate consequence of the first, which one has to check. □

Proposition 2.4.3 *Let Γ be any subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index. There is a free $\mathbb{Z}$-module $\mathit{CMS}_k(\Gamma)$, called the space of* cuspidal modular symbols, *together with an isomorphism*

$$\mathit{CMS}_k(\Gamma) \otimes \mathbb{C} \cong S_k(\Gamma, \mathbb{C}) \oplus \overline{S_k(\Gamma, \mathbb{C})}.$$

One can define Hecke operators T_n on $\mathit{CMS}_k(\Gamma)$, which correspond to $T_n \oplus \overline{T_n}$ via the isomorphism. Moreover, the Hecke algebra $\mathbb{T}$ generated by the T_n as a subring of $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma, \mathbb{C}))$ is isomorphic with the algebra generated by the T_n as a subring of $\mathrm{End}_{\mathbb{C}}(\mathit{CMS}_k(\Gamma) \otimes \mathbb{C})$.

Proof. That is proved in [M]. □

Proposition 2.4.4 *Let A be an abelian group. Then we have:*

(a) $\mathbb{T}$ *contains all operators* $< a >$ *for* $a \in (\mathbb{Z}/N)^*$.

(b) $\mathbb{T}$ *is generated by the* T_n *as an abelian group (not only as a ring).*

(c) $\mathbb{T}$ *is commutative.*

(d) There is a natural isomorphism $S_k(\Gamma_1(N), A) \rightarrow \mathrm{Hom}_{A-lin}(\mathbb{T} \otimes A, A)$ *given by* $f \mapsto (T \mapsto a_1(Tf))$.

Proof. (a) Let l_1 and l_2 be two distinct primes such that $l_i \equiv a(N)$. The result is immediate from the formula

$$l_i^{k-1} < a >= T_{l_i}^2 - T_{l_i^2}.$$

(b,c) These are immediate consequences of the formulae defining Hecke operators T_n for composite n.
(d) A good way to rephrase the statement over a field, say $\mathbb{C}$, is to say that

$$<,>: \mathbb{T} \times S_k(\Gamma_1(N), \mathbb{C}) \to \mathbb{C}, \quad < T, f >:= a_1(Tf)$$

is a perfect pairing. This follows from the formula $a_1(T_n f) = a_n(f)$ as follows. If for all n we have $0 = a_1(T_n f) = a_n(f)$, then $f = 0$ by the uniqueness of the q-expansion. Conversely, if $a_1(Tf) = 0$ for all f, then $a_1(T(T_n f)) = a_1(T_n T f) = a_n(Tf) = 0$ for all f and all n. As $S_k(\Gamma_1(N), \mathbb{C})$ is by definition a faithful $\mathbb{T}$-module, we find $T = 0$, proving the perfectness.

Having established the result over $\mathbb{C}$, the statement with $A = \mathbb{Z}$ is just the definition of $S_k(\Gamma_1(N), \mathbb{Z})$ as the subspace of forms with Fourier coefficients in $\mathbb{Z}$. The general result follows by tensoring with A. We also note that $\mathbb{T}$ does not have any torsion, since we defined it as a subset of a vector space in characteristic 0. $\square$

Remark 2.4.5 Let K be a perfect field (of characteristic not dividing N). Then the freeness of $\mathbb{T}$ implies (by the proposition above)

$$\begin{aligned} S_k(\Gamma_1(N), \overline{K}) &= \mathrm{Hom}_{\overline{K}-lin}(\mathbb{T} \otimes \overline{K}, \overline{K}) \\ &= \mathrm{Hom}_{K-lin}(\mathbb{T} \otimes K, \overline{K}). \end{aligned}$$

In words: The q-expansions of cusp forms with coefficients in $\overline{K}$ are precisely the K-linear maps $\mathbb{T} \otimes K \to \overline{K}$.

Remark 2.4.6 Let us consider more generally $\mathbb{T}$ just as a finite dimensional (i.e. Artinian) commutative K-algebra over a perfect field K.

By a *system of eigenvalues* of a $\mathbb{T}$-module M we understand a map $\lambda : \mathbb{T} \to K$ such that there exists an element $0 \neq m \in M$ satisfying $T.m = \lambda(T)m$ for all $T \in \mathbb{T}$.

In particular, let us consider the $\mathbb{T}$-module

$$S := \mathrm{Hom}_{K-lin}(\mathbb{T}, \overline{K}),$$

for the action $(T.f)(\tilde{T}) = f(T\tilde{T})$. It is in fact a faithful $\mathbb{T}$-module because $(T.f)(1) = f(T) = 0$ for all f implies that $T = 0$.

Given a system of eigenvalues λ, an element $f \in S$ is by definition a *normalised eigenform* for λ if

(i) $(T.f)(\tilde{T}) = f(T\tilde{T}) = \lambda(T)f(\tilde{T})$, which implies $(T.f)(1) = \lambda(T)f(1)$, and

(ii) $f(1) = 1$.

This is immediately seen to be equivalent to f being a K-algebra homomorphism (and necessarily also λ).

Furthermore, we have

$$\begin{aligned}|\mathrm{Hom}_{K-alg}(\mathbb{T}, \overline{K})| &= |\mathrm{Hom}_{\overline{K}-alg}(\mathbb{T} \otimes \overline{K}, \overline{K})| \\ &\leq \dim_{\overline{K}}(\mathbb{T} \otimes \overline{K}) = \dim_K(\mathbb{T}) = \dim_{\overline{K}}(\mathrm{Hom}_{K-lin}(\mathbb{T}, \overline{K})).\end{aligned}$$

One has equality for square-free N in characteristic 0. In that case we can hence conclude that S has a $\overline{K}$-basis consisting of eigenforms (with image in a finite extension of K because of the finite dimensionality of $\mathbb{T}$).

Moreover, we have a left $G_K = G(\overline{K}|K)$-action S via

$$\sigma.f = \sigma \circ f.$$

Remark 2.4.7 We now apply the above remark to the Hecke algebra $\mathbb{T}$. A system of eigenvalues λ (with normalised eigenform f) is then uniquely determined by $\lambda(T_n)$. This value is, however, by the proposition precisely the n-th Fourier coefficient of f. Thus, calculating Fourier coefficients just means calculating eigenvalues of the Hecke operators. Those, however, are provided as matrices via the desciption of parabolic cohomology resp. modular symbols.

We also remark that the G_K-action is just applying the Galois automorphism to the Fourier coefficients.

There remains the problem of keeping apart the different systems of eigenvalues. This is solved by the following proposition.

Proposition 2.4.8 *In the setting of remark 2.4.6 there is a bijection*

$$\mathrm{Hom}_{K-alg}(\mathbb{T}, \overline{K})/_{G_K-\text{conjugacy}} \quad \leftrightarrow \quad \textit{maximal ideals of } \mathbb{T},$$

given by sending a K-algebra homomorphism $f : \mathbb{T} \to \overline{K}$ to its kernel.

Proof. We point out that in an Artinian algebra every prime ideal is maximal. Since for every maximal ideal $\mathfrak{m}$ the ring $\mathbb{T}/\mathfrak{m}$ is contained (via f) in $\overline{K}$ the kernel is a maximal ideal. If $g = \sigma \circ f$ for some field automorphism σ, the kernel of f is, of course, equal to the kernel of g. Hence the allocation is well defined.

The surjectivity is clear: given $\mathfrak{m}$, just take $f : \mathbb{T} \to \mathbb{T}/\mathfrak{m} \leq \overline{K}$.

Suppose now that f and g have the same kernel $\mathfrak{m}$. That precisely means that f and g give two embeddings of the field $\mathbb{T}/\mathfrak{m}$ into $\overline{K}$. By well known field theory, one can be obtained from the other by composing with an element of G_K, which proves the injectivity. □

Remark 2.4.9 By the proposition one can localize $\mathbb{T}$ at its maximal ideals in order to keep exactly one particular system of eigenvalues modulo G_K-conjugacy. Linear algebra techniques (calculation of characteristic polynomials) then directly produce the Fourier coefficients of one eigenform. It is not difficult to calculate its (finite) G_K-orbit.

2.5 Calculation of Katz modular forms of weight 1 over finite fields

In this section we present Edixhoven's results ([E], section 4) on how to calculate Katz modular forms (in the "dashed" setting as presented in [G]) of weight 1 over finite fields.

Let us, for this section, fix a prime p, a finite extension $\mathbb{F}$ of $\mathbb{F}_p$, a character $\epsilon : (\mathbb{Z}/N)^* \to \mathbb{F}^*$ and an integer $N \geq 5$ coprime to p.

The result to be presented is based on the following homomorphisms of spaces of Katz modular forms.

(i) <u>The Frobenius F:</u> The homomorphism

$$F : \mathcal{S}_1(\Gamma_1(N), \mathbb{F}_p)' \to \mathcal{S}_p(\Gamma_1(N), \mathbb{F}_p)'$$

is defined by sending f to f^p, meaning the following: If $f(E/S, \alpha) \in \underline{\omega}_{E/S}(S)$, then $f^p(E/S, \alpha) = (f(E/S, \alpha))^{\otimes p} \in \underline{\omega}_{E/S}^{\otimes p}(S)$. For the action of F on q-expansions at infinity, one immediately finds:

$$a_n(F(f)) = a_{n/p}^p(f) = a_{n/p}(f),$$

where we have made use of working over $\mathbb{F}_p$ for the last equality (here one needs the modified definition of Katz modular forms). As before, the coefficient $a_{n/p}(f)$ has to be interpreted as 0 if $p \nmid n$.

Let us observe the compatibility of F with diamond operators:

$$F\circ < a >=< a > \circ F.$$

As $\mathbb{F}$ is flat over $\mathbb{F}_p$ we can extend F to forms over $\mathbb{F}$ with the same action on q-expansions. The compatibility with the diamond operators hence gives rise to the homomorphism (also denoted by F)

$$F : \mathcal{S}_1(\Gamma_1(N), \epsilon, \mathbb{F})' \to \mathcal{S}_p(\Gamma_1(N), \epsilon, \mathbb{F})',$$

which on q-expansions is also given by $a_n(F(f)) = a_{n/p}(f)$.

(ii) The Hasse invariant A: The Hasse invariant A is a Katz modular form for $\mathrm{SL}_2(\mathbb{Z})$ of weight $p-1$, which is defined over $\mathbb{F}_p$ and hence also over $\mathbb{F}$ (see e.g. [K], section 2.0). All the q-expansions of A are identically 1.

Also by the letter A we shall denote the multiplication by A map:

$$A : \mathcal{S}_1(\Gamma_1(N), \epsilon, \mathbb{F})' \to \mathcal{S}_p(\Gamma_1(N), \epsilon, \mathbb{F})', f \mapsto Af,$$

in the sense $(Af)(E/S, P) = A(E/S, P)\otimes f(E, P) \in \underline{\omega}_{E/S}^{\otimes p-1} \otimes \underline{\omega}_{E/S}$. That this map is well defined comes from the fact that A is a modular form for $\mathrm{SL}_2(\mathbb{Z})$ and hence in particular for $\Gamma_0(N)$, so that the character remains fixed.

Since A has all q-expansions identically 1, we see

$$a_n(A(f)) = a_n(f).$$

(iii) The derivation θ: In [K2] Katz constructs a homomorphism

$$\theta : \mathcal{S}_p(\Gamma_1(N), \epsilon, \mathbb{F})' \to \mathcal{S}_{p+2}(\Gamma_1(N), \epsilon, \mathbb{F})',$$

the effect of which on the q-expansions is given by

$$a_n(\theta(f)) = na_n(f),$$

i.e. it acts like the logarithmic derivative $q\frac{d}{dq}$, whence the name.

Lemma 2.5.1 *(a) The homomorphsims A and F are injective.*

(b) We have the commutative diagram

$$\begin{tikzcd}
\mathcal{S}_1(\Gamma_1(N),\epsilon,\mathbb{F})' \arrow[r, hook, "F"] \arrow[dr, hook, "A"'] & \mathcal{S}_p(\Gamma_1(N),\epsilon,\mathbb{F})' \arrow[d, "T_p"] \\
& \mathcal{S}_p(\Gamma_1(N),\epsilon,\mathbb{F})'.
\end{tikzcd}$$

(c) $F \circ T_l^{(1)} = T_l^{(p)} \circ F$ *if* $l \neq p$ *is a prime.*

(d) $A \circ T_p^{(1)} = T_p^{(p)} \circ A + \epsilon(p) \circ F$.

Proof. All statements are immediately verified on the q-expansions using the formulae presented. $\square$

Proposition 2.5.2 *There is the exact sequence of* $\mathbb{F}$*-vector spaces*

$$0 \to \mathcal{S}_1(\Gamma_1(N),\epsilon,\mathbb{F})' \xrightarrow{F} \mathcal{S}_p(\Gamma_1(N),\epsilon,\mathbb{F})' \xrightarrow{\theta} \mathcal{S}_{p+2}(\Gamma_1(N),\epsilon,\mathbb{F})'.$$

Moreover, the kernel of θ*, hence also the image of* F*, is explicitly given by*

$$\{\ f \in \mathcal{S}_p(\Gamma_1(N),\epsilon,\mathbb{F})' \mid a_n(f) = 0\ \forall n \text{ s.t. } p \nmid n\ \}.$$

Proof. An element f in the kernel of θ is characterised by $na_n(f) = 0$ for all n. As the characteristic is p, this is equivalent to $a_n(f) = 0$ for all n such that $p \nmid n$. Hence, the kernel of θ is indeed equal to the set in the assertion.

On the q-expansions the formula $a_n(F(f)) = a_{n/p}(f)$ makes it obvious that the image of F is contained in the kernel of θ.

The other inclusion is more difficult and is proved in [K2]. Bas Edixhoven, however, also explained to me a more direct argument. $\square$

Proposition 2.5.3 *Let* K *be a perfect field. A modular form* $f \in \mathcal{S}_k(\Gamma_1(N),\epsilon,K)'$ *is uniquely determined by the first* Bk *coefficients of its* q*-expansion at infinity, where*

$$B = \frac{1}{12} N \prod_{l \mid N, l \text{ prime}} (1 + \frac{1}{l}).$$

Proof. This follows from the proof of [E], proposition 4.2. $\square$

Corollary 2.5.4 *Let* f *be an element of* $\mathcal{S}_p(\Gamma_1(N),\epsilon,\mathbb{F})'$*. Then* $f \in \mathrm{Im}(F)$ *if and only if* $a_n(f) = 0$ *for all* $n \leq B(p+2)$ *such that* $p \nmid n$*.*

Proof. The image of F is equal to the kernel of θ by proposition 2.5.2. f is in the kernel of θ if and only if $\theta(f) = 0$, which is equivalent of $a_n(\theta(f)) = 0 = na_n(f)$. The result is now clear from the preceding proposition. □

Theorem 2.5.5 (Edixhoven) *Let $\mathbb{F}$ be a finite field of characteristic p, $N \geq 5$ an integer coprime to p and $\epsilon : (\mathbb{Z}/N)^* \to \mathbb{F}^*$ a character.*

The Hecke algebra $\mathbb{T}$ is defined as the subring of $\mathrm{End}_{\mathbb{C}}(S_p(\Gamma_1(N), \mathbb{C}))$ generated by the Hecke operators T_n. It can be generated as an abelian group by all T_n with $n \leq \frac{pN^2}{24} \prod_{l|N, l \text{ prime}}(1 - \frac{1}{l^2})$.

Let $\mathcal{R} \leq \mathbb{T} \otimes \mathbb{F}$ be the sub $\mathbb{F}$-vector space generated by the images of

- *T_n for all $n \leq B(p+2)$ with B as before such that $p \nmid n$ and*
- *$\epsilon(l) - < l >$ for all $l \in (\mathbb{Z}/N)^*$.*

Then there is an isomorphism of $\mathbb{F}$-vector spaces

$$\mathcal{S}_1(\Gamma_1(N), \epsilon, \mathbb{F})' \to \big((\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F})/\mathcal{R}\big)^{\vee_{\mathbb{F}}}.$$

Under this isomorphism the weight 1 Hecke operator $T_l^{(1)}$ for $l \neq p$ prime corresponds to $(T_l^{(p)} \bmod \mathcal{R})^\vee$, and $T_p^{(1)}$ corresponds to $(T_p^{(p)} + < p > \circ F \bmod \mathcal{R})^\vee$. The operator F is given by $F(T_n) = T_{n/p}$ if p divides n and by $F(T_n) = 0$ otherwise.

Proof. The mentioned bound on the generators of the Hecke algebra follows the proof of [E], proposition 4.2.

Let us now describe the main isomorphism.

$$\begin{array}{ccc}
f \in & \mathcal{S}_1(\Gamma_1(N), \epsilon, \mathbb{F})' \xhookrightarrow{F} & \mathcal{S}_p(\Gamma_1(N), \epsilon, \mathbb{F})' \\
\Big\downarrow & & \Big\downarrow \sim \\
& & \big((S_p(\Gamma_1(N), \mathbb{Z}[1/N])) \otimes \mathbb{F}\big)(\epsilon) \\
& & \Big\downarrow \sim \ \text{prop. 2.4.4} \\
& & \big((\mathrm{Hom}_{\mathbb{Z}[1/N]-lin}(\mathbb{T}, \mathbb{Z}[1/N]) \otimes \mathbb{F}\big)(\epsilon) \\
& & \Big\downarrow \sim \ \text{freeness} \\
& & (\mathbb{T} \otimes \mathbb{F})^{\vee_{\mathbb{F}}}(\epsilon) \\
& & \Big\| \\
\big(T_n \otimes \mathbb{F} \mapsto a_{n/p}(f)\big) & & (\mathbb{T} \otimes \mathbb{F})^{\vee_{\mathbb{F}}}\big[\ \epsilon(l) - < l > \ \mid l \in (\mathbb{Z}/N)^*\ \big]
\end{array}$$

Hence using corollary 2.5.4 we find that the image of F is

$$(\mathbb{T} \otimes \mathbb{F})^\vee[\mathcal{R}] \cong (\mathbb{T} \otimes \mathbb{F}/\mathcal{R})^\vee,$$

as claimed.

It remains to check the claims on the Hecke operators. But they follow immediately from lemma 2.5.1 (c) and (d). □

2.6 Results on $\Gamma_0(N)$

In the previous section we have seen how to calculate Katz modular forms of weight 1 over a finite field $\mathbb{F}$ of characteristic p of level N ($N \geq 5$ and $(N,p) = 1$) with respect to a character ϵ.

It is natural to ask whether in the case of the trivial character we may replace the Hecke algebra $\mathbb{T}$ for $\Gamma_1(N)$ by the one for $\Gamma_0(N)$ in the theorem. In this section we shall establish a sufficient criterion for this.

Let us first of all note that we ought to choose $p = 2$ as otherwise the theory is empty (there being no non-trivial modular forms of weight 1 for $\Gamma_0(N)$). Let us continue to assume $N \geq 5$ with N odd.

Lemma 2.6.1 *Let $N > 1$ be an odd integer. Then the following three statements are equivalent:*

(i) All stabilizers of the action of $\Gamma_0(N)/\{\pm 1\}$ on $\mathbb{H}$ are of odd order.

(ii) For all $a, c \in \mathbb{Z}$ such that $(a,c) = 1$ we have: $a^2 + c^2 \not\equiv 0\ (N)$.

(iii) There exists a prime l dividing N such that $l \equiv 3(4)$.

Proof. It is well known that the stabilizer of $\tau \in \mathbb{H}$ is 1 except in the cases $\tau \in \mathrm{SL}_2(\mathbb{Z})i$ and $\tau \in \mathrm{SL}_2(\mathbb{Z})\zeta_3$. In the latter case, the stabilizer is of order 3 and conjugate (in $\mathrm{SL}_2(\mathbb{Z})$) to the group generated by the matrix $\begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}$. The stabilizer of i is the group of order 2 generated by the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

So condition (i) is equivalent to the statement

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \notin \Gamma_0(N).$$

Performing the matrix multiplication we find immediately that (i) is equivalent to (ii).

We shall now study equation $a^2 + c^2 \not\equiv 0\ (N)$ in the principal ideal domain $\mathbb{Z}[i]$, in which we have

$$a^2 + c^2 = (a + ic)\sigma(a + ic) = (a + ic)(a - ic),$$

where σ is complex conjugation (the non-trivial Galois automorphism of $\mathbb{Q}(i)$ over $\mathbb{Q}$). Let us further recall that a prime number $l \neq 2$ splits in $\mathbb{Z}[i]$ if and only if $l \equiv 1\ (4)$.

not (iii) $\Rightarrow$ not (ii): In this case all primes l dividing N are split. From what we recalled above, we can write $l = (x_l + iy_l)(x_l - iy_l)$ with $x_l, y_l \in \mathbb{Z}$. If $N = \prod_l l^{r_l}$, then we put $a + ic = \prod_l (x_l + iy_l)^{r_l}$. This implies $N = (a + ic)(a - ic)$.

(iii) $\Rightarrow$ (ii): Let l be a prime dividing N, which is $l \equiv 3\ (4)$ and let $a, c \in \mathbb{Z}$ with $(a, c) = 1$ be given. Suppose there is an $r \in \mathbb{Z}$ such that $rN = a^2 + c^2 = (a + ic)(a - ic)$. The prime decomposition of $a + ic$ can only consist of primes $\mathfrak{P}$ lying over split primes, because otherwise a and c would not be coprime. Since l divides N it must also divide one of those $\mathfrak{P}$, which is impossible since l is non-split. $\square$

Proposition 2.6.2 *Assume that there exists a prime l dividing N s.t. $l \equiv 3\ (4)$. Then we have isomorphisms*

$$S_2(\Gamma_0(N), \mathbb{F}) = S_2(\Gamma_1(N), \mathbb{F})^{\Delta} = \mathcal{S}_2(\Gamma_0(N), \mathbb{F})',$$

where $\Delta = \Gamma_0(N)/\Gamma_1(N)\{\pm 1\} = (\mathbb{Z}/N)^*/\{\pm 1\}$.

Proof. This follows from the proof of [E], theorem 5.6. One of the ingredients quoted therein is that the stabilizers of the covering group of $Y_1(N) \twoheadrightarrow Y_0(N)$ have odd order. This, however, follows directly from lemma 2.6.1. $\square$

Theorem 2.6.3 *Let $\mathbb{F}$ be a finite field of characteristic 2 and $N \geq 5$ an odd integer, which is divisible by a prime number q s.t. $q \equiv 3\ (4)$.*

The Hecke algebra $\mathbb{T}_0$ is defined as the subring of $\mathrm{End}_{\mathbb{C}}(S_2(\Gamma_0(N), \mathbb{C}))$ generated by the Hecke operators T_n. It can be generated as abelian group by all T_n with $n \leq 2B$ with B as before.

Let $\mathcal{R} \leq \mathbb{T}_0 \otimes \mathbb{F}$ be the sub $\mathbb{F}$-vector space generated by the images of T_n for all odd $n \leq 4B$.

Then there is an isomorphism of $\mathbb{F}$-vector spaces

$$\mathcal{S}_1(\Gamma_0(N), \mathbb{F})' \to \big((\mathbb{T}_0 \otimes_{\mathbb{Z}} \mathbb{F})/\mathcal{R}\big)^{\vee_{\mathbb{F}}}.$$

Under this isomorphism the weight 1 Hecke operator $T_l^{(1)}$ for $l \neq 2$ prime corresponds to $(T_l^{(2)} \bmod \mathcal{R})^\vee$, and $T_2^{(1)}$ corresponds to $(T_2^{(2)} + <2> \circ F \bmod \mathcal{R})^\vee$. The operator F is given by $F(T_n) = T_{n/2}$ if n is even and by $F(T_n) = 0$ if n is odd.

Proof. Denote by $\mathbb{T}_1$ the subring of $\mathrm{End}_{\mathbb{C}}(S_2(\Gamma_1(N), \mathbb{C}))$ generated by all Hecke operators T_n and by $\mathcal{M}$ the sub $\mathbb{F}$-vector space of $\mathbb{T}_1 \otimes \mathbb{F}$ generated by the images of the T_n with n odd. Furthermore, let $I = ((1- < l >) \otimes \mathbb{F} \mid l \in (\mathbb{Z}/N)^*) \lhd \mathbb{T}_1 \otimes \mathbb{F}$.

The claims on the bounds follow again from [E], proposition 4.2.

By theorem 2.5.5 we have an isomorphism

$$\mathcal{S}_1(\Gamma_0(N), \mathbb{F})' \cong \big((\mathbb{T}_1 \otimes \mathbb{F})/(\mathcal{M} + I)\big)^\vee.$$

Hence it suffices to have an isomorphism

$$(\mathbb{T}_1 \otimes \mathbb{F})/I \cong \mathbb{T}_0 \otimes \mathbb{F},$$

which is compatible with the Hecke operators. This isomorphism is obtained from proposition 2.6.2 using the isomorphisms

$$S_2(\Gamma_0(N), \mathbb{F}) \cong (\mathbb{T}_0 \otimes \mathbb{F})^\vee \quad \text{and}$$
$$S_2(\Gamma_1(N), \mathbb{F})^\Delta \cong (\mathbb{T}_1 \otimes \mathbb{F})^\vee[I] \cong \big((\mathbb{T}_1 \otimes \mathbb{F}/I)\big)^\vee,$$

where the latter is obtained from 2.4.4 and the former by analogous arguments. □

3 Calculations of characteristic p modular forms of weight 1 and relation to Serre's conjecture

This talk was given on 29 January 2003.

Very vaguely speaking, we will try to outline links - partly conjectural - between the theory of modular forms and number theory, more precisely the study of the absolute Galois group of the rational numbers.

The starting point is a theorem by Deligne, which associates to an eigenform over an algebraic closure of $\mathbb{F}_p$ a 2-dimensional odd Galois representation over the same field. Serre conjectured that there is a converse to Deligne's result: given an odd irreducible 2-dimensional Galois representation there exists an eigenform of a precisely specified level, weight and character giving rise to this representation. The conjecture was extended to suggest that the minimal weight ought to be 1 if and only if the representation is unramified at p.

Serre's conjecture has spectacular consequences, among them a direct proof of Fermat's last theorem, which we sketch.

We will present some of the known results, focussing on dihedral representations.

Finally, we will discuss some calculations giving evidence for Serre's conjecture, which were originally carried out by Mestre, and which we verified.

As mentioned before Serre's conjecture was slightly modified and extended. Here we only treat the "currently up to date" form, as presented in Edixhoven's paper [E2].

3.1 Deligne's theorem

We will keep the notations of the previous talk, except that the condition $N \geq 5$ has to be dropped. However, N will always be coprime to the characteristic p.

Let k be an integer, $\mathbb{F}$ a finite extension of $\mathbb{F}_p$ and $\epsilon : (\mathbb{Z}/N)^* \to \mathbb{F}^*$ a character. Then we consider the space $\mathcal{S}_k(\Gamma_1(N), \epsilon, \mathbb{F})'$ of Katz modular forms and we denote by $\mathbb{T} = \mathbb{T}(\mathcal{S}_k(\Gamma_1(N), \epsilon, \mathbb{F})')$ its Hecke algebra, which is a finite dimensional $\mathbb{F}$-vector space. Then the Hecke algebra of $\mathcal{S}_k(\Gamma_1(N), \epsilon, \overline{\mathbb{F}_p})' = \mathcal{S}_k(\Gamma_1(N), \epsilon, \mathbb{F})' \otimes \overline{\mathbb{F}_p}$ is isomorphic to $\mathbb{T} \otimes \overline{\mathbb{F}_p}$.

From the formula

$$a_1(T_n f) = a_n(f)$$

we obtain (by the uniqueness of the q-expansion) an injection

$$\mathcal{S}_k(\Gamma_1(N), \epsilon, \overline{\mathbb{F}_p})' \to \mathrm{Hom}_{\overline{\mathbb{F}_p}-lin}(\mathbb{T} \otimes \overline{\mathbb{F}_p}, \overline{\mathbb{F}_p}) \cong \mathrm{Hom}_{\mathbb{F}-lin}(\mathbb{T}, \overline{\mathbb{F}_p}), \quad f \mapsto \big(T_n \mapsto a_n(f)\big).$$

In fact, the map is an isomorphism as one sees considering (more conceptually) $a_1(T, f) =< T, f >$ as a bilinear pairing, which is non-degenerate in both variables. It remains to check one non-degeneracy: Given $T \in \mathbb{T} \otimes \overline{\mathbb{F}_p}$, assume $a_1(Tf) = 0$ for all f. Then in particular $a_1(T(T_n f)) = a_1(T_n T f) = a_n(Tf) = 0$ for all f and all n. By the uniqueness of the q-expansion, we conclude $Tf = 0$ for all f. Due to the faithfulness of the Katz forms as a $\mathbb{T} \otimes \overline{\mathbb{F}_p}$ module, we conclude $T = 0$.

$\mathrm{Hom}_{\mathbb{F}-lin}(\mathbb{T}, \overline{\mathbb{F}_p})$ is naturally equipped with a $\mathbb{T}$-action via

$$(T_n.f)(T_m) = f(T_n T_m),$$

which is compatible with the $\mathbb{T}$-action on the space of Katz modular forms.

Inside $\mathrm{Hom}_{\mathbb{F}-lin}(\mathbb{T}, \overline{\mathbb{F}_p})$ we can consider the set $\mathrm{Hom}_{\mathbb{F}-alg}(\mathbb{T}, \overline{\mathbb{F}_p})$. Given an $\mathbb{F}$-linear homomorphism $f : \mathbb{T} \to \overline{\mathbb{F}_p}$, we see immediately

$$f \text{ is a } \mathbb{F}\text{-algebra hom.} \Leftrightarrow f \text{ is a normalised eigenform with eigenvalues } f(T_n).$$

Using the isomorphism above we find that the $\mathbb{F}$-algebra homomorphisms correspond precisely to the normalised Katz modular forms, which are eigenfunctions for all Hecke operators T_n with eigenvalues $a_n(f)$.

Remark 3.1.1 We should note at this point that eigenspaces in $\mathcal{S}_k(\Gamma_1(N), \epsilon, \overline{\mathbb{F}_p})'$ are necessarily 1-dimensional. Just because of the formula $a_1(T_n f) = a_n(f)$: if $(\lambda_n)_n$ is a system of eigenvalues then $a_n(f) = a_1(T_n f) = a_1(\lambda_n f) = \lambda_n a_1(f)$ for any eigenform corresponding to $(\lambda_n)_n$.

Moreover, there is a natural $G_{\mathbb{F}} = G(\overline{\mathbb{F}_p}|\mathbb{F})$-action on $\mathrm{Hom}_{\mathbb{F}-lin}(\mathbb{T}, \overline{\mathbb{F}_p})$ given by composition. One has:

Proposition 3.1.2 *In the setting above there is a bijection*

$$\mathrm{Hom}_{\mathbb{F}-alg}(\mathbb{T}, \overline{\mathbb{F}})/_{G_{\mathbb{F}}-\textit{conjugacy}} \quad \leftrightarrow \quad \textit{maximal ideals of } \mathbb{T},$$

given by sending an $\mathbb{F}$*-algebra homomorphism* $f : \mathbb{T} \to \overline{\mathbb{F}}$ *to its kernel.*

Proof. We point out that in an Artinian algebra every prime ideal is maximal. Since for every maximal ideal $\mathfrak{m}$ the ring $\mathbb{T}/\mathfrak{m}$ is contained (via f) in $\overline{\mathbb{F}}$ the kernel is a maximal ideal. If $g = \sigma \circ f$ for some field automorphism σ, the kernel of f is, of course, equal to the kernel of g. Hence the allocation is well defined.

The surjectivity is clear: given $\mathfrak{m}$, just take $f : \mathbb{T} \to \mathbb{T}/\mathfrak{m} \leq \overline{\mathbb{F}}$.

Suppose now that f and g have the same kernel $\mathfrak{m}$. That precisely means that f and g give two embeddings of the field $\mathbb{T}/\mathfrak{m}$ into $\overline{\mathbb{F}}$. By well known field theory, one can be obtained from the other by composing with an element of $G_{\mathbb{F}}$, which proves the injectivity. $\square$

Remark 3.1.3 By the proposition one can localize $\mathbb{T}$ at its maximal ideals in order to keep exactly one particular system of eigenvalues modulo $G_{\mathbb{F}}$-conjugacy. Linear algebra techniques (calculation of characteristic polynomials) then directly produce the Fourier coefficients of one eigenform. It is not difficult to calculate its (finite) $G_{\mathbb{F}}$-orbit.

One can show that in characteristic 0 there exists a basis of eigenforms for the space of (Katz) cusp forms, at least if the level is square-free. This, however, is no longer true in general for positive characteristic. We shall see examples of that in the end of this talk.

Before we can state Deligne's theorem we have to introduce some notation. Let $L|\mathbb{Q}$ be a Galois extension and let $\mathfrak{P}$ be a prime above l. Then the other primes above l are given by $\sigma\mathfrak{P}$ for $\sigma \in G(L|\mathbb{Q})$. We denote by $G_{\mathfrak{P}}(L|\mathbb{Q})$ the decomposition group of $\mathfrak{P}$, i.e. the subgroup of $G(L|\mathbb{Q})$ consisting of those σ s.t. $\sigma(\mathfrak{P}) = \mathfrak{P}$. One has a natural isomorphism

$$G_{\mathfrak{P}}(L|\mathbb{Q}) \to G(L_{\mathfrak{P}}|\mathbb{Q}_l)$$

given by extending the automorphisms by continuity to the completions. It is immediate that one has $G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}$. Furthermore, reduction modulo the maximal ideal of the ring of integers of $L_{\mathfrak{P}}$ gives a surjection

$$0 \to G_0(L_{\mathfrak{P}}|\mathbb{Q}_l) \to G(L_{\mathfrak{P}}|\mathbb{Q}_l) \to G(\lambda_{\mathfrak{P}}|\mathbb{F}_l) \to 0,$$

where $\lambda_{\mathfrak{P}}$ is the residue field of $L_{\mathfrak{P}}$. The kernel is called the *inertia group*.

We need a special case. Assume that $L|\mathbb{Q}$ is unramified at l, which by definition means that the right hand side map is an isomorphism (i.e. the inertia group is trivial). Then one has the element *Frobenius at l* $\mathrm{Frob}_l \in G(L_{\mathfrak{P}}|\mathbb{Q}_l) \subseteq G(L|\mathbb{Q})$, which is the usual map $x \mapsto x^l$ on the finite field side. A different choice of prime $\mathfrak{P}$ would have resulted in a conjugate Frobenius. All the statements below will only depend on the conjugacy class, so there is no need to specify the ideal chosen any further.

Theorem 3.1.4 (Deligne) *Let p be a prime, N a positive integer prime to p, $k \geq 1$, $\mathbb{F}$ an extension of $\mathbb{F}_p$ and $\epsilon : (\mathbb{Z}/N)^* \to \mathbb{F}^*$ a character.*

For any normalised eigenform $f \in \mathcal{S}_k(\Gamma_1(N), \epsilon, \overline{\mathbb{F}_p})$ of the Hecke algebra, there is a unique semi-simple continuous representation

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

satisfying

(i) ρ_f is unramified outside pN and

(ii) $\mathrm{Tr}(\rho_f(\mathrm{Frob}_l)) = a_l(f)$ and $\det(\rho_f(\mathrm{Frob}_l)) = \epsilon(l)l^{k-1}$ for all primes l not dividing pN.

Remark 3.1.5 Let us note some equivalent formulations.

Statement (ii) can be summarized by saying that the characteristic polynomial of $\rho_f(\mathrm{Frob}_l)$ is $X^2 - a_l(f) + \epsilon(l)l^{k-1}$ for all primes $l \nmid pN$.

In a more representation theoretic language, one also defines the (degree 2) *character* of the representation

$$\chi_f = \mathrm{Tr} \circ \rho_f$$

and the (degree 1) *determinant character*

$$\delta_f = \det \circ \rho_f.$$

Then (ii) has obvious reformulations. But there is more to it: one has

$$\det \circ \rho_f = (\epsilon \circ \psi_N) \cdot \psi_p^{k-1},$$

where ψ_n denotes the *n-th cyclotomic character* $\psi_n : G_{\mathbb{Q}} \to (\mathbb{Z}/n)^*$, which is defined by $\sigma(\zeta_n) = \zeta_n^{\psi(\sigma)}$ for any primitive n-th root of unity ζ_n. In particular, one has $\psi_N(\mathrm{Frob}_l) = l \in (\mathbb{Z}/N)^*$ and $\psi_p(\mathrm{Frob}_l) = l \in (\mathbb{Z}/p)^*$ by the assumption on l. Hence, the claimed equality holds for a set of primes of density 1, and hence by Chebotarev always.

Let c now denote a *complex conjugation* (this is the "infinite Frobenius"). It is again well-defined up to conjugacy. It is obtained by completing $\overline{\mathbb{Q}}$ for an absolute value above the absolute value of $\mathbb{Q}$, or, equivalently, by choosing an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and using the complex conjugation on $\mathbb{C}$. In particular, $c(\zeta_n) = \zeta_n^{-1}$ for any n, whence $\psi_N(c) = \psi_p(c) = -1$. Accordingly, $\det(\rho_f(c)) = \epsilon(\psi_N(c)) \cdot \psi_p^{k-1}(c) = \epsilon(-1)(-1)^{k-1} = (-1)^k(-1)^{k-1} = -1$, where we used that f is a non-zero modular form with character ϵ, and that is only possible if $\epsilon(-1) = (-1)^k$.

A representation ρ with $\det(\rho(c)) = -1$ is called an *odd representation*. Consequently, the representations obtained from Deligne's theorem are all odd.

3.2 Serre's conjecture

We shall start by associating to a given 2-dimensional representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

a triple $(N(\rho), \epsilon(\rho), k(\rho))$. By $\chi = \mathrm{Tr} \circ \rho$ we denote the character of ρ. Call $L|\mathbb{Q}$ the Galois extension cut out by ρ, i.e. $G(L|\mathbb{Q}) = G_{\mathbb{Q}}/\mathrm{Ker}(\rho)$.

Ideally, if $\rho = \rho_f$, then this triple should correspond to the minimal level, character and the weight of f. We shall later see a theorem making this precise.

$\underline{N(\rho) = \text{the } p\text{-primary part of the Artin conductor:}}$

We will introduce the Artin conductor and try to motivate it a little bit. Fix a prime l (not necessarily distinct from p) and a prime $\mathfrak{P}$ of L lying above l.

We shall first introduce the *ramification groups*:

- $G_{-1}(L_{\mathfrak{P}}|\mathbb{Q}_l) = G_{\mathfrak{P}}(L|\mathbb{Q}) = G(L_{\mathfrak{P}}|\mathbb{Q}_l)$ is the decomposition group, which we have already defined above.

- $G_i(L_{\mathfrak{P}}|\mathbb{Q}_l) = \{ \ \sigma \in G_{-1}(L_{\mathfrak{P}}|\mathbb{Q}_l) \mid \sigma x \equiv x \ (\mathfrak{P}^{i+1}) \ \forall x \in \mathcal{O}_{L_{\mathfrak{P}}} \ \}$ is the *i-th ramification group (in lower numbering)* for an integer $i \geq 0$.

- $G_0(L_{\mathfrak{P}}|\mathbb{Q}_l)$ is the *inertia group* as defined above.

- $G_1(L_{\mathfrak{P}}|\mathbb{Q}_l)$ is the unique l-Sylow subgroup of $G_0(L_{\mathfrak{P}}|\mathbb{Q}_l)$ and is called the *(wild) ramification group*.

- $G_i(L_{\mathfrak{P}}|\mathbb{Q}_l) \supseteq G_{i+1}(L_{\mathfrak{P}}|\mathbb{Q}_l)$ for all $i \geq -1$.

- The subfield cut out by G_0 is the maximal unramified subextension, and the subfield cut out by G_1 is the maximal tamely ramified subextension of $L_{\mathfrak{P}}|\mathbb{Q}_l$.

- Let us write: $g_{i,l} = |G_i(L_{\mathfrak{P}}|\mathbb{Q}_l)|$. This number does not depend on the choice of prime $\mathfrak{P}$ above l.

- The number $c_{i,l} = \operatorname{codim}\big((\overline{\mathbb{F}_p}^2)^{G_i(L_{\mathfrak{P}}|\mathbb{Q}_l)}\big)$ does not depend on the choice of prime $\mathfrak{P}$ over l.

Definition 3.2.1 Given a representation ρ as above, we associate to it the numbers:

$$f_l(\rho) = \sum_{i \geq 0} \frac{g_{i,l}}{g_{0,l}} c_{i,l}.$$

It is a theorem that these numbers are integers greater equal 0.

The *local Artin conductor of* ρ *at* l is defined to be the number

$$\mathfrak{f}_l(\rho) = \mathfrak{f}_l(\chi) = l^{f_l(\rho)}.$$

The *global Artin conductor of* ρ is defined to be the number

$$\mathfrak{f}(\rho) = \mathfrak{f}(\chi) = \prod_{l \text{ prime}} \mathfrak{f}_l(\rho).$$

Our number $N(\rho)$ is defined as

$$\mathfrak{f}(\rho) = \prod_{l \text{ prime},\, l \neq p} \mathfrak{f}_l(\rho).$$

We recall the analogously defined injective function ($s \geq 1$)

$$\eta_{L_{\mathfrak{P}}|\mathbb{Q}_l}(s) = \sum_{i=1}^{s} \frac{g_{i,l}}{g_{0,l}},$$

which defines the *ramification groups in upper numbering*:

$$G^{\eta_{L_{\mathfrak{P}}|\mathbb{Q}_l}(s)}(L_{\mathfrak{P}}|\mathbb{Q}_l) = G_s(L_{\mathfrak{P}}|\mathbb{Q}_l).$$

In particular, if the representation ρ is 1-dimensional, we have

$$f_l(\rho) = \eta_{L_{\mathfrak{P}}|\mathbb{Q}_l}(j) + 1,$$

where j is the maximal integer, s.t. $\rho|_{G_i} \neq 1_{G_i}$. The ramification groups in upper numbering have important properties. First of all they are compatible with quotients. Secondly, they are the images (in the case of an abelian local extension) of the i-th group of principal units ($1+p^i$, "one-units", "Einseinheiten") under the norm residue symbol of local class field theory. Certainly, one should at this philosophical point not forget to appreciate the *conductor-discriminant formula*

$$\mathfrak{d}_{L|\mathbb{Q}} = N_{L|\mathbb{Q}} \mathfrak{D}_{L|\mathbb{Q}} = \prod_l l^{f_{L_{\mathfrak{P}}|\mathbb{Q}_l} \sum_{i \geq 0}(g_{i,l}-1)} = \prod_\chi \mathfrak{f}(\chi)^{\chi(1)},$$

where the last product runs over all irreducible characters over the complex numbers of $G(L|\mathbb{Q})$.

Let us note explicitly that $N(\rho)$ is a measure for the ramification outside p and that ρ is unramified at $l \neq p$ if and only if $l \nmid N(\rho)$.

$\underline{\epsilon(\rho) \text{ and } k(\rho) \text{ modulo } p-1:}$

Let us denote by $\delta_\rho = \det \circ \rho$ the *determinant character*. One can check that we have the commutative diagram

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[rrrr, "\delta_\rho"] \arrow[dr, "\psi_{N(\rho)p}"] & & & & \overline{\mathbb{F}_p}^* \\
& (\mathbb{Z}/N(\rho)p)^* \arrow[r, "\sim"] \arrow[urrr] & (\mathbb{Z}/N(\rho))^* \arrow[urr, "\epsilon(\rho)"'] & \times & (\mathbb{Z}/p)^*, \arrow[u, "\phi"']
\end{tikzcd}$$

where the homomorphism ϕ is given by raising to some power $a = k(\rho) - 1$, where the last equality defines $k(\rho)$ modulo $p-1$. This means precisely that the determinant character is given by

$$\delta_\rho = (\epsilon(\rho) \circ \psi_{N(\rho)}) \cdot \psi_p^{k(\rho)-1}.$$

$\underline{k(\rho)}$:

There is a slightly complicated recipe for specifying $k(\rho)$ in all cases. One should consult [E2] for that. We shall content ourselves with the following:

- $k(\rho)$ depends only on the ramification of ρ at p.
- $k(\rho) = 1$ if and only if ρ is unramified at p.

Conjecture 3.2.2 (Serre) *Let p be a prime number and $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ a continuous irreducible odd representation.*

Then there exists an eigenform $f \in \mathcal{S}_{k(\rho)}(\Gamma_1(N(\rho)), \epsilon(\rho), \overline{\mathbb{F}_p})'$ such that ρ is isomorphic with ρ_f.

Theorem 3.2.3 *Let $p \neq 2$ be a prime, $g \in \mathcal{S}_k(\Gamma_1(N), \epsilon, \overline{\mathbb{F}_p})'$ be a Hecke eigenform and $\rho = \rho_g$ be the representation constructed by Deligne and assume additionally that it is irreducible.*

Then there is an eigenform $f \in \mathcal{S}_{k(\rho)}(\Gamma_1(N(\rho)), \epsilon(\rho), \overline{\mathbb{F}_p})'$ such that ρ is isomorphic with ρ_f.

Moreover, N is a multiple of $N(\rho)$, $k \geq k(\rho)$ and ϵ is obtained from $\epsilon(\rho)$ by composing with $\mathbb{Z}/N \to \mathbb{Z}/N(\rho)$.

Remark 3.2.4 Serre's conjecture implies Fermat's last theorem directly, i.e. without using the more difficult fact that it also implies Taniyama-Shimura.

The argumentation can be sketched quickly. Assume given a prime $p \geq 5$, $a, b, c \in \mathbb{Z}$ satisfying $abc \neq 0$ and

$$a^p + b^p = c^p.$$

Wlog. one can assume $a \equiv 3\ (4)$ and that b is even. Then one considers the elliptic curve

$$E : y^2 = x(x - a^p)(x + b^p).$$

One finds that E is semi-stable with discriminant

$$\Delta_E = \frac{-1}{256}(abc)^{2p}.$$

To every elliptic curve over $\mathbb{Q}$ one can associate a mod p Galois representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(E_p) \cong \mathrm{GL}_2(\mathbb{F}_p),$$

which is irreducible by a theorem by Mazur. The triple associated with ρ is

$$N(\rho) = 2, \quad k(\rho) = 2, \quad \epsilon(\rho) = 1.$$

BUT there are no non-trivial eigenforms of weight 2 for $\Gamma_0(2)$. Hence, assuming Serre's conjecture, one finds a contradiction. (This section was copied from [D].)

In order to see another very useful consequence of Serre's conjectures, we state the following consequence of Chebotarev's density theorem.

Theorem 3.2.5 *Let p be a prime, $\mathbb{F}$ a finite extension of $\mathbb{F}_p$ and $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ a continuous, semi-simple representation.*

(i) If $\underline{p \geq 3}$, then ρ is uniquely determined by Tr$(\rho(\text{Frob}_l))$ for any set of unramified primes l of density 1.

(ii) If $\underline{p = 2}$, then ρ is uniquely determined by Tr$(\rho(\text{Frob}_l))$ and $\det(\rho(\text{Frob}_l))$ for any set of unramified primes l of density 1.

Proof. This is proved (in fact also cited) in [F], proposition 2.6 (b). We just have to note that the trace of the second exterior power of ρ is given by the determinant, which one can check by a simple calculation. $\square$

Serre's conjecture can also be seen as an analogue of the following conjecture over $\mathbb{C}$ ([F], conjecture 3.7, implying a special case of Artin's conjecture).

Conjecture 3.2.6 *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ a continuous irreducible odd representation. Then ρ is equivalent to ρ_g for some newform g of weight 1 (One can associate to such a newform a representation of the requested type, which is a result by Deligne-Serre.)*

Serre's conjecture says more about the structure of the absolute Galois group of $\mathbb{Q}$ than the above conjecture, because all the finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ are

- C_n for $n \geq 1$,
- D_n for $n \geq 1$,,
- A_4, S_4 and A_5,

whereas the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}_p})$ are

- conjugates of the upper triangular matrices,
- C_n, D_n for $n \geq 1$ with $p \nmid n$,
- $\mathrm{PSL}_2(\mathbb{F}_{p^r})$, $\mathrm{PGL}_2(\mathbb{F}_{p^r})$ both for any $r \geq 1$,
- A_4, S_4 and A_5.

Knowing this, the following theorem is a nearly full proof of conjecture 3.2.6.

Theorem 3.2.7 (Langlands-Tunnel) *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ a continuous irreducible odd representation such that $\rho(G_{\mathbb{C}})$ is solvable. Then ρ is equivalent to ρ_g for some newform g of weight 1, which is a Hecke eigenform.*

Remark 3.2.8 In the case of dihedral image, this was already known to Hecke.

3.3 Modularity of dihedral representations

In this section we rapidly develop the representation theory of dihedral groups and, using the theorem of Langlands-Tunnel, we conclude that any odd dihedral representation is modular. Furthermore, we shall consider a test case for weight 1 modular forms; namely the dihedral extensions obtained from a quadratic number field that ramifies precisely at a given prime q.

- (My working definition, might not be the standard one.) A finite group G is called *dihedral* ($\cong D_A$) if there is an abelian group A of odd order, so that we have a split exact sequence of finite groups

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & G \arrow[r] & \mathbb{Z}/2 \arrow[r] \arrow[l, bend right, "\phi"'] & 0, \end{tikzcd}$$

where the non-trivial element $\sigma \in \phi(\mathbb{Z}/2)$ satisfies $\sigma a \sigma = a^{-1}$. Then G is a semidirect product of A and $\mathbb{Z}/2$.

- Given any character $\chi : A \to \overline{\mathbb{F}_p}^{\times}$, we define the *induced representation*

$$\mathrm{Ind}_A^G \chi = \{\ f : G \to \overline{\mathbb{F}_p} \text{ map} \mid f(ag) = \chi(a) f(g)\ \forall a \in A\ \} \cong \overline{\mathbb{F}_p}^2,$$

  where the isomorphism is given by sending f to $\rho_\chi(f) = (f(1), f(\sigma))$. G acts on $\mathrm{Ind}_A^G \chi$ by $(g.f)(\tilde{g}) = f(\tilde{g}g)$. Via the isomorphism above we find immediately that

$$\rho_\chi(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \rho_\chi(a) = \begin{pmatrix} \chi(a) & 0 \\ 0 & \chi(a^{-1}) \end{pmatrix} \text{ for all } a \in A.$$

- ρ_χ is irreducible if and only if χ is not the trivial character.

  This is easily proved by observing that the eigenvectors of $\rho_\chi(\sigma)$ are $(1,1)^T$ and $(1,-1)^T$. The matrix of $\rho_\chi(a)$ stabilizes them if and only if $\chi(a) = \chi(a^{-1})$ for all $a \in A$, implying the assertion.

- Two representations ρ_χ and ρ_ψ are conjugate (i.e. equivalent) if and only if either $\chi = \psi$ or $\chi = \psi^{-1}$.

  This can be seen by considering $M\rho_\chi(a) = \rho_\psi(a) M$ for a matrix M and all $a \in A$.

- Any 2-dimensional representation $\rho : G \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ is induced from a character as above.

  To see this, one restricts ρ to A, where it becomes reducible as A is abelian. So, after a suitable base change, one finds $\rho(a) = \begin{pmatrix} \psi_1(a) & 0 \\ 0 & \psi_2(a) \end{pmatrix}$ for two characters ψ_1, ψ_2 of A. Writing down the condition that $\rho(\sigma)$ acts as inversion on A, one sees $\psi_1(a) = \psi_2(a^{-1})$. Replacing the basis vectors by a suitable scalar multiple, one can further assume that $\rho(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Hence, we have precisely recovered the form above.

- Assume now that p does not divide the order of A. Then there are $(|A| - 1)/2$ distinct irreducible 2-dimensional representations of G. For that is the number of pairs (χ, χ^{-1}) of non-trivial characters of A. As the character table is square, we also know that we have thus described all irreducible representations of G.

Proposition 3.3.1 *Any odd representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ with dihedral image in $\mathrm{PGL}_2(\overline{\mathbb{F}_p})$ comes from a modular form, which is the reduction modulo p of a form in characteristic 0.*

Proof. We know that ρ is induced from a character χ. We can lift the character to characteristic 0. Choose a lift and call it ψ. It can be induced to give an odd representation Φ in characteristic 0, whose reduction is ρ. By the Langlands-Tunnel theorem (in fact already by results of Hecke), there is an eigenform in characteristic 0 corresponding to Φ. One can reduce this modular form to characteristic p, in order to obtain the desired modular form. $\square$

In a similar manner one can prove the

Proposition 3.3.2 *Any odd representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ comes from a modular form, which is the reduction modulo p of a form in characteristic 0.*

Proof. One uses a split surjection $\mathrm{GL}_2(\mathbb{Z}[\sqrt{-2}]) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ in order to lift the representation into characteristic 0. Then the Langlands-Tunnel theorem can be applied to give an eigenform in characteristic 0 with the desired reduction. $\square$

We shall now construct for each prime $q \nmid 2p$ dihedral representations of $G_{\mathbb{Q}}$, which are of Artin conductor q. We already know their modularity, so they provide a good testing ground for any calculations of modular forms of weight 1 over $\overline{\mathbb{F}_p}$.

Let K be the quadratic extension of $\mathbb{Q}$ defined by

$$K = \begin{cases} \mathbb{Q}(\sqrt{q}) & \text{for } q \equiv 1 \ (4) \\ \mathbb{Q}(\sqrt{-q}) & \text{for } q \equiv 3 \ (4). \end{cases}$$

It has discriminant ideal $\mathfrak{d}_{K|\mathbb{Q}} = (q)$. Let now H_K be the Hilbert class field of K, and consider inside H_K the maximal field L such that the degree $L|K$ is odd. This degree is then u, where $h_K = 2^r u$ is the class number of K. If we write $A = G(L|K)$, then $G(L|\mathbb{Q})$ is the dihedral group D_A.

Let now χ be a character of A. We compute the Artin conductor of the induced representation ρ_χ using the formula

$$\mathfrak{f}(L|\mathbb{Q}, \mathrm{Ind}\chi) = \mathfrak{d}_{K|\mathbb{Q}}^{\chi(1)} N_{K|\mathbb{Q}}(\mathfrak{f}(L|K, \chi))$$

and find that it is (q). (In fact, I should have introduced the Artin conductor for any extension of number fields, and not just extensions of $\mathbb{Q}$. But that is possible extending the definitions in an evident way.)

3.4 Explicit examples

We implemented the algorithm deriving from theorem 2.6.3 for the calculation of Katz cusp forms of weight 1 for $\Gamma_0(N)$ over $\overline{\mathbb{F}_2}$ for odd $N \geq 5$ (recall that there are only non-zero modular forms if $p = 2$).

Let us recall some notation:

- The number B is defined as $\frac{1}{12}N\prod_{l|N, l \text{ prime}}(1+\frac{1}{l})$.
- The Hecke algebra $\mathbb{T}_i$ for $i \in \{0,1\}$ is defined as the subring of $\mathrm{End}_{\mathbb{C}}(S_2(\Gamma_i(N),\mathbb{C}))$ generated by the Hecke operators T_n. It can be generated as an abelian group by all T_n with $n \leq 2B$ for $i = 0$.
- The sub $\mathbb{F}$-vector space $\mathcal{R} \leq \mathbb{T}_0 \otimes \mathbb{F}$ is generated by the images of T_n for all odd $n \leq 4B$.

Explicitly, we calculate in MAGMA the $\mathbb{F}_2$-vector space

$$\big((\mathbb{T}_0 \otimes_{\mathbb{Z}} \mathbb{F}_2)/\mathcal{R}\big)^{\vee_{\mathbb{F}_2}},$$

on which we have described the action of the Hecke operators.

Theorem 2.6.3 states that there is an isomorphism

$$\mathcal{S}_1(\Gamma_0(N),\overline{\mathbb{F}_2})' \to \big((\mathbb{T}_0 \otimes_{\mathbb{Z}} \overline{\mathbb{F}_2})/\mathcal{R}\big)^{\vee_{\overline{\mathbb{F}_2}}}$$

compatible with the Hecke operators *if* there is a prime $q|N$ that is $q \equiv 3\ (4)$. Otherwise, there are certainly counter examples.

Let us recall that we have seen, when deriving theorem 2.6.3 from theorem 2.5.5, that we needed the surjection

$$\mathbb{T}_1 \otimes \overline{\mathbb{F}_2}/(\mathcal{R}+I) \twoheadrightarrow \mathbb{T}_0 \otimes \overline{\mathbb{F}_2}/\mathcal{R}$$

to be an isomorphism, which we found to be true if there is such a q dividing N with $q \equiv 3\ (4)$. Dualizing, we obtain in any case an injection (from theorem 2.5.5)

$$\big((\mathbb{T}_0 \otimes_{\mathbb{Z}} \overline{\mathbb{F}_2})/\mathcal{R}\big)^{\vee_{\overline{\mathbb{F}_2}}} \hookrightarrow \mathcal{S}_1(\Gamma_0(N),\overline{\mathbb{F}_2})'.$$

So, we always get Katz cusp forms of the good weight and level, but if $q \equiv 1\ (4)$ we are not certain to find them all.

Let us note also, that in the case of $q|N$ with $q \equiv 3\ (4)$, we know that all Katz modular forms are reductions of characteristic 0 modular forms (proposition 2.6.2). We shall below see an example of level $N = 1429$, where we have a form not coming from characteristic 0 in weight 1.

This method was already used by Mestre in 1987 to produce evidence for Serre's conjecture ([MS]). In fact, Serre thanks Mestre in the introduction to his paper presenting the conjectures ([S]) for his computational work. Apparently, Mestre was only able to do prime levels, and he did not prove the method (maybe because the condition on the q was missing).

We redid most of the calculations of [MS] and verified them with one exception ($p = 1367$). Our aim for the future is, of course, to go beyond that.

The computational results, which I will present in the rest of this talk/section, were hence originally obtained by Mestre.

Let us look at some examples.

Mestre's table:

$N = q$	229	257	283	331	491	563	577	643	**653**
$\equiv$ (4)	1	1	3	3	3	3	1	3	1
d	2	2	3	3	6	6	3	3	4
h	3	3	3	3	9	9	7	3	1
#dih	1	1	1	1	4	4	3	1	**0**
#ef	1	1	1	1	4	4	3	1	**2**
$B(m)$	2	2	3	3	3	3	1	3	2
$\mathbb{F}$	$\mathbb{F}_2$	$\mathbb{F}_2$	$\mathbb{F}_2$	$\mathbb{F}_2$	$\mathbb{F}_{2^3}$	$\mathbb{F}_{2^3}$	$\mathbb{F}_{2^3}$	$\mathbb{F}_2$	$\mathbb{F}_{2^2}$

$N = q$	751	761	1129	1229	1367	**1381**	1399	1423	**1429**
$\equiv$ (4)	3	1	1	1	3	1	3	3	1
d	9	2	5	2	16	4	15	6	8
h	15	3	9	3	25	1	27	9	5
#dih	7	1	4	1	12	**0**	13	4	**2**
#ef	7	1	4	1	12	**2**	13	4	**5**
$B(m)$	3	2	2	2	3	2	3	3	2
$\mathbb{F}$	$\mathbb{F}_{2^4}$	$\mathbb{F}_2$	$\mathbb{F}_{2^3}$	$\mathbb{F}_2$	$\mathbb{F}_{2^{10}}$	$\mathbb{F}_{2^2}$	$\mathbb{F}_{2^9}$	$\mathbb{F}_{2^3}$	$\mathbb{F}_{2^6}$

$d = \dim \mathbb{T}_0 \otimes \mathbb{F}_2/\mathcal{R}$ $h =$ class number of K

$K = \mathbb{Q}(\sqrt{q})$ for $q \equiv 1$ (4) $K = \mathbb{Q}(\sqrt{-q})$ for $q \equiv 3$ (4)

#dih $=$ #{dihedral reps}   #ef $=$ #{eigenforms}

$B(m) =$ max $T_l - a_l$ nilp. deg. m $\mathbb{F} =$ minimal field

We see that there are three cases, where there are non-dihedral representations, i.e. also fields ramifying only at q.

The condition $(B(m))$ can be rephrased to say that there is a Hecke operator having a Jordan block of size m and that m is maximal with that property. Hence, $B(m)$ with $m \geq 2$ means that there is no basis of eigenforms for the space of Katz cusp forms.

An important example is $p = 1429$. Looking at the eigenvalues of the Hecke operators, one finds that the image of the associated Galois representation is the group $\mathrm{SL}_2(\mathbb{F}_8)$, which is not a subgroup of $\mathrm{GL}_2(\mathbb{C})$. Hence, there are eigenforms that are not reductions of forms in characteristic 0. This means that there are more Katz modular forms than classical ones in weight 1.

References

[D] Darmon, H.: *Serre's Conjectures* in Murty, K. (Ed.): *Seminar on Fermat's last theorem* CMS Conference Proceedings Vol. 17, AMS Publ., Providence

[DI] Diamond, F., Im, J.: *Modular forms and modular curves* in Murty, K. (Ed.): *Seminar on Fermat's last theorem* CMS Conference Proceedings Vol. 17, AMS Publ., Providence

[E] Edixhoven, B.: *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod* 2 *of weight* 1, submitted.

[E2] Edixhoven, B.: *Serre's conjecture*, in Cornell, Silverman (Ed.): *Fermat's Last Theorem*, Springer

[F] Darmon, H., Diamond, F., Taylor, R.: *Fermat's Last Theorem* in *Elliptic Curves and Modular Forms,* International Press, 1997

[G] Gross, B.H.: *A Tameness Criterion for Galois Representations Associated to Modular Forms (MOD* p*),* in Duke Mathematical Journal, Vol. 61, No. 2, pp. 445-517

[K] Katz, N.: p*-adic properties of modular schemes and modular forms,* in *Modular Functions of One Variable III,* LNM 350, Springer

[K2] Katz, N.: *A Result on Modular Forms in Characteristic* p in *Modular Functions of One Variable V,* LNM 601, Springer

[M] Merel, L.: *Universal Fourier Expansions of Modular Forms,* in Frey, G. (Ed.) *On Artin's conjecture for odd* 2*-dimensional representations*, pp. 59–94, Lecture Notes in Math., 1585, Springer, Berlin, 1994

[MS] Mestre, J.-F.: *Lettre à Serre* dated 8 October 1987

[S] Serre, J.P.: *Sur les représentations modulaires de degré 2 de Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$ in Duke Mathematical Journal, Vol. 54, 1987, pp. 179-230