ALGEBRAIC VALUES OF MODULAR FUNCTIONS

Abstract. These are notes of lectures for students given by M. Vlasenko at the Institute of Mathematics of NAS of Ukraine

1. The Riemann sphere $\mathbb{C}P^1$

$\mathbb{C}P^1 = \mathbb{C} \cup \{\infty\}$ is a compact complex manifold obtained by glueing of two complex planes $\mathbb{C}$ and $\mathbb{C}$ by the map $z \mapsto \frac{1}{z}$. The underlying topological space is the 2-dimensional sphere S^2.

Theorem 1. *Any complex structure on S^2 is isomorphic to $\mathbb{C}P^1$.*

Theorem 2. *The only holomorphic maps $f : \mathbb{C}P^1 \to \mathbb{C}P^1$ are rational functions, i.e. $f(z) = \frac{P(z)}{Q(z)}$ with $P, Q \in \mathbb{C}[X]$.*

Proof. f is either constant or takes every value in a finite number of points. Indeed, suppose $\{x | f(x) = a\}$ is infinite. Since $\mathbb{C}P^1$ is compact there exist a limit point x_0. Since f is holomorphic it follows that $f(x) \equiv a$ in a neighbourhood of x_0. Hence $f(x) \equiv a$ everywhere.

Thus $f|_{\mathbb{C}}$ has finite number of zeros and poles. We multiply f by a rational function so that $g(z) = f(z)\frac{Q(z)}{P(z)}$ has no zeros or poles in $\mathbb{C}$. g is defined on $\mathbb{C}P^1$, i.e. $g(\frac{1}{z})$ is meromorphic at $z = 0$. Hence $g(z)$ has limit on ∞, either finite or infinite. Thus either $|g|$ or $1/|g|$ is bounded, and g is constant by Liouville's boundedness theorem. □

Note that $\deg f = max(\deg P, \deg Q)$, and the only 1-to-1 holomorphic maps are $f(z) = \frac{az+b}{cz+d}$ with $ad - bc \neq 0$.

2. The function j

The group $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm 1\}$ acts on $H = \{z \in \mathbb{C} | \operatorname{Im} z > 0\}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}.$$

This action is free and discontinious. The set

$$\Delta = \{-\frac{1}{2} < \operatorname{Re} z \leq \frac{1}{2}, |z| > 1\} \cup \{z = e^{i\phi}, \frac{\pi}{3} \leq \phi \leq \frac{\pi}{2}\}$$

is a fundamental domain. The boundary of Δ is glued by $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, so the quotient $X = H/PSL_2(\mathbb{Z})$ is topologically a sphere without one point. This quotient X inherits the complex structure from H. In fact we can compactify X introducing a proper complex coordinate in a neighbourhood of this missed point. Consider the map $q : H \to \{0 < |z| < 1\}$, $q(z) = e^{2\pi i z}$. Then $q(z) = q(z')$ implies $z' = z + n = T^n z$, so complex structure on X factors through q. Since $q(\infty) = 0$, we have complex structure on X arround the missed point. Due to Theorem 1 we now have that

Theorem 3.

$$\overline{X} = H \cup \mathbb{Q}P^1/PSL_2(\mathbb{Z}) \cong \mathbb{C}P^1$$

Consider the holomorphic map making an isomorphism of the Theorem above explicit. We can fix any value at any point, so we want it to map the additional point $\infty = \overline{X} - X$ to $\infty \in \mathbb{C}P^1$. Now the map is fixed up to a composition with a linear map $z \mapsto az + b$ $(a \neq 0)$ since such maps only preserve $\infty \in \mathbb{C}P^1$. Let us lift this map to H, so we have a holomorphic function $j : H \to \mathbb{C}$ such that
1) $j(gz) = j(z)$ for any $g \in PSL_2(\mathbb{Z})$
2) $j(q)$ has a pole of order 1 at $q = 0$
Indeed, j can be considered as a function of q due to 1) and the order of pole is 1 since j represents a map from $\overline{X}$ to $\mathbb{C}P^1$ which is 1-to-1. Since j is defined up to composition with a linear function, we can fix first two Laurent coefficients to be arbitrary. They are traditionally chosen as below:

Definition 1. *j is a unique holomorphic function on H such that $j(gz) = j(z)$ for $g \in PSL_2(\mathbb{Z})$ and*

$$j(q) = \frac{1}{q} + 744 + o(q),\ q \to 0.$$

Theorem 4. *j has integer Fourier coefficients, i.e. $j(q) = \frac{1}{q} + \sum_{n=0}^{\infty} a_n q^n$ whith $a_n \in \mathbb{Z}$.*

To prove this theorem we need to construct j in another way.

3. Modular forms and Eisenstein series

For each nonnegative integer k we define the action "of weight $2k$" of $PSL_2(\mathbb{Z})$ on functions in H by

$$f\Big|_{2k} \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = (cz+d)^{-2k} f(\frac{az+b}{cz+d}).$$

(Note that this is a right action.)

Definition 2. *Modular form f of weight $2k$ is a holomorphic function on H which*
1) is invariant under this action, i.e. $f\Big|_{2k} g = f$ for any $g \in PSL_2(\mathbb{Z})$;
2) has finite limit at ∞, i.e. $f(q) = \sum_{n=0}^{\infty} a_n q^n$.

The space of modular forms is denoted by M_{2k}, the subspace of forms with $a_0 = 0$ is denoted by S_{2k}. Elements of S_{2k} are called cusp forms.

Example. For $k > 1$ the function $G_{2k}(z) = \sum'_{m,n \in \mathbb{Z}} \frac{1}{(mz+n)^{2k}} \in M_{2k}$. It is called an Eisenstein series of weight $2k$. Let us calculate Fourier coefficients of G_{2k}. It is known (see [1]) that $\pi \operatorname{ctg}(\pi z) = \lim_{N \to \infty} \sum_{n=-N}^{N} \frac{1}{z+n}$. So

$$\sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^{2k}} = -\frac{1}{(2k-1)!} \left(\frac{d}{dz}\right)^{2k-1} \pi \operatorname{ctg}(\pi z)$$

$$= -\frac{1}{(2k-1)!}\left(2\pi i q\frac{d}{dq}\right)^{2k-1}\pi i\frac{q+1}{q-1}$$

$$= \frac{(2\pi i)^{2k}}{(2k-1)!}\left(q\frac{d}{dq}\right)^{2k-1}\sum_{n=0}^{\infty} q^n = \frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=0}^{\infty} n^{2k-1}q^n.$$

Thus we have

$$G_{2k}(z) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$$

where $\sigma_m(n) = \sum_{d|n} d^m$.

So, G_{2k} is not a cusp form and $M_{2k} = S_{2k} + \mathbb{C}G_{2k}$ for $k > 1$. In fact all M_{2k} are finite dimensional vector spaces (see [2]).

Recall that $\zeta(2k) \in \pi^{2k}\mathbb{Q}$. Then the modular form E_{2k} such that $G_{2k} = 2\zeta(2k)E_{2k}$ has rational Fourier coefficients. We will need

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n,\ E_6(z) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n.$$

This forms obviously have integer fourier coefficients. E_4^3 and E_6^2 are in M_{12} both. Then

$$E_4^3 - E_6^2 = 1728q + ... \in S_{12}.$$

Let us introduce the cusp form $\Delta = \frac{E_4^3 - E_6^2}{1728}$.

Theorem 5. *(Jacobi)*

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

Proof. See [2]. □

Exercise. Show that $\Delta(z) \neq 0$ for $z \in H$ (as a concequence of Jacobi theorem).

Due to this exercise the function $f = \frac{E_4^3}{\Delta}$ is holomorphic in H. It is $PSL_2(\mathbb{Z})$-invariant since numerator and denominator are modular forms of the same weight. Calculating two first Fourier coefficients we get

$$f = \frac{1}{q} + 744 + \dots$$

So, $f = j$. We have proved the identity

$$j = \frac{1728E_4^3}{E_4^3 - E_6^2}.$$

Now we can prove Theorem 4. Due to Jacobi theorem $\frac{\Delta}{q} \in \mathbb{Z}[[q]]^\times$, i.e. $\frac{q}{\Delta}$ has integer Fourier coefficients. Thus j also has.

4. Algebraic values

Theorem 6. *Let $z \in H$ is quadratic over $\mathbb{Q}$, i.e. $z^2 + pz + q = 0$ for some $p, q \in \mathbb{Q}$. Then $j(z) \in \overline{\mathbb{Z}}$.*

This means that $j(z)$ satisfies a monic equation with integer coefficients. The proof occupies the rest of this section.

Let A be a 2×2 matrix with integer coefficients, and $\det A = N > 0$. Then for $z \in H$ we have $Az \in H$. If $MPSL_2(\mathbb{Z}) \neq PSL_2(\mathbb{Z})M$ then $j \circ M$ is not a modular function. But we can construct modular functions as follows. Let M_N be the set of integer matrices with determinant N, let $A_1, \ldots, A_K$ be all representatives of the orbits $SL_2(\mathbb{Z})\backslash M_N$. Then obviously $(j(A_1 gz), \ldots, j(A_K gz))$ is a permutation of $(j(A_1 z), \ldots, j(A_K z))$ for any $g \in SL_2(\mathbb{Z})$. Thus for any symmetric polynomial $P(X_1, \ldots, X_K)$ the function

$$f_P(z) = P(j(A_1 z), \ldots, j(A_K z))$$

is modular. Then due to Theorem 2 it is a rational function of j. Moreover, it is a polynomial of j since f_P has no poles in H. So, there exist a polynomial $Q_P \in \mathbb{C}[X]$ such that

$$f_P(z) = Q_P(j(z))$$

for any $z \in H$.

Now we can explain the idea of the proof of the Theorem 6. For each $N \geq 1$ we have a polynomial in two variables Q_N such that

$$Q_N(j(z), j(w)) = \prod_{A \in PSL_2(\mathbb{Z})\backslash M_N} (j(z) - j(Aw)).$$

Note that z is a quadratic irrationality iff there exist for some $N > 1$ a matrix A with integer coefficients and $\det A = N$ such that $Az = z$. Moreover, N can be chosen to be nonsquare. Then

$$Q_N(j(z), j(z)) = 0.$$

We have found an equation for $j(z)$! It remains to show that $Q_N(X, X)$ is a nontrivial monic polynomial with integer coefficients for nonsquare N. (If $N = N_1^2$, then $Q_N(j, j) = 0$.) We do it below.

Lemma 1. *$K = \sigma_1(N)$ and for representatives A_i one can take all matrices*

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with $ad = N$, $a, d > 0$, $0 \leq b < d$.

Exercise. Prove the lemma.

The idea of the next lemma is often called the q-expansion principle.

Lemma 2. *If $P \in \mathbb{Z}[X_1, \ldots, X_K]$ then the modular function f_P has integer Fourier coefficients.*

Proof. We denote $\zeta_m = e^{\frac{2\pi i}{m}}$, $q^{\frac{1}{m}} = e^{\frac{2\pi i z}{m}}$. Then for $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ we have $q(Az) = \zeta_d^b q^{\frac{a}{d}}$. Since Fourier coefficients of j are integers f_P has expansion of the form

$$f_P(z) = \sum_{n=n_0}^{\infty} b_n(\zeta_N) q^{\frac{n}{N}}$$

with $b_n \in \mathbb{Z}[X]$. This can be considered as Fourier expansion for $f_P(Nz)$. By uniqueness of such expansion we get $b_n = 0$ if $N \nmid n$.

Let's show that remaining b_n doesn't depend on ζ_N in fact. Take h such that $(h, N) = 1$ and substitute ζ_N by ζ_N^h in our expression. Then $q(Az) = \zeta_d^b q^{\frac{a}{d}}$ becomes $\zeta_d^{bh} q^{\frac{a}{d}} = q(A'z)$ where $A' = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}$, $b' = bh (mod\ d)$. Since $(h, d) = 1$ the mapping $b \mapsto b' = bh(mod\ d)$ permutes matrices with given a and d. So, our expression doesn't change. We have

$$\sum_{n=n_0}^{\infty} b_n(\zeta_N) q^{\frac{n}{N}} = \sum_{n=n_0}^{\infty} b_n(\zeta_N^h) q^{\frac{n}{N}},$$

so $b_n(\zeta_N) = b_n(\zeta_N^h)$ due to the uniqueness of the Fourier expansion again. So $b_n(\zeta_N) \in \mathbb{Q}(\zeta_N)$ is integer and is stable under the action of Galois group. Thus $b_n \in \mathbb{Z}$. □

Lemma 3. *Let $Q \in \mathbb{C}[X]$. Then $Q(j)$ has integer Fourier coefficients iff $Q \in \mathbb{Z}[X]$.*

Exercise. Prove the lemma (look at the Fourier expansion of j).

The last two lemmas imply that $Q_N(X, Y) \in \mathbb{Z}[X, Y]$. To show that $Q_N(X, X)$ is nontrivial for nonsquare N we look at the lowest term in the Fourier expansion of $Q_N(j, j)$:

$$Q_N(j, j) = \prod_{ad=N, a,d>0, 0 \le b < d} \left(\frac{1}{q} - \frac{1}{\zeta_d^b q^{\frac{a}{d}}} + o(1) \right) = \frac{(-1)^{u(N)}}{q^{v(N)}} + \dots$$

where $v(N) = \sum_{a|N} \max(a, \frac{N}{a})$ and $u(N) = \sum_{d|N, d^2<N} d$.

5. Some consequences

Definition 3. *The field of definition of a modular form $f \in M_{2k}$, $f = \sum_{n=0}^{\infty} a_n q^n$ is the field $\mathbb{Q}(a_0, a_1, \dots)$ generated over $\mathbb{Q}$ by its Fourier coefficients.*

Let us take to modular forms $f \in M_{2p}$, $g \in M_{2q}$ defined over $\mathbb{Q}$ both. Then

$$\frac{f^{2q}}{g^{2p}}$$

is a modular function (with poles), hence a rational function of j by Theorem 2.

Exercise. Prove that $\frac{f^{2q}}{g^{2p}}$ has rational Fourier coefficients. Prove that

$$\frac{f^{2q}}{g^{2p}} = F(j) \ \text{ with } F \in \mathbb{Q}(X),$$

i.e. F is a rational function with rational coefficients. (Use ideas of q-expansion principle. See Lemma 2.)

Corollary 4. *Let $z \in H$ is quadratic over $\mathbb{Q}$, i.e. $z^2 + pz + q = 0$ with some $p, q \in \mathbb{Q}$. Then for any $f \in M_{2p}$, $g \in M_{2q}$ defined over $\mathbb{Q}$ one has*

$$f^{\frac{1}{2p}}(z) \in \overline{\mathbb{Q}} g^{\frac{1}{2q}}(z).$$

Another generalization of our proofs can be as follows. Take two modular forms $f, g \in M_{2k}$ defined over $\mathbb{Q}$. Then the polynomial

$$P_N(X) = \prod_{A \in PSL_2(\mathbb{Z}) \backslash M_N} \left(X - \frac{f|_{2k} A(z)}{g(z)} \right) = \sum_n b_n(z) X^n$$

has modular coefficients whith rational q-expansions again. Here

$$f\Big|_{2k} \begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{1}{(cz+d)^{2k}} f\left(\frac{az+b}{cz+d}\right)$$

as usual. So, b_n are rational functions of j with rational coefficients. Thus $b_n(z) \in \mathbb{Q}(j(z))$, and finally we have

Theorem 7. *Let $f, g \in M_{2k}$ are defined over $\mathbb{Q}$. Then*

$$\frac{f|_{2k} A(z)}{g(z)} \in \overline{\mathbb{Q}}$$

for any integer matrix A with $\det A > 0$ and quadratic $z \in H$.

In particular, $\frac{f(Nz)}{f(z)} \in \overline{\mathbb{Q}}$ for any rational $f \in M_{2k}$.

Theorem 8. *Let $f_1, f_2 \in M_{2k}$ have Fourier expansions of the form $q^{n_0^{(i)}} + \sum_{n > n_0^{(i)}} a_n^{(i)} q^n$ with $a_n^{(i)} \in \mathbb{Z}$, $i = 1, 2$ correspondingly. Suppose f_1 has no poles in H and f_2 has no zeros. Then*

$$(detA)^{2k} \frac{f_1|_{2k} A(z)}{f_2(z)} \in \overline{\mathbb{Z}}$$

for any integer matrix A with $\det A > 0$ and quadratic $z \in H$.

Exercise. Check numerically that $f_N(z) = N^{12} \frac{\Delta(Nz)}{\Delta(z)} \in \overline{\mathbb{Z}}$ for different N and quadratic $z \in H$. For example,

$$f_2(I) = 8, \; f_2(2I) = 0.01428534987281966273436738835.. = 198\sqrt{2} - 280.$$

Exercise. Prove Theorem 7 and Theorem 8.

References

[1] A.Weil, Elliptic functions according to Eisenstein and Kronecker // Springer-Verlag, 1976

[2] J.-P.Serre, A course in arithmetic // Springer-Verlag, 1973

[3] D.Zagier, Aspects of complex multiplication // notes of the seminar written by J. Voight (2000) http://www.ima.umn.edu/ voight/notes/274-Zagier.pdf

[4] H.M.Stark, Values of L-functions at s=1 I. L-functions of quadratic forms //Advances in Mathematics 7 (1971), 301-343 (chapter 4 only !)