# $196884 = 1 + 196883$

# A Monstrous tale

## Finite simple groups, quantum logic, replicable functions, dispersionless flow, and Witten's manifold

John McKay
Concordia University, Montreal

CRM Nov. 5th. 2K3 - Fields Mar. 8th. 2K4

Montreal & Toronto

CRM/Fields prize lecture

**Kronecker: Die natürlich Zahlen hat der liebe Gott gemacht. Alles andere ist Menschenwerk.**

Ingredients: $\mathbf{N} = 1, 2, 3, \ldots$

The Oxford English Dictionary tells us:

MONSTROUS:
of unnaturally or extraordinarily huge dimensions; greatly to be marvelled at; astounding.

MOONSHINE:
something unsubstantial, of dubious quality.

## **(Toy) Example:** Symmetric group

$$P_g(q) = \mathrm{det}(1 - R(g)q)$$

$$f_{\langle g \rangle} = 1/P_g(q)$$

$$\mathrm{f}_{\langle 13 \rangle} = \frac{1}{(1-q)2}, \quad f_{\langle 2,1 \rangle} = \frac{1}{1-q2}, \quad f_{\langle 3 \rangle} = \frac{1-q}{1-q3}$$

$$\left.\begin{array}{lrrr}
q0 & 1 & 1 & 1 \\
q1 & 2 & 0 & -1 \\
q2 & 3 & 1 & 0 \\
q3 & 4 & 0 & 1 \\
q4 & 5 & 1 & -1 \\
q5 & 6 & 0 & 0
\end{array}\right\} = B_0$$

$$\begin{array}{lrrr}
q6 & 7 & 1 & 1 \\
q7 & 8 & 0 & -1 \\
\vdots & \vdots & \vdots & \vdots
\end{array}$$

$$B_k = B_0 + k[6, 0, 0]$$

Less naïve:

Replace $P_g(q)$ by

$$\prod_{k\geq 1} P_g(q^k)$$

to get:

$$f_{\langle 13\rangle} = \prod_{k\geq 1} \frac{1}{(1-q^k)2}, \quad f_{\langle 2,1\rangle} = \prod_{k\geq 1} \frac{1}{1-q^{2k}}, \quad f_{\langle 3\rangle} = \prod_{k\geq 1} \frac{1-q^k}{1-q^{3k}}.$$

Now replace $f_{\langle\cdot\rangle}$ by $q^{-\frac{r}{24}} f_{\langle\cdot\rangle}$ to get

$$f_{\langle 13\rangle} = \eta(q)^{-2}, \quad f_{\langle 2,1\rangle} = \eta(q2)^{-1}, \quad f_{\langle 3\rangle} = \frac{\eta(q)}{\eta(q3)}$$

with Dedekind's $\eta$ function:

$$\eta(q) = q^{\frac{1}{24}} \prod_{k\geq 1} \left(1-q^k\right).$$

$|\mathbb{M}| =$

$8080174247945 \cdots 617107570057543680000000000$

$= 2^{46}3^{15}5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$

a product of the fifteen supersingular primes $p$ for which $\Gamma_0(p)^+$ has genus zero.

**Riemann maps:**

$$w(z) = cz + a_0 + \sum_{k \geq 1} a_k/z^k$$

from the exterior of a disk to the simply connected complement of a Jordan curve in $\mathbf{C} \cup \{\infty\}$. We take $a_0 = 0$ and $c = 1$, and compose with $z \to \exp(-2\pi i z) = 1/q$.

Our interest is in

$$f(z) = \frac{1}{q} + \sum_{k \geq 1} a_k q^k, \quad q = e^{2\pi i z}, \quad z \in \mathcal{H}$$

where $\widehat{G_f \backslash \mathcal{H}}$ has genus zero and $f(\gamma z) = f(z)$ if and only if $\gamma \in G_f$.

For $\mathfrak{L}$ an ordered lattice, we define an equivalence relation on $\mathfrak{L} \times \mathfrak{L}$ by:

$$\{a, b\} \equiv \{c, d\} \quad \text{if} \quad a \wedge b = c \wedge d \quad \& \quad a \vee b = c \vee d.$$

When $\mathfrak{L}$ is the division lattice on $\mathbf{N}$, this relation becomes

**Norton's equivalence relation** on $\mathbf{N} \times \mathbf{N}$:

**Norton**: $\{a, b\} \equiv \{c, d\}$ if $\mathrm{gcd}(a, b) = \mathrm{gcd}(c, d)$ and $\mathrm{lcm}(a, b) = \mathrm{lcm}(c, d)$.

**Faber polynomials:** For $f$ as above, the Faber polynomial of degree $n$ in $f$ is defined (as are the **Grunsky coefficients**, $h_{m,n}$) by:

$$F_{n,f}(f) = \frac{1}{q^n} + n \sum_{m \geq 1} h_{m,n} q^m$$

They are generated by

$$\frac{qf'(q)}{f(p) - f(q)} = \sum_{n=0}^{\infty} F_n(f(p)) q^n$$

with $F_0(f) = 1$, $F_1(f) = f$,
$F_2(f) = f2 - 2a_1$, $F_3(f) = f3 - 3a_1 f - 3a_2$,
$F_4(f) = f4 - 4a_1 f2 - 4a_2 f + 2a_1 2 - 4a_3$,
& more generally:

$$F_n(f) = \det(fI - A_n),$$

where

$$A_n = \left( \begin{array}{c|cccccc} a_0 & 1 & & & & \\ 2a_1 & a_0 & 1 & & 0 & \\ \vdots & \vdots & \vdots & & & \\ (n-2)a_{n-3} & a_{n-4} & a_{n-5} & \dots & 1 & \\ (n-1)a_{n-2} & a_{n-3} & a_{n-4} & \dots & a_0 & 1 \\ na_{n-1} & a_{n-2} & a_{n-3} & \dots & a_1 & a_0 \end{array} \right)$$

The index grading is

$$\mathrm{ind}(h_{r,s}) = r + s,$$

so that $\mathrm{ind}(a_k) = k + 1$, and

$$\mathrm{ind}(h_{a,b}.h_{c,d}) = \mathrm{ind}(h_{a,b}) + \mathrm{ind}(h_{c,d}).$$

Norton's remarkable result is that when the Grunsky coefficients of $f$ are compatible with Norton's equivalence relation in that $h_{a,b} = h_{c,d}$ if $\{a, b\} \equiv \{c, d\}$, then $h_{a,b}$ is polynomially dependent on $\{a_k\}$, $k \in B$, the **Norton basis**,

$$B = \{\, 1,\, 2,\, 3,\, 4,\, 5,\, 7,\, 8,\, 9,\, 11,\, 17,\, 19,\, 23 \,\},$$

$$|B| = 12.$$

This compatibility is Norton's **definition** of replicability of $f$.

The Faber polynomial, $F_{n,f}(f)$ may be interpreted as the action of a generalized **Hecke operator**:

For the elliptic modular function, $j$, we have:

$\forall n \in \mathbf{N}$

$$nT_n(j) \; = \sum_{\substack{ad=n \\ 0\leq b<d}} j\left(\frac{az+b}{d}\right) = F_{n,j}(j) \; .$$

This property we generalize to replicable functions by defining replicable functions as those functions $f = f^{(1)}$, such that there are functions of the same form satisfying

$\forall n \in \mathbf{N}$

$$n\widehat{T}(n)(f) \; = \sum_{\substack{ad=n \\ 0\leq b<d}} f^{(a)}\left(\frac{az+b}{d}\right) = F_{n,f}(f) \; .$$

We find

$$h_{m,n}(f) = \widehat{T}_n(f)|_{q^m} \ .$$

Replicability encapsulates the property that

$$f^{(n)}(q^n) = F_{n,f}(f) - \sum{}'$$

is a series in $q^n$.

For prime $p$,

$$T_p = \frac{1}{p} V_p + U_p$$
$$V_p : f(q) \longrightarrow f(q^p).$$

We define a generalized Hecke operator (cf. Bott: **Cannibalistic class**)

$$\widehat{T}_p = \frac{1}{p} \widehat{V}_p + U_p$$
$$\widehat{V}_p = \Psi^p \circ V_p, \quad \Psi^p = \text{“}\textbf{Adams operator}\text{”}$$
$$\widehat{V}_p : f(q) \longrightarrow f^{(p)}(q^p)$$
$$a_n^{(p)} = p h_{pn,p} - p a_{p^2 n}$$

On $\mathbb{M}$:

$$\begin{array}{ccc} f & \longrightarrow & f^{(k)} \\ \downarrow & & \downarrow \\ f_g & \longrightarrow & f_{g^k} \end{array}$$

**The Grunsky coefficients:**

There are identities, $h_{m,1} = a_m$, $h_{r,s} = h_{s,r}$. Norton's basis theorem follows a descent argument on the index. The rows are in decreasing index.

The coefficients $\widehat{h}_{r,s} = (r+s)h_{r,s}$ satisfy

$$\widehat{h}_{r,s} = (r+s)a_{r+s-1} + \sum_{m=1}^{r-1} \sum_{n=1}^{s-1} a_{m+n-1}\widehat{h}_{r-m,s-n}.$$

$$\vdots$$

$$a_6 = h_{1,6} \quad h_{2,5} \quad h_{3,4} \quad h_{4,3} \quad h_{5,2} \quad h_{6,1} = a_6$$

$$a_5 = h_{1,5} \quad h_{2,4} \quad h_{3,3} \quad h_{4,2} \quad h_{5,1} = a_5$$

$$a_4 = h_{1,4} \quad h_{2,3} \quad h_{3,2} \quad h_{4,1} = a_4$$

$$a_3 = h_{1,3} \quad h_{2,2} \quad h_{3,1} = a_3$$

$$a_2 = h_{1,2} \quad h_{2,1} = a_2$$

$$a_1 = h_{1,1} = a_1$$

It is conjectured that the replicable functions are either:

- “modular fictions” $f = 1/q + cq$.
  For $c \in \{0, 1, -1\}$ we have exp, cos, and sin.

or

- principal moduli with invariance groups, $G_f$ such that $\widehat{G_f \backslash \mathcal{H}}$ is a genus zero Riemann surface and $\Gamma_0(N_f) \subseteq G_f$ is commensurable with $\Gamma$.

It has been proved that all such principal moduli with $q$-coefficients in $\mathbf{Z}$ are replicable.

## The Schwarz derivative

We define the Schwarz derivative (a quadratic differential) of $f$ with respect to $z$ as

$$\{f, z\} = 2u' - u2, \qquad u = f''/f',$$

for which, if

$$f(z) = \frac{ag(z) + b}{cg(z) + d}, \qquad ad - bc \neq 0,$$

we have $\{f, z\} = \{g, z\}$ and conversely.

For $f$ of modular weight 0, $\{f, z\}$ has modular weight 4. When $f$ is a principal modulus this implies that

$$\{f, z\} = R(f) f'^2,$$

where $R$ is a rational function of $f$.

This is related to the Grunsky coefficients of the Hecke operator by

$$\zeta(-1)\{f, q\} = \sum_{m,n\geq 1} m\, n\, h_{m,n} q^{m+n-2} \, .$$

**Dispersionless Hirota hierarchy**

The $\tau$-function satisfies the dispersionless Hirota equation

$$\zeta(-1)\{w, z\} = -z^2 \sum_{m,n\geq 1} z^{-m-n} \frac{\partial \ln \tau}{\partial t_m \partial t_n} \, .$$

Comparing this with the above equation we see that

$$\frac{\partial \ln \tau}{\partial t_m \partial t_n} = -m\, n\, h_{m,n} \, .$$

The relation above between the Schwarzian derivative and the Grunsky coefficients is a differential generalization of Borcherds product for $j$.

The Borcherds product for

$$j(q) = \frac{1}{q} + \sum_{k \geq 0} c_k q^k$$

is

$$j(p) - j(q) = \frac{1}{p} \prod_{\substack{m>0 \\ n \in \mathbf{Z}}} (1 - p^m q^n)^{c_{mn}}.$$

**Z(1-p**$^m q^n)^{c_{mn}}$

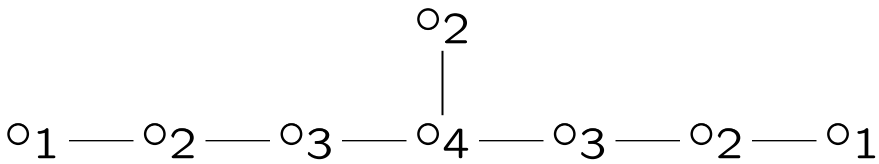
## Affine Dynkins and sporadic correspondences

There is a distinguished set of nine conjugacy classes of $\mathbb{M}$ in which the product of any pair of Fischer involutions lies. These classes are described in the Atlas. By monstrous moonshine, each class corresponds to a unique modular function and thus we have a replicable function attached to each node of the affine $E_8$ diagram. Here class names lie below the modular levels.

$E_8$

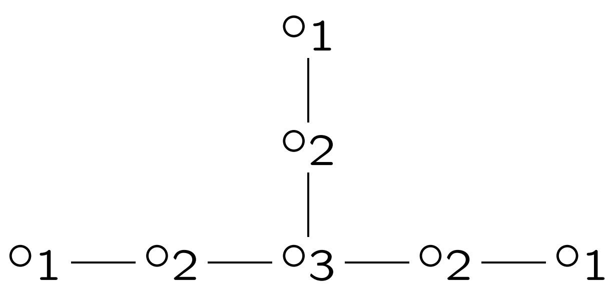
$$\begin{tikzcd}[column sep=small]
 & & & & & \begin{smallmatrix}9\\3C\end{smallmatrix} \arrow[d, dash] & & \\
\begin{smallmatrix}1\\1A\end{smallmatrix} \arrow[r, dash] & \begin{smallmatrix}2\\2A\end{smallmatrix} \arrow[r, dash] & \begin{smallmatrix}3\\3A\end{smallmatrix} \arrow[r, dash] & \begin{smallmatrix}4\\4A\end{smallmatrix} \arrow[r, dash] & \begin{smallmatrix}5\\5A\end{smallmatrix} \arrow[r, dash] & \begin{smallmatrix}6\\6A\end{smallmatrix} \arrow[r, dash] & \begin{smallmatrix}8\\4B\end{smallmatrix} \arrow[r, dash] & \begin{smallmatrix}4\\2B\end{smallmatrix}
\end{tikzcd}$$

$E_7$




$F_4$


$E_6$




$G_2$

A question: What operator takes a Monstrous Moonshine function to its neighbours? In the "McKay correspondence" it is tensoring by the restriction of the fundamental representation of $SU_2$.

**References**


| | |
|---|---|
| Conway & Norton | Bull. Lond. Math. Soc. 1979 |
| Bonora & Sorin | hep-th/0211283 |
| Carroll & Kodama | hep-th/9506007 |
| Teo, Lee-Peng | hep-th/0305005 |