TOWARD THE HOMOTOPY GROUPS OF THE HIGHER REAL K-THEORY EO_2

VASSILY GORBOUNOV AND PETER SYMONDS

Abstract. In this note we compute the initial term of the spectral sequence which converges the homotopy groups of the higher real K-theory EO_2 at the prime 3. We also describe precisely the way in which the integral modular forms are embedded in this initial term.

1. Introduction

Our main result is the calculation of the initial term of the spectral sequence $H^*(G,E)^{\mathrm{Gal}} \Rightarrow \pi_* EO_2$, which converges to the homotopy groups of the higher real K-theory EO_2 at the prime 3. Here G is the group $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$ and E is an infinitely generated module for G over $\mathbb{Z}_3$, which arises from the theory of formal groups. We also show how the integral modular forms of Deligne appear naturally in this initial term. This calculation was originally sketched by Hopkins and Miller [5], but the details were never published, so we have proceeded by our own methods.

For each prime p and natural number n there is a p-adic Lie group $\mathbb{S}_n$, which is the group of absolute endomorphisms of the Honda formal group law $\bar{F}$ over $\mathbb{F}_p$. There is also a ring E_n^0, which can be considered as the moduli space of lifts of $\bar{F}$ to a formal group law of height n over a p-local ring. Thus $\mathbb{S}_n$ acts on E_n^0. This action is extended to an action on $E_n = E_n^0[u, u^{-1}]$. According to the Morava Change of Rings Theorem, there is a spectral sequence $H_c^*(\mathbb{S}_n, E_n)^{\mathrm{Gal}} \Rightarrow \pi_* L_{K(n)}$, where $L_{K(n)}$ is the localization of the sphere spectrum at the nth Morava K-theory $K(n)$ [7].

Morava [10] introduced a spectrum $\mathbb{E}_n$ such that $\pi_* \mathbb{E}_n = E_n$. Later, Hopkins and Miller [5] sketched how to construct a nice action of $\mathbb{S}_n$ on $\mathbb{E}_n$ that induces the original action on E_n.

It is known that if $n = p - 1$, then $\mathbb{S}_n$ has a unique maximal finite subgroup G_n, up to conjugation. When $p = 3$ and $n = 2$, this is the group G of order 12 mentioned above. Hopkins and Miller define EO_n to be the homotopy fixed point spectrum of the action of G_n on $\mathbb{E}_n$, so there is a spectral sequence $H^*(G_n, E_n)^{\mathrm{Gal}} \Rightarrow \pi_* EO_n$. When $p = 2$

and $n = 1$, EO_1 turns out to be KO, ordinary real K-theory, whilst $K(1)$ is ordinary complex K-theory. This justifies the name "higher real K-theories". When $n = 2$ this construction can be generalized to give an integral version of elliptic cohomology, which agrees with the usual elliptic cohomology when 6 is inverted [6]. The spectrum which represents this cohomology theory is called the spectrum of topological modular forms, TMF.

The calculation presented here is for the case $p = 3$ and $n = 2$, and can be viewed as a computation of the initial term of the spectral sequence which converges to $\pi_* TMF_{(3)}$. It has the interesting property that $(E^G)^{\mathrm{Gal}}$, which is part of the initial term, is related to the ring of integral modular forms of Deligne [1]. A problem here is that the Morava Change of Rings Theorem concerns a specific formal group of height n over the field $\mathbb{F}_p$, the Honda formal group. When $n = 2$, a supersingular elliptic curve yields another formal group, which is naturally connected to the integral modular forms. These two formal groups only become isomorphic after a field extension.

The authors wish to thank Mark Mahowald for helpful discussions.

2. The moduli space

As a general reference for this section we recommend [3]. Let F_{u_1} be the formal group law over $\mathbb{Z}_3$ which is obtained from the usual universal commutative 3-typical formal group law over $\mathbb{Z}_3[v_1, v_2, \dots]$ by setting $v_1 = u_1$, $v_2 = 1$, $v_i = 0$, $i \geq 3$.

$$F_{u_1}(x, y) = x + y - u_1(x^2y + xy^2) - (x^6y^3 + x^3y^6) + \dots .$$

Its reduction modulo 3 and u_1 is

$$\bar{F}(x, y) = x + y - (x^6y^3 + x^3y^6) + \dots .$$

Now $\mathbb{S}_2 \subset \mathbb{F}_9[[x]]$ is the ring of absolute endomorphisms of $\bar{F}$: it also can be characterized as the group of units in the maximal order O of a certain division algebra. This O, in turn, can be described as follows. Let W be the ring of Witt vectors over $\mathbb{F}_9$, ie the integers of the unramified extension of degree 2 of $\mathbb{Q}_3$. Then $\mathbb{S}_2$ contains an element S such that, additively, $O \cong W \oplus SW$, and the multiplication is described by $S^2 = 3$, $wS = S\bar{w}$, $w \in W$. Thus $\mathbb{S}_2$ contains a finite group $G \cong \mathbb{Z}/3 \rtimes \mathbb{Z}/4$ generated by $a = \dfrac{\zeta S - 1}{2}$, of order 3, and $b = \zeta^2$, of order 4, where $\zeta \in W$ is a primitive 8^{th} root of unity.

Now we must identify these elements in $\mathbb{F}_9[[x]]$. Any $w \in W$ corresponds to $f^{-1}(wf(x))$, where $f(x)$ is the logarithm of $\bar{F}$,

$$f(x) = x + \tfrac{1}{3}x^9 + \tfrac{1}{9}x^{81} + \dots .$$

Therefore $f(\zeta x) = \zeta f(x)$, and so multiplication by ζ corresponds to ζx and b corresponds to $\zeta^2 x$. Now S corresponds to x^3 and $\zeta S - 1$ has series

$$\zeta x^3 +_{\bar{F}} (-x) = -x + \zeta x^3 + \zeta^3 x^{15} + \dots .$$

Also $[2]_{\bar{F}} = x +_{\bar{F}} x = -x + x^9 + \dots$, so $[\frac{1}{2}]_{\bar{F}} = -x - x^9 - x^{81} - \dots$ and thus a has series $x - \zeta x^3 + x^9 - \zeta^3 x^{15} + \dots$.

A theorem of Lubin and Tate [9, 3] shows that the group S_2 acts continuously on $E_0 = W[[u_1]]$ according to the formula

$$F_{u_1}(\hat{g}\alpha x, \hat{g}\alpha y) = \hat{g}\alpha F_{g(u_1)}(x, y),$$

where $g \in S_2 \subset \mathbb{F}_9[[x]]$, $\hat{g}$ is a lift of g to $E_0[[x]]$, and $\alpha \in E_0[[x]]$ is such that its reduction to $\mathbb{F}_9[[x]]$ is the identity. Here $g(u_1) \in E_0$. Both $g(u_1)$ and $\hat{g}\alpha$ are uniquely determined by this equation, which we shall simplify by writing $\tilde{g} = \hat{g}\alpha$ so that

$$F_{u_1}(\tilde{g}x, \tilde{g}y) = \tilde{g}F_{g(u_1)}(x, y).$$

The action can be extended to $E = E_0[u, u^{-1}]$ by the formula $g(u) = (\tilde{g}'(0))u$.

Proposition 2.1. *Suppose that $g \in S_2$, $\tilde{g} = \gamma_1 x + \gamma_2 x^2 + \gamma_3 x^3 + \dots$, $\gamma_i \in E_0$. Then $g(u_1) = \gamma_1^2 u_1 + 3\gamma_3\gamma_1^{-1}$ and $\gamma_2 = 0$ in E_0.*

Proof. Notice that

$$F_{u_1}(\tilde{g}x, \tilde{g}y) = \tilde{g}x + \tilde{g}y - u_1\gamma_1^3(x^2y + xy^2)$$

modulo degree 4 in x and y and

$$\tilde{g}F_{g(u_1)}(x, y) = \gamma_1(x + y - g(u_1)(x^2y + xy^2)) +$$

$$\gamma_2(x^2 + y^2 + 2xy) + \gamma_3(x^3 + y^3 + 3(x^2y + xy^2))$$

modulo degree 4 in x and y. Examing the coefficients of x^2y and xy yields the result. □

Corollary 2.2. *All of $\mathbb{S}_2$ fixes $u^{-2}u_1 \in \bar{E}$.*

3. The Action of G on E

Let $\bar{E} = \mathbb{F}_9 \otimes_W E = \mathbb{F}_9[[u_1]][u, u^{-1}]$.

Proposition 3.1. *In $\bar{E}$ we have:*

$$a(u_1) = u_1 + \zeta^3 u_1^2 \mod u_1^3$$

and

$$a(u) = u(1 - \zeta^3 u_1) \mod u_1^2.$$

Proof. Let $\tilde{a}(x) = \alpha_1 x + \alpha_2 x^2 + \dots$, $\alpha_i \in \bar{E}_0$. Then $\alpha_1 = 1$, $\alpha_3 = -\zeta$, $\alpha_9 = 1$ modulo u_1, and the other α_i, $i \leq 9$ satisfy $\alpha_i = 0$ modulo u_1. We work in $\bar{E}$ throughout.

$$F_{u_1}(\tilde{a}(x), \tilde{a}(y)) = \tilde{a}x + \tilde{a}y - u_1[(x-\zeta x^3)^2(y-\zeta y^3) + (x-\zeta x^3)(y-\zeta y^3)^2] - \alpha_1^9(x^6y^3 + x^3y^6)$$

modulo u_1^2 and degree 4 in x and y.

The coefficient of x^6y^3 is $-1 + \zeta^3 u_1$ modulo u_1^2. Now

$$\tilde{a}F_{a(u_1)}(x, y) = \tilde{a}[x + y - a(u_1)(x^2y + xy^2)] - \alpha_1(x^6y^3 + x^3y^6)$$

modulo degree 10 in x and y.

The only terms in $\tilde{a}$ which could possibly yield an x^6y^3 term in $\tilde{a}[x+y-a(u_1)(x^2y+xy^2)]$ without a u_1^2 (remember that $a(u_1)$ is divisible by u_1) are the powers 1, 3 and 9. It is easy to check that these do not infact do so, hence the coefficient of x^6y^3 is $-\alpha_1$. We have $-\alpha_1 = -1 + \zeta^3 u_1 \mod u_1^2$ and so $\alpha_1^2 = 1 + \zeta^3 u_1 \mod u_1^2$. The result follows from Proposition 2.1 and the definition of the action on u. □

Proposition 3.2. *We have $b(u_1) = -u_1$, $b(u) = \zeta^2 u$ in E.*

Proof. $\zeta F_{\zeta^2 u_1}(x, y) = F_{u_1}(\zeta x, \zeta y)$ by construction. So $\tilde{b}(x) = \zeta^2 x$. □

4. The Module Structure of $\bar{E}$

Let $k = \mathbb{F}_9$ and consider the group algebra of $\langle a \rangle$. Let $A = a - 1 \in k\langle a \rangle$. Then $k\langle a \rangle = k[A]/(A^3)$. We know that $a(u_1) = u_1 + \zeta^3 u_1^2 + X u_1^3$, $X \in \bar{E}_0$, so $Au_1 = \zeta^3 u_1^2 + X u_1^3$, and $A^2 u_1 = -\zeta^2 u_1^3$ mod deg 4.

Let $y = A^2 u_1 \neq 0$. Since y is invariant under a, so is $k[[y]] \subset \bar{E}_0$. Let F be the $k\langle a \rangle$-submodule generated by u_1, which has k-basis u_1, Au_1, $A^2 u_1$. Then as F has dimension 3 it must be free and $\bar{E}_0 = k \oplus (F \otimes k[[y]])$. Note that $b(y) = -y$, and that F is easily checked to be a kG-module.

It will be convenient for us to discuss the ring $\mathcal{L}E = E[\frac{1}{u_1}]$, and similarly $\mathcal{L}\bar{E}$. Note that $\mathcal{L}\bar{E}_0 = F \otimes k[[y]][\frac{1}{y}]$.

By Proposition 2.1, $u^2 \mathcal{L}\bar{E}_0$ contains an invariant element $u^2 u_1^{-1}$, and multiplication by $u^2 u_1^{-1}$ yields an isomorphism of kG-modules $\mathcal{L}\bar{E}_0 \to$

$u^2\mathcal{L}\bar{E}_0$. The invariants of $u^2\mathcal{L}\bar{E}_0$ under $\langle a\rangle$ are therefore $u^2u_1^{-1}k[[y]][\frac{1}{y}]$ so occur in u_1-filtration -1 modulo 3. Now if $w \in u\mathcal{L}\bar{E}_0$ is invariant under a and is an eigenvector for b, then so is w^2, and so w must have u_1 filtration 1 modulo 3. After multiplying by a suitable power of y we may assume that w is in filtration 1, so its leading term is uu_1 and the eigenvalue under the action of b must be $-\zeta^2$, ie $b(w) = -\zeta^2 w$. Multiplication by w^r yields an isomorphism of $k\langle a\rangle$-modules $\mathcal{L}\bar{E}_0 \to u^r\mathcal{L}\bar{E}_0$.

Finally set $x = y^{-1}w^3$, which has u_1-filtration 0. To sum up we have: $A = a-1$, $y = A^2u_1$, $Aw = Ax = Ay = 0$, and $bu_1 = -u_1$, $bw = -\zeta^2 w$, $bx = -\zeta^2 x$, $by = -y$.

This is represented pictorially in figure 1. The blocks in unbroken lines represent indecomposable summands of $\bar{E}$ as a kG-module, and each block has a k-basis with u_1-filtration and u-grading corresponding to the points in the block with integral rectangular coordinates. The dotted lines indicate the blocks of $\mathcal{L}\bar{E}$. Each complete block of dimension 3 is projective.

The picture has vertical periodicity 3 as an $\langle a\rangle$-module (given by multiplication by x) and periodicity 12 as a G-module (multiplication by x^4).

This decomposition into blocks also lifts to E and to $\mathcal{L}E$. This is because there is a one-to-one correspondence between the finite dimensional indecomposable modules for G over W and over k. It can be seen explicitly as follows: Let m be the left-most basis element in of any block of $\mathcal{L}\bar{E}$. Lift m to an element $\tilde{m}$ of $\mathcal{L}E$ that is an eigenvector under the action of b. Then the WG-lattice generated by $\tilde{m}$ is a direct summand of $\mathcal{L}E$ that is equal to the original block modulo 3.

Let B denote the submodule of $\bar{E}$ with basis $\{1, wy^{-1}Au_1, w\}$. In other words B consists of the two incomplete blocks in u-grading 0 and 1. Then $\bar{E} = B \otimes k[x, \frac{1}{x}] \oplus \Pi(\text{projective})$.

Now $x \in \bar{E}$ lifts to $\tilde{x} \in E$ such that $a\tilde{x} = \tilde{x}$, $b\tilde{x} = -\zeta^2\tilde{x}$, and B lifts to $\tilde{B}$. Thus $E = (\tilde{B} \otimes \mathbb{Z}_3[\tilde{x}, \frac{1}{\tilde{x}}]) \oplus \Pi(\text{projective})$.

Remark 4.1. *We have a product of projectives because E involves power series in u_1. Over k a product of projectives is also projective, but over W this is not true, since since it is not even projective over W (According to* [8]*, $\Pi_\Lambda \mathbb{Z}_p$ is not a free $\mathbb{Z}_p$-module when Λ is infinite). However Π(projective) is at least cohomologically trivial.*

5. Cohomology

In Tate cohomology, $\tilde{H}^*(\langle a\rangle, E) = \hat{H}^*(\langle a\rangle, B) \otimes \mathbb{Z}_3[\tilde{x}, \tilde{x}^{-1}]$, where we identify $\tilde{x}$ with its image in $\hat{H}^0(\langle a\rangle, E)$.

The cohomology of $\tilde{B}$ is easy to calculate: One part is $\hat{H}^*(\langle a\rangle, W) = k[z, z^{-1}]$, deg $z = 2$, and $b(z) = -z$, as is known from the calculation of the cohomology of the dihedral group of order 6. The cohomology of the other part is calculated using dimension shifting in the block of $\mathcal{L}E$ that contains it to reduce to the case of the 1-dimensional WG-lattice on $wy^{-1}u_1$. The result is a free $k[z, z^{-1}]$-module on a generator t of degree 1, and $bt = -\zeta^2 t$.

Hence $\hat{H}^*(\langle a\rangle, E) = k[\tilde{x}, \tilde{x}^{-1}, z, z^{-1}] \otimes E(t)$.

Now $\hat{H}^*(G, E) = \hat{H}^*(G, E)^{\langle b\rangle}$, and calculating the invariants yields:

Theorem 5.1. $\hat{H}^*(G, E) = \mathbb{F}_9[\tilde{x}^4, \tilde{x}^{-4}, \tilde{x}^2 z, (\tilde{x}^2 z)^{-1}] \otimes E(\tilde{x}^{-1}t)$

There is an action of $\mathrm{Gal}(W/\mathbb{Z}_3) = \langle\sigma\rangle \cong \mathbb{Z}/2$ on G by conjugation with S. There is also an action on E via the action on the coefficients of the series. But conjugation by S has the same effect on a as conjugation by b, so does not affect $\hat{H}^*(G, \mathbb{Z}_3)$, and thus $\mathrm{Gal}(W/\mathbb{Z}_3)$ acts on $\hat{H}^*(G, E)$ via its action on E only. Now $\hat{H}^*(G, W) = \hat{H}^*(G, \mathbb{Z}_3) \otimes W$, so z could have been chosen invariant under the action. Consider the action of σ on $\tilde{x}$. We seek a replacement $\hat{x}$ for x that is invariant under σ. Now $\tilde{x} = (\frac{\sigma+1}{2})x + (\frac{\sigma-1}{2})x$, so at least one of the two terms on the right hand side, taken modulo 3, has u_1-filtration 0. If it is the first, take $\hat{x} = (\frac{\sigma+1}{2})x$. If it is the second, take $\hat{x} = \zeta^2(\frac{\sigma-1}{2})x$. It is easy to check that $\hat{x}^4$ is still invariant under G. A similar argument applies to $\hat{x}^{-1}t$ and we obtain

Theorem 5.2. *We have:*

$$\hat{H}^*(G, E)^{Gal} = \mathbb{F}_3[\hat{x}^4, \hat{x}^{-4}, \hat{x}^2 z, (\hat{x}^2 z)^{-1}] \otimes E(\hat{x}^{-1}t),$$

$$H^*(G, E)^{Gal} = \mathbb{F}_3[\hat{x}^4, \hat{x}^{-4}, \hat{x}^2 z] \otimes E(\hat{x}^{-1}t), \quad * > 0.$$

6. Invariants

In $\bar{E}$, y is not invariant under G, but y^2 is. Also $r = u^{-2}u_1$ is invariant. Together with x, these generate the invariants (see figure 2).

Theorem 6.1. $\bar{E}^G = \mathbb{F}_9[[y^2]][x^4, x^{-4}, r]/(r^6 = x^4 y^2)$

There are no invariant elements with odd u-grading.

When we lift this to W, each invariant element lifts to an invariant element in the corresponding block of $\mathcal{L}E$, but its u_1-filtration may increase by 1 or 2. In particular y lifts to $\tilde{y} \in E$, invariant under a, $b\tilde{y} = -\tilde{y}$, and we have seen that x^4 lifts to $\tilde{x}^4 \in E$. But r cannot lift to an invariant element of E because the 2-dimensional integral representation above it contains no non-zero invariants. On the other hand $p = r^2$ lifts to $\tilde{p}$ and $q = r^3$ lifts to $\tilde{q} = \tilde{x}^{-2}\tilde{y}$. Thus the image of E^G in $\bar{E}^G$ misses precisely the part with basis the monomials rx^i (this could also be seen from the long exact sequence in cohomology for $3E \to E \to \bar{E}$). By construction, $\tilde{p}^3 = \tilde{q}^2 \pmod 3$.

Theorem 6.2. *$E^G = W[[\tilde{y}^2]][\tilde{x}^4, \tilde{x}^{-4}, \tilde{p}, \tilde{q}]$, where $\tilde{q}^2 = \tilde{x}^{-4}\tilde{y}^2$, and $\tilde{p}^3 - \tilde{q}^2 = 3\delta$ for some $\delta \in E^G$.*

(see figure 3). As before,

Theorem 6.3. *$(E^G)^{Gal} = \mathbb{Z}_3[[\hat{y}^2]][\hat{x}^4, \hat{x}^{-4}, \hat{p}, \hat{q}]$, where $\hat{q}^2 = \hat{x}^4\hat{y}^2$, and $\hat{p}^3 - \hat{q}^2 = 3\delta$ for some $\delta \in (E^G)^{Gal}$.*

7. The Ring Structure of the Invariants

Theorem 7.1. *The invariant elements p and q can be chosen in such a way that $p^3 - q^2$ is divisible by 3^3. This is the best possible: they can not be chosen so as to make $p^3 - q^2$ divisible by 3^4. In fact, if $\delta = (p^3 - q^2)/3^3 \in E$, then the leading term of δ is a unit times u^{-12}.*

Proof. The first part will follow from section 8 using modular forms, but we give an elementary proof here. Chose $p \in E_0u^{-4}$ to be any element invariant under both G and Gal that reduces to r^2 modulo 3. Normalize it so that the coefficient of $u_1^2u^{-4}$ is 1.

Then $p = (u_1^2 + 3s)u_1^{-4}$ for some $s \in E_0$ which is an even function of u_1, and so
$p^3 = (u_1^6 + 3u_1^4 s)u^{-12} \bmod 3^3$.
Let $\tilde{q} = (u_1^3 + \frac{3^2}{2}u_1 s)u^{-1}$, so that $p^3 - \tilde{q}^2 = 0 \pmod{3^3}$.

Now since p is invariant, so is $\tilde{q}^2 \pmod{3^3}$. In other words $a(\tilde{q}^2) - \tilde{q}^2 = 0 \pmod{3^3}$ or $3^3|(a(\tilde{q}) - \tilde{q})(a(\tilde{q}) + \tilde{q})$. But $a(\tilde{q}) + \tilde{q} = (2u_1^3 + \dots)u^{-6}$ (mod3), so we must have $3^3|a(\tilde{q}) - \tilde{q}$.

Now $\tilde{q} \in E_0u^{-6}$, and from the decomposition of E as a sum of indecomposables we can see that $H^1(G, E_0u^{-6}) = 0$. Let $H = G \rtimes \langle\sigma\rangle$, so that $H^1(H, E_0u^{-6}) = 0$.

The long exact sequence for cohomology becomes

$$0 \to (E_0u^{-6})^H \to (E_0u^{-6})^H \to (E_0u^{-6}/3^3)^H \to 0,$$

and so $\tilde{q}$ lifts to an invariant element $q \in E_0u^{-6}$ such that $q = \tilde{q}$ (mod 3^3) and $p^3 - q^2 = 0 \pmod{3^3}$.

To show that this is the best possible power of 3, note that p must be an even function of u_1 and that q must be odd, so it suffices to prove that the constant term (in u_1) of p is not divisible by 3^2.

Let $\mathfrak{m}$ denote the maximal ideal of E_0: it is generated over W by 3 and u_1. Then $p = (c + u_1^2)u^{-4} \pmod{\mathfrak{m}^3}$ for some constant c, and an argument similar to the proof of 3.1, but working modulo $\mathfrak{m}^2$ instead of 3, shows us that $a(u_1) = -3\zeta + u_1 \pmod{\mathfrak{m}^2}$, so $a(u_1) = -3\zeta + u_1 + e$, say, where the constant term of e is divisible by 3^2.

Also $a(u) = \alpha_1 u \pmod{\mathfrak{m}}$, where $\alpha_1 = 1 \pmod{\mathfrak{m}}$. Thus

$$a(p) = (c + (-3\zeta + u_1 + e)^2)\alpha_1^{-4}u^{-4} \mod \mathfrak{m}^3.$$

But since p is invariant this must be equal to $(c + u_1^2)u^{-4} \pmod{\mathfrak{m}^3}$, and in particular the constant terms should be equal (mod 3^3). Using the subscript 0 to denote the constant term, this yields

$$(c + (-3\zeta + e_0)^2)(\alpha_1)_0^{-4} = c \quad (\text{mod} 3^3)$$

and hence

$$c((\alpha_1)_0^4 - 1) = (-3\zeta + e_0)^2 \quad (\text{mod} 3^3).$$

Now $3^2|e_0$ and $3|((\alpha_1)_0^4 - 1)$ so we see that if $3^2|c$ then $3|\zeta$, a contradiction. □

According to 7.1, if $p^3 - q^2 = 3^3\delta$ then the leading term of δ is u^{-12}, up to a unit. This enables us to express $\hat{x}^{-4}$ in terms of δ and y^2, hence:

Theorem 7.2.

$$(E^G)^{Gal} = \mathbb{Z}_3[[q^2\delta^{-1}]][\delta, \delta^{-1}, p, q]/(p^3 - q^2 = 3^3\delta)$$

8. Modular Forms

In this section we describe a connection between the ring of integral modular forms computed by Deligne [1] and the ring of invariants E^G.

We recall some standard material about elliptic curves and modular forms. An elliptic curve over a scheme S is a smooth morphism $p\colon C \to S$, whose geometric fibers are connected curves of genus one, together with a section $e\colon S \to C$. We denote by $\underline{\omega}_{C/S}$ the invertible sheaf $p_*(\Omega^1_{C/S})$ on S. The following definition is taken from [1]:

Definition 8.1. *An integral modular form of weight $k \in \mathbb{Z}$ and level one is a rule which assigns to any elliptic curve over any scheme S a section $f(C/S)$ of $(\underline{\omega}_{C/S})^{\otimes k}$ over S such that the following two conditions are satisfied.*
1. $f(C/S)$ depends only on the S-isomorphism class of the elliptic curve C/S.
2. The formation of $f(C/S)$ commutes with arbitrary change of base $g\colon S' \to S$ (meaning that $f(C'/S') = g^*f(C/S)$.

We are interested in the situation in which the base S is an affine scheme, $S = \mathrm{Spec}(R)$, R is a ring, and $\underline{\omega}_{C/R}$ is a free R-module of rank one with basis ω. Then any section of $\underline{\omega}^k_{C/R}$ can be written as $f(C/R,\omega)\cdot\omega^{\otimes k}$, where f is a rule which assigns to every pair $(C/R,\omega)$ consisting of an elliptic curve C over a ring R and a nowhere vanishing section of $\Omega^1_{C/R}$ on C, an element $f(C/R,\omega)\in R$, such that the following three conditions are satisfied:
1. $f(C/R,\omega)$ depends only on the R-isomorphism class of the pair $(C/R,\omega)$.
2. f is homogeneous of degree $-k$ in the second variable; for any $\lambda\in R^\times$, $f(C/R,\lambda\omega)=\lambda^{-k}f(C/R,\omega)$.
3. The formation of $f(C/R,\omega)$ commutes with arbitrary extension of scalars $g: R\to R'$ (meaning that $f(C_{R'/R'},\omega') = g(f(C/R,\omega)))$.

Let $(C/R,\omega)$ be a pair of the type considered above. Choose coordinate functions x and y such that the image of y in $\underline{\omega}^{-1}_{C/R}\otimes\underline{\omega}^{-1}_{C/R}\otimes\underline{\omega}^{-1}_{C/R}$ is $\omega^{-1}\otimes\omega^{-1}\otimes\omega^{-1}$ and the image of x in $\underline{\omega}^{-1}_{C/R}\otimes\underline{\omega}^{-1}_{C/R}$ is $\omega^{-1}\otimes\omega^{-1}$. Consider the corresponding Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

of the curve C. The symbols c_4, c_6 and Δ denote the usual polynomials in the a_i's [1]. An elementary computation shows that the rules which assign to the pair $(C/R,\omega)$ the differential forms $c_4\omega^4$, $c_6\omega^6$ and $\Delta\omega^{12}$ are indeed modular forms. Denote the ring of the integral modular forms of level one by $\mathfrak{M}$.

Theorem 8.2. *(Deligne)* $\mathfrak{M} = \mathbb{Z}[c_4, c_6, \Delta]/(c_4^3 - c_6^2 = 12^3\Delta)$

Let us also recall the Serre-Tate Theorem. A good reference is [2]. Let R be a ring and I an ideal such that the ideal (p, I) is nilpotent.

Theorem 8.3. *The following categories are equivalent:*
a. The category $\mathfrak{A}$ of elliptic curves over R and R-homomorphisms.
b. The category $\mathfrak{B}$ of triples (F, C_0, i) where F is a p-divisible group over R, C_0 is an elliptic curve over $R/(p,I)$, i is an isomorphism between the reduction of F modulo (p,I) and F_{C_0}. Morphisms are pairs (r_1, r_2), where r_1 is an R-homomorphism of p-divisible groups and r_2 is an $R/(p,I)$-homomorphism of elliptic curves which make the obvious diagram commutative.

Denote by FG and Ell the functors which provide the equivalence of the above categories.

The argument we will present below works for all primes, but for the purposes of this paper we restrict ourselves to the case when the prime p is equal to 3. Denote by $\mathbb{F}_{sep}$ the separable closure of $\mathbb{F}_3$ and by S

the ring of integers of the maximal unramified extension of $\mathbb{Z}_3$, (which has residue class field $\mathbb{F}_{sep}$). From now on take R to be the ring $S[[u_1]]$. Note that R is the inverse limit of rings R_n to which the Serre-Tate Theorem applies. Take for example R_n to be $R/(3, u_1)^n$. Denote by r_n and p_n the canonical homomorphisms $R_n \to R_{n-1}$ and $R \to R_n$ respectively. The ideal $(3, u_1)$ is invariant under G, so G also acts on R_n.

Take C_0 to be a supersingular elliptic curve over $\mathbb{F}_{sep}$. There is only one such up to isomorphism. Recall [1] that $\mathrm{Aut}(C_0)$ is isomorphic to $G \cong \mathbb{Z}/3 \rtimes \mathbb{Z}/4$, and denote by F_0 the formal group of C_0.

First we construct a map from $\mathfrak{M}$ to $R_n[u^{-1}, u]^G$ for each n. According to the classification of formal groups over $\mathbb{F}_{sep}$, see for example [3], F_0 is isomorphic to $\bar{F}$. Let i be such an isomorphism, and consider the triple (F_{u_1}, F_0, i). Denote by T_n the triple $(p_n^* F_{u_1}, F_0, i)$. Let $r = (r_1, r_2) : T_n \to FG(Ell(T_n)$ be part of the natural isomorphism $id_{R_n} \to FG \circ Ell$. Let $C_n = Ell(T_n)$.

Lemma 8.4. *There is a choice of coordinates on the elliptic curve C_n over R_n such that the corresponding formal group law F_n is strictly isomorphic to $p_n^* F_{u_1}$. Furthermore, this can be done in such a way that F_n has the form*

$$F_n(x, y) = x + y - u_1(x^2 y + xy^2) \ \ (\textit{mod deg 4})$$

modulo 3.

Proof. Choose coordinates x and y on C_n. Then r_1 becomes a series over R_n such that $r_1'(0)$ is an invertible element of R_n. Then

$$x' = (r_1'(0))^2 x,$$
$$y' = (r_1'(0))^3 y$$

provide the required coordinates.

Next we want to show that we can make a choice of coordinates such that the strict isomorphism between $p_n^* F_{u_1}$ and F_n has the form $r_1(z) = z \bmod \deg 3$ and modulo 3. Then F_n has to be of the form given in the statement of the lemma. Suppose that the strict isomorphism had the form $r_1(z) = z + \alpha z^2 \bmod \deg 3$ and modulo 3. An elementary computation shows that the change of coordinates $x' = x$ and $y' = y - \alpha x$ on C_n yields the change of the coordinate on F_n given by the series $Z(z) = z - \alpha z^2 \bmod \deg 3$ and modulo 3. The resulting formal group law is strictly isomorphic to $p_n^* F_{u_1}$ and the strict isomorphism is $Z(r(z))$, which is equal to $z \bmod \deg 3$ and modulo 3. □

Let $g \in G$. We denote by the same letter the element of $\mathrm{Aut} R$ associated to it in Section 2. Let $g(x)$ be the representative of g in $\mathbb{F}_{sep}[[x]]$

and denote by $\tilde{g}(x)$ the Lubin-Tate lift of $g(x)$. Recall that it has the following property

$$\tilde{g}^{-1}F_{u_1}(\tilde{g}(x),\tilde{g}(y)) = g^*F_{(u_1)}(x,y).$$

Denote by $\tilde{g}_n(x)$ the series $\tilde{g}(x)$ with the coefficients reduced modulo the ideal $(3,u_1)^n$. The following proposition is an immediate consequence of the Serre-Tate Theorem. We are using standard notation from the theory of elliptic curves (see [1]).

Proposition 8.5. *For every $g \in G$ the elliptic curves C_n and $g^*C_n = C'_n$ are isomorphic. In terms of the Weierstrass equations of C_n and C'_n such an isomorphism is given by a substitution $l_n(g)$:*

$$x = a^2x' + b$$

$$y = a^3y' + a^2cx' + d, \quad a,b,c,d \in R_n.$$

With coordinates on C_n chosen as in 8.4 and corresponding coordinates on C'_n, the substitution $l_n(g)$ which provides an isomorphism between C'_n and C_n has the property $\tilde{g}'_n(0) = a^{-1}$.

Proof. If $FG(C_n) = (F_1,E_1,i_1)$, then by definition of FG we have $FG(g^*C_n) = (g^*F_1,E_1,i_1)$. There is the following diagram, all the maps of which are isomorphisms in the category $\mathfrak{B}$ which corresponds to the ring R_n:

$$\begin{array}{ccc} T_n & \xleftarrow[(\tilde{g}_n,g)]{} & g^*T_n \\ {\scriptstyle (r_1,r_2)}\downarrow & & {\scriptstyle g^*(r_1,r_2)}\downarrow \\ (F_1,E_1,i_1) & & (g^*F_1,E_1,i_1). \end{array} \tag{8.6}$$

This shows that $FG(C_n)$ and $FG(g^*C_n)$ are isomorphic in $\mathfrak{B}$, therefore we obtain the required R_n-isomorphism $l_n(g)$ of C_n and g_*C_n from Serre-Tate Theorem and we have a commutative diagram

$$\begin{array}{ccc} T_n & \xleftarrow[(\tilde{g},g)]{} & g^*T_n \\ {\scriptstyle (r_1,r_2)}\downarrow & & {\scriptstyle g^*(r_1,r_2)}\downarrow \\ (F_1,E_1,i_1) & \xleftarrow[(FG(l_n(g)),g)]{} & (g^*F_1,E_1,i_1). \end{array} \tag{8.7}$$

By 8.4 we can choose coordinates on C_n such that the series r_1 provides a strict isomorphism of the corresponding formal group laws. For this choice of coordinates $FG(l_n(g))$ becomes a series such that its derivative at zero is equal to a^{-1}, as follows from the definition of the functor FG. □

We now construct a ring homomorphism $j_n\colon \mathfrak{M} \to R_n[u, u^{-1}]$. Let C_n be the elliptic curve defined above. Choose coordinates on C_n as in 8.4 and denote by ω the corresponding section of $\underline{\omega}$. Let f be a modular form of weight k. Define $j_n(f)$ to be equal to $f(C_n, \omega)u^k$.

Corollary 8.8. $j_n(\mathfrak{M}) \subset R_n[u, u^{-1}]^G$.

Proof. Indeed, taking into account the properties of modular forms and the formula for the action of $l_n(g)$ on the invariant differential from [1], we obtain:

$$g(f(C_n, \omega)u^k) = f(g^*C_n, \omega)g(u^k) = f(C_n, l_n(g)^{-1}\omega)a^{-k}u^k = \\ f(C_n, a^{-1}\omega)a^{-k}u^k = f(C_n, \omega)u^k.$$

□

It is hard to identify the images of the generators of $\mathfrak{M}$ in $R_n[u, u^{-1}]$ directly, because we know very little about the curve C_n. We can however say something in this direction if we change the base to $\bar{R}_n = R_n \otimes \mathbb{F}_3$. First we need to recall the structure of the ring of modular forms in characteristic 3 as computed in [1].

Theorem 8.9. *The ring $\mathfrak{M}_3$ of modular forms in characteristic 3 is isomorphic to*

$$\mathbb{F}_3[b_2, \Delta]$$

and $c_4 = b_2^2$, $c_6 = -b_2^3$.

An argument like the one presented above provides us with a map

$$j_n^{(3)}\colon \mathfrak{M}_3 \to \bar{R}_n[u, u^{-1}]^G.$$

Proposition 8.10. $j_3^{(3)}(b_2) = u_1u^2$

Proof. From Proposition 8.4 we know that there is a choice of coordinates over R_n for C_n such that its formal group law has the form

$$F'_n(x, y) = x + y - u_1(x^2y + xy^2) \pmod{\deg 4}$$

modulo 3. On the other hand according to a computation presented in [11], p115, this means that the element b_2 of the Weierstrass equation which corresponds to this choice of coordinates is equal to u_1. □

Finally we show that the maps j_{n-1} and r_nj_n are equal for all n and, therefore, that we have constructed a map $j\colon \mathfrak{M} \to R[u^{-1}, u]^G$. Indeed, since the triples T_{n-1} and $r_n^*T_n$ coincide, the elliptic curves C_{n-1} and $r_n^*C_n$ are isomorphic over R_{n-1} by the Serre-Tate theorem. Furthermore, since this isomorphism induces a strict isomorphism of the formal groups laws of C_{n-1} and C_n (with respect to the coordinates chosen), the maps j_{n-1} and r_nj_n coincide by construction. The same argument shows that the maps $j_n^{(3)}$ and $\bar{r}_n j_n^{(3)}$ are equal, where $\bar{r}_n$ is the reduction of r_n modulo 3.

This implies that $j(c_4)$ and $j(c_6)$ are suitable candidates for the elements p and q of Theorem 7.2, and since $(c_4^3 - c_6^2)/3^3 = 4^3\Delta$, Theorem 7.1 shows that $j(\Delta)$ is a suitable replacement for δ. Identifying $\mathfrak{M}$ with its image under j, we can rewrite 7.2 as:

Corollary 8.11. $(S \otimes E)^G = S[[c_6^2\Delta^{-1}]][\Delta, \Delta^{-1}, c_4, c_6]/(c_4^3 - c_6^2 = 12^3\Delta)$.

This can be expressed more succinctly as follows.

Corollary 8.12. *$(S \otimes E)^G$ is isomorphic as a ring to $\mathfrak{M}[\Delta^{-1}] \otimes S$ completed with respect to $c_6^2\Delta^{-1}$.*

References

[1] P. Deligne, Courbes Elliptiques: Formulaire (d'après J. Tate), in Modular Functions of One Variable IV, *Springer LNM 476*, 53–74.

[2] V. Drinfeld, Coverings of p-adic symmetric domains(Russian), *Func. Anal. i Prilozen*, **10**, no. 2, (1976), 29-40.

[3] M. Hazewinkel, Formal Groups and Applications, *Academic Press*, 1978.

[4] M. J. Hopkins, B. H. Gross, The rigid analytic period mapping, Lubin-Tate space, and stable homotopy theory, *Bull. Amer. Math. Soc.* **30** (1994), 76-86.

[5] M. Hopkins, H. Miller, Midwest Topology Seminar, Fall 1994.

[6] M. Hopkins, H. Miller, AMS Summer Research Institute, Seattle, 1996.

[7] M. Hopkins, M. Mahowald, H. Sadofsky, Constructions of elements in Picard Groups, in Topology and Representation Theory, *Contemporary Mathematics*, **158**, (1994).

[8] Kaplansky, Infinite Abelian Groups, *Univ. Michigan Press* 1954.

[9] J. Lubin, J. Tate, Formal moduli for one parameter formal Lie groups, *Bull. Soc. Math. France* **94** (1966), 49-60.

[10] J. Morava, Noetherian localisation of categories of cobordism comodules, *Ann. Math.*, **121** (1985), 1-39.

[11] J. H. Silverman, The Arithmetic of Elliptic Curves, *Springer Graduate Texts in Mathematics*, **106**, 1986.

Department of Mathematics, University of Kentucky, Lexington, KY 40506-0027

E-mail address: vgorb@ms.uky.edu, symonds@ms.uky.edu