

Mit diesen Bezeichnungen gilt

4

Korollar 1

Es gilt

$$\widetilde{\mathcal{H}}(1) = \widetilde{\mathcal{H}}(2) = \widetilde{\mathcal{H}}(2^2) = \dots = \widetilde{\mathcal{H}}(2^\infty) = \widetilde{\mathcal{M}} \quad \text{für } l \equiv 3(4),$$

$$\widetilde{\mathcal{H}}(1) \subsetneq \widetilde{\mathcal{H}}(2) \subseteq \widetilde{\mathcal{H}}(2^2) = \dots = \widetilde{\mathcal{H}}(2^\infty) = \widetilde{\mathcal{M}} \quad \text{für } l \equiv 1(4).$$

Insbesondere ist $\widetilde{\mathcal{H}}(2^\infty)$ eine endlich erzeugte
 \mathbb{F}_2 -Algebra.

Beweis:

Es ist bekannt, daß $\mathcal{M} = \mathbb{Z}_2[E_4, E_6]$, wo $E_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \frac{1}{n^{k-1}} q^n$
für gerades k und wo B_k die k -te Bernoulli'sche Zahl
ist $(\frac{q}{24} = \sum \frac{B_k}{k!} q^k)$, und daß $E_4 = \Theta_{\mathbb{F}_8}$, wo \mathbb{F}_8
die bis auf Äquivalenz über \mathbb{Z} eindeutig bestimmte positive
Form in 8 Variablen mit Determinante 1 ist.

Nach dem Satz genügt es daher zum Nachweis
von $\widetilde{\mathcal{H}}(1) = \widetilde{\mathcal{M}}$ bzw. $\widetilde{\mathcal{H}}(2^2) = \widetilde{\mathcal{M}}$ zu zeigen, daß
 $\widetilde{E}_6 \in \widetilde{\mathcal{H}}(1)$ für $l \equiv 3(4)$ bzw. $\widetilde{E}_6 \in \widetilde{\mathcal{H}}(2^2)$ für $l \equiv 1(4)$.

Sei zunächst $l \equiv 3(4)$:

Nach der Steudt-Kongruenz ist $E_{l-1} \equiv 1 \pmod{l}$,
daher $E_6 \equiv E_6 E_{l-1} \pmod{l}$; insbesondere ist also $\widetilde{E}_6 \in \widetilde{\mathcal{M}}_{2l+5}$
und $2l+5 \equiv 0 \pmod{4}$. Es ist aber für $k \equiv 0 \pmod{4}$
jede Form aus \mathcal{M}_k eine \mathbb{Z}_2 -Linearkombination von
Reihen Θ_Q mit $r(Q) = 2k$, $d(Q) = +1$. (Ein Beweis
hierfür ergibt sich etwa durch Induktion über k
unter Beachtung von $\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \frac{\Theta_{\mathbb{F}_8}^3 - \Theta_{\text{Leech}}}{2^4 \times 3^2 \times 5}$)
wo Θ_{Leech} die zum Leech-Gitter gehörige Thetareihe
bezeichnet (d.h. $\Theta_{\text{Leech}} = \Theta_Q$, wo Q für die bis auf Äquivalenz
über \mathbb{Z} eindeutig bestimmte positive Form in 24
Variablen mit $d(Q) = +1$ und $Q(x) \neq 1$ für alle $x \in \mathbb{Z}^{24}$
steht)