A group-invariant version of Lehmer’s conjecture on heights

Jan-Willem M. van Ittersum
Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, 3508 TA Utrecht, The Netherlands

Abstract

We state and prove a group-invariant version of Lehmer’s conjecture on heights, generalizing papers by Zagier (1993) and Dresden (1998) which are special cases of this theorem. We also extend their three cases to a full classification of all finite cyclic groups satisfying the condition that the set of all orbits for which every non-zero element lies on the unit circle is finite and non-empty.

Keywords: Lehmer’s conjecture, Mahler Measure, Weil height, G-orbit height

2010 MSC: 11G50, 11R04, 11R06, 12D10.

1. A Lehmer-type problem for the Weil height

The Mahler measure of a non-zero polynomial \( f \in \mathbb{Z}[x] \) given by

\[
f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)
\]

is defined as

\[
M(f) = |a_n| \prod_{i=1}^{n}\max(|\alpha_i|, 1).
\]

In 1933, Lehmer asked whether there exists a lower bound \( D > 1 \) such that for all \( f \in \mathbb{Z}[x] \) it holds that

\[
M(f) = 1 \quad \text{or} \quad M(f) \geq D.
\]

He showed that if such a \( D \) exists, then \( D \leq 1.1762808 \ldots \), the largest real root of the polynomial \( x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 \). Nowadays, this is still the smallest known value of \( M(f) > 1 \) for \( f \in \mathbb{Z}[x] \).

Mahler’s measure is related to the Weil height of an algebraic number. Let \( K \) be an algebraic number field and \( v \) a place of \( K \). We assume that this \( v \)-adic
valuation is normalized in such a way that for all non-zero \(\alpha \in K\) the product of \(|\alpha|_v\) over all places \(v\) is equal to 1 and the product of \(|\alpha|_v\) over all Archimedean \(v\) is equal to the absolute value of \(N_{K/Q}(\alpha)\). Then, for \(\alpha \in K^*\) the (logarithmic) Weil height \(h\) is defined by

\[
h(\alpha) = \frac{1}{[K:Q]} \sum_v \log^+ |\alpha|_v,
\]

where the sum is over all places \(v\) of \(K\). We used the notation \(\log^+ (z)\) to refer to \(\log \max(z, 1)\) for \(z \in \mathbb{R}\). The Weil height is independent of \(K\) and if the polynomial (1) is the minimal polynomial of \(\alpha\) over \(Q\), then 

\[
h(\alpha) = \frac{1}{n} \log M(f).
\]

Definition 1. Let \(G\) be a finite subgroup of \(\text{PGL}_2(Q)\). The \(G\)-orbit height of \(x \in \mathbb{P}^1(\overline{Q})\) is defined as

\[
h_G(x) = \sum_{\sigma \in G} h(\sigma x).
\]

Note that \(h_G(x) \geq 0\) and \(h_G(\sigma \alpha) = h_G(\alpha)\) for all \(\sigma \in G\). We can now state the \(G\)-invariant Lehmer problem, namely: given a finite group \(G\) does there exist a positive lower bound \(D\) such that

\[
h_G(x) = 0 \quad \text{or} \quad h_G(x) \geq D
\]

for all \(x \in \mathbb{P}^1(\overline{Q})\)? As Zagier pointed out \[\text{[8]}\], if \(G\) is trivial such a constant does not exist (e.g., \(h(e)(\sqrt{2}) = n^{-1} \log 2 \to 0\)). Assuming a mild restriction on \(G\), which we will state next, we will prove that this lower bound \(D\) exists for \(h_G\).

Recall that as a consequence of Kronecker’s lemma \[\text{[8]}\], for \(\alpha \in K\) we have that \(h(\alpha) = 0\) if and only if \(\alpha = 0\) or \(\alpha\) is a root of unity. We will now define a set \(O\) of orbits such that elements of these orbits are precisely the zeros of \(h_G\) over \(K\).

Definition 2. Let \(Q\) be the set of all orbits of the action of \(G\) on \(\hat{C} = \mathbb{C} \cup \{\infty\}\). Let \(O \subset Q\) be the set of all orbits for which every non-zero element lies on the unit circle, i.e.

\[
O = \{O \in Q \mid \forall z \in O : z = 0 \text{ or } |z| = 1\}.
\]

The main purpose of this note is to solve the \(G\)-invariant Lehmer problem in the case that \(h_G\) has finitely many zeros:

Theorem 1. If \(O\) is finite, then there exists a positive \(D\) such that

\[
h_G(\alpha) = 0 \quad \text{or} \quad h_G(\alpha) \geq D
\]

for all \(\alpha \in K\).
Remark 1. For a finite $G \leq \text{PGL}_2(\mathbb{Q})$ this theorem can also be stated in terms of Mahler measures instead of heights. Let $\alpha$ be a given algebraic integer with minimal polynomial $f \in \mathbb{Z}[x]$ of degree $n$. Assume $\sigma \in G$ and write $\sigma = \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)$. Let

$$f_\sigma(z) = C(cz + d)^n f(\sigma(z)),$$

where $C \in \mathbb{Q}$ is chosen in such a way that $f_\sigma$ is primitive, so that $f_\sigma$ is the minimal polynomial of $\sigma^{-1} \alpha$. Then, this theorem implies that there exists a constant $E > 1$ such that

$$\prod_{\sigma \in G} M(f_\sigma) = 1 \quad \text{or} \quad \prod_{\sigma \in G} M(f_\sigma) \geq E^n$$

for all primitive irreducible polynomials $f \in \mathbb{Z}[x]$.

Later we will see that if $\mathcal{O}$ is infinite, its subsets contain all roots of unity. Moreover, if $\mathcal{O}$ is finite, its subsets can only contain 0 and the roots of cyclotomic polynomials of degree at most 2. For the cyclic case $G = \{\sigma\}$, we will use this to classify all $\sigma \in \text{PGL}_2(\mathbb{Q})$ for which $\mathcal{O}$ is finite and non-empty. In nearly all cases, it is also possible to calculate the maximal value of $D$ for which Theorem 1 holds. For three of these cases, these values are already known. By a theorem of Zhang, for which Zagier gave an elementary proof, we have that $D = \frac{1}{3} \log \frac{1 + \sqrt{5}}{2} = 0.2406059 \ldots$ for $G = \{z, 1 - z\}$ [2]. Here we identified $\text{PGL}_2(\mathbb{Q})$ with the Möbius transformations, maps $\sigma : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ of the form $\sigma(z) = \frac{az + b}{cz + d}$ for $a, b, c, d \in \mathbb{Q}$. Dresden proved that $D = \log |\beta| = 0.4217993 \ldots$ for $G = \{z, \frac{1}{1 - z}, 1 - \frac{1}{z}\}$, where $\beta$ is a maximal root in absolute value of $\left(z^2 - z + 1\right)^3 - \left(z^2 - z\right)^2$ and mentioned that for $G = \{z, \frac{1}{z + 1}, -\frac{1}{2}, \frac{1}{z + 1}\}$ one has $D = \log |\gamma| = 0.7328576 \ldots$ for $\gamma$ a maximal root in absolute value of $\left(z^2 + 1\right)^4 + z^2 \left(z^2 - 1\right)^2$ [3].

2. Proof of Theorem 1

Set $\mathcal{O} = \{O_i \mid i \in \{1, 2, \ldots, k\}\}$. For each orbit $O_i \in \mathcal{O}$ we choose $\alpha_i \in O_i$ and define $p_i \in \mathbb{Z}[x]$ as the minimal polynomial of $\alpha_i$. Let $N$ be the maximum of the degrees of all the $p_i$ and let

$$n_v = \begin{cases} 0 & \text{if } v \text{ is non-Archimedean}, \\ 1 & \text{if } v \text{ is real}, \\ 2 & \text{if } v \text{ is complex}. \end{cases}$$

The proof of Theorem 1 will follow directly from the following lemma:

Lemma 2. Let $v$ be a place of $K$ and $\alpha \in K$. There exists $B_{\text{max}} > 0$ such that for all $B$ with $0 < B < B_{\text{max}}$ there exists a positive $D$ such that

$$\sum_{\sigma \in G} \left( \log^+ |\sigma(\alpha)|_v - \frac{1}{2} \log |\sigma(\alpha)|_v - B \sum_{i=1}^k \log |p_i(\sigma(\alpha))|_v \right) \geq n_v D. \quad (3)$$
Proof. Firstly, assume \( v \) is finite. We will show that the summand

\[
\log^+ |\sigma(\alpha)|_v - \frac{1}{2} \log |\sigma(\alpha)|_v - B \sum_{i=1}^k \log |p_i(\sigma(\alpha))|_v
\]

(4)

of (3) is nonnegative for all \( \sigma \in G \). If \( \sigma(\alpha) \) is integral at \( v \), it follows that \( \log^+ |\sigma(\alpha)|_v = 0 \) and \( \frac{1}{2} \log |\sigma(\alpha)|_v \leq 0 \). By writing \( p_j(\sigma(\alpha)) = b_{j_1}\sigma(\alpha)^{\alpha_1} + \ldots + b_{j_0} \) for \( j \in \{1, 2, \ldots, k\} \) and \( b_{ji} \in \mathbb{Z} \) we obtain

\[
|p_j(\sigma(\alpha))|_v \leq \max(|b_{j_1}|_v \cdot |\sigma(\alpha)|_v^{\alpha_1}, \ldots, |b_{j_0}|_v) \leq 1.
\]

Therefore, \( \sum_{i=1}^k \log |p_i(\sigma(\alpha))|_v \leq 0 \), which implies that the summand (4) is nonnegative for all \( B \in \mathbb{R}^+ \). If \( |\sigma(\alpha)|_v > 1 \), we find that \( \log^+ |\sigma(\alpha)|_v - \frac{1}{2} \log |\sigma(\alpha)|_v = \frac{1}{2} \log |\sigma(\alpha)|_v > 0 \). Using the same notation as above,

\[
\log |p_j(\sigma(\alpha))|_v \leq \log \max(|b_{j_1}|_v \cdot |\sigma(\alpha)|_v^{\alpha_1}, \ldots, |b_{j_0}|_v) \leq N \log |\sigma(\alpha)|_v.
\]

Therefore, for

\[
B_{\text{max}} \leq \frac{1}{2kN} \leq \frac{\log |\sigma(\alpha)|_v}{2 \sum_{i=1}^k \log |p_i(\sigma(\alpha))|_v}
\]

the summand (4) is positive for all \( B \) with \( 0 < B < B_{\text{max}} \) and all \( \sigma \in G \).

Secondly, if \( v \) is Archimedean, then \( |\alpha|_v = |\iota(\alpha)|^{\nu(v)} \) for some embedding \( \iota \) of \( K \) into \( \mathbb{C} \). Let

\[
g_1(z) = \sum_{\sigma \in G} (\log^+ |\sigma(z)| - \frac{1}{2} \log |\sigma(z)|) \quad \text{and} \quad g_2(z) = -\sum_{\sigma \in G} \sum_{i=1}^k \log |p_i(\sigma(z))|.
\]

The claim is that for \( z \in \mathbb{C} \) the function

\[
f(z) = g_1(z) + B \cdot g_2(z) = \sum_{\sigma \in G} \left( \log^+ |\sigma(z)| - \frac{1}{2} \log |\sigma(z)| - B \sum_{i=1}^k \log |p_i(\sigma(z))| \right)
\]

is bounded below by some constant \( D > 0 \). Clearly, \( f \) tends to infinity as \( \sigma(z) \) tends to zero or to one of the roots of the \( p_i \). As \( \sum_{i=1}^k \log |p_i(\sigma(z))| \leq k \log |C|^{\nu(v)} \) for some \( C \in \mathbb{R}^+ \) and \( \sigma(z) \) sufficiently large, assuming \( B_{\text{max}} < 1 \) we find that if \( \sigma(z) \) tends to infinity then \( f \) tends to infinity. As \( f \) is continuous elsewhere and harmonic if \( |\sigma(z)| \neq 1 \) for all \( \sigma \in G \), it attains a minimum on a circle \( \{|\sigma(z)| = 1\} \) for some \( \sigma \in G \). As \( f(z) = f(\sigma(z)) \) for all \( \sigma \in G \), we can assume that this minimum is attained on the unit circle. If this minimum is strictly positive, we are done. Otherwise, \( g_2(z) \leq 0 \) and this minimum is attained in the set \( S = \{z \in \mathbb{C} \mid |z| = 1 \text{ and } g_2(z) \leq 0\} \). Let \( q \in S \) and let \( Q \) be the orbit of \( q \). If \( Q \in \mathcal{O} \), write \( Q = O_i \). Then, there is a \( \tau \in G \) such that \( \tau(q) \) is a root of \( p_i \). It follows that \( g_2 \) tends to infinity as \( z \) tends to \( q \), contradicting \( q \in S \). Therefore, \( Q \notin \mathcal{O} \). Hence, there exists a \( \tau \in G \) such that \( \tau(q) \neq 0 \) and \( |\tau(q)| \neq 1 \). This implies that \( \log^+ |\tau(q)| - \frac{1}{2} \log |\tau(q)| > 0 \). As for
all $z \in \mathbb{C}$ we have that $\log^+ |z| - \frac{1}{2} \log |z| \geq 0$, it follows that $g_1(q) > 0$ for all $q \in S$. As $S$ is compact, $g_1$ attains a minimum $m > 0$ in $S$. Also, $g_2$ attains a minimum $n$ in $S$. Letting $B_{\text{max}} < -m/n$, it follows that $f$ attains a positive minimum $D$ in $S$.

Proof of Theorem 1. Observe that for $\beta \in K^*$ we have

$$\sum_v n_v = [K : \mathbb{Q}] \quad \text{and} \quad \sum_v \log |\beta|_v = 0. \quad (5)$$

Then, for $\alpha$ for which there is no $\sigma \in G$ such that $\sigma(\alpha)$ is zero, infinite or a root of some $p_i$, we can sum the inequality (3) in Lemma 2 over all places $v$ of $K$ and apply (5). After dividing by $[K : \mathbb{Q}]$ we find that $h_G(\alpha) \geq D$ for all but finitely many $\alpha \in K$. Hence, it follows that for some possibly smaller value of $D$ and all $\alpha \in K$ we have $h_G(\alpha) = 0$ or $h_G(\alpha) \geq D$.

3. When is $\mathcal{O}$ finite?

We will investigate how strong the condition is that $\mathcal{O}$ is finite.

Proposition 3. The set $\mathcal{O}$ is finite if and only if there exists a root of unity $\zeta$ such that $h_G(\zeta) > 0$.

Proof. If $\mathcal{O}$ is finite, we can choose a root of unity $\zeta$ and $\tau \in G$ with $|\tau\zeta| \neq 0, 1$. As $h(\sigma\zeta) \geq 0$ for all $\sigma \in G$ and $h(\tau\zeta) > 0$, we find $h_G(\zeta) > 0$.

Conversely, if there exists a root of unity $\zeta$ with $h_G(\zeta) > 0$, then there exists a $\tau \in G$ such that $\tau\zeta$ is not a root of unity. It is known that Möbius transformations map real circles on $\hat{\mathbb{C}}$ to real circles on $\hat{\mathbb{C}}$ provided that we regard a line through $\infty$ as a circle. Hence, $\tau$ maps the unit circle to another circle. As two circles intersect in at most two different points, there are at most two roots of unity $\eta$ such that $\tau\eta$ is also a root of unity. Hence, $\mathcal{O}$ is finite. □

Corollary 4. Let $G \leq \text{PGL}_2(\mathbb{Q})$ be finite. Then, $\mathcal{O}$ is infinite if and only if $G$ is a subgroup of

$$\left\{ I, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} a & b \\ -b & -a \end{pmatrix}, \begin{pmatrix} b & a \\ -a & -b \end{pmatrix} \right\} \quad (6)$$

for some $a, b \in \mathbb{Q}$ with $a^2 \neq b^2$.

Proof. If $\mathcal{O}$ is infinite then $\sigma(1) = \pm 1$ and $\sigma(-1) = \mp 1$. Hence, an element $\sigma \in G$ is of the form

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} a & b \\ -b & -a \end{pmatrix}$$

for some $a, b \in \mathbb{Q}$ with $a^2 \neq b^2$. The first is of infinite order unless $a = 0$ or $b = 0$. The product of two elements

$$\begin{pmatrix} a & b \\ -b & -a \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a' & b' \\ -b' & -a' \end{pmatrix}$$
of PGL$_2(\mathbb{Q})$ is of finite order if and only if $ab' = ba'$ or $aa' = bb'$. Hence, $G$ must be a subgroup of $[0, 0]$. It can easily be checked that $O$ is infinite for subgroups of $[0, 0]$. \hfill \Box

4. When is the $G$-orbit height zero?

Denote with $\pm \frac{1}{2} \pm' \frac{1}{2}i\sqrt{3}$ the four primitive third and sixth roots of unity, where the sign $\pm'$ can be chosen independently from the sign $\pm$.

**Lemma 5.** Let $O$ be finite and $G \leq \text{PGL}_2(\mathbb{Q})$. Then $h_G(\alpha) = 0$ if and only if $\alpha$ equals $0, \pm 1, \pm i$ or $\pm\frac{1}{2} \pm' \frac{1}{2}i\sqrt{3}$.

**Proof.** If $h_G(\alpha) = 0$, we have for all $\sigma \in G$ that $\sigma \alpha$ equals $0$ or is a root of unity. Assuming $\alpha \in \mathbb{Q}$, we find $\alpha$ equals $0$ or $\pm 1$. If $\alpha \notin \mathbb{Q}$, then for all $\sigma \in G$ we also have $\sigma \alpha \notin \mathbb{Q}$, so $\sigma \alpha$ is a root of unity. By the proof of the previous proposition there is a $\tau \in G$ which maps at most two roots of unity to other roots of unity. As $h_G(\alpha) = h_G(\alpha')$ for all algebraic conjugates $\alpha'$ of $\alpha$, it follows that the minimal polynomial of $\alpha$ has degree at most two. Hence, $\alpha$ equals $\pm i$ or $\pm\frac{1}{2} \pm' \frac{1}{2}i\sqrt{3}$. \hfill \Box

5. Explicit constants

Dresden proved that all finite subgroups of PGL$_2(\mathbb{Q})$ are isomorphic to the cyclic group $C_n$ or the dihedral group $D_n$ (where the latter is of order $2n$) for $n = 1, 2, 3, 4$ or $6$ [2]. By the previous lemma, there are only 9 possible elements in orbits in $O$. Hereby, it is possible to determine all finite cyclic groups $G \leq \text{PGL}_2(\mathbb{Q})$ for which $O$ is finite and non-empty. Moreover, by generalizing Zagier’s and Dresden’s proofs [3, 4], it is possible to explicitly find the best value of $D$ in Theorem 1. We have collected these data in Table 1:

| $\phi(z)$ | 1 | $z$ | $p_1(\sigma(z))$ |
|-----------|---|-----|-----------------|
| $\sum_{i=0}^{\text{ord}\sigma-1} \log^+ |\sigma^i(z)| - B \log |\phi(z)| \geq D$ |

holds where the values of $B$ and $\exp(D)$ can be found in the corresponding row of the columns ‘$B$’ and ‘$\exp(D)$’. From this, in a similar fashion as the proof of Theorem 1, one deduces $h_G(\alpha) = 0$ or $h_G(\alpha) \geq D$ for all $\alpha \in \mathbb{Q}$. The element $\alpha$ in the last column is such that equality holds in $h_G(\alpha) \geq D$. However, it is not unique. Here, a maximal root of a polynomial is defined as a root which
Table 1: Classification of cyclic groups with $O$ non-empty and finite, together with data to find the optimal constant $D$ of Theorem 1. In Section 5, the meaning of these data is explained.

| $\sigma$ | Elts. of $O$ | ord $\sigma$ | $B$ | $\exp(D)$ | $D \approx$ (for $p/q=5$) | Equality |
|----------|---------------|--------------|-----|------------|--------------------------|---------|
| \begin{pmatrix} 1 & 0 \\ p/q & -1 \end{pmatrix} | \{0\} | 2 | 1 | $\max(||p| - q|, |q|)$ | 1.38629 | \begin{align*} 1 & \text{ if } p/q > 0 \\ -1 & \text{ if } p/q < 0 \end{align*} |
| \begin{pmatrix} 1 & \pm 1 \\ p/q & -1 \end{pmatrix} | \{0, \mp 1\} | 2 | 1 | $\max(|p - q|, |q|)$ | 0.69315 | $\pm 1$ if $2 \mid p \mp q$ |
| \begin{pmatrix} 1 & p/q \\ p/q + 2 & -1 \end{pmatrix} | \{\pm 1\} | 2 | 1 | $\max(|p \mp 3q|, |p \mp q|)$ | 0.69315 | $\mp 1$ if $4 \mid p \mp q$ |
| \begin{pmatrix} 1 & -1 \\ 3 & 1 \end{pmatrix} | \{0, -1, 1\} | 3 | 1 | 5 | 1.60944 | $\sqrt{-1}$ |
| \begin{pmatrix} 1 & p/q \\ p/q - 1 \end{pmatrix} | \{i, -i\} | 2 | $\frac{1}{2}$ | $||p| + q|/2$ | 1.09861 | 1, $-1$ if $2 \mid p + q$ |
| \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} | \{i\}, \{-i\} | 4 | 0.19408 \ldots \ |\alpha| | 0.73286 | $\alpha$, maximal root of $(z^2 + 1)^4 + z^2(z^2 - 1)^2$ |
| \begin{pmatrix} 1 & p/q \pm 1 \\ p/q - 1 \end{pmatrix} | \{\omega_{\pm +}, \omega_{\pm -}\} | 2 | $\frac{1}{2}$ | $\max(|p \mp 2q|, |p \mp q|)$ | 0.84730 | $\mp 1$ if $3 \mid p \mp q$ |
| \begin{pmatrix} 0 & 1 \\ -1 & \pm 1 \end{pmatrix} | \{\omega_{\pm +}\}, \{\omega_{\pm -}\} | 3 | 0.11724 \ldots \ |\alpha| | 0.42180 | $\alpha$, maximal root of $(z^2 \mp z + 1)^3 - (z^2 \pm z)^2$ |
| \begin{pmatrix} 2 & \mp 1 \\ \pm 1 & 1 \end{pmatrix} | \{\omega_{\pm +}\}, \{\omega_{\pm -}\} | 6 | 0.30503 \ldots \ |\alpha(2\alpha - 1)\alpha + 1| | 1.75737 | $\alpha$, maximal root of $(z^2 \mp z + 1)^6 + z^2(2z^2 \mp 5z + 2)^2(z^2 - 1)^2$ |
Table 2: Cyclic groups $\langle \sigma \rangle$ with $O$ non-empty and finite which appear twice in Table 1, together with data to find the optimal constant $D$ of Theorem 1. In Section 5, the meaning of these data is explained.

| $\sigma$ | Elts. of $O$ | $B_1$ | $B_2$ | $\exp(D)$ | $D \approx$ | Equality |
|---------|--------------|-------|-------|------------|------------|----------|
| $\left( \begin{array}{cc} 1 & 0 \\ \pm 1 & -1 \end{array} \right)$ | $\{0\}, \{\omega_{\pm+}, \omega_{\pm-}\}$ | 1/2 | 1/2 | $\sqrt{\frac{1+\sqrt{5}}{2}}$ | 0.24061 | $\mp e^{\frac{2\pi i}{5}}$ |
| $\left( \begin{array}{cc} 1 & 0 \\ \pm 2 & -1 \end{array} \right)$ | $\{0\}, \{\pm 1\}$ | 2/3 | 1/3 | $\sqrt{3}$ | 0.54931 | $\omega_{\pm+}$ |
| $\left( \begin{array}{cc} 1 & \mp 1 \\ 0 & -1 \end{array} \right)$ | $\{0, \pm 1\}, \{\omega_{\pm+}, \omega_{\pm-}\}$ | $\frac{\sqrt{5}-1}{2\sqrt{3}}$ | $\frac{1}{4\sqrt{3}}$ | $\sqrt{\frac{1+\sqrt{5}}{2}}$ | 0.24061 | $\pm e^{\frac{2\pi i}{5}}$ |
| $\left( \begin{array}{cc} 1 & \mp 1 \\ \mp 1 & -1 \end{array} \right)$ | $\{0, \pm 1\}, \{i, -i\}$ | | | | | |
| $\left( \begin{array}{cc} 1 & \mp 1 \\ \mp 2 & -1 \end{array} \right)$ | $\{0, \pm 1\}, \{\omega_{\mp+}, \omega_{\mp-}\}$ | | | | | |
| $\left( \begin{array}{cc} 1 & \mp 1 \\ \mp 3 & -1 \end{array} \right)$ | $\{0, \pm 1\}, \{\mp 1\}$ | | | | | |

is maximal in absolute value and which imaginary part is nonnegative. For the polynomials we apply this definition to, this uniquely determines the root.

**Example 1.** Consider the second row of Table 1 and choose $\pm$ to be $+$, that is $\sigma(z) = \frac{z+1}{p/q \mp 1}$ and $p/q \neq -1$. Then, $O = \{\{0, -1\}\}$, $\phi(z) = \frac{z(z+1)}{p \mp q}$ and $D = \log(\max(|p - q|/2, |q|))$. Then

$$\log^+ |z| + \log^+ |\sigma(z)| - \log |\phi(z)| \geq D,$$

which yields $h_G(0) = 0$, $h_G(-1) = 0$ and $h_G(\alpha) \geq D$ for all $\alpha \in \mathbb{Q}$ with $\alpha \neq 0, -1$. We have $h_G(\alpha) = D$ for $\alpha = 1$ if $2 | p - q$.

There are $\sigma \in \text{PGL}_2(\mathbb{Q})$ which can be found twice in Table 1. For these $\sigma$ we have that the corresponding value of $D$ is not positive, so this value of $D$ is not allowed in Theorem 1. All these $\sigma$ can be found in Table 2. They all have order 2. Using another inequality, it is in some cases still possible to find the optimal (positive) value of $D$. Namely, it holds that $\log^+ |z| + \log^+ |\sigma(z)| - B_1 \log |\phi_1(z)| - B_2 \log |\phi_2(z)| \geq D$ for corresponding values in the columns ‘$B_1$’, ‘$B_2$’ and ‘$\exp(D)$’. Here, $\phi_1$ and $\phi_2$ are similarly defined, that is, $\phi_i(z) = \frac{1}{E_i} \prod_{\sigma \in G} p_i(\sigma(z))$ where $p_i$ corresponds to the $i$th orbit in $O$ as in the proof of Theorem 1 and $E_i$ is such that the numerator and denominator of $\phi_i(z)$ are relatively prime. Again, it follows that $h_G(\alpha) = 0$ or $h_G(\alpha) \geq D$ for all $\alpha \in \mathbb{Q}$. In three of the cases, the author was not able to find the optimal value of $D$ with corresponding values of $B_1$ and $B_2$.  

8
6. Generalizations

It is possible to extend Table 1 and Table 2 to non-cyclic subgroups of $\text{PGL}_2(\mathbb{Q})$. For example consider

$$G = \langle \begin{pmatrix} 1 & -1 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle \cong D_3,$$

the dihedral group with 6 elements. Then $\mathcal{O} = \{-1, 0, 1\}$ and one can show that $h_G(\alpha) \geq \log(25)$ for $\alpha \neq -1, 0, 1$ with equality for $\alpha = i$. Similarly, for

$$G = \langle \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \rangle \cong D_2,$$

one has $\mathcal{O} = \{\omega_+, \omega_-\}$ and one can show that $h_G(\alpha) \geq \log(2)$ for $\alpha \neq \omega_+, \omega_-$ with equality for $\alpha = -1$. It would be interesting to specify for which other subgroups one can find a similar statement.

Another way to extend these tables, is by considering finite $G \leq \text{PGL}_2(\overline{\mathbb{Q}})$. For example, $\sigma(z) = \frac{z - \sqrt{3}}{\sqrt{3} + 1}$ has order 3 and one finds $\mathcal{O} = \{\{i\}, \{-i\}\}$ for $G = \langle \sigma \rangle$.

Although the value of $D$ is computed in some cases, this note does not explain how $G$ determines the value of $D$. It would be interesting to find a universal lower bound on $D$ or to strengthen Theorem 1 by proving that $D$ is greater than some invariant depending on $G$.

7. Acknowledgement

I would like to thank my supervisor Gunther Cornelissen for helpful discussions and suggestions.

References

[1] Gregory Dresden, *Orbits of algebraic numbers with low heights*, Math. Comp. 67 (1998), no. 222, 815–820. MR 1468942 (98h:11128)

[2] Gregory Dresden, *There Are Only Nine Finite Groups of Fractional Linear Transformations with Integer Coefficients*, Math. Mag. 77 (2004), no. 3, 211–218. MR 1573751

[3] Leopold Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coeffizienten*, J. Reine Angew. Math. 53 (1857), 173–175.

[4] Derrick Henry Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) 34 (1933), no. 3, 461–479. MR 1503118

[5] Don Zagier, *Algebraic numbers close to both 0 and 1*, Math. Comp. 61 (1993), no. 203, 485–491. MR 1197513 (94c:11004)

[6] Shouwu Zhang, *Positive line bundles on arithmetic surfaces*, Ann. of Math. (2) 136 (1992), no. 3, 569–587. MR 1189866 (93j:14024)