Hurwitz’s Freeness Property

In [2] Gauss devised an algorithm to solve in integers the equation

\[ a x^2 + 2 b x y + c y^2 = m, \]  

(1)

where \( a, b, c, m \) are given integers.

Consider the groups

\[ G := \text{GL}(2, \mathbb{Z})/\{\pm 1\} \supset \text{SL}(2, \mathbb{Z})/\{\pm 1\} =: H. \]

Let \( \Delta \) be an integer, let \( F \) be the set all quadratic forms

\[ f(X, Y) := a X^2 + 2 b X Y + c Y^2 \]  

(2)

with \( a, b, c \) integers and \( b^2 - ac = \Delta \), and let \( \mathcal{F} \) be the groupoid attached to the natural action of \( H \) on \( F \). In Article 169 of [2] Gauss reduces the solution of (1) to the computation of certain hom-sets in \( \mathcal{F} \) (see below).

Assume from now on that \( \Delta \) is a fixed positive nonsquare integer.

The group \( G \) acts on the set \( \mathbb{I} \) of irrational real numbers by linear fractional transformations. Let \( \mathcal{I} \) be the corresponding groupoid, and \( \mathbb{I}_\Delta \) the set of real numbers

\[ \frac{-b - \sqrt{\Delta}}{a} \]

where \( f \) as in (2) runs over the elements of \( F \). Then \( H \) preserves \( \mathbb{I}_\Delta \), and we can form the restricted groupoid \( \mathcal{I}_\Delta^H \) issued from the action of \( H \) on \( \mathbb{I}_\Delta \).

In Section 73 of [1] Dirichlet notes that above formula gives a canonical groupoid isomorphism from \( \mathcal{F} \) to \( \mathcal{I}_\Delta^H \).

In Section 63 of [3] Hurwitz shows that the groupoid \( \mathcal{I} \) is free over one of its sub oriented graph, giving a very simple description of the hom-sets of \( \mathcal{I}_\Delta^H \), which Dirichlet had identified to the hom-sets of \( \mathcal{F} \), whose computation Gauss had reduced the solution of (1) to.

We wish to phrase Hurwitz’s statement in today’s language.

Say that the derivative \( x' \) of a point \( x \) in \( \mathbb{I} \) is the inverse of its fractional part, let \( g_x \) be the image in \( G \) of
\[
\begin{pmatrix} [x] & 1 \\ 1 & 0 \end{pmatrix},
\]
so that we have \( x = g_x x' \), let \( \gamma(x) \) be the corresponding morphism in \( \mathcal{I} \) from \( x' \) to \( x \), and let \( \Gamma \) be the sub oriented graph of \( \mathcal{I} \) whose vertices are the points of \( \mathbb{I} \) and whose arrows are the \( \gamma(x) \).

Then \( \mathcal{I} \) is the groupoid freely generated by \( \Gamma \) in the following sense.

Let \( \varphi \) be an oriented graph morphism from \( \Gamma \) into any groupoid \( \mathcal{G} \). Then \( \varphi \) extends uniquely to a groupoid morphism from \( \mathcal{I} \) to \( \mathcal{G} \).

The groupoid \( \mathcal{I} \) has a very simple structure, which can be described as follows. To ease notation put \( x_i := x^{(i)} \).

Let \( g \) be a nontrivial morphism in \( \mathcal{I} \) from \( x \) to \( y \). Then there is a unique pair \((i, j)\) of nonnegative integers satisfying \( x_i = y_j \),

\[
g = \gamma(y_0) \cdots \gamma(y_{j-1}) \gamma(x_{i-1})^{-1} \cdots \gamma(x_0)^{-1},
\]
and \( x_{i-1} \neq y_{j-1} \) if \( i \) and \( j \) are positive.

The composition of two such elements is tedious but easy to compute.

Let \( x \) be in \( \mathbb{I} \). Recall that the sequence \((x_i)\) is eventually periodic if and only if \( x \) has degree 2 over \( \mathbb{Q} \). This makes \( \mathcal{I}_\Delta \) computable. In particular the stabilizer in \( H \) of \( f \) in \( F \) is infinite cyclic. However, \( \mathcal{I} \) is highly uncomputable.

\*

We said above that Gauss reduced the solution of (1) to the computation of certain hom-sets in \( F \). Let’s be more precise. (We only indicate some of the main statements, directing the reader to [3] for a full treatment.) Assume that \( m \) is nonzero.

Say that a solution of (1) is a representation of \( m \) by \( f \) (\( f \) being given by (2)), and that such a representation is proper of \( X \) and \( Y \) are relatively prime. It clearly suffices to describe the set \( P \) of proper representations of \( m \) by \( f \).

As a general notation, write \([a, b, c]\) for the form (2). Let \( n \) be in \( \mathbb{N} \). Put

\[
\ell_n := \frac{n^2 - \Delta}{m}, \quad f_n := [m, n, \ell_n],
\]
form the set $S_n$ of those substitutions $h$ in $\text{SL}(2, \mathbb{Z})$ which satisfy $f h = f_n$, and let $u_n$ be the map from $S_n$ to $P$ attaching to $h \in S_n$ its first column.

Then the $u_n$ induce a bijection form the disjoint union of the $S_n$ onto $P$.

References

[1] Dirichlet, Peter Gustav; Vorlesungen über Zahlentheorie, 1863. (“Lectures on Number Theory”, AMS translation).

http://gallica.bnf.fr/
http://gdz.sub.uni-goettingen.de/no_cache/dms/load/img/?IDDOC=159254
http://books.google.com/books?id=PycPAAAAQAAJ&output=text

[2] Gauss, Carl Friedrich; Disquisitiones Arithmeticae, 1801. I won’t try to list all the online and offline versions available.

[3] Hurwitz, Adolf; Lectures on Number Theory, Springer 1986.