A PROOF OF HURWITZ'S THEOREM.

By K. MAHLER, Manchester.

Lemma 1: *Let* x *be an irrational real number*, ϵ *a positive number. Then there is a modular substitution*

$$\Omega = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad \alpha\delta - \beta\gamma = 1 \qquad (\alpha, \beta, \gamma, \delta \text{ integers}),$$

such that

$$|\alpha x + \beta| < \epsilon, \quad |\gamma x + \delta| < \epsilon, \quad |\gamma(\gamma x + \delta)| \leq 1, \quad 0 \leq \alpha \leq \gamma.$$

Proof: Since x is irrational, there exists a positive monotone increasing function $\psi(t)$ of the variable $t > 1$, such that

$$\lim_{t \to \infty} \psi(t) = \infty,$$

and that the inequalities

$$0 < \gamma < \psi(t), \quad |\gamma x + \delta| \leq \frac{1}{t}$$

have no solutions in integers γ, δ. Suppose that t is already so large that

$$\frac{1}{t} < \epsilon, \quad \frac{2}{\psi(t)} < \epsilon.$$

By Dirichlet's principle (the Schubfachprinzip) there are two integers γ and δ, such that

$$0 < \gamma \leq t, \quad |\gamma x + \delta| \leq \frac{1}{t},$$

and therefore

$$| \gamma x + \delta | < \epsilon, \quad | \gamma(\gamma x + \delta) | \leq 1, \quad \psi(t) \leq \gamma \leq t.$$

Obviously, γ and δ may be supposed to be relatively prime. Hence we can find two other integers α_0, β_0, such that $\alpha_0\delta - \beta_0\gamma = 1$. The most general solution of $\alpha\delta - \beta\gamma = 1$ is given by

$$\alpha = \alpha_0 + \gamma k, \quad \beta = \beta_0 + \delta k,$$

where k is an arbitrary integer. We chose k such that

$$0 \leq \alpha \leq \gamma \leq t.$$

From the identity

$$\alpha(\gamma x + \delta) - \gamma(\alpha x + \beta) = 1$$

then follows that

$$| \alpha x + \beta | = \left| \frac{1}{\gamma} \right| \; | \alpha(\gamma x + \delta) - 1 | \leq$$
$$\leq \left| \frac{1}{\gamma} \right| \{ | \gamma(\gamma x + \delta) | + 1 \} \leq \frac{2}{\psi(t)} < \epsilon,$$

as was to be proved. —

Notation: If $\Omega = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is an arbitrary matrix, x a real or complex number, then we write

$$\Omega x = \frac{\alpha x + \beta}{\gamma x + \delta}.$$

Lemma 2: Let x and y be two different real numbers, ϵ a positive number. Then there is a modular substitution $\Omega = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, for which

$$| \Omega x - \Omega y | \geq \sqrt{5}, \quad | \gamma x + \delta | < \epsilon.$$

Proof: For rational x, there exists a substitution Ω in which $\gamma x + \delta = 0$, so that the lemma is obvious. Suppose therefore that x is irrational. By Lemma 1, applied with $\frac{\epsilon}{5}$ instead of ϵ, there is a modular substitution $\Omega_0 = \begin{pmatrix} \alpha_0 & \beta_0 \\ \gamma_0 & \delta_0 \end{pmatrix}$ such that

$$| \alpha_0 x + \beta_0 | < \frac{\epsilon}{5}, \quad | \gamma_0 x + \delta_0 | < \frac{\epsilon}{5},$$
$$| \gamma_0(\gamma_0 x + \delta_0) | \leq 1, \qquad 0 \leq \alpha \leq \gamma.$$

Without loss of generality

$$\epsilon \leq 5, \quad \epsilon \leq |x - y|, \quad \epsilon^2 \leq 5\,|x - y|.$$

Hence

$$|(\gamma_0 x + \delta_0)(\gamma_0 y + \delta_0)| = |(\gamma_0 x + \delta_0)^2 + \gamma_0(\gamma_0 x + \delta_0)(y - x)| \leq$$
$$\leq |x - y|\,(\tfrac{1}{5} + 1) = \tfrac{6}{5}\,|x - y|,$$

and therefore

$$|\Omega_0 x - \Omega_0 y| = \left| \frac{x - y}{(\gamma_0 x + \delta_0)(\gamma_0 y + \delta_0)} \right| \geq \tfrac{5}{6}.$$

If $|\Omega_0 x - \Omega_0 y| \geq \sqrt{5}$, then Ω_0 has the required properties. Hence assume that

$$\tfrac{5}{6} \leq |\Omega_0 x - \Omega_0 y| < \sqrt{5}.$$

Let k be an integer and

$$X = \Omega_0\, x, \quad Y = \Omega_0\, y, \quad \lambda = X - Y, \quad \mu = X + Y,$$

so that identically

$$U(k) = \frac{-1}{X + k} - \frac{-1}{Y + k} = \frac{4\lambda}{(\mu + 2k)^2 - \lambda^2}.$$

If
$$\tfrac{5}{6} \leq |\lambda| = |\Omega_0 x - \Omega_0 y| \leq \frac{4}{\sqrt{5}},$$

then chose k such that

$$|\mu + 2k| \leq 1;$$

hence

$$|(\mu + 2k)^2 - \lambda^2| \leq \max(1^2, \lambda^2),$$

and therefore

$$|U(k)| \geq \begin{cases} 4\,|\lambda| > \frac{10}{3} > \sqrt{5} \text{ for } \frac{5}{6} \leq |\lambda| \leq 1, \\ \dfrac{4\,|\lambda|}{\lambda^2} = \dfrac{4}{|\lambda|} \geq \sqrt{5} \text{ for } 1 \leq |\lambda| \leq \dfrac{4}{\sqrt{5}}. \end{cases}$$

If, however,
$$\frac{4}{\sqrt{5}} \leq |\lambda| < \sqrt{5},$$

then we determine k such that either

$$-2 \leq \mu + 2k \leq -1 \text{ or } 1 \leq \mu + 2k \leq 2;$$

hence

$$|(\mu + 2k)^2 - \lambda^2| \leq \max\left(2^2 - \left(\frac{4}{\sqrt{5}}\right)^2, \lambda^2 - 1\right) =$$
$$= \max(\tfrac{4}{5}, \lambda^2 - 1) = \lambda^2 - 1,$$

and therefore

$$|U(k)| \geq \frac{4\,|\lambda|}{\lambda^2 - 1} \geq \sqrt{5},$$

since

$$\frac{4\,|\,\lambda\,|}{\lambda^2 - 1} \geq \sqrt{5} \text{ for } \frac{4}{\sqrt{5}} \leq |\,\lambda\,| < \sqrt{5}.$$

Hence in all cases

$$|\,U(k)\,| \geq \sqrt{5}$$

for a certain integer k; if Ω denotes the matrix

$$\Omega = \begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix} = \begin{pmatrix} -\gamma_0 & -\delta_0 \\ \alpha_0 + k\gamma_0 & \beta_0 + k\gamma_0\end{pmatrix} = \begin{pmatrix}0 & -1 \\ 1 & k\end{pmatrix}\Omega_0,$$

then

$$|\,\Omega\, x - \Omega\, y\,| \geq \sqrt{5}.$$

In order to show that

$$|\,\gamma x + \delta\,| = |\,(\alpha_0 x + \beta_0) + k(\gamma_0 x + \delta_0)\,| < \epsilon,$$

it is obviously sufficient to prove that $|\,k\,| \leq 4$. Now

$$Y = \Omega_0 y = \frac{\alpha_0 y + \beta_0}{\gamma_0 y + \delta_0} = \frac{\alpha_0(y - x) + (\alpha_0 x + \beta_0)}{\gamma_0(y - x) + (\gamma_0 x + \delta_0)};$$

hence, since $0 \leq \alpha_0 \leq \gamma_0$, $\gamma_0 \geq 1$,

$$|\,Y\,| \leq \frac{\gamma_0\,|\,x - y\,| + \dfrac{\epsilon}{5}}{\gamma_0\,|\,x - y\,| - \dfrac{\epsilon}{5}} \leq \frac{|\,x - y\,| + \frac{1}{5}\,|\,x - y\,|}{|\,x - y\,| - \frac{1}{5}\,|\,x - y\,|} = \tfrac{3}{2}.$$

Therefore

$$|\,\mu\,| \leq |\,\lambda + 2Y\,| \leq \sqrt{5} + 2 \,.\, \tfrac{3}{2} \leq 6,$$

and

$$2\,|\,k\,| \leq |\,\mu\,| + 2, \quad |\,k\,| \leq 4.$$

Lemma 3: If

$$x = \frac{1 + \sqrt{5}}{2}, \quad y = \frac{1 - \sqrt{5}}{2},$$

then for all modular substitutions $\Omega = \begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}$

$$|\,\Omega x - \Omega y\,| \leq \sqrt{5}.$$

Proof: Obviously

$$|\,\Omega x - \Omega y\,| = \frac{4\sqrt{5}}{|\,\Phi(\gamma, \delta)\,|},$$

where

$$\Phi(\gamma, \delta) = (\gamma + 2\delta)^2 - 5\gamma^2$$

is always divisible by 4 and does not vanish.

Theorem of Hurwitz: *Let* a, b, c, d *be four real numbers of* *determinant* $ad - bc = 1$, ϵ *a positive number. Then there are two integers* u *and* v, *such that*

$$|(au + bv)(cu + dv)| \leq \frac{1}{\sqrt{5}}, \ |au + bv| < \epsilon, \quad u^2 + v^2 > 0.$$

If

$$a = \frac{1 + \sqrt{5}}{2\sqrt[4]{5}}, \ b = \frac{1}{\sqrt[4]{5}}, \ c = \frac{1 - \sqrt{5}}{2\sqrt[4]{5}}, \ d = \frac{1}{\sqrt[4]{5}},$$

then

$$|(au + bv)(cu + dv)| \geq \frac{1}{\sqrt{5}}$$

for all integers u *and* v, *which do not vanish simultaneously.*

Proof: It suffices to prove the theorem for integers u and v, which are relatively prime. There is, therefore, a modular substitution $\Omega = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, such that $\gamma = u$, $\delta = v$. Put

$$\frac{a}{b} = x, \ \frac{c}{d} = y, \text{ so that } \frac{a}{b} - \frac{c}{d} = \frac{1}{bd} = x - y;$$

then identically

$$\frac{1}{(au + bv)\ (cu + dv)} = \frac{x - y}{(\gamma x + \delta)\ (\gamma y + \delta)} = \Omega x - \Omega y;$$

and the theorem follows at once from the last two lemmas.