What is Abel's Theorem Anyway?
(Steven Kleiman)

Selberg: "It still stands for me as pure magic. Neither with Gauss nor Riemann, nor with anybody else, have I found anything that really measures up to this."

The formula $\frac{a'x+b'y+c}{ax+by+c}$ can be used to construct a function of order 2 with given poles P, Q and given zero O.

To find the sum S of P and Q, find a rational function on the curve that has poles at P and Q and nowhere else, and that is zero at O. Then S is its other zero.

The parabola

$$y = ax^2 + bx + c$$

intersects the elliptic curve

$$y^2 = 1 - x^4$$

in 4 points.

The formula $\frac{y-a'x^2-bx-c}{y-ax^2-bx-c}$ can be used to construct a function of order 2 with given poles P, Q and given zero O.

To “add” P and Q, find a function of order 2 with poles at P and Q. Their “sum” (relative to O) is the other point S where it has the same value as at O.

$$\int_O^P \frac{dx}{\sqrt{1-x^4}} + \int_O^Q \frac{dx}{\sqrt{1-x^4}} = \int_O^S \frac{dx}{\sqrt{1-x^4}}$$

$\int_O^P \frac{dx}{\sqrt{1-x^4}} + \int_O^Q \frac{dx}{\sqrt{1-x^4}} = \int_O^S \frac{dx}{\sqrt{1-x^4}}$

$$\int_O^P \rho(x,y)\,dx + \int_O^Q \rho(x,y)\,dx = \int_O^S \rho(x,y)\,dx + \mathcal{R}$$

$\int_O^P \rho(x,y)\,dx + \int_O^Q \rho(x,y)\,dx = \int_O^S \rho(x,y)\,dx + \mathcal{R}$

More generally, the sum of *any number* of integrals $\int_O^P \rho(x,y)\,dx$ can be written as $\int_O^S \rho(x,y)\,dx + \mathcal{R}$, where S depends algebraically on the upper limits P.

$$\int_O^{P_0} \rho(x,y)\,dx + \int_O^{P_1} \rho(x,y)\,dx + \cdots + \int_O^{P_N} \rho(x,y)\,dx = \int_O^{S_1} \rho(x,y)\,dx + \cdots + \int_O^{S_g} \rho(x,y)\,dx + \mathcal{R}$$

$$\int_O^{P_0} \rho(x,y)\,dx + \int_O^{P_1} \rho(x,y)\,dx + \cdots + \int_O^{P_N} \rho(x,y)\,dx = \int_O^{S_1} \rho(x,y)\,dx + \cdots + \int_O^{S_g} \rho(x,y)\,dx + \mathcal{R}$$

$$\int_O^P \frac{dx}{y} + \int_O^Q \frac{dx}{y} = \int_O^S \frac{dx}{y}$$

i.e. $$\int_O^P \frac{dx}{y} + \int_S^Q \frac{dx}{y} = 0$$

If X has poles at P, Q and zeros at O, S then $\frac{dX}{Y}$ is a nonzero constant times $\frac{dx}{y}$, so the desired integral is a constant times $\int_O^P \frac{dX}{Y} + \int_S^Q \frac{dX}{Y}$ which is zero because Y has opposite signs on the two branches over X.

More generally, the integral from O to P plus the integral from S to Q is

$$\int_0^\infty ((\bar{\rho}(X, Y_1) + \bar{\rho}(X, Y_2))\, dX$$

which is the integral of a rational function of X.

When $N = g$ the general formula is

$$\int_O^{P_0} \rho(x,y)\,dx + \int_{S_1}^{P_1} \rho(x,y)\,dx + \cdots$$

$$+ \int_{S_g}^{P_g} \rho(x,y)\,dx = \mathcal{R}$$

or, what is the same

$$\int_O^{P_0} + \int_O^{P_1} + \cdots + \int_O^{P_g} = \int_O^{S_1} + \int_O^{S_2} + \cdots + \int_O^{S_g} + \mathcal{R}.$$

Given an algebraic function y of x, there is a number g with the property that the sum of any $g+1$ integrals $\int_O^{P_i} \rho(x,y)\,dx$ can be written as a sum of just g such integrals $\int_O^{S_i} \rho(x,y)\,dx$ plus a remainder $\mathcal{R}$, which is an integral of a rational function. The S_i depend *algebraically* on the P_i and do not depend on the integrand $\rho(x,y)\,dx$.

When it is coupled with some simple observations about the "holomorphic" integrands $\rho(x, y)\,dx$ for which the remainder term $\mathcal{R}$ is necessarily zero, this theorem is a natural and far-reaching generalization of the basic addition formula $\int_O^P \frac{dx}{\sqrt{1-x^4}} + \int_O^Q \frac{dx}{\sqrt{1-x^4}} = \int_O^S \frac{dx}{\sqrt{1-x^4}}$

Compute with expressions

$$\frac{\psi(x,y)}{\phi(x)}$$

(numerator and denominator are polynomials with integer coefficients) in the usual way but with the added relation $y^2 = 1 - x^4$.

Given any z in $\mathbf{Q}(x, y)$ that is not a constant, there is a "primitive element" w that satisfies a relation of the form $\chi(z, w) = 0$ with the property that adjunction of one root w of $\chi(z, w)$ to $\mathbf{Q}(z)$ gives the entire field $\mathbf{Q}(x, y)$. In short, there is a w for which the given $\mathbf{Q}(x, y)$ has a presentation as $\mathbf{Q}(z, w)$.

The degree of $\chi(z, w)$ in w is the **order** of z, the number of times z assumes each of its values (multiplicities counted).

$$\frac{y - ax^2 - bx - c}{x^2} = \frac{y}{x^2} - a - bu - cu^2$$

is integral over $u = \frac{1}{x}$ because

$$(\frac{y}{x^2})^2 = \frac{1 - x^4}{x^4} = u^4 - 1.$$

The curves $y^2 = 1 - x^4$ and $v^2 = u^4 - 1$ are birationally equivalent via $u = \frac{1}{x}$ and $v = \frac{y}{x^2}$. The points where $x = \infty$ are the points where $u = 0$.

The nature of

$$\frac{y - a'x^2 - bx - c}{y - ax^2 - bx - c}$$

at $x = \infty$ can be seen by dividing numerator and denominator by x^2 to find

$$\frac{v - a' - b'u - c'u^2}{v - a - bu - cu^2}.$$

It has no zero or pole at $u = 0$ as long as a and a' avoid the values of v at this point (which are $v = \pm i$).

To say that a basis y_1, y_2, …, y_n of the function field over x is *normal* means that

$$\phi_1(x)y_1 + \phi_2(x)y_2 + \cdots + \phi_n(x)y_n$$

is integral over x if and only if the $\phi_i(x)$ are polynomials and it has poles of order at most ν at $x = \infty$ if and only that is apparent—that is, if and only if $\deg \phi_i + e_i \leq \nu$ where e_i is the multiplicity of the poles of the y_i. (In other words, e_i is the smallest integer for which $\frac{y_i}{x^{e_i}}$ is finite at $x = \infty$.)

Functions of the form

$$\phi_1(x)y_1 + \phi_2(x)y_2 + \cdots + \phi_n(x)y_n$$

where $\deg \phi_i + e_i \leq \nu$ all have the same $n\nu$ poles at $x = \infty$ (provided zeros of $x^{-\nu}$ times it at $x = \infty$ are avoided) and contain $n\nu - g + 1$ variable coefficients when $g - 1 = \Sigma(e_i - 1)$. Therefore, a quotient of two such functions can be constructed with $g + 1$ chosen zeros and no others, by virtue of a count of parameters.

The count: Number of variable coefficients: $\Sigma(\nu - e_i + 1)$.

Number of zeros: $n\nu$.

Number of unwanted zeros in the numerator: $n\nu - g - 1$.

Number of degrees of freedom in the variation of the zeros: $\Sigma(\nu - e_1 + 1) - 1$.

Need: $\Sigma(\nu - e_i + 1) - 1 > n\nu - g - 1$ i.e., $-\Sigma(e_i - 1) > -g$, i.e.,

$$g \geq 1 + \Sigma(e_i - 1).$$

Abel's Theorem *For the field of rational functions on the curve* $\chi(x, y) = 0$, *the number* $g = 1 + \Sigma(e_i - 1)$ *found by constructing a normal basis has the property that any set of* $g + 1$ *points on the curve is the zero set of a rational function on the curve (i.e., there is a rational function of order* $g + 1$ *that is zero at them). Moreover, no smaller* g *has this property.*

Abel: Si l'on a plusieurs fonctions dont les dérivées peuvent être racines d'une *même équation algébrique,* dont tous les coefficients sont des fonctions *rationelles* d'une même variable, on peut toujours exprimer la somme d'un nombre quelconque de semblables fonctions par une fonction *algébrique* et *logarithmiques,* pourvu qu'on établisse entre les variables des fonctions en question un certain nombre de relations *algébriques.*

Le nombre de ces relations ne dépend nullement du nombre des fonctions, mais seulement de la nature des fonctions particulières qu'on considère.