RATIONAL PARAMETRIZATION OF CONICS

1. The General Situation

Let k denote any field, and let K be any extension field of k, possibly $K = k$.

A *line defined over* k is an equation

$$\mathcal{L} : Ax + By = C, \quad A, B, C \in k,$$

where at least one of A, B is nonzero. A K*-rational point of* $\mathcal{L}$ is a solution $(x, y) \in K^2$ of $\mathcal{L}$. The set of K-rational points of $\mathcal{L}$ is denoted $\mathcal{L}_K$.

Similarly, a *conic curve defined over* k is an equation

$$\mathcal{C} : ax^2 + bxy + cy^2 + dx + ey + f = 0, \quad a, b, c, d, e, f \in k,$$

where at least one of a, b, c nonzero. A K*-rational point of* $\mathcal{L}$ is a solution $(x, y) \in K^2$ of $\mathcal{C}$, and the set of K-rational points of $\mathcal{L}$ is denoted $\mathcal{C}_K$. (Note: $\mathcal{C}_K$ may not contain any points at all. For example, let $k = K = \mathbb{R}$ and consider the conic curve $C : x^2 + y^2 = -1$.)

Proposition 1.1. *Suppose that $\mathcal{C}_K$ contains a point $P = (x_P, y_P)$ not in $\mathcal{L}_K$. Then the points of $\mathcal{C}_K$ other than P are in bijective correspondence with the points of $\mathcal{L}_K$.*

Proof. First note that after a coordinate translation, we may let $P = (0, 0)$, although now the coefficients of $\mathcal{L}$ and $\mathcal{C}$ could lie in K rather than k.

For any given point $Q = (x_Q, y_Q) \in \mathcal{C}_K$ such that $Q \neq P$, let $t = y_Q/x_Q \in K$ and then solve the equation $\mathcal{L}(x, tx)$ for a unique $x_R \in K$. Let $y_R = tx_R$. The point $R = (x_R, y_R) \in \mathcal{L}_K$ is collinear with P and Q.

Conversely, for any given point $R = (x_R, y_R) \in \mathcal{L}_K$ such that $R \neq P$, let $t = y_R/x_R \in K$ and then consider the equation $\mathcal{C}(x, tx)$. This quadratic equation has $x = 0$ as a solution, but after dividing the equation through by x there is a unique second solution $x_Q \in K$. (Possibly $x_Q = 0$ as well.) Let $y_Q = tx_Q$. The point $Q = (x_Q, y_Q) \in \mathcal{C}_K$ is collinear with P and R.

The argument here has left out the case where all the x-coordinates agree. This situation can be handled as a special case. $\square$

Note that the fields k and K in this discussion are completely general. For example, k could be the field of p elements for some prime p, and K could be the field of $q = p^e$ elements for some positive integer e.

2. The Circle in Particular

Now define

$$\mathcal{L} : x = 0,$$
$$\mathcal{C} : x^2 + y^2 = 1,$$

and let $P = (-1, 0)$, an element of $\mathcal{C}_k$ for any field k.

Given a point $Q = (x_Q, y_Q) \in \mathcal{C}_K$, the corresponding point on $\mathcal{L}_K$ is

$$R = \left(0, \frac{y_Q}{x_Q + 1}\right).$$

Conversely, given a point $R = (0, y_R) \in \mathcal{L}_K$, let $t = y_R$. We seek a point $Q = (x, t(x+1)) \in \mathcal{C}_K$. But

$$x^2 + y^2 = ((x+1) - 1)^2 + t^2(x+1)^2 = (1+t^2)(x+1)^2 - 2(x+1) + 1,$$

so we want

$$(1+t^2)(x+1)^2 - 2(x+1) = 0,$$

or $(1+t^2)(x+1) = 2$, or $x + 1 = 2/(1+t^2)$. Since $y = t(x+1)$ it follows that $y = 2t/(1+t^2)$, so that finally,

$$Q = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

3. An Application From Calculus

Let θ denote the angle to a point $(x, y) \in \mathcal{C}_{\mathbb{R}}$. Then the quantity t in the previous discussion is

$$t = \tan(\theta/2).$$

Thus $\theta = 2\arctan(t)$, giving the third of the equalities

$$\boxed{\cos(\theta) = \frac{1-t^2}{1+t^2}, \quad \sin(\theta) = \frac{2t}{1+t^2}, \quad \mathrm{d}\theta = \frac{2\,\mathrm{d}t}{1+t^2}.}$$

The rational parametrization of the circle gives rise to the substitution in elementary calculus that reduces any integral of a rational function of the transcendental functions $\cos(\theta)$ and $\sin(\theta)$ of the variable of integration θ to the integral of a rational function of the variable of integration t.

4. An Application From Elementary Number Theory

A *primitive Pythagorean triple* takes the form

$$(a, b, c) \in \mathbb{Z}^3, \quad a^2 + b^2 = c^2, \quad a, b, c > 0, \quad \gcd(a, b, c) = 1.$$

It follows that in fact a, b, and c are pairwise coprime. We may take a odd, b even, and c odd. (Inspection modulo 4 shows that the case where a and b are odd but c is even can't arise.)

Given such a triple, let $x = a/c$ and $y = b/c$. Then (x, y) is a point of $\mathcal{C}_{\mathbb{Q}}$,

$$(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right), \quad t = s/r \in \mathbb{Q}.$$

It follows that

$$(x, y) = \left(\frac{r^2 - s^2}{r^2 + s^2}, \frac{2rs}{r^2 + s^2}\right), \quad s, r \in \mathbb{Z}.$$

Here we take $0 < s < r$, $\gcd(r, s) = 1$. If in addition, r and s have opposite parities then the quotients will be in lowest terms, so that

$$\boxed{(a, b, c) = (r^2 - s^2, 2rs, r^2 + s^2).}$$

Thus we can systematically write down all Pythagorean triples in a table. The table begins as follows.

	$r = 2$	$r = 3$	$r = 4$	$r = 5$	$r = 6$	$r = 7$
$s = 1$	$(3, 4, 5)$		$(15, 8, 17)$		$(35, 12, 37)$	
$s = 2$		$(5, 12, 13)$		$(21, 20, 29)$		$(45, 28, 53)$
$s = 3$			$(7, 24, 25)$			
$s = 4$				$(9, 40, 41)$		$(33, 56, 65)$
$s = 5$					$(11, 60, 61)$	
$s = 6$						$(13, 84, 85)$