August 2001.

Circle Group and Projective Line.

1. For any field K of characteristic $\neq 2$, the *circle group* $S^1(K)$ consists of ordered pairs $x, y \in K$ such that $x^2 + y^2 = 1$, with multiplication

$$(x, y) \cdot (u, v) = (xu - yv, xv + yu)\,. \qquad (*)$$

By abuse of language, K will be called "real" or "complex" depending on whether X^2+1 is or is not irreducible. In either case, let $K[i]$ be the quadratic ring extension with $i^2 = -1$, and $N : K[i] \longrightarrow K$ denote its norm map. For a typical element $a + bi$ of $K[i]$, this norm equals $(a + bi)(a - bi) = a^2 + b^2$. Thereby $S^1(K)$ becomes the subgroup $\ker N \subseteq K[i]^\times$.

Proposition: *If K is complex, and $\iota \in K$ satifies $\iota^2 = -1$, the map $(a, b) \mapsto (a+\iota b)$ defines an isomorphism $S^1(K) \simeq K^\times$. If K is real, the inclusion $\ker N \subset S^1(K[i])$ identifies $S^1(K)$ with a multiplicative subgroup of the complex field $K[i]$.*

The first statement comes from $(a + bi) \mapsto (a + \iota b, a - \iota b)$ defining a ring isomorphism $K[i] \longrightarrow K \oplus K$ which maps $\ker N$ onto $\{(c, c^{-1})\}$. The second statement is obvious.

If K has q elements, the cardinality of $S^1(K)$ is $(q^2 - 1)/(q - 1) = q + 1$ or $q - 1$ elements, depending on whether K is real or complex. In either case, $S^1(K)$ is cyclic.

2. As we all know, the Ancients invented the famous map

$$\delta :\ P^1(K) \longrightarrow P^2(K) \quad \text{by} \quad \delta(u, v) = (u^2 - v^2,\, 2uv, u^2 + v^2)\,, \qquad (\dagger)$$

whose image lies on the curve Δ defined by $x^2 + y^2 = z^2$. It is clearly injective, since any given $u^2 - v^2 = a$ and $u^2 + v^2 = c$ determine a $(u, \pm v)$, and the sign is fixed (up to homogeneity) by the second component of $\delta(u, v)$. In fact, $\delta : P^1(K) \longrightarrow \Delta$ is bijective, since $(2uv)^2$ is the difference $c^2 - a^2$ so that $2uv$ could be set equal to b, if we are aiming at a point (a, b, c) such that $a^2 + b^2 = c^2$.

If K is closed under square roots, any "conic" can be given the form $x^2 + y^2 = z^2$, and therefore is isomorphic to $P^1(K)$.

A more geometric view of the bijection $\delta :\ P^1(K) \longrightarrow \Delta$ is obtained by identifying $P^1(K)$ with the pencil of lines passing through the point $(-1, 0, 1)$. Their equations are of the form $x + z = ty$, and each of them (except the one with $t = 0$) intersects Δ in exactly one other point. Indeed, $y^2 = z^2 - x^2 = (z + x)(z - x)$ together with $t^2y^2 = (z + x)^2$ and $z + x \neq 0$ implies $z + x = t^2(z - x)$, i.e., $(t^2 + 1)x = (t^2 - 1)z$. Unravelling that equation yields $(x, y, z) = \delta(t, 1)$.