On Finite Conics

Hendrik Van Maldeghem*

A conic in a (classical) finite projective plane is never empty. This well-known result usually is proved by elementary algebra, using the properties of squares in a finite field, manipulating a quadratic equation, distinguishing between odd and even characteristic. Teaching projective geometry to students of the second year, I discovered a very nice geometric proof of that fact, independent of the characteristic. I do not claim originality, but I do not know of any source where one might find this proof.

Of course, since conics are algebraic creatures (in odd characteristic, one might think of a *non-degenerate* conic as the set of absolute points of a certain kind of polarity, but this goes wrong for even characteristic), we must use algebra at a certain point, but we can arrange it so that we do not need to write down algebraic expressions. Hence we have a fairly complete synthetic proof. Let us start with the definition and the reduction to *non-degenerate* conics.

Definition. Let $\mathbf{PG}(2,q)$ be the projective plane coordinatized by the field $\mathbf{GF}(q)$ of q elements. A *conic* in $\mathbf{PG}(2,q)$ is the set of points whose coordinates (x,y,z) satisfy a homogenious quadratic equation in X,Y,Z (with obvious notation).

Let $\mathcal{C}$ be a conic in $\mathbf{PG}(2,q)$. If the corresponding quadratic equation splits over $\mathbf{GF}(q^2)$ into the product of two linear equations, then $\mathcal{C}$ is non-empty. Indeed, either the two linear equations have coefficients in $\mathbf{GF}(q)$ (and obviously $\mathcal{C}$ is non-empty in $\mathbf{PG}(2,q)$), or the two linear equations are conjugate (and the intersection point of the corresponding distinct lines is a point of $\mathbf{PG}(2,q)$). Hence we may assume that the quadratic equation of $\mathcal{C}$ is irreducible over $\mathbf{GF}(q^2)$. We say that $\mathcal{C}$ is *non-degenerate*. We need one more algebraic observation:

A line meets a conic in either 0, 1, 2 *or* $q+1$ *points.*

Indeed, the intersection of a line and a conic boils down to a quadratic equation in one variable.

Now note that we did not need any explicit calculation to prove the foregoing properties. Nothing depends on the field either and all properties (also the last!) can be stated for general fields.

*Senior Research associate of the Belgian National Fund for Scientific Research

We can now prove that $\mathcal{C}$ is non-empty. Suppose on the contrary that $\mathcal{C}$ is empty. Let $\mathcal{C}'$ be the conic in $\mathbf{PG}(2, q^2)$ obtained from $\mathcal{C}$ by considering the quadratic equation defining $\mathcal{C}$ over $\mathbf{GF}(q^2)$. Let L be any line of $\mathbf{PG}(2, q)$. The intersection of L with $\mathcal{C}$ is given by a quadratic equation. This equation has no solution in $\mathbf{GF}(q)$, hence it has exactly two solutions in $\mathbf{GF}(q^2)$. Consequently every line of $\mathbf{PG}(2, q)$ contains two points of $\mathbf{PG}(2, q^2)$ on $\mathcal{C}'$. If x is such a point, then it does not lie on two distinct lines of $\mathbf{PG}(2, q)$, otherwise it is a point of $\mathcal{C}$. Hence we deduce that $\mathcal{C}'$ has at least $2(q^2 + q + 1)$ points. Let x be such a point. There are precisely $q^2 + 1$ lines in $\mathbf{PG}(2, q^2)$ through x. It follows that at least one of them, say M, must contain at least 3 points of $\mathcal{C}'$, hence, by the above observation, $\mathcal{C}'$ contains all points of M. So $\mathcal{C}'$ contains also all points of the conjugate M' of M, and hence also the intersection point of M and M', which is a point of $\mathbf{PG}(2, q)$. This implies that $\mathcal{C}$ is non-empty.