Chapter 8

Conics over Finite Fields

Note that the conic \( X^2 + Y^2 = 3Z^2 \) does not have a point defined over \( \mathbb{Q} \). Over finite fields, the situation is different:

**Proposition 8.0.4.** Let \( C \) be a nondegenerate conic defined over a finite field \( \mathbb{F}_p \). Then \( C(\mathbb{F}_p) \) contains an affine point defined over \( \mathbb{F}_p \).

In particular this implies that every nondegenerate conic over \( \mathbb{F}_p \) is equivalent to the standard conic \( XY + YZ + ZX = 0 \).

**Proof.** The general conic is defined by an equation

\[
ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{8.1}
\]

Assume first that \( p > 2 \). If \( c = 0 \), the claim is clear (note that if \( c = b = e = 0 \), then the conic is degenerate). Assume therefore that \( c \neq 0 \). Multiplying through by \( a \) and completing the square shows that the substitution \( x' = ax + \frac{b}{2}y \) leads to a new equation in which \( b = 0 \). Afterwards, we can get rid of the term \( aey \) by a similar trick. Finally, we can achieve that \( c = 1 \).

Thus we may assume that the conic has the form \( y^2 = f(x) \) for some linear or quadratic polynomial \( f \). If \( f \) is linear, it has a zero \( x = r \), and \((r, 0)\) is a point on the affine conic.

If \( f \) is quadratic, it attains exactly \( \frac{p+1}{2} \) different values (this is trivial for \( f(x) = x^2 \), to which the general case easily reduces). Since there are exactly \( \frac{p+1}{2} \) nonsquares in \( \mathbb{F}_p \), at least one of the values of \( f \) must be a square, say \( f(r) = s^2 \); then \((r, s)\) is a point on the affine conic.

Now consider the case \( p = 2 \) and assume that the conic (8.1) defined over \( \mathbb{F}_2 \) does not have an affine point. Plugging in \( x = 0 \) we immediately see that we must have \( c = e = f = 1 \). Plugging in \( y = 0 \) we similarly get \( a = d = 1 \). Plugging in \( x = 1 \) finally gives \( b = 0 \). Thus the only conic without an affine point over \( \mathbb{F}_2 \) is \( x^2 + y^2 + x + y + 1 = 0 \). Its projective closure is \( x^2 + y^2 + xz + yz + z^2 \); it has three points at infinity, namely \([0 : 1 : 0] \), \([1 : 0 : 0] \) and \([1 : 1 : 0] \). Thus \( C \) contains the line at infinity and must be degenerate. In fact, the last point is singular. \( \square \)
Thus there is essentially only one smooth conic with a $K$-rational point over $K$. Something similar does not hold for cubics: it can be shown that smooth cubics defined over $K$ and with a $K$-rational point (such curves are called elliptic curves) can be transformed into cubics of Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

but the necessary transformations are in general not projective but birational. Thus the world of elliptic curves is much richer than that of conics.

### 8.1 Group Laws on Nonsingular Conics

Let $C$ be a nondegenerate conic defined over some field $K$, and assume that $C$ has a $K$-rational point, which we will denote by $N$. We then can define a group law on $C(K)$ as follows: given $P, Q \in C(K)$, let $P + Q$ be the second point of intersection with $C$ of the line through $N$ parallel to $PQ$; if $P = Q$, the line $PQ$ is taken to be the tangent at $P$.

This addition law is clearly abelian; the neutral element is $N$, and the inverse of a point $P$ is the second point of intersection with $C$ of the line through $P$ parallel to the tangent at $N$.

It remains to show that the addition is associative. Assume that we are given points $P, Q, R$ on the conic; let $A = P + Q$ and $B = Q + R$. Then $PQRANB$ is a hexagon on the conic. Moreover, we know that

- $PQ \parallel AN$ since $P + Q = A$, and
- $QR \parallel BN$ since $Q + R = B$.

Now associativity is equivalent to $A + R = P + B$, i.e. to $AR \parallel PB$. But since the points of intersection $PQ \cap AN$ and $QR \cap BN$ lie on the line at infinity, by Pascal’s theorem the same must be true of $AR \cap PB$. Note that this proof is only valid if no two of the six points $P, Q, R, A, B, N$ coincide. The other cases must be handled one by one.