Lesson 3 – The Group Law on the Unit Circle – Just for Fun!

In algebraic geometry, an *algebraic group* or *group variety* is a variety that is also a group. Elliptic curves are group varieties, and so is the unit circle. Here we present the group law on the unit circle $\mathcal{C}: x^2 + y^2 = 1$ in three different contexts: algebraic, analytic and geometric.

The Algebraic Approach

The algebraic group law is the one that is described most easily. Given two points $P = (x, y)$ and $Q = (u, v)$ in $\mathbb{R}^2$, we simply define the sum $P + Q$ by

$$P + Q = (ux - vy, xv + yu). \qquad (1)$$

It is then trivial (tedious!) to verify the group axioms. As usual, checking associativity is the hardest part - and best accomplished with the help of a computer. Below is the code you might use to compute $(P_1 + P_2) + P_3 = (w, z)$, where $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and $P_3 = (x_3, y_3)$.

```
> u = x1*x2-y1*y2: v = x1*y2+y1*x2: w = u*x3-v*y3: z = u*y3 + vx3
```

In a similar way, you can compute $P_1 + (P_2 + P_3)$, and check that the two sums are equal.

Exercise 1 What does this really mean??? Where is this formula for the sum coming from?

The Analytic Approach

We have seen already that the real points on the unit circle are parameterized by trigonometric functions; in particular, there is a bijection between the real interval $[0, 2\pi)$ and the unit circle $\mathcal{C}$ via the map $\varphi: \mathbb{R}/2\pi\mathbb{Z} \to \mathcal{C}$, defined by $\varphi(\alpha) = (\cos\alpha, \sin\alpha)$. Since $\mathbb{R}/2\pi\mathbb{Z}$ is an abelian group under addition, we can make $\mathcal{C}$ into a group by a "transport of structure"...

Exercise 2 Derive the addition formula (1) by transporting the group structure of $\mathbb{R}/2\pi\mathbb{Z}$ onto $\mathcal{C}$.

The Geometric Approach

When defining the geometric group law, we start by choosing a "neutral" element (which will serve as the identity in the group). Any rational point on the unit circle will do, but in order to get the same group law as above, we need to pick $N = (1, 0)$. Given two points $P = (x, y)$ and $Q = (u, v)$, consider the line parallel to PQ through N; it will intersect the unit circle in N and a second point (possibly coinciding with N) that we call $P + Q$.

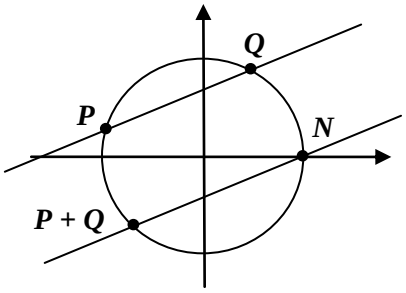

Figure 2: The Geometric Group Law

It is easy to verify all group axioms with the exception of associativity: this requires a special case of Pascal's Theorem in the general case. A geometric argument can be used to show that the addition law just defined corresponds to adding angles: $\angle NO(P + Q) = \angle NOP + \angle NOQ$. It is also clear that the sum of two rational points has to be rational again, so we also get a group law on the set of rational points on $\mathcal{C}$.

Exercise 3 Show that

$$P + Q = \left(\frac{(y-v)^2 - (x-u)^2}{(y-v)^2 + (x-u)^2}, -2\frac{(y-v)(x-u)}{(y-v)^2 + (x-u)^2}\right)$$

This might not look like the addition formulas we computed from the algebraic definition – yet they are the same, as a simple (though tedious) calculation can show.