

Borcherd Algebraic Geometry 1

Rindra Razafy, “Hagamenana”

July 13, 2022

Contents

| | | |
|----------|---------------------------------|----------|
| 0 | Prologue | 2 |
| 1 | Introduction | 3 |
| 1.1 | Examples | 3 |
| 1.1.1 | Pythagorean triangles | 3 |
| 2 | Two cubic curves | 4 |
| 3 | Bézout, Pappus, Pascal | 5 |
| 3.1 | Bézout’s theorem | 5 |
| 3.2 | Pappus’ theorem | 5 |
| 3.3 | Pascal’s theorem | 5 |

0 Prologue

Some quick notes summarising the “Algebraic geometry 1” video lectures from R.E. Borcherds, found [here](#)

1 Introduction

1.1 Examples

1.1.1 Pythagorean triangles

Problem: How do we classify all Pythagorean triangles.

We will look at two ways of solving this:

1. **Algebraic way:** We want to solve

$$x^2 + y^2 = z^2 \text{ with } x, y, z \text{ coprime integers} \quad (1)$$

If we look at the equation mod 4 we notice that $x^2, y^2, z^2 \equiv 0, 1 \pmod{4}$, since the squares mod 4 all take these forms. So z is odd and WLOG we assume that x is even and y is odd. We rearrange the equation:

$$y^2 = z^2 - x^2 = (z - x)(z + x) \quad (2)$$

Assume that $z - x = dm_1$ and $z + x = dm_2$, therefore we have that $2z = d(m_1 + m_2)$ and $2x = d(m_2 - m_1)$, then since $d \mid 2z$ and $d \mid 2x$, and $\gcd(x, z) = 1$ we have two cases, either d divides both x and z , which would imply that $d = 1$.

Or d divides 2 which means that $d = 1$, or $d = 2$. But note that since x, z are of opposite parity $z + x$ is odd so $d \neq 2$.

So in all cases, $d = 1$. So $(z - x)$ and $(z + x)$ are coprime.

But since their product is a square this implies that $z - x$ and $z + x$ are squares, so:

$$z - x = r^2, \text{ and } z + x = s^2, \text{ where } s, r \text{ are odd and coprime} \quad (3)$$

So we conclude that $z = \frac{r^2 + s^2}{2}$, $x = \frac{s^2 - r^2}{2}$, $y = rs$ for any r, s odd and coprime.

2. **Geometric solution** Let $X = \frac{x}{z}$, $Y = \frac{y}{z}$ and we want to solve

$$X^2 + Y^2 = 1, \quad X, Y \text{ rational} \quad (4)$$

So we are looking for rational points on the unit circle.

Note if we draw the line from $(-1, 0)$ to (X, Y) on the unit circle with $X, Y \in \mathbb{Q}$. It will intersect the y -axis at the point $(0, t)$ where $t = \frac{Y}{X+1} \in \mathbb{Q}$.

Conversely, if we are given t we can find (X, Y) , since we know that

$$Y = t(X + 1) \text{ and } t^2(X + 1)^2 + X^2 = 1 \Rightarrow (X + 1)((t^2 + 1)X + t^2 - 1) = 0$$

And finding roots we see that $X = \frac{1-t^2}{1+t^2}$ and $Y = \frac{2t}{1+t^2}$, for $t \in \mathbb{Q}$.

So there is a correspondence between points on the circle except for the point at $(-1, 0)$ and points on the y -axis. This is what is called a Birational Equivalence.

Definition 1.1. Birational Equivalence An equivalence excepts on subsets of co-dimension at least 1.

Treating this problem as a geometrical problem gives us additional insights. Indeed, for example the circle forms a group of rotations with operation:

$$(x_1, y_1) \times (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \quad (5)$$

This is the cosine and sign of the sum of two angles, indeed if $(x_1, y_1) = (\cos \theta_1, \sin \theta_1)$ and $(x_2, y_2) = (\cos \theta_2, \sin \theta_2)$ then:

$$(\cos \theta_1, \sin \theta_1) \times (\cos \theta_2, \sin \theta_2) = (\cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2, \dots) = (\cos(\theta_1 + \theta_2), \sin(\theta_1 + \theta_2)) \quad (6)$$

This is the simplest example of what is called an Algebraic group.

Definition 1.2. Algebraic Groups We can think of this as functor from (commutative) Rings to Groups.

$$G: R \rightarrow (\{(x, y) \in R^2 \mid x^2 + y^2 = 1\}, \times) \quad (7)$$

Where the operation is defined as above, and the identity is $(1, 0)$ and $(x, y)^{-1} = (x, -y)$.

Example 1.2.1. $G(\mathbb{C}) = \{(x, y) \in \mathbb{C} \mid x^2 + y^2 = 1\}$

But note that $1 = x^2 + y^2 = \underbrace{(x + iy)}_z \underbrace{(x - iy)}_{\bar{z}}$. So we see that

$$G(\mathbb{C}) = \{(x, y) \in \mathbb{C} \mid x^2 + y^2 = 1\} \simeq \{z \in \mathbb{C} \mid z \text{ is invertible}\} = \mathbb{C}^* \quad (8)$$

Summary There are many ways to view a circle:

1. Subset of \mathbb{R}^2
2. Polynomial $x^2 + y^2 - 1 \rightarrow$ Algebraic set
3. Ideal $(x^2 + y^2 - 1)$ in ring $\mathbb{R}[x, y]$.
4. Ring $\mathbb{R}[x, y]/(x^2 + y^2 - 1) =$ coordinate ring of S^1 . Can be seen as the set of polynomials on the circle.
5. (Smooth) manifold
6. Group (Algebraic Group)
7. Functor from Rings to Groups or Sets (Grothendieck)

2 Two cubic curves

In this section we will discuss some cubic curves.

1. $y^2 = x^3 + x^2$

There is almost a 1-to-1 correspondence between (x, y) rational on this curve and $t \in \mathbb{Q}$, via $t = \frac{y}{x}$, the slope of the line through (x, y) and the origin. Indeed since $y = tx$, if $x \neq 0$, we have:

$$t^2 x^2 = x^3 + x^2 \Rightarrow t^2 = 1 + x \Rightarrow x = t^2 - 1 \text{ and } y = t^3 - t \quad (1)$$

We don't quite get a 1-1 correspondence because $t = 1$ and $t = -1$ both correspond to $(x, y) = (0, 0)$.

So we can think of this cubic curve as a copy of \mathbb{Q} , but two of these points are mapped to the same point.

Definition 2.1. Resolution of Singularity A singularity is a “bad” point of our curve, and a resolution is getting a “nice” map from a curve without singularities to our curve.

The resolution in the above case is done by a process called “blowing-up”.

Remark. Hironaka, showed that blowing-up resolves singularities in zero characteristic. (The problem in non-zero characteristic is still unsolved).

Remark. Finding rational points on curves can be difficult. For example:

$$x^n + y^n = 1 \Rightarrow X^n + Y^n = Z^n \text{ where } x = X/Z \text{ and } y = Y/Z \quad (2)$$

This is Fermat's Last Theorem, which was very hard to solve.

2. $x^3 + y^3 = 9$

Note on this curve we can define an algebraic operation “+”, if we add in a point at infinity. In that case, the point at infinity is the identity “0”, and a, b, c on the curve lie on a line if and only if $a + b + c = 0$ in the group. To check that the group operation is associative we use the fact that: $a_1 + a_2 + \dots = b_1 + b_2 + \dots \iff$ there is a rational function with poles at a_i and zeroes at the b_i .

Definition 2.2. Groups of this kind are called **elliptic curves**, there are the 1-dimensional case of what is called **Abelian varieties**. Abelian varieties are algebraic groups that are “projective”, roughly they have no missing points.

3 Bézout, Pappus, Pascal

3.1 Bézout's theorem

Theorem 1. Bézout *Informally: Two curves of degree m, n in the plane have at most mn intersection, if they have no components in common.*

Stronger version of Bézout *There have exactly mn intersection points if:*

1. We are working over \mathbb{C}
2. Count points at infinity
3. Counting multiplicities (for example a straight line tangent to a parabola, we need to count the intersection point as two points).

This theorem was originally stated by Newton, though he didn't really prove it.

It is actually quite difficult to make sense of multiplicities.

Proof. Informal proof: Suppose the curves are $f(x, y) = 0$ of degree m and $g(x, y) = 0$ of degree n .

Perturb f, g so that $f = p_1 \dots p_m$ and $g = q_1 \dots q_n$, with p_i, q_j linear.

Problem: How do we know the number of intersection points doesn't change as we perturb f, g □

This style of proof was very common in the Italian School of Algebraic Geometry, but with these informal reasonings caused them to introduce many false theorems.

Weil and Zariski put Algebraic Geometry on much firmer foundations, but the proofs became much more complicated.

Nowadays, these informal proofs are mostly useful just to guess what the right answer is (for example understanding the reasoning for the above proof, we can understand the reasoning for the analogue of Bézout's theorem in higher dimensions).

3.2 Pappus' theorem

Theorem 2. *Informally: Take two straight lines in the plane and on each line choose any three points. Number them and join them to every point of a different number on the other line, looking at the intersection point of these lines. These three intersection points lie on a straight line.*

This theorem is equivalent to commutativity in multiplication. If we look at the analogous result in a plane over a division ring then:

Pappus' theorem is true \iff The division ring is a field (so multiplication commutes)

3.3 Pascal's theorem

Theorem 3. *Informally: Choose any six points on an ellipse, separate your ellipse into two, so that three points lie on one side and three points lie on the other side. Number the points on the first side as 1,2,3 and likewise for the points on the other side. then join them to every point of a different number on the opposite side, looking at the intersection point of these lines. These three intersection points lie on a straight line.*

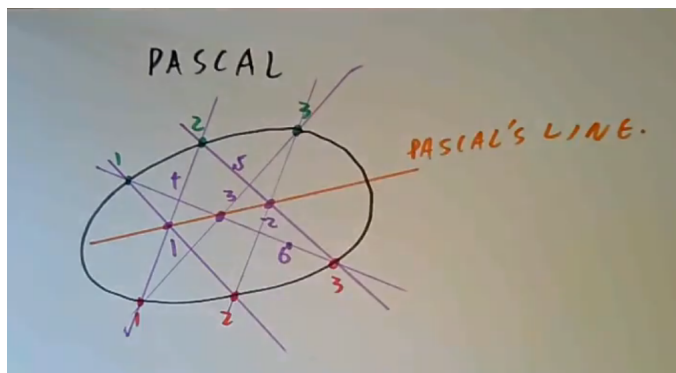


Illustration from the lecture video

The line on which their intersection lies is called the **Pascal line**.

Pappus' theorem is a degenerate case of Pascal's theorem, Pascal's theorem holds for any degree two curve and two straight lines are a degenerate case of a degree 2 curve.

How do we prove Pascal's theorem? We will use a proof using Algebraic Geometry and Bézout's theorem.

Proof. We number the lines as in the picture above (noting that they form a funny kind of hexagon) and choose six linear polynomials, p_i , for $i \in \{1, \dots, 6\}$ where $p_i = 0$ on line i .

Now look at $p_1p_3p_5$ and $p_2p_4p_6$, these polynomials vanish on all six points, so choose λ such that:

$$p_1p_3p_5 - \lambda p_2p_4p_6 \text{ this is of degree 3 curve} \tag{1}$$

Vanishes on a seventh point of the conic. Since the conic is of degree 2, by Bézout there are at most 6 intersection points UNLESS they have a common component. So the conic must be contained in the degree 3 curve.

So this degree 3 curve is equal to the union of a conic and a line, which is Pascal's line. Indeed since $p_1p_3p_5$ and $p_2p_4p_6$ both vanish on the three intersection points, since they are on the curve but not on the conic, they must be on the line. \square