

Pries: M466-Groups, Rings, and Fields

Homework 11: Projective plane and elliptic curves.

Due Wednesday 11/7

Read: Handouts.

Problems:

- Using lines through $P = (-1, 0)$, find an explicit bijection between $\mathbb{P}_{\mathbb{Q}}^1 = \mathbb{Q} \cup \{\infty\}$ and the rational points on the circle $x^2 + y^2 = 1$. Explain your proof geometrically.
- Find the points at ∞ in $\mathbb{P}_{\mathbb{R}}^2$ and in $\mathbb{P}_{\mathbb{C}}^2$ for the following curves (where a and b are positive real numbers):
 - Ellipse $ax^2 + by^2 = 1$;
 - Hyperbola $ax^2 - by^2 = 1$;
 - Parabola $y = ax^2 + b$.
- Fano's geometry:
 - Draw a circle inscribed in an equilateral triangle. Draw dots at the vertices, midpoints of edges, and center of the triangle. Draw a line segment from each vertex to the midpoint of the opposite side.
 - How many equivalence classes of points $P = [x : y : z]$ does the projective plane $\mathbb{P}_{\mathbb{F}_2}^2$ have? How many lines $L : \alpha x + \beta y + \gamma z = 0$ does $\mathbb{P}_{\mathbb{F}_2}^2$ have?
 - Label the vertices of the triangle with points P and the line segments (and circle) with lines L so that P is situated on L iff P satisfies the equation for L .
- Suppose P is a point on the elliptic curve $y^2 = x^3 + ax^2 + bx + c$. Find a formula for the y -coordinate of $2P$.
- Find all points of order 2 and 3 on the elliptic curve $y^2 = x^3 + 1$ using complex numbers.
- If $t \in \mathbb{Q}$ with $t \notin \{1, 1/4\}$, show that $P = (t, t)$ is a rational point of order 4 on $E : y^2 = x^3 - (2t - 1)x^2 + t^2x$. Hint: look at $2P$.
- Consider the point $P = (3, 8)$ on $E : y^2 = x^3 - 43x + 166$. Compute $2P$, $4P$, and $8P$. What conclusion can you draw comparing $8P$ with P ?
- Hand in a typed rough outline and bibliography for your project.