

**2. Übungsblatt Elliptische Kurven****Aufgabe 1**

Sei  $p \neq 2$  eine Primzahl und

$$V_p: X^2 + Y^2 = pZ^2.$$

Zeige:

a)  $V_p \simeq_{\mathbb{Q}} \mathbb{P}^1 \iff p \equiv 1 \pmod{4}$ .

b) Für zwei verschiedene Primzahlen  $p_1 \equiv p_2 \equiv 3 \pmod{4}$ , sind  $V_{p_1}$  und  $V_{p_2}$  nicht isomorph über  $\mathbb{Q}$ .

Hinweis: Ohne Beweis können Sie eventuell benutzen:

$$\exists a, b \in \mathbb{Z} \text{ mit } p = a^2 + b^2 \iff p \equiv 1 \pmod{4}.$$

**Aufgabe 2** Studieren Sie Appendix B (Galois-Kohomologie) in Silvermans Buch. Nutzen Sie die Resultate, um Aufgabe I.1.12 in Silvermans Buch zu lösen:

(a) Sei  $V/K$  eine affine Varietät. Zeige:  $K[V] = (\bar{K}[V])^{G_K}$ .

(b)  $\mathbb{P}^n(K) = (\mathbb{P}^n)^{G_K}$ .

(c) Sei  $\varphi: V_1 \rightarrow V_2$  eine rationale Abbildung zwischen projektiven Varietäten. Zeige:  $\varphi$  ist genau dann über  $K$  definiert, wenn  $\varphi^\sigma = \varphi$  gilt für alle  $\sigma \in G_K$ .

Bemerkung: Beachten Sie die Hinweise in Silvermans Buch. Falls Sie Galoiskohomologie noch nicht kennen gelernt haben, ist das vielleicht etwas viel für ein Übungsblatt. Wir werden sowohl in der nächsten Übung als auch später in der Vorlesung darauf eingehen.

Besprechung: Do 04.11.2021 in der Übung.