Vi vil her give et bevis for Hasse's sætning. Til dette formål skal vi først opbygge nogle resultater vedrørende endomorfier på endelige legemer.

Definition 4 (Algebraisk aflukning)**.** En algebraisk aflukning af et legeme K, er et legeme $K \subseteq \overline{K}$, hvor $\overline{K}$ er en algebraisk udvidelse af K samt, at ethvert ikke-konstant polynomium fra $\overline{K}[X]$ har en rod i $\overline{K}$.

Det kan vises, at ethvert legeme har en algebraisk aflukning og at to algebraiske aflukninger for det samme legeme vil være isomorfe. Derfor giver det mening for os, at snakke om *den* algebraiske aflukning for et givent legeme. Lad nu $\mathbb{F}_q$ være et endeligt legeme med algebraisk aflukning $\overline{\mathbb{F}}_q$. Vi ser på Frobenius afbildningen

$$\phi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q,$$

som er givet ved, at $x \mapsto x^q$. For en elliptisk kurve E over $\mathbb{F}_q$ virker ϕ_q på koordinaterne $E(\overline{\mathbb{F}}_q)$ ved, at

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(\infty) = \infty.$$

I det følgende udnytter vi, at q er et primtal (men bogen arbejder måske blot med at $q = p^r$, hvor p er et primtal. Da skal der tilføjes lidt resultater.

Lemma 3. *Lad E være en elliptisk kurve over $\mathbb{F}_q$, og lad $(x, y) \in E(\overline{\mathbb{F}}_q)$. Da gælder der, at*

1. $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$,
2. $(x, y) \in E(\mathbb{F}_q) \Leftrightarrow \phi_q(x, y) = (x, y)$.

Bevis. Vi har, at $y^2 = x^3 + ax + b$, hvor $a, b \in \mathbb{F}_q$. Vi opløfter denne ligning til den q'ende potens og får, at

$$(y^q)^2 = (x^q)^3 + (a^q x^q) + b^q,$$

hvor vi har brugt Freshman's dream. Men dette betyder netop, at $(x^q, y^q) \in E(\overline{\mathbb{F}}_q)$, hvilket viser (1). For at vise (2) husker vi, at $\phi_q(x) = x \Leftrightarrow x \in \mathbb{F}_q$. Det følger da, at

$$\begin{aligned}(x, y) \in E(\mathbb{F}_q) &\Leftrightarrow x, y \in \mathbb{F}_q \\ &\Leftrightarrow \phi_q(x) = x \text{ og } \phi_q(y) = y \\ &\Leftrightarrow \phi_q(x, y) = (x, y),\end{aligned}$$

hvilket fuldfører beviset for (2). □

Lemma 4. *Lad E være en elliptisk kurve over $\mathbb{F}_q$. Da er ϕ_q en endomorfi for E af grad q, desuden er ϕ_q ikke seperabel.*

Bevis. Beviset går på at vise, at $\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ er en homomorfi. Dette gøres vha. additionsformlerne. Se f.eks. [1]. □

Det næste resultat bliver afgørende for beviset for Hasses sætning. Det fortæller os om graden af en endomorfi for en elliptisk kurve E, som eksempelvis ϕ_q er det.

Proposition 1. *Lad E være en elliptisk kurve. Lad $\alpha \neq 0$ være en seperabel endomorfi for E. Da er*

$$\deg \alpha = |\ker(\alpha)|,$$

hvor $\ker(\alpha)$ angiver kernen for α homomorfien $\alpha : E(\overline{K}) \to E(\overline{K})$.