

Quadratische Erweiterung

Ziel:

- \mathbb{F}_p^2 besitzt Ordnung $|\mathbb{F}_p^2| = p^2 - 1 = (p + 1)(p - 1)$.
- Wir konstruieren eine Untergruppe von \mathbb{F}_p^2 mit Ordnung $p + 1$.
- Unsere Hoffnung ist, dass $p + 1$ in kleine Primfaktoren zerfällt.

Definition

Sei R ein kommutativer Ring, $D \in R$ kein Quadrat. $R[\sqrt{D}] = R \oplus R\sqrt{D}$ heißt *quadratische Erweiterung* von R . Sei $\omega = x + y\sqrt{D} \in R[\sqrt{D}]$.

- 1 Das zu ω *konjugierte* Element ist definiert als $\bar{\omega} = x - y\sqrt{D}$.
- 2 Die *Spur* ist definiert als $\text{Tr} : R[\sqrt{D}] \rightarrow R, \omega \mapsto \omega + \bar{\omega}$ mit
$$\text{Tr}(x + y\sqrt{D}) = 2x.$$
- 3 Die *Norm* ist definiert als $N : R[\sqrt{D}] \rightarrow R, \omega \mapsto \omega\bar{\omega}$ mit
$$N(x + y\sqrt{D}) = x^2 - Dy^2.$$

Anmerkung: Die Spur ist additiv, die Norm multiplikativ.

Eigenschaften von Norm und Spur

Lemma Eigenschaften von Norm und Spur

Sei $\omega \in R[\sqrt{D}]$ beliebig. Es gilt

- 1 $\omega \in R[\sqrt{D}]^*$ gdw $N(\omega) \in R^*$.
- 2 $\omega, \bar{\omega}$ sind Nullstellen des Polynoms $X^2 - \text{Tr}(\omega)X + N(\omega)$.

Beweis:

(1) \Rightarrow : Sei $\omega \in (R[\sqrt{D}])^*$. Dann gilt

$$1 = N(1) = N(\omega\omega^{-1}) = N(\omega)N(\omega^{-1}).$$

- D.h. $N(\omega) \mid 1$ und damit $N(\omega) \in R^*$.
- \Leftarrow : Sei $N(\omega) \in R^*$. Für $\omega^{-1} := \bar{\omega}N(\omega)^{-1}$ gilt

$$\omega\omega^{-1} = \omega\bar{\omega}N(\omega)^{-1} = N(\omega)N(\omega)^{-1} = 1.$$

(2) Offenbar sind ω und $\bar{\omega}$ Nullstellen des Polynoms

$$(X - \omega)(X - \bar{\omega}) = X^2 - (\omega + \bar{\omega})X + \omega\bar{\omega} = X^2 - \text{Tr}(\omega)X + N(\omega).$$

Der Körper \mathbb{F}_p^2

Satz Körper \mathbb{F}_p^2

Sei p prim und $\left(\frac{D}{p}\right) = (-1)$. Dann ist $\mathbb{F}_{p^2} := \mathbb{F}_p[\sqrt{D}]$ ein Körper mit p^2 Elementen.

Beweis:

- Wir betrachten die Norm-Abbildung $N : \mathbb{F}_{p^2} \rightarrow \mathbb{F}_p$ mit $\omega \mapsto \omega\bar{\omega}$.
- Zeigen $N(\omega) \not\equiv 0 \pmod{p}$ für alle $\omega = x + y\sqrt{D} \in \mathbb{F}_p[\sqrt{D}] \setminus \{0\}$.
- Damit ist $N(\omega) \in \mathbb{F}_p^*$ und ω ist invertierbar.
- Annahme: $N(\omega) = x^2 - y^2D \equiv 0 \pmod{p}$.
- Damit gilt $x^2 \equiv y^2D \pmod{p}$.
- Es gilt $y \in U_p$, denn für $y \equiv 0$ folgt $x \equiv 0$. (Widerspruch: $\omega \neq 0$)
- Es folgt $D \equiv \left(\frac{x}{y}\right)^2 \pmod{p}$. (Widerspruch: D ist ein Nichtrest.)
- Ferner gilt $\mathbb{F}_p[\sqrt{D}] \cong \mathbb{F}_p \oplus \mathbb{F}_p\sqrt{D}$. D.h. $|\mathbb{F}_p[\sqrt{D}]| = p^2$.

Der Frobenius-Automorphismus

Definition Froebenius-Automorphismus

Sei $p \in \mathbb{P} \setminus \{2\}$. Der *Frobenius-Automorphismus* auf \mathbb{F}_p^2 ist die Abbildung

$$f_p : \mathbb{F}_p^2 \rightarrow \mathbb{F}_p^2 \text{ mit } \omega \mapsto \omega^p.$$

Anmerkungen:

- Wir wissen bereits, dass f_p homomorph ist, d.h.

$$f_p(xy) = f_p(x)f_p(y) \text{ und } f_p(x + y) = f_p(x) + f_p(y).$$

- Damit ist f_p ein Ring-Homomorphismus.
- Da $\text{Ker}(f_p) = \{0\}$ ist f_p bijektiv, d.h. f_p ist ein Automorphismus.

Eigenschaften des Frobenius

Satz Eigenschaften des Frobenius

Sei $p \in \mathbb{P} \setminus \{2\}$. Dann gilt

- 1 $\{\omega \in \mathbb{F}_p^2 \mid f_p(\omega) = \omega\} = \mathbb{F}_p$
- 2 $f_p(\omega) = \bar{\omega}$ für alle $\omega \in \mathbb{F}_p^2$.

Beweis:

- (1) Mittels Kleinem Fermat gilt $f_p(x) = x^p = x$ für alle $x \in \mathbb{F}_p$.
 - Damit gilt $f_p(\omega) = \omega = \bar{\omega}$ bereits für alle $\omega \in \mathbb{F}_p$.
 - Das Polynom $g(X) = X^p - X$ besitzt also die p Nullstellen $\omega \in \mathbb{F}_p$.
 - $g(X)$ kann aber in \mathbb{F}_p^2 höchstens p Nullstellen besitzen.
 - D.h. die Fixpunkte des Frobenius sind genau die Elemente aus \mathbb{F}_p .
- (2) Sei $\omega \in \mathbb{F}_p^2 \setminus \mathbb{F}_p$ und damit $f_p(\omega) \neq \omega$. Wir betrachten das Polynom
$$h(X) = X^2 - \text{Tr}(\omega)X + N(\omega).$$
 - Wir wissen $h(\omega) = 0$. Mit Hilfe der Linearität des Frobenius folgt
$$h(f_p(\omega)) = f_p(h(\omega)) = f_p(0) = 0.$$
 - Damit ist $f_p(\omega)$ eine Nullstelle von $h(X)$.
 - Die einzigen beiden Nullstellen sind aber ω und $\bar{\omega}$. D.h. $f_p(\omega) \equiv \bar{\omega}$.

Eigenschaften des Frobenius

Korollar

Es gilt $N(\omega) = \omega\bar{\omega} = \omega^{p+1}$ für alle $\omega \in \mathbb{F}_p^2$.

Satz Norm-1 Gruppe

Sei $p \in \mathbb{P} \setminus \{2\}$ und $G_p := \{\omega \in \mathbb{F}_{p^2}^* \mid N(\omega) = 1\}$. Dann ist (G_p, \cdot) eine Gruppe mit Ordnung $p + 1$.

Beweis:

- Da die Norm multiplikativ ist, bildet (G_p, \cdot) eine Gruppe.
- z.z.: $|G_p| = p + 1$. Betrachte die Norm-Abbildung $N : \mathbb{F}_{p^2}^* \rightarrow \mathbb{F}_p^*$.
- $N(\omega) = \omega^{p+1} = 1$ kann in $\mathbb{F}_{p^2}^*$ höchstens $p + 1$ Lösungen besitzen.
- Damit gilt $|G_p| = |\text{Ker}(N)| \leq p + 1$.
- Außerdem gilt $|\text{Im}(N)| \leq |\mathbb{F}_p^*| = p - 1$. Insgesamt erhalten wir
$$|\mathbb{F}_{p^2}^*| = p^2 - 1 = (p + 1)(p - 1) = |\text{Ker}(N)| \cdot |\text{Im}(N)|.$$
- Damit folgt $|\text{Im}(N)| = p - 1$ und $|G_p| = |\text{Ker}(N)| = p + 1$.

Quadratwurzeln, revisited

Korollar

Es gilt $|\{\omega \in \mathbb{F}_{p^2} \mid N(\omega) = a\}| = p + 1$ für alle $a \in \mathbb{F}_p^*$.

Beweis: Alle Nebenklassen von G_p besitzen Kardinalität $p + 1$.

Idee des Quadratwurzel-Ziehens in quadratischen Erweiterungen:

- Sei $a \in U_p$ mit $\left(\frac{a}{p}\right) = 1$. Gesucht ist ein x mit $x^2 \equiv a \pmod{p}$.
- Wir konstruieren dazu ein $\omega \in \mathbb{F}_{p^2}^*$ mit $N(\omega) = a$.
- Setze $x := \omega^{\frac{p+1}{2}} \pmod{p}$. Es folgt $x^2 \equiv \omega^{p+1} \equiv N(\omega) \equiv a \pmod{p}$.

Ziel: Konstruktion von $\omega \in \mathbb{F}_{p^2}^*$ mit $N(\omega) = a$.

Konstruktion eines Elements mit Norm a

Lemma Konstruktion eines Elements mit Norm a

Sei $p \in \mathbb{P} \setminus \{2\}$, $\left(\frac{a}{p}\right) = 1$. Sei $b \in \mathbb{F}_p$, $D := b^2 - a$ mit $\left(\frac{D}{p}\right) = (-1)$.

- Das Element $\omega := b + \sqrt{D} \in \mathbb{F}_p[\sqrt{D}]$ besitzt Norm $N(\omega) = a$.
- Die Anzahl aller $b \in \mathbb{F}_p$ mit $\left(\frac{b^2 - a}{p}\right) = (-1)$ ist mindestens $\frac{1}{2}(p - 1)$.

Beweis:

(1) Für $\omega = b + \sqrt{D} \in \mathbb{F}_p[\sqrt{D}]$ gilt

$$N(\omega) = (b + \sqrt{D})(b - \sqrt{D}) = b^2 - D = a.$$

(2) Für alle $\omega \in \mathbb{F}_{p^2}^* \setminus \mathbb{F}_p^*$ mit $N(\omega) = a$ gilt für $b := \frac{1}{2}\text{Tr}(\omega)$

$$\omega^2 - 2b\omega + a \equiv 0 \pmod{p}, \text{ d.h. } \omega = b \pm \sqrt{b^2 - a}.$$

- Wegen $\omega \notin \mathbb{F}_p^*$ folgt, dass für dieses b gilt $\left(\frac{b^2 - a}{p}\right) = (-1)$.
- Wir zählen die Anzahl der $\omega \in \mathbb{F}_{p^2}^* \setminus \mathbb{F}_p^*$ mit verschiedener Spur.
- Jedes dieser ω liefert ein verschiedenes $b \in \mathbb{F}_p$ mit $\left(\frac{b^2 - a}{p}\right) = (-1)$.
- Korollar zuvor: Für $M = \{\omega \in \mathbb{F}_{p^2} \mid N(\omega) = a\}$ gilt $|M| = p + 1$.

Konstruktion eines Elements mit Norm a

Beweis: (Fortsetzung)

- M enthält beide Quadratwurzeln von a in \mathbb{F}_p , d.h. $|M \setminus \mathbb{F}_p| = p - 1$.
- Falls für $\omega \in M \setminus \mathbb{F}_p$ auch das konjugierte $\bar{\omega} \in M \setminus \mathbb{F}_p$, entferne $\bar{\omega}$.
- Die entstehende Menge M' besitzt Kardinalität mindestens $\frac{p-1}{2}$.
- Angenommen es existieren zwei verschiedene Elemente $m_1 = x + y\sqrt{D}, m_2 = x + y'\sqrt{D} \in M'$ mit gleicher Spur.
- Es folgt $x^2 - Dy^2 = a = x^2 - Dy'^2$ und $D(y^2 - y'^2) \equiv 0 \pmod{p}$.
- Wegen $D \not\equiv 0 \pmod{p}$ folgt mit $m_1 \neq m_2$ dass $y \equiv -y' \pmod{p}$.
(Widerspruch: Konjugierte wurden aus M' entfernt.)
- Damit besitzen in M' alle Elemente verschiedene Spur. Es folgt

$$|\{b \in \mathbb{F}_p \mid (\frac{b^2-a}{p}) = (-1)\}| \geq |M'| \geq \frac{p-1}{2}.$$