Der Körper $\mathbb{F}_p^2$

Lemma

Sei $D \in R^*$, aber D kein Quadrat in R. Dann gilt $R[\sqrt{D}] \cong R \times R$.

Beweis:

- Wir definieren den Isomorphismus $\phi : R[\sqrt{D}] \to R \times R$ mit
$$x + y\sqrt{D} \mapsto (x + yD, x - yD).$$
- Die Bijektivität von ϕ folgt mit der Umkehrabbildung
$$\phi^{-1}(u, v) = \frac{u+v}{2} + \frac{u-v}{2D}\sqrt{D}.$$
- Die Verträglichkeit von ϕ mit $+, \cdot$ lässt sich leicht nachrechnen.

Der Körper $\mathbb{F}_p^2$

Satz Körper $\mathbb{F}_p^2$

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

Beweis:

- Wir betrachten die Norm-Abbildung $N : \mathbb{F}_{p^2} \to \mathbb{F}_p$ mit $\omega \mapsto \omega\bar{\omega}$.
- Zeigen $N(\omega) \not\equiv 0 \bmod p$ 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: $N(\omega) = x^2 - y^2 D \equiv 0 \bmod p$.
- Damit gilt $x^2 \equiv y^2 D \bmod p$.
- Es gilt $y \in U_p$, denn für $y \equiv 0$ folgt $x \equiv 0$. (Widerspruch: $\omega \neq 0$)
- Es folgt $D \equiv (\frac{x}{y})^2 \bmod p$. (Widerspruch: D ist ein Nichtrest.)
- Das vorige Lemma liefert $\mathbb{F}_p[\sqrt{D}] \cong \mathbb{F}_p \times \mathbb{F}_p$. 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* ist die Abbildung

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

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 $\mathrm{Ker}(f_p) = \{0\}$ 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 $f_p(\omega) = \bar{\omega}$ für alle $\omega \in \mathbb{F}_p^2$.

Beweis:

- 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 gerade die Elemente aus $\mathbb{F}_p$
$$\mathbb{F}_p = \{\omega \in \mathbb{F}_p^2 \mid f_p(\omega) = \omega\}.$$
- Sei $\omega \in \mathbb{F}_p^2 \setminus \mathbb{F}_p$ und damit $f_p(\omega) \neq \omega$. Wir betrachten das Polynom
$$h(X) = X^2 - \mathrm{Tr}(\omega)X + N(\omega).$$
- 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 $f(\omega)$ eine Nullstelle von $h(X)$.
- Die einzigen beiden Nullstellen sind aber ω und $\bar{\omega}$. D.h. $f_p(\omega) = \bar{\omega}$.

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 $N : \mathbb{F}_{p^2}^* \to \mathbb{F}_p^*$.
- $N(\omega) = \omega^{p+1} = 1$ kann in $\mathbb{F}_{p^2}^*$ höchstens $p + 1$ Lösungen besitzen.
- Damit gilt $|G_p| = |\mathrm{Ker}(N))| \leq p + 1$.
- Außerdem gilt $|\mathrm{Im}(N)| \leq |\mathbb{F}_p^*| = p - 1$. Insgesamt erhalten wir
$$|\mathbb{F}_{p^2}^*| = p^2 - 1 = (p + 1)(p - 1) = |\mathrm{Ker}(N)| \cdot |\mathrm{Im}(N)|.$$
- Damit folgt $|\mathrm{Im}(N)| = p - 1$ und $|G_p| = |\mathrm{Ker}(N)| = p + 1$.

Quadratwurzeln, revisited

Korollar

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

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

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

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

- Wegen $\omega \notin \mathbb{F}_p^*$ folgt, dass für dieses b gilt $(\frac{b^2-a}{p}) = (-1)$.
- 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 $(\frac{b^2-a}{p}) = (-1)$.
- 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 $\frac{p-1}{2}$.
- Alle Elemente aus M' besitzen verschiedene Spur. Damit folgt

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

Algorithmus von Cippola

Algorithmus von Cippola

EINGABE: $p \in \mathbb{P}$, $a \bmod p$ mit $(\frac{a}{p}) = 1$

1. REPEAT
   1. Wähle $b \in \{1, \ldots, p-1\}$ zufällig. Setze $D := b^2 - a$.

   UNTIL $(\frac{D}{p}) = (-1)$.
2. Berechne $x := (b + \sqrt{D})^{\frac{p+1}{2}}$ in $\mathbb{F}_p[\sqrt{D}]$.

AUSGABE: $x \bmod p$ mit $x^2 \equiv a \bmod p$

Laufzeit: erwartete Laufzeit $\mathcal{O}(\log^3 p)$.

Bsp: : Wir berechnen die Quadratwurzel von $a = 2$ in $\mathbb{F}_7$.

- Für $b = 1$ gilt $(\frac{D}{p}) = (\frac{-1}{7}) = (-1)$. Es folgt

$$(b + \sqrt{D})^{\frac{p+1}{2}} = (1 + \sqrt{-1})^4 = (2\sqrt{-1})^2 = -4 \equiv 3 \bmod 7.$$

- Wir prüfen $3^2 = 9 \equiv 2 \bmod 7$.