# 14. Vorlesung

- irreduzible Polynome $f(x)$ über einem Körper $K$
- Konstruktion endlicher Körper $\mathrm{GF}(q)$
  - Rechnen im Ring $(K[x]/f(x), \oplus, \otimes)$
  - Beispiel zur Konstruktion eines endlichen Körpers $\mathrm{GF}(p)[x]/f(x)$ mit einem irreduziblen Polynom $f(x)$
  - Berechnung des multiplikativen Inversen (mit dem erweiterten EUKLIDischen Algorithmus)
- primitive Polynome $f(x)$ über einem Körper $K$

  Anwendung primitiver Polynome $f(x)$ zur Konstruktion des Körpers $\mathrm{GF}(p)[x]/f(x)$

# Irreduzible Polynome

- Ein Polynom $p(x)$ wird irreduzibel über einem Körper $K$ genannt, wenn es keine Polynome $a(x)$, $b(x)$ in $K[x]$ gibt, die $p(x) = a(x) \cdot b(x)$ und $0 < \mathrm{Grad}(a(x)) < \mathrm{Grad}(p(x))$ sowie $0 < \mathrm{Grad}(b(x)) < \mathrm{Grad}(p(x))$ erfüllen.

- Beispiele für Zerlegungen von Polynomen in Faktoren, die über $\mathbb{Z}_2$ irreduzibel sind:

$$x^3 + 1 = (x+1)(x^2+x+1)$$
$$x^4 + 1 = (x+1)^4$$
$$x^5 + 1 = (x+1)(x^4+x^3+x^2+x+1)$$
$$x^7 + 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$$
$$x^9 + 1 = (x+1)(x^2+x+1)(x^6+x^3+1)$$

- Ist $n$ ungerade, dann sind die über $\mathbb{Z}_2$ irreduziblen Faktoren von $x^n - 1$ paarweise verschieden.

# Endliche Körper GF($q$)

<u>G</u>ALOIS <u>F</u>IELD

- Ein endlicher Körper GF($q$) mit $q$ Elementen existiert genau dann, wenn $q$ eine Primzahlpotenz ist.
- Gilt $q = p^k$ ($p$ prim, $k \in \mathbb{N}, k \geq 1$), dann gibt es bis auf Isomorphie genau einen Körper mit $q$ Elementen.

Evariste Galois (1811-1832)

# Konstruktion endlicher Körper

| Ring der ganzen Zahlen | Polynomring über einem Körper $K$ |
|---|---|
| $\mathbb{Z}$ | $K[x]$ |
| $\downarrow$ *Rechnen modulo $n$* | $\downarrow$ *Rechnen modulo $p(x)$* |
| $\mathbb{Z}_n$ | $K[x]/p(x)$ |
| Restklassenring modulo $n$ | Polynomring modulo $p(x)$ |
| Untersuchung der Einheiten ergibt $(*)$ | Untersuchung der Einheiten ergibt $(**)$ |

$(*)$ $\mathbb{Z}_p$ ist Körper $\iff$ $p$ ist Primzahl

$(**)$ $K[x]/p(x)$ ist Körper $\iff$ $p(x)$ ist irreduzibles Polynom in $K[x]$

# Rechnen im Ring $(K[x]/f(x); \oplus, \otimes)$

Sei $K$ ein endlicher Körper und $f(x) \in K[x]$ mit $\text{Grad}(f(x)) = n$.

$$\begin{aligned} K[x]/f(x) &:= \{r(x) \in K[x] \mid r(x) = 0 \text{ oder } \text{Grad}(r(x)) < n\} \\ &= \{r_0 + r_1 x + \cdots + r_{n-1} x^{n-1} \mid r_i \in K \text{ für } i = 0, ..., n-1\} \end{aligned}$$

- Addition $\oplus$:

$$\begin{aligned} a(x) \oplus b(x) &= (a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) \oplus (b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}) \\ &= (a_0 + b_0) + (a_1 + b_1) x + \cdots + (a_{n-1} + b_{n-1}) x^{n-1} \end{aligned}$$

- Multiplikation $\otimes$:

$$\begin{aligned} a(x) \otimes b(x) &= a(x) \odot b(x) \quad (\text{mod } f(x)) \\ &= \cdots + \left( \sum_{i=0}^{k} a_i \cdot b_{k-i} \right) x^k + \ldots \quad (\text{mod } f(x)) \end{aligned}$$

# Endliche Körper $\mathrm{GF}(p)[x]/f(x)$

Es sei $q = p^k$ $(k \in \mathbb{N},\ k \geq 1)$ für eine Primzahl $p$ und $f(x) \in \mathrm{GF}(p)[x]$ ein irreduzibles Polynom vom Grad $k$ über $\mathrm{GF}(p)$.

Dann gilt:

$$\mathrm{GF}(p)[x]/f(x) = \{a(x) \in \mathrm{GF}(p)[x] \mid a(x) = 0 \text{ oder } \mathrm{Grad}(a(x)) < k\}$$

- $(\mathrm{GF}(p)[x]/f(x); \oplus, \otimes)$ ist ein Körper.
- $\mathrm{GF}(p)[x]/f(x)$ hat genau $p^k$ Elemente.

# Beispiel: GF($2^3$)

- Konstruktion von GF($2^3$)

  $$GF(2)[x]/\underbrace{1+x+x^3}_{\text{irreduzibel}} = \{0, 1, x, 1{+}x, x^2, 1{+}x^2, x{+}x^2, 1{+}x{+}x^2\}$$

- Beispiel für das Rechnen in diesem Körper:

  Für $a(x) = 1 + x$, $b(x) = 1 + x + x^2$ gilt:

  - $a(x) \oplus b(x) = x^2$
  - $a(x) \otimes b(x) = 1 + x^3 \pmod{1 + x + x^3} = x$
  - $a(x)^{-1}$ kann mit dem erweiterten Euklidischen Algorithmus berechnet werden.

    Es gilt $a(x)^{-1} = x + x^2$, denn
    $a(x) \otimes (x + x^2) = x + x^3 \pmod{1 + x + x^3} = 1$

# Primitive Polynome

- Ein irreduzibles Polynom $f(x)$ aus $\mathrm{GF}(p)[x]$ vom Grad $k$ heißt primitiv, wenn

  $$\min\{\ell \in \mathbb{N} \setminus \{0\} \mid f(x) \text{ teilt } x^\ell - 1 \text{ in } \mathrm{GF}(p)[x]\} = p^k - 1$$

  gilt.

- Jedes primitive Polynom aus $\mathrm{GF}(p)[x]$ ist irreduzibel über $\mathrm{GF}(p)[x]$.

- $f_1(x) = 1 + x + x^2 + x^3 + x^4, \quad f_2(x) = 1 + x + x^4$, $f_3(x) = 1 + x^3 + x^4$ sind die einzigen irreduziblen Polynome vom Grad 4 über $\mathrm{GF}(2)$.

  $f_1(x)$ ist nicht primitiv.

  $f_2(x)$ und $f_3(x)$ sind primitive Polynome.

# Primitive Polynome über GF($p$)

$\underline{p = 2:}$

$x^2 + x + 1$
$x^3 + x + 1$
$x^4 + x + 1$
$x^5 + x^2 + 1$
$x^6 + x + 1$
$x^7 + x^3 + 1$
$x^8 + x^4 + x^3 + x^2 + 1$
$x^9 + x^4 + 1$
$x^{10} + x^3 + 1$
$x^{11} + x^2 + 1$
$x^{12} + x^6 + x^4 + x + 1$
$x^{13} + x^4 + x^3 + x + 1$
$x^{14} + x^{10} + x^6 + x + 1$
$x^{15} + x + 1$
$x^{16} + x^{12} + x^3 + x + 1$
$x^{17} + x^3 + 1$
$x^{18} + x^7 + 1$
$x^{19} + x^5 + x^2 + x + 1$
$x^{20} + x^3 + 1$
$x^{24} + x^7 + x^2 + x + 1$
$x^{32} + x^{22} + x^2 + x + 1$

$\underline{p = 3:}$

$x^2 + x + 2$
$x^3 + 2x + 1$
$x^4 + x + 2$
$x^5 + 2x + 1$
$x^6 + x + 2$
$x^7 + x^2 + 2x + 1$

$\underline{p = 5:}$

$x^2 + x + 2$
$x^3 + 3x + 2$
$x^4 + x^2 + 2x + 2$
$x^5 + 4x + 2$

$\underline{p = 7:}$

$x^2 + x + 3$
$x^3 + 3x + 2$
$x^5 + x^2 + 3x + 5$