Unterlagen zu endlichen Körpern

Erhard Aichinger

Linz, im November 2005

Alle Rechte vorbehalten

KAPITEL 1

Endliche Körper

1. Definition endlicher Körper

DEFINITION 1.1. Ein Ring mit Eins $\mathbf{R} = (R, +, -, \cdot, 0, 1)$ ist ein *Körper*, wenn

(1) $|R| \geq 2$,
(2) für alle $x, y \in R$ gilt $x \cdot y = y \cdot x$,
(3) für alle $x \in R \setminus \{0\}$ gibt es ein $y \in R$ mit $x \cdot y = 1$.

ÜBUNGSAUFGABEN 1.2.

(1) Zeigen Sie, dass es in einem Körper für jedes x höchstens ein y mit $x \cdot y = 1$ geben kann.
(2) Zeigen Sie, dass das Produkt zweier Elemente in einem Körper nur dann 0 ist, wenn einer der Faktoren gleich 0 ist.

In einem Körper hat jedes Element $a \neq 0$ genau ein multiplikativ inverses Element; wir bezeichnen es mit a^{-1}. Für jede Primzahl p ist der Ring $\mathbb{Z}_p$ ein Körper.

2. Körper aus irreduziblen Polynomen

Sei f ein Polynom in $K[x]$. Für $a, b \in K[x]$ definieren wir

$$a \equiv b \pmod{f},$$

falls $f | a - b$. Wir definieren

$$[a]_f := \{a + q \cdot f \mid q \in K[x]\}.$$

Jede Restklasse modulo f enthält genau ein Polynom, dessen Grad kleiner als $\deg(f)$ ist.

SATZ 1.3. *Sei* $\mathbf{K}$ *ein Körper, sei* $f \in K[x]$ *mit* $\deg(f) \geq 1$, *und sei* $a \in K[x]$. *Dann gibt es genau ein* $b \in K[x]$, *sodass* $\deg(b) < \deg(f)$ *und* $[a]_f = [b]_f$.

Beweis: Wir zeigen als erstes, dass es so ein b gibt: Durch Division erhalten wir q und r in $K[x]$, sodass

$$a = q \cdot f + r \text{ und } \deg(r) < \deg(f).$$

Wir setzen $b := r$. Es gilt $[a]_f = [a - q \cdot f]_f = [r]_f = [b]_f$. Nun zeigen wir, dass es höchstens ein solches b geben kann. Seien $b_1, b_2 \in K[x]$ so, dass $[b_1]_f = [b_2]_f$ und

$\deg(b_1) < \deg(f)$, $\deg(b_2) < \deg(f)$. Dann gilt $f | b_2 - b_1$. Da $b_2 - b_1$ kleineren Grad als f hat, gilt $b_2 - b_1 = 0$. ■

Wir kürzen den Rest r der Division von a durch f mit

$$a \bmod f$$

ab. Es gilt also $a \equiv b \pmod f$ genau dann, wenn $a \bmod f = b \bmod f$.

Wenn f ein Polynom in $\mathbb{Z}_p[x]$ vom Grad n ist, gibt es genau p^n Restklassen modulo f. Um zu bestimmen, ob zwei Polynome zur gleichen Restklasse modulo f gehören, kann man ihren Rest bei der Division durch f bestimmen. Die folgende Mathematica-Funktionen berechnen Quotient und Rest einer Division in $\mathbb{Z}_p[x]$.

```
Deg [f_, var_] := Length [ CoefficientList [ f, var ] ] - 1;
(* Berechnet den Grad des Polynoms f in der Variablen var *)

Lcf [f_, var_] := CoefficientList [f, var] [[Deg[f,var] + 1]];
(* Liefert den fuehrenden Koeffizienten von f
   in der Variablen var *)

PolynomialQuotientP [f_,g_,var_,p_] :=
(* Liefert das q, sodass es r mit deg r < deg g gibt, sodass
   f = q*g + r. Alle Rechnungen in Z_p [x]. *)
Module[{lf, lg, f1, g1,q},
   f1 = PolynomialMod[f,p];
   g1 = PolynomialMod[g,p];
   If [Deg[g1, var] > Deg[f1, var],
         0,
      lf = Lcf [f1, var];
      lg = Lcf [g1, var];
      q = lf * PowerMod[lg, -1, p] * var^(Deg[f1,var]-Deg[g1,var]);
      (* compute return value *)
      q + PolynomialQuotientP [
             PolynomialMod [f1 - q * g1, p],
             g1,
             var,
             p]
   ]];


PolynomialRemainderP [f_,g_,var_,p_] :=
(* Liefert den Rest bei der Division von f durch g *)
   PolynomialMod [f - g * PolynomialQuotientP [f,g,var,p], p];
```

Sei $K[x]/f$ definiert durch

$$K[x]/f := \{[a]_f \mid a \in K[x]\}.$$

Auf $K[x]/f$ definieren wir $+, -, \cdot$ durch

$$\begin{aligned} [a]_f + [b]_f &:= [a+b]_f \\ [a]_f - [b]_f &:= [a-b]_f \\ [a]_f \cdot [b]_f &:= [a \cdot b]_f. \end{aligned}$$

SATZ 1.4. *Sei* $\mathbf{K}$ *ein Körper, und sei* $f \in K[x]$. *Dann ist* $\left(K[x]/f, +, -, \cdot, [0]_f, [1]_f\right)$ *ein Ring mit Eins.*

SATZ 1.5. *Sei* $\mathbf{K}$ *ein Körper, und sei* $f \in \mathbf{K}[x]$ *irreduzibel über* $\mathbf{K}$. *Dann ist* $\mathbf{K}[x]/f$ *ein Körper.*

$\mathbf{K}[x]/f$ wieder ein kommutativer Ring mit 1. Es bleibt zu zeigen, dass jedes $h \in \mathbf{K}[x]/f$ mit $h \neq [0]_f$ invertierbar ist. Sei $h' \in \mathbf{K}[x]$ so, dass $h = [h']_f$. Da f irreduzibel ist, und h' kein Vielfaches von f ist, gilt $\mathrm{ggT}(h', f) = 1$. Es gibt also $u, v \in \mathbf{K}[x]$, sodass $u \cdot h' + v \cdot f = 1$. Es gilt also $[u]_f \cdot [h']_f = [u \cdot h']_f = [1 - v \cdot f]_f = [1]_f$. ■

Wenn $\mathbf{K}$ ein endlicher Körper mit q Elementen ist, und f ein über $\mathbf{K}$ irreduzibles Polynom vom Grad n, dann ist $\mathbf{K}[x]/f$ ein Körper mit q^n Elementen. Wenn wir also irreduzible Polynome über $\mathbb{Z}_p$ finden, können wir daraus größere endliche Körper konstruieren. In [**Lidl and Niederreiter, 1983**, p.142, 3.27] finden wir eine untere Schranke für die Anzahl der irreduziblen Polynome über einem endlichen Körper.

SATZ 1.6. *Sei* $\mathbf{K}$ *ein endlicher Körper mit q Elementen. Von den* q^n *normierten Polynomen vom Grad n über* $\mathbf{K}$ *sind zumindest* $\frac{1}{2n}q^n$ *Polynome irreduzibel.*

Der folgende Satz liefert einen Test, ob ein Polynom irreduzibel über einem endlichen Körper mit q Elementen ist.

SATZ 1.7. *Sei* $\mathbf{K}$ *ein Körper mit q Elementen, sei* $n \in \mathbb{N}$ *und sei* $f \in K[x]$ *mit* $\deg(f) = n$. *Äquivalent sind:*

(1) *Für alle* $i \in \{1, 2, \ldots, \lfloor \frac{n}{2} \rfloor\}$ *gilt:*

$$\mathrm{ggT}(f, x^{q^i} - x) = 1.$$

(2) f *ist irreduzibel über* $\mathbf{K}$.

3. Eigenschaften endlicher Körper

Für $n \in \mathbb{N}$ kürzen wir $\underbrace{1 + 1 + \cdots + 1}_{n \text{ mal}}$ mit $n * 1$ ab.

DEFINITION 1.8. Sei $\mathbf{K}$ ein Körper und sei N die Menge, die durch

$$N = \{n \in \mathbb{N} \mid n * 1 = 0\}$$

definiert ist. Wenn N leer ist, dann definieren wir die *Charakteristik* von $\mathbf{K}$ als 0, wenn N nicht leer ist, dann definieren wir die *Charakteristik* von $\mathbf{K}$ als das kleinste Element in N.

Für einen endlichen Körper ist die Charakteristik also das kleinste $a \in \mathbb{N}$ mit $a * 1 = 0$. Die Charakteristik von $\mathbb{Z}_p$ ist p.

SATZ 1.9. *Sei $\mathbf{K}$ ein endlicher Körper. Dann ist seine Charakteristik eine Primzahl.*

Beweis: Da K endlich ist, gibt es $a, b \in \mathbb{N}$ mit $a > b$ und $a*1 = b*1$, also $(a-b)*1 = 0$. Wir zeigen nun, dass

$$\min\{n \in \mathbb{N} \mid n * 1 = 0\}$$

eine Primzahl ist. Sei p dieses Minimum. Wenn es $c, d < p$ gibt, sodass $cd = p$, dann gilt $(c * 1) \cdot (d * 1) = 0$, also entweder $c * 1 = 0$ oder $d * 1 = 0$. Das widerspricht der Minimalität von p. Also ist p eine Primzahl. ■

SATZ 1.10. *Sei $\mathbf{K}$ ein endlicher Körper mit q Elementen, und sei p die Charakteristik von $\mathbf{K}$. Dann gibt es ein $n \in \mathbb{N}$, sodass $q = p^n$.*

SATZ 1.11. *Sei $\mathbf{E}$ ein Körper der Charakteristik p mit $q = p^m$ Elementen. Dann gilt für alle $x, y \in E$:*

(1) $(x + y)^p = x^p + y^p$.
(2) $x^q = x$.

Beweis: (1): Nach dem binomischen Lehrsatz gilt

$$(x + y)^p = x^p + \sum_{i=1}^{p-1} \binom{p}{i} * x^i y^{p-i} + y^p.$$

Da $\binom{p}{i}$ für alle $i \in \{1, 2, \ldots, p-1\}$ Vielfache von p sind, gilt $(x+y)^p = x^p + y^p$. (2): Wir verwenden den Satz von Fermat für die Gruppe $(E^*, \cdot)$ und erhalten, dass alle $x \neq 0$ die Gleichung $x^{q-1} = 1$ erfüllen. ■

ÜBUNGSAUFGABEN 1.12.

(1) Sei $\mathbf{K}$ ein Körper der Charakteristik p, sei $m \in \mathbb{N}$, und seien $x, y \in K$. Zeigen Sie: $(x + y)^{p^m} = x^{p^m} + y^{p^m}$.
(2) Sei $\mathbf{K}$ ein Körper, und sei $f \in \mathbf{K}[x]$. Seien $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$ paarweise verschiedene Nullstellen von f. Zeigen Sie, dass $\prod(x - \alpha_i)$ ein Teiler von f in $\mathbf{K}[x]$ ist.
(3) Zeigen Sie, dass ein Polynom in $\mathbf{K}[x]$ vom Grad $\leq n$, das $n + 1$ verschiedene Nullstellen hat, automatisch das Nullpolynom sein muss.

DEFINITION 1.13. Sei $\mathbf{K}$ ein endlicher Körper mit q Elementen. Ein Element $\alpha \in K$ ist ein *primitives Element* von $\mathbf{K}$, wenn

$$K = \{0\} \cup \{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{q-2}\}.$$

Ein Element ist also genau dann primitiv, wenn jedes von Null verschiedene Körperelement eine Potenz von α ist.

DEFINITION 1.14. Sei $\mathbf{K}$ ein endlicher Körper, und sei $\alpha \in K \setminus \{0\}$. Die *Ordnung* von α in $\mathbf{K}$ ist gegeben durch

$$\mathrm{ord}(\alpha) := \min\{k \in \mathbb{N} \mid \alpha^k = 1\}.$$

LEMMA 1.15. *Sei $\mathbf{K}$ ein endlicher Körper mit q Elementen, und sei $\alpha \in K \setminus \{0\}$, und sei $m \in \mathbb{N}$ so, dass $\alpha^m = 1$. Dann gilt:*

(1) *Die Ordnung von α ist ein Teiler von m.*
(2) *Die Ordnung von α ist ein Teiler von $q - 1$.*

Für $n \in \mathbb{N}$ ist $\varphi(n)$ die Anzahl der zu n teilerfremden Elemente in $\{1, 2, \ldots, n-1\}$.

SATZ 1.16. *Sei $\mathbf{K}$ ein endlicher Körper mit q Elementen. Dann gibt es genau $\varphi(q-1)$ primitive Elemente in $\mathbf{K}$.*

Beweis: Wir zeigen zunächst, dass $\mathbf{K}$ zumindest ein primitives Element α besitzt. Sei $h := q - 1$. Für $h = 1$ und $q = 2$ ist 1 ein primitives Element. Wir nehmen also nun $h \geq 2$ an. Wir bilden die Primfaktorzerlegung von h und finden also $N \in \mathbb{N}$, Primzahlen $p_1, p_2, \ldots, p_N$ und $r_1, r_2, \ldots, r_N \in \mathbb{N}$ sodass

$$h = \prod_{m=1}^{N} {p_m}^{r_m}.$$

Wir werden nun für jedes $i \in \{1, 2, \ldots, N\}$ ein Element a_i und ein Element $b_i \in K \setminus \{0\}$ wählen: Es gilt $\frac{h}{p_i} < h$. Da das Polynom $x^{\frac{h}{p_i}} - 1$ höchstens $\frac{h}{p_i}$ Nullstellen hat, gibt es ein Element $a_i \in K \setminus \{0\}$, sodass $a_i^{\frac{h}{p_i}} \neq 1$. Wir setzen

$$b_i := a_i^{\frac{h}{p_i^{r_i}}}.$$

Es gilt dann

$$b_i^{p_i^{r_i}} = 1. \tag{3.1}$$

Sei nun k die Ordnung von b_i, also das kleinste $n \in \mathbb{N}$, sodass $(b_i)^n = 1$. Aus Gleichung (3.1) folgt, dass

$$k | {p_i}^{r_i}.$$

Folglich gibt es ein $s_i \in \{0, 1, \ldots, r_i\}$, sodass $k = {p_i}^{s_i}$. Wir zeigen nun

$$s_i = r_i. \tag{3.2}$$

Nehmen wir an $s_i \leq r_i - 1$. Dann gilt

$$b_i^{p_i^{r_i-1}} = 1,$$

also

$$a_i^{\frac{h}{p_i}} = 1.$$

Das widerspricht der Wahl von a_i; dieser Widerspruch beweist (3.2). Die Ordnung von b_i ist also $p_i^{r_i}$. Wir bilden nun

$$c = \prod_{i=1}^{N} b_i.$$

Klarerweise gilt $c^h = 1$. Wir zeigen nun, dass c wirklich Ordnung h hat. Wenn c kleinere Ordnung hätte, dann gibt es ein $j \in \{1, \ldots, N\}$, sodass $c^{\frac{h}{p_j}} = 1$. Daher gilt

$$\prod_{i=1}^{N} b_i^{\frac{h}{p_j}} = 1. \tag{3.3}$$

Falls $i \neq j$, so gilt $p_i^{r_i} | \frac{h}{p_j}$. Wegen (3.1) sind also Faktoren in (3.3) mit $i \neq j$ gleich 1. Wir erhalten also

$$b_j^{\frac{h}{p_j}} = 1.$$

Da b_j wegen (3.2) die Ordnung $p_j^{r_j}$ hat, gilt $p_j^{r_j} | \frac{h}{p_j}$. Daher gilt $p_j^{r_j+1} | h$, was im Widerspruch zur Primfaktorzerlegung von h steht. Das Element c hat also wirklich Ordnung h, und ist somit ein primitives Element von $\mathbf{K}$.

Man kann dann zeigen, dass die primitiven Elemente von $\mathbf{K}$ genau die Elemente in $\{c^i \mid i \in \{1, 2, \ldots, q-1\} \text{ und } \mathrm{ggT}(i, q-1) = 1\}$ sind. ■

SATZ 1.17. *Sei $n \in \mathbb{N}$, $n \geq 6$. Dann gilt $\varphi(n) \geq \frac{n}{6 \log(\log(n))}$. (Dabei nehmen wir den Logarithmus zur Basis e.)*

SATZ 1.18. *Sei $\mathbf{K}$ ein Körper mit q Elementen, und sei $\alpha \in K$. Dann ist α genau dann primitiv, wenn für jede Primzahl p, die $q - 1$ teilt, folgendes gilt:*

$$\alpha^{\frac{q-1}{p}} \neq 1.$$

SATZ 1.19. *Sei p eine Primzahl, sei $m \in \mathbb{N}$, und sei $q = p^m$. Sei f ein normiertes, über $\mathbb{Z}_p$ irreduzibles Polynom in $\mathbb{Z}_p[x]$ vom Grad m. Dann ist jeder Körper mit q Elementen zu $\mathbb{Z}_p[x]/f$ isomorph.*

Literaturverzeichnis

[Lidl and Niederreiter, 1983] Lidl, R. and Niederreiter, H. (1983). *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA. With a foreword by P. M. Cohn.