Endliche Körper

Sven Klingler

3. Mai 2008

Im folgenden bezeichne R immer einen kommutativen Ring mit 1.

1 Algebraische Grundlagen

Definition und Bemerkung 1.1.: Sei $\mathbf{a} \subset R$ ein Ideal in R

(a) $R_{/\mathbf{a}} := \{r + \mathbf{a} \mid r \in R\}$ ist ebenfalls ein kommutativer Ring mit 1. Für $x \in R$ definieren wir die Elemente aus $R_{/\mathbf{a}}$ wie folgt: $\overline{x} := x + \mathbf{a} \in R$. Dann erhalten wir äquivalent zu der Konstruktion von $\mathbb{Z}_{/m\mathbb{Z}}$ für $m \in \mathbb{N}$, folgende Regeln für Addition und Multiplikation:

$$\overline{x} + \overline{y} = x + \mathbf{a} + y + \mathbf{a} = x + y + \mathbf{a}$$

$$\overline{x} \cdot \overline{y} = \cdots = x \cdot y + \mathbf{a}$$

(b) Nach dem Euklidischen Algorithmus gilt für $x, a \in R$ mit ggt(x, a)=1 $\exists r_1, r_2 \in R : r_1 x + r_2 a = 1$. Also ist in $R_{/(a)} r_1$ invers zu x.
Folglich gilt: $x \in (R_{/(a)})^* \Leftrightarrow \text{ggT}(x, a) = 1$. Das funktioniert natürlich nur wenn der ggT existiert, d.h. wenn R ein euklidischer Ring ist.

(c) Die **eulersche φ Funktion**
$\varphi : \mathbb{N}_{\geq 1} \to \mathbb{N}_{\geq 1}$ mit
$\varphi(m) := (\mathbb{Z}_{m\mathbb{Z}})^* = \#\{0 \leq n < m : \text{ggT}(m, n) = 1\}$ und
$\varphi(1) := 1$ heißt eulersche φ Funktion.

(d) Einige Eigenschaften:
$\varphi(p) = p - 1$, falls p eine Primzahl ist.
$\varphi(p^k) = \#\{n \in \{1, \cdots, p^k\}$ mit $\text{ggT}(n, p^k) = 1\} =$
$= \#\{\{1, \cdots, p^k\} - \{p, 2p, \cdots, p^2, \cdots, p^k\}\} = p^k - p^{k-1}$.
ohne Beweis: $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ für ggT(a,b) = 1.

Definition 1.2:

(a) Ein Ring R heißt **faktoriell**, falls:
Jedes $x \in R - \{0\}$ eine eindeutige Darstellung der Form $x = u \prod_{p:prim,normiert} p^{s_p}$ mit $u \in R^*$ und $s_p \in \mathbb{N}$ besitzt.

(b) $p \in R$ heißt **Prim(ideal)**, falls:
$\forall r, s \in R : p \mid r \cdot s \Rightarrow p \mid r$ oder $p \mid s$

(c) $p \in R$ heißt **irreduzibel**, falls:
für alle Zerlegungen $p = x \cdot y$ mit $x, y \in R : x \in R^*$ oder $y \in R^*$

(d) Ein Ideal $\wp$ heißt **Primideal**, falls:
$\wp \neq R$ und für $a \cdot b \in \wp$ stets $a \in \wp$ oder $b \in \wp$ gilt.
Bem.: p Primelement $\Leftrightarrow (p)$ ist Primideal.

(e) Ein Ideal $\mathbf{m}$ heißt maximal, falls
$\mathbf{m} \neq R$ und aus $\mathbf{a} \subset R$ Ideal mit $\mathbf{m} \subset \mathbf{a} \subset R$ folgt, dass $\mathbf{a} = \mathbf{m}$ oder $\mathbf{a} = R$

Lemma 1.3:

Seien $\wp$ und $\mathbf{m}$ Ideale in R

(i) $\wp$ ist prim $\Leftrightarrow R_{/\wp}$ ist Nullteilerfrei

(ii) $\mathbf{m}$ ist maximal $\Leftrightarrow R_{/\mathbf{m}}$ ist ein Körper

(iii) $\wp$ maximal $\Rightarrow \wp$ ist prim

Beweis:

(c) Diese Aussage ist eine direkte Folgerung aus Teil (a) und (b), denn wenn $\wp$ ein maximales Ideal ist, ist $R_{/\wp}$ ein Körper. Und da Körper bekanntermaßen nullteilerfrei sind ist $\wp$ auch ein Primideal.

(a) Seien $\overline{a}, \overline{b} \in R_{/\wp}$. Dann gilt definitionsgemäß:
$a \cdot b \in \wp \Rightarrow a \in \wp$ oder $b \in \wp$
Nun überlegen wir uns: wenn $ab + \wp = \wp$ und somit $ab \in \wp$ gilt, erhalten wir $\overline{a} = 0$ oder $\overline{b} = 0$. Also ist obige Aussage äquivalent zu:
$\overline{a} \cdot \overline{b} = 0 \Leftrightarrow \overline{a} = 0$ oder $\overline{b} = 0$,
Was gerade der Definition von Nullteilerfreiheit entspricht.

(b) $\wp$ maximales Ideal, ist äquivalent zu: $\forall a \in R - \wp : \wp + (a) = R$, sonst wäre $\wp$ kein maximales Ideal! Dies wiederum ist äquivalent zu der Aussage, dass es $p \in \wp$ und $r \in R$ gibt, mit: $r \cdot a + p = 1$, denn 1 ist ja ein Element aus R. Dies wiederum ist dazu äquivalent, dass

das Nullideal maximal in $R_{/\wp}$ ist (und $R_{/\wp}$ somit ein Körper ist), denn nach dem bisher gesagten, gibt es für alle $\overline{a} \in R_{/\wp} - \{0\}$ ein $\overline{r} \in R_{/\wp}$ mit $\overline{a \cdot b} = 1$. Somit ist jedes vom Nullideal verschiedene Ideal in $R_{/\wp}$ schon der gesamte Restklassenring. Damit ist alles gezeigt.

Lemma 1.4:

In einem Hauptidealring sind folgende Aussagen äquivalent:

(i) $p \in R$ ist prim

(ii) $p \in R$ ist irreduzibel

(iii) $(p) \subset R$ ist maximales Ideal

Beweis:

$(iii) \Rightarrow (ii)$ (p) maximales Ideal $\Rightarrow^{1.3.}$ (p) Primideal $\Rightarrow p$ ist Primelement.

$(ii) \Rightarrow (i)$ Sei $p = x \cdot y$ mit $x, y \in R$, dann gilt definitionsgemä"s: $p \mid x$ oder $p \mid y$ Œ gelte $p \mid x \Rightarrow \exists c \in R : pc = x \Rightarrow p = xy = pcy \Rightarrow cy = 1$. Also ist y eine Einheit in R, womit die Definition eines irreduziblen Elements erfüllt ist.

$(i) \Rightarrow (iii)$ Sei $p \in R$ irreduzibel und $a \in R$ mit: $(p) \subset (a) \subset R$. Also muss es ein $c \in R$ geben mit: $p = c \cdot a$. Da p irreduzibel ist, gilt entweder $c \in R^*$, womit (wegen $p = ca \Leftrightarrow c^{-1}p = a$) $(p) = (a)$ wäre. Oder $a \in R^*$, womit $(a) = R$ gelten würde, denn dann wäre ja $1 \in R$. Also ist p ein maximales Ideal. Damit ist alles gezeigt.

Satz 1:

Euklidische Ringe sind faktoriell

Beweis:
Zeige hierzu: R euklidisch $\Rightarrow^{(i)}$ R Hauptidealring $\Rightarrow^{(ii)}$ R faktoriell

(i) Diese Aussage wurde bereits im ersten Vortrag bewiesen.

(ii) Aus Lemma 1.4. wissen wir, dass in einem Hauptidealring irreduzible Elemente Primelemente sind.
Zeige nun: Jedes $x \in R - \{0\}$ lässt sich als Produkt irreduzibler Elemente schreiben.

Sei $x \in R$ mit der Eigenschaft: x lässt sich nicht als Produkt irreduzibler Elemente darstellen. $\Rightarrow x$ ist nicht in R^* und x ist nicht irreduzibel.
$\Rightarrow x = x_1 y_1$ mit $x_1, y_1 \notin R^*$
Œ sei x_1 wieder ein Element, das sich nicht als Produkt irreduzibler Elemente darstellen lässt.
$\Rightarrow x_1 = x_2 y_2$ mit $x_2, y_2 \notin R^*$. Erhalte wieder Œ x_2 als Element, das sich nicht als Produkt irreduzibler Elemente in R darstellen lässt. Wenn wir dieses Verfahren induktiv fortsetzen, erhalten wir auch noch $x_3, x_4, \cdots$ mit diesen Eigenschaften und somit eine aufsteigende Kette von Idealen d.h.: $(x_1) \subset (x_2) \subset \cdots$ Definiere nun $I := \bigcup_{i=1}^{\infty} x_i$. I ist Ideal. Da wir in einem Hauptidealring sind folgt: $\exists a \in R : I = (a) \Rightarrow \exists i \in \mathbb{N} : a \in (x_i) \Rightarrow x_j \in (x_i)$ für $j > i$ Das ist ein Widerspruch! Damit kann es kein x mit obigen Eigenschaften geben und die Aussage ist gezeigt.

Bemerkung 1.5. (Satz von Lagrange)

Seien $(G, \cdot)$ eine endliche Gruppe und H eine Untergruppe von G
Sei außerdem $\#G = n$ und $a \in G$.

(a) Der Satz von Lagrange sagt dann: $\#H \mid \#G$

(b) Außerdem gilt für $a \in G$: $a^n = 1$ Dann gilt: $a^n = 1$.

Beweis:

(a) vgl. LA1 Skript 2.11.2.

(b) Sei ord$(a) = d$ und $H := \{1, a, a^2, \cdots, a^{n-1}\}$.
Dann ist H eine Untergruppe von G.
Mit dem Satz von Lagrange gilt dann $\#H \mid \#G \Rightarrow \exists k \in \mathbb{N} : n = kd$
Also haben wir: $a^n = a^{kd} = (a^d)^k = 1^k = 1$.
Damit ist alles gezeigt.

2 Körpererweiterungen und endliche Körper

Definition und Bemerkung 2.1: Seien p eine Primzahl, $h \in \mathbb{F}_p[X]$ ein irreduzibles Polynom mit grad$(h) =$ d und $q := p^d$.

(a) $\mathbb{Z}_{/p\mathbb{Z}} =: \mathbb{F}_p$ ist ein Körper, denn er hat nach eulers φ Funktion $p - 1$ Einheiten.

(b) (**Kronecker Konstruktion**) $\mathbb{F}_p[X]_{/(h(X))} =: \mathbb{F}_q$ ist ein Körper mit p^d Elementen.

(c) (ohne Beweis) Alle Körper mit p^d Elementen sind isomorph

Beweis:
Bleibt nur noch Aussage (b) zu zeigen:
Aus dem ersten Kapitel folgt direkt, dass $\mathbb{F}_q$ ein Körper ist.
Es gibt genau p^d Polynome in $\mathbb{F}_p$, die Grad kleiner d haben.
Diese sind gerade die Elemente von $\mathbb{F}_q$.

Beispiel 2.2:
Betrachte: $\mathbb{R}[X]_{/(X^2+1)} = \{a + bX + (X^2+1) \cdot \mathbb{R}[X] \mid a, b \in \mathbb{R}\}$
Es gilt $X^2 + 1 = 0 \Leftrightarrow X^2 = -1$ und für $a + bX \neq 0$ gilt:
$(a + bX) \cdot (\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}X) = 1$ Es gilt $\mathbb{R}[X]_{/(X^2+1)} \cong \mathbb{C}$ ist ein Körper.

Lemma 2.3: Seien $\mathbb{K}$ ein Körper, $f \in \mathbb{K}[X]$ und $\text{grad}(f) = d \geq 1$

(a) $\#\{\alpha \in \mathbb{K} : f(\alpha) = 0\} \leq d$

(b) Für alle $h \in \mathbb{K}[X]$ existieren eindeutig bestimmte, irreduzible Polynome $g_1, \ldots, g_m \in \mathbb{K}[X]$ mit $f(X) = \prod_{i=1}^{m} g_i(X)$

Beweis

(b) Diese Behauptung folgt direkt aus Satz 1.

(a) Angenommen es gäbe mehr als d Nullstellen von f in $\mathbb{K}[X]$
Seie $\alpha_1, \ldots, \alpha_{d+1}$ die ersten $d+1$ Nullstellen.
Dann können wir diese induktiv von f abgespalten werden:
$f(X) : (X - \alpha_1) =: r_1(X)$ wobei grad(r_1)=d-1
$\vdots$
$r_d(X) : (X - \alpha_{d+1}) =: r_{d+1}(X)$ wobei grad(r_{d+1})=-1
Ein solches Polynom kann es aber nicht geben.

Satz 2:

Die multiplikative Gruppe $\mathbb{F}^*$ eines endlichen Körpers ist zyklisch.

Beweis:
Sei $q := \#\mathbb{F}$ Œ können wir $q > 3$ annehmen. (Das geht, weil Körper mindestens zwei Elemente haben (vgl Def. aus LA) und für $q = 3$ wäre $\mathbb{F}_3 \cong \mathbb{Z}_{/3\mathbb{Z}}$ Sei außerdem $h := q - 1 = \#\mathbb{F}_q^*$ mit zugehöriger Primfaktorzerlegung $\prod_{i=1}^{m} p_i^{r_i}$

Für alle $1 \leq i \leq m$ hat das Polynom $X^{\frac{h}{p_i}}$ höchstens $\frac{h}{P_i}$ Nullstellen in $\mathbb{F}_q$. (gilt nach letztem Lemma)

Wegen $\frac{h}{p_i} < h$ gilt: $\exists a_i \in \mathbb{F}_q^* : a_i^{\frac{h}{p_i}} \neq 1$. Sei $b_i := a^{\frac{h_i}{p_i^{r_i}}}$ Dann gilt: $b_i^{p_i^{r_i}} = a_i^h = 1 \Rightarrow e_i := ord(b_i) \mid p_i^{r_i}$ Da p_i eine Primzahl ist, existiert ein $s_i \leq r_i$, sodass $e_i = p_i^{s_i}$. Annahme: $s_i \leq r_i - 1 \Rightarrow b_i^{p_i^{s_i}} = 1$ ABER: $b_i^{p_i^{r_i-1}} = a_i^{\frac{h}{p_i}} \neq 1$.
Also ist $s_i = r_i$ und somit $e_i = p_i^{r_i}$.
Sei $b := \prod_{i=1}^m b_i$ und $e := ord(b)$
Annahme: $< b > \neq \mathbb{F}^x$. Dann wäre e ein echter Teiler von h klar: $b^h = 1$ und $e \mid h$ Weil e ein echter Teiler von h ist, gibt es ein p_i, sodass: $e \mid \frac{h}{p_i}$ Œ sei $p_i = p_1$. Wegen $b^e = 1$ ist auch $b^{h/p_1} = 1 \Rightarrow 1 = b^{h/p_1} = \prod_{i=1}^m b_i^{h/p_1} = b_1^{h/p_1}$
$\Rightarrow e_1 \mid \frac{h}{p_1}$, da $e_1 = p_1^{r_1}$ und $\frac{h}{p_1} = p_1^{r_1-1} \cdot \prod_{i=2}^m b_i^{h/p_1}$
Da p_i für $i = 1, \cdots, m$ teilerfremd sind (Primzahlen!!!) haben wir einen Widerspruch gefunden.

3 Erste Vorbereitungen für den Primzahlalgorithmus

Lemma 3.1: Seien $n \geq 2, k \geq 1$ und $d \geq 1 \in \mathbb{Z}$
Dann gilt: $(n^k - 1) \mid (n^d - 1) \Rightarrow k \mid d$

Beweis:
Schreibe $d = kq + r$ mit $q \geq 0$
Zu zeigen: $r = 0$
$\frac{n^d-1}{n^k-1} = \frac{n^r(n^{qk}-1)+(n^r-1)}{(n^k-1)} = n^r(n^{(q-1)k} + \ldots + n^k + 1) + \frac{n^r-1}{n^k-1}$.
Für $r \neq 0$ ist aber $0 < \frac{n^r-1}{n^k-1} < 1$.
Das wäre aber ein Widerspruch.
Damit ist alles gezeigt.

Lemma 3.1:
Sei p eine Primzahl und $f(X) \in \mathbb{F}_p$[X]. Dann gilt in $\mathbb{F}_p$

$$f(X^p) = (f(X))^p$$

Beweis:
Wir führen den Beweis durch Induktion über $d := grad(f)$
IA: $d = 0$. Nach Fermat gilt: $a^p \equiv a \bmod p \Rightarrow$ Beh.

IS: $d \geq 1$ und die Beh. gilt für alle Polynome mit Grad kleiner als d. Schreibe $f(X) = aX^d + g(X)$ mit $a \in \mathbb{F}_p$ und $g(X) \in \mathbb{F}_p$[X] mit $grad(g) < d$ $(f(X))^p = (aX^d + g(X))^p = \sum_{i=0}^{p} \binom{p}{i} a^i \cdot X^{i-d}(g(X))^{p-i}$ wegen den bekannten Eigenschaften des Binomialkoeffizienten ist das aber genau $(g(X))^p + a^p x^{pd} =^I Vg(X^p) + a^p(X^p)^d = f(X^p) \Rightarrow$ Beh.

Satz 3:
Seien p, r verschiedene Primzahlen und sei d die Ordnung von p modulo r. Alle irreduziblen Polynome in $\mathbb{F}_p$[X], die $\frac{X^r-1}{X-1}$ teilen haben den Grad d.

Beweis:
Genüge $h(X)$ den obigen Anforderungen. Sei $k := grad(h)$. Wir zeigen die Aussage $k = d$, indem wir zuerst $k \mid d$ und dann $d \mid k$ beweisen.
Schritt 1: $k \mid d$
$\mathbb{F}_p/(h(X))$ ist Körper mit p^k Elementen. Sei $< g >= \mathbb{F}_{p^k}^* \Rightarrow ord(g) = p^k - 1$
nach obigem Lemma gilt: $(g(X))^{p^d} = g(X^{p^d})$ in $\mathbb{F}_p$[X].
Wegen $p^d \equiv 1 \bmod r \Rightarrow \exists k \leq 1 : p^d = 1 + kr$.
Sei $f \in \mathbb{F}_p$[X]: $f(X)h(X) = X^r - 1$
$\Rightarrow X^{pd} = X \cdot X^{kr} = X \cdot (1 + f(X)h(X))^k \equiv X \bmod h(X)$
$g \neq 1$ da Erzeuger von $\mathbb{F}_{p^k}^* \Rightarrow (g(X))^{p^d-1} \equiv 1 mod h(X)$.
Wegen $ord(g) = p^k - 1 \Rightarrow (p^k - 1) \mid (p^d - 1) \Rightarrow^($ 3.1.$) k \mid d$.
Schritt 2: $d \mid k$
Nach Konstruktion gilt: $h(X) \mid X^r - 1 \Rightarrow x^r \equiv x \bmod h(X)$
$\Rightarrow ord(X) = r$ in $\mathbb{F}_{p^k} = \mathbb{Z}/p\mathbb{Z}/(h(X))$.
Andererseits ist $\#\mathbb{F}_p^* = p^k - 1 \Rightarrow^{1.5.} X^{p^k-1} \equiv 1 \bmod h(X)$
$\Rightarrow r \mid (p^k - d) \Leftrightarrow p^k \equiv \bmod h(X)$, da p modulo r die Ordnug d hat folgt $d \mid k$
Damit ist alles gezeigt.