technische universität dortmund

fakultät für mathematik

Endliche Körper

Vanessa Lisewski

Seminar Algebra & Zahlentheorie LA Gym,

angefertigt am

Institut für Algebra und Geometrie

Fakultät für Mathematik

Technische Universität Dortmund

Seminarleitung: Prof. Dr. Detlev Hoffmann

Dortmund, Sommersemester 2018

Inhaltsverzeichnis

0. Wichtige Hilfssätze

.

Satz 1.0.6

Sei K/F eine algebraische Körpererweiterung. Dann gelten folgende Äquivalenzen:

a) K/F ist galoissch

b) K/F ist normal und seperabel

c) K ist Zerfällungskörper einer Menge seperabler Polynome über F

Korollar 1.0.9

Sei K/F eine endliche Körpererweiterung. Dann gilt:

K/F galoissch $\Leftrightarrow$ |Gal(K/F)| = [K:F]

Satz über isomorphe Erweiterungen

Sei σ : F $\rightarrow$ F' ein Körperisomorphismus, S = f_i(x) eine Menge von Polynomen über F und S' = $\sigma(f_i)$ die zugehörige Menge über F'. Sei zudem K ein Zerfällungskörper für S über F und K' der Zerfällungskörper für S' über F'.
Dann gibt es einen Isomorphismus τ : K $\rightarrow$ K' mit $\tau_F = \sigma$. Weiterhin kann man τ so wählen, dass τ(a) = a', falls a aus K und a' eine beliebeige Nullstelle von σ(min(F,a)) in K' ist.

Gradsatz

Seien L/K und M/L Körpererweiterungen. Dann gilt:

$[M : K] = [M : L][L : K]$

Proposition 1.0.3

Sei f(x) $\in$ F[x] ein nichtkonstantes Polynom. f hat keine mehrfachen Nullstellen in einem Zerfällungskörper, wenn der ggt(f,f')= 1 in F[x] ist.

1. Einleitung

.

In den Kapiteln zuvor wurden verschiedene Mechanismen zur Galois-Theorie entwickelt.
Im Folgenden werden diese Theorien dazu verwendet um spezielle Arten von Körpererweiterungen zu untersuchen.
Das vorliegende, ausgearbeitete Unterkapitel beschäftigt sich mit der Erforschung endlicher Körper, genauer mit der Erforschung endlicher Erweiterungen endlicher Körper.
Sei beispielsweise F ein endlicher Körper mit der Charakteristik p. Dann können wir F als eine Körpererweiterung von $\mathbb{F}_p$ sehen. Da F als endlich gegeben ist, ist dieser ein endlicher $\mathbb{F}_p$ - Vektorraum.
Falls [F:$\mathbb{F}_p$] = n, dann sind F und $\mathbb{F}_p{}^n$ als $\mathbb{F}_p$ - Vektorräume isomorph. Daraus folgt $|F| = p^n$.

Zu Beginn dieses Abschnittes werden einige körpertheoretische Informationen über ein solches, endliches F entwickelt, indem die multiplikative Gruppe F^* genauer betrachtet wird.
Für das erste Lemma benötigt man jedoch zunächst die folgende Definition (und die sich ergebenden Eigenschaften) des Gruppenexponenten.

Definition 6.0

Sei G eine endliche Gruppe. Der **Gruppenexponent** exp(G) bezeichnet die kleinste Zahl n > 0 für die gilt
$g^n = e, \forall\ g \in G$

Aus dieser Definition ergeben sich einige Eigenschaften, welche für den Beweis des ersten Lemmas dieses Kapitels wichtig sind:
1) In einer abelschen Gruppe G gilt: G ist zyklisch ⇔ Die Ordnung und der Exponent der Gruppe stimmen überein
2) Nach dem Satz von Lagrange ist der Gruppenexponent für eine endliche Gruppe ein Teiler von der Gruppenordnung und somit insbesondere endlich.

2. Endliche Körper

.
Lemma 6.1

Sei K ein Körper und G eine endliche Untergruppe von K^*. Dann ist G zyklisch.

Beweis

Sei $n = |G|$ und $m = \exp(G)$ der Gruppenexponent.
Dann folgt mit der Endlichkeit von G und Definition 6.0, dass
$m \mid n$
$\Rightarrow m \leq n$

Sei nun $g \in G$. Dann gilt durch $m = \exp(G)$

$g^m = 1$

Das bedeutet alle Elemente von G sind Nullstellen des Polynoms

$x^m - 1$

Dieses Polynom besitzt maximal m Nullstellen. Da alle Elemente von G Nullstellen dieses Polynoms darstellen folgt nun

$n \leq m$

$\Rightarrow m = n$
$\Rightarrow |G| = \exp(G)$
$\Rightarrow$ G ist zyklisch

□

Der Beweis liefert als Produkt folgendes Korollar:

Korollar 6.2

Ist F ein endlicher Körper, dann ist F^* zyklisch.

Korollar 6.4

Ist K/F eine endliche Körpererweiterung, dann ist K eine einfache Erweiterung von F.

Beweis

Da K endlich ist wissen wir durch Korollar 6.2, dass die Gruppe K^* zyklisch ist.
Sei a nun ein Erzeuger dieser zyklischen Gruppe, das bedeutet

$K^* = < a > = \{a^n \mid n \in \mathbb{Z} \text{ und } a \neq 0 \}$

⇒ Alle von Null verschiedenen Elemente von K sind Potenzen von a
⇒ Die Körpererweiterung wird von einem Element, nämlich von a, erzeugt
⇒ K = F(a)
⇒ K ist eine einfache Erweiterung von F

□

Wir kommen nun zu einem für das vorliegende Unterkapitel wichtigem Theorem. Dieses beinhaltet im Großen und Ganzen drei elementare Aussagen:

Theorem 6.5

Sei F ein endlicher Körper mit char(F) = p und man setze $|F| = p^n$

a) Dann ist F der Zerfällungskörper des seperablen Polynoms x^{p^n}-x über $\mathbb{F}_p$

b) $F/\mathbb{F}_p$ ist galoissch

c) Ist weiter σ über F definiert als $\sigma(a) = a^p$ dann erzeugt σ die Galoisgruppe $Gal(F/\mathbb{F}_p)$, sodass diese Galoisgruppe zyklisch ist.

Beweis

zu a)
Sei $|F| = p^n$. Dann ist $|F^*| = p^n$-1.
Nach dem Satz von Lagrange, der besagt, dass insbesondere die Elementordnung die Gruppenordnung teilt und somit die Gruppenordnung ein Vielfaches der Elementordnung darstellt, gilt nun:
Ist $a \in F^*$, dann ist

$a^{p^n-1} = 1$ (Jedes Vielfache der Elementordnung bildet unter der Potenz des Elementes wieder auf das neutrale Element ab)

Multipliziert man auf beiden Seiten mit a ergibt sich

$a^{p^n} = a$

Dies gilt dann auch für a = 0.

⇒ Alle Elemente von F sind Nullstellen des Polynoms

x^{p^n} - x

Dieses Polynom besitzt maximal p^n Nullstellen.
⇒ Die Elemente von F sind *genau* die Nullstellen dieses Polynoms

Dies beweist, dass F der Zerfällungskörper von x^{p^n} - x darstellt. Dadurch ist F normal über $\mathbb{F}_p$

Bleibt zu zeigen, dass dieses Polynom seperabel über F ist, das bedeutet, wir wollen beweisen, dass x^{p^n} - x keine mehrfachen Nullstellen in F besitzt.
Da bereits gezeit wurde, dass die Nullstellen dieses Polynoms genau die Elemente von F sind, und sich diese nicht wiederholen, ist x^{p^n} - x bereits seperabel.

zu b)
Wir wollen zeigen, dass $F/\mathbb{F}_p$ galoissch ist

Wir haben bereits gezeigt, dass F den Zerfällungskörper von x^{p^n} - x über $\mathbb{F}_p$ darstellt, also F normal über $\mathbb{F}_p$ ist. Nach Satz 1.0.6 (4.9 im Buch) reicht nun noch zu zeigen, dass das Polynom x^{p^n} - x seperabel ist. Dies haben wir bereits am Ende des Beweises zu a) getan.

$\Rightarrow F/\mathbb{F}_p$ ist galoissch

zu c)
Wir definieren nun $\sigma : F \to F$ mit $\sigma(a) = a^p$
Zunächst zeigen wir, dass σ einen Homomorphismus auf sich, also einen Endomorphismus, darstellt. Dazu müssen wir zeigen, dass diese Abbildung verträglich unter der Multiplikation und Addition ist.

Es ist klar, dass gilt:

$\sigma(0) = 0^p = 0$ und
$\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\ \sigma(b)$

Somit ist σ verträglich mit der Multiplikation. Um zu zeigen, dass diese Funktion einen Endomorphismus darstellt, muss noch

$\sigma\ (a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$

bewiesen werden.
Seien also $a, b \in F$ beliebig.
Dann ist nach dem Binominalsatz

$$(a+b)^p = \left(\begin{array}{c} p \\ i \end{array} \right) a^i b^{p-i}$$

Betrachtet werden zunächst die Randfälle:

Sei i=0. Dann gilt:

$$\left(\begin{array}{c} p \\ 0 \end{array} \right) a^0 b^{p-0} = b^p$$

Sei i=p. Dann gilt:

$$\left(\begin{array}{c} p \\ p \end{array} \right) a^p b^{p-p} = a^p$$

Sei nun i= 1,...,p-1. Dann gilt, $p \mid \left(\begin{array}{c} p \\ i \end{array} \right)$, denn

$\left(\begin{array}{c} p \\ i \end{array} \right) = \frac{p!}{i!(p-i)!}$, $p \mid p!$, $p \nmid i!$ und $p \nmid (p-1)!$

Und da p als Charakteristik des Körpers F gleich Null ist und p den Binominalkoeffizienten teilt verschwinden die Summanden für i= 1,...,p-1

$\Rightarrow (a+b)^p = a^p\ b^p$

$\Rightarrow \sigma$ ist ein Endomorphismus

Homomorphismen von Körpern sind immer injektiv und da F endlich ist folgt somit auch, dass σ surjektiv ist. Somit ist σ insgesamt bijektiv und so ein Automorphismus.

Der Fixkörper von σ ist $\{ a \in F : a^p = a \} \supseteq \mathbb{F}_p$

$\Rightarrow$ Jedes Element von dem Fixkörper ist eine Lösung des Polynoms x^p - x
$\Rightarrow$ Es existieren maximal p Elemente im Fixkörper
$\Rightarrow \mathbb{F}_p$ ist der ganze Fixkörper
$\Rightarrow \forall\, x \in \mathbb{F}_p : \sigma(x) = x$

σ lässt alle Elemente des Unterkörpers fix und ist als Automorphismus somit in der Galoisgruppe $\mathrm{Gal}(F/\mathbb{F}_p)$ enthalten. Es bleibt zu beweisen, dass die ganze Gruppe von diesem σ erzeugt wird und diese somit zyklisch ist.
Wir wissen mit $|\mathbb{F}_p| = p$ und $|F| = p^n$ dass
$[F:\mathbb{F}_p] = n = |\mathrm{Gal}(F/\mathbb{F}_p)|$ (da diese Erweiterung galoissch ist)
Also befindne sich n Elemente in der Galoisgruppe.
Betrachten wir nun die Gruppe

$< \sigma > = \{ \mathrm{id}, \sigma, \sigma^2, ..., \sigma^{n-1} \}$

Wir wollen zeigen, dass alle Elemente von $< \sigma >$ verschieden sind.

Sei x ein Erzeuger der zyklischen, multiplikativen Gruppe F^* und betrachte die Bilder von

$\mathrm{id}(x) = x$, $\sigma(x) = x^p$, $\sigma^2(x) = x^{p^2}$, ..., $\sigma^{n-1}(x) = x^{p^{n-1}}$

Sind die Bilder dieser Abbildungen verschieden, so sind auch die Automorphismen selbst verschieden. Betrachte das letzte Bild genauer:

$\sigma^{n-1}(x) = x^{p^{n-1}}$

Da F^* zyklisch ist gilt, dass sich die Elemente erst bei der Potenz der Ordnung von F^* p^n-1 wiederholen.

$p^{n-1} < p^n$-1

$\Rightarrow$ Alle Bilder sind verschieden
$\Rightarrow$ Alle n Elemente von $< \sigma >$ sind verschieden
$\Rightarrow \mathrm{Gal}(F/\mathbb{F}_p) = < \sigma >$
$\Rightarrow \mathrm{Gal}(F/\mathbb{F}_p)$ wird von σ erzeugt und ist somit zyklisch

□

Definition 6.5.1

Der aus dem Beweis 6.5 eingeführte Automorphismus σ mit

σ: $F \to F$ mit $\sigma(x) = x^p$

wird als **Frobenius-Automorphismus** bezeichnet.

Korollar 6.6

Zwei endliche Körper derselben Größe sind isomorph

Beweis

Der Beweis aus Theorem 6.5 hat gezeigt, dass jeder Körper der Ordnung p^n Zerfällungskörper von x^{p^n}-x über $\mathbb{F}_p$ darstellt.
Der Beweis des vorliegenden Korollars ergibt sich nun einfach aus dem Satz über isomorphe Erweiterungen.
Sei der Körperisomorphismus id: $\mathbb{F}_p \to \mathbb{F}_p$ gegeben. Weiter seien dann die Menge der Polynome
S ={ x^{p^n}-x } = S' und die Zerfällungskörper K = F und K' = F' mit |F| = |F'| = p^n.
Dann existiert nach dem Satz über isomorphe Erweiterung ein Isomorphismus von F nach F'
⇒ F und F' sind isomorph

□

Korollar 6.7

Ist K/F eine Erweiterung endlicher Körper, dann ist K/F galoissch mit einer zyklischen Galoisgruppe.
Weiter ist char(F) = p und $|F| = p^n$, dann wird Gal(K/F) erzeugt durch den definierten Automorphismus τ mit $\tau(a) = a^{p^n}$.

Beweis

Sei $[K:\mathbb{F}_p]$ = m. Dann ist Gal $(K/\mathbb{F}_p)$ eine zyklische Gruppe der Ordnung m (nach Theorem 6.5)

⇒ Ordnung des Frobenius-Automorphismus σ von K ist m

Die Gruppe Gal(K/F) ist eine Untergruppe von Gal$(K/\mathbb{F}_p)$

⇒ Gal(K/F) ist ebenfalls zyklisch

Sei s = | Gal(K/F) | = [K:F] und m=ns.
Wir wollen zeigen, dass σ^n einen Erzeuger der Gruppe Gal(K/F) darstellt. Dazu nutzen wir den Satz 12.1 im Skript Algebra 1 / Algebra und Zahlentheorie LA Gym von Detlev W. Hoffmann (WS 2017/18, TU Dortmund)

Satz 12.1
Sei $C_n = \langle g \rangle$ zyklisch der Ordnung n aus den natürlichen Zahlen. Zu jedem Teiler d von n existiert genau eine Untergruppe H_d mit | H_d | = d, nämlich $H_d = \langle g^{n/d} \rangle$. Dies sind alle Untergruppen von C_n und es gilt $H_d \leq H'_d$ genau dann wenn d | d'

Aus diesem Satz folgt, dass Gal(K/F) = $\langle \sigma^n =: \tau \rangle$ (mit s ein Teiler der Ordnung m von Gal$(F/\mathbb{F}_1)$).

□

Wir haben nun endliche Körper als Erweiterungen von $\mathbb{F}_p$ beschrieben und haben gezeigt, dass jede endliche Erweiterung von $\mathbb{F}_p$ p^n Elemente besitzt für ein n.
Wir haben jedoch noch nicht ergründet, für welche n es Körper mit p^n Elementen gibt.
Mithilfe des Hauptsatzes und der Beschreibung von endlichen Körpern als Zerfällungskörper (wie in Theorem 6.5) werden wir nun beweisen, dass für alle n ein bis auf Isomorphie eindeutiger Körper mit p^n Elementen gibt.

Theorem 6.8

Sei N ein algebraischer Abschluss von $\mathbb{F}_p$.

a) Für jede positive ganze Zahl n gibt es einen eindeutigen Unterkörper von N mit der Ordnung p^n

b) Sind K und L Unterkörper von N mit den Ordnungen p^m und p^n, dann gilt

$K \subseteq L \Leftrightarrow m \mid n$

Wenn das gilt ist L galoissch über K mit der Galoisgruppe, die von $\tau(a) = a^{p^n}$ erzeugt wird.

Beweis

zu a)
Sei n eine positive, ganze Zahl und N ein algebraischer Abschluss von $\mathbb{F}_p$.
Die Menge der Nullstellen in N des Polynoms x^{p^n}-x über $\mathbb{F}_p$ besitzt p^n Elemente und stellt einen Unterörper von N dar. Dies gilt es nun zu beweisen. Dazu muss gezeigt werden, dass die Menge

$M = \{x \in \mathbb{R}^{\,n} \mid x^{p^n}\text{-x} = 0\}$

folgende Kriterien erfüllt:
1. (M,+) ist eine Untergruppe von (N,+)
2. (M,·) ist abgeschlossen und das multiplikative Inverse liegt in der Menge
3. $1 \in M$ und M ist kommutativ

zu 3.

1^{p^n} -1 $= 0 \Rightarrow 1 \in M$
Da N ein Körper ist wird die Kommutativität an M vererbt

zu 2.

Sei $x \in M$ beliebig. Dann gilt:

x^{p^n}-x $= 0 \mid \cdot -\frac{1}{x^{p^n+1}}$

$\Leftrightarrow -\frac{1}{x} + \frac{1}{x^{p^n}} = 0$

$\Rightarrow \frac{1}{x} \in M$

Seien $x,y \in M$ beliebig
$(xy)^{p^n}$ - xy $= x^{p^n}\, y^{p^n}$ -xy $= x^{p^n}\, y^{p^n}$ $-x^{p^n}$y $+x^{p^n}$y -xy $= x^{p^n}\,(y^{p^n}\text{-y}) + y\,(x^{p^n}\text{-x}) = 0$

$\Rightarrow xy \in M$

zu 1.

1.1 Zu zeigen: $0 \in M$
0^{p^n} - 0 $= 0 \Rightarrow 0 \in M$

1.2 Zu zeigen: Sind $x,y \in M \Rightarrow x+y \in M$
Seien $x,y \in M$
$(x+y)^{p^n}$ - (x+y) $= x^{p^n} + y^{p^n}$ -x-y $= x^{p^n}$ - x + y^{p^n} - y $= 0 \Rightarrow x+y \in M$

1.3 Zu zeigen: Für $x \in M$ gilt: $(-x) \in M$
Sei $x \in M$ beliebeig
$(-\,x^{p^n}\,) + x = -(\,x^{p^n} + x) = 0 \Rightarrow (-x) \in M$

⇒ Die Menge der Nullstellen des Polynoms x^{p^n}-x über $\mathbb{F}_p$ stellt einen Unterkörper von N mit p^n Elementen dar.

⇒ Es existiert ein Unterkörper von N mit der Ordnung p^n

Wir wollen nun die Eindeutigkeit des Körpers zeigen. Durch 6.5 wissen wir, dass 2 beliebige Körper der Ordnung p^n aus N Zerfällungskörper von x^{p^n}-x über $\mathbb{F}_p$ darstellen.
Weiter wissen wir durch 6.5, dass jeder Unterkörper von N der Ordnung p^n exakt aus den Nullstellen von x^{p^n}-x besteht.

⇒ Der Unterkörper ist eindeutig

zu b)
Seien nun K,L Unterkörper von N mit Ordnungen p^m und p^n. Zu zeigen: K⊆L ⇔ m| n

" ⇒ " Sei K⊆ L
Dann gilt nach dem Gradsatz

n = [L:$\mathbb{F}_p$] = [L:K] [K:$\mathbb{F}_p$] = [L:K] m ⇒ m|n

" ⇐ " Sei nun m|n gegeben

Da |K| = p^m und K ⊆ N erfüllen alle Elemente a ∈ K

a^{p^m} = a

Da m|n gilt für alle a ∈ K ebenfalls

a^{p^n} = a

⇒ a ∈ L
⇒ K ⊆ L
⇒L ist eine Erweiterung von K und da L und K endlich sind gilt nach 6.7 dass L/K galloisch ist und erzeugt wird von $\tau(a) = a^{p^n}$

□

Wir wollen nun die Theoreme 6.5 und 6.8 dazu nutzen um den Zerfällungskörper von eines Polynoms f eines endlichen Körpers F zu bestimmen.

Korollar 6.9

Sei F ein endlicher Körper und sei f ein irreduzibles Polynom über F mit Grad n.

a) Ist a eine Nullstelle von f in einer Körpererweiterung von F, dann ist F(a) ein Zerfällungskörper von f über F

b) Ist |F| = q, dann stellt { a^{q^r} | r ≥ 1 } die Menge der Nullstellen dar

Beweis

zu a)
Sei K ein Zerfällungskörper von f über F. Ist a ∈ K eine Nullstelle von f(x), dann ist F(a) eine n-dimensionale Erweiterung von F in K

⇒ Nach 6.5 ist F(a) eine Galoiserweiterung von F

$\Rightarrow$ f(x) = min(F,a) zerfällt über F(a)
$\Rightarrow$ F(a) ist Zerfällungskörper von f über F
$\Rightarrow$ K = F(a)

zu b)
Sei |F| = q und Gal(F/K) = $< \sigma >$ mit $\sigma(c) = c^q$ für alle c $\in$ K
Jede Nullstelle von f ist somit der Form

$\sigma^{\,r}(a) = a^{q^r}$

$\Rightarrow$ { a^{q^r} | r $\geq$ 1 } stellt die Menge der Nullstellen dar

□

Zu diesem Korollar folgt nun ein kleines Beispiel:

Beispiel 6.10

Sei F = $\mathbb{F}_2$ und K = F(a), wobei a eine Nullstelle darstellt von

$f(x) = x^3 + x^2 + 1$

Dieses Polynom hat keine Nullstellen in F = $\mathbb{F}_2$, wie man anhand von

$f(0) = 0^3 + 0^2 + 1 = 1$ und
$f(1) = 1^3 + 1^2 + 1 = 1$

erkennen kann

$\Rightarrow$ f(x) ist irreduzibel über F und nach dem vorangegangenen Korollar wissen wir, dass

[K:F] = 3

$\Rightarrow$ K ist Zerfällungskörper von f über F (6.9)
$\Rightarrow$ a, a^2 und a^4 sind Nullstellen von f (6.9)

Da f(a) = 0 gilt, ist

$0 = a^3 + a^2 + 1$
$\Leftrightarrow a^3 = a^2 + 1 \mid \cdot a$
$a^4 = a^3 + a = a^2 + a + 1$

$\Rightarrow$ a, a^2 und a^2 +a +1 sind die Nullstellen von f

Dies zeigt, dass F(a) den Zerfällungskörper von f über F darstellt

3. Zusammenfassung

.

Folgendes wurde in diesem Kapitel gezeigt:
Wenn F einen endlichen Körper darstellt ist jede endliche Erweiterung von F galloisch über F.
Daraus folgt, dass jede algebraische Erweiterung von F seperabel über F ist, somit ist F perfekt.
Diese Erkentnnis wollen wir als Endprodukt dieser Ausarbeitung in einem weiteren Korollar festhalten:

Korollar 6.13

Jeder endlicher Körper ist perfekt

4. Literatur

.

[1] Hoffmann, Detlev: *Algebra*, Vorlesungsskript, 2017/2018

[2] Morandi, Patrick: *Field and Galois Theory.* Springer, 1996