UE Einführung in die Algebra und Diskrete Mathematik
KV Algebra und Diskrete Mathematik

12. Übungszettel, 18. Juni 2013

Lösungen

1. Bilden Sie GF(9) auf 2 Arten, d.h. mit 2 verschiedenen irreduziblen Polynomen.

   Lösung:
   Wir suchen uns 2 irreduzible Polynome 2. Grades über $\mathbb{Z}_3$:

   $$p_1 = x^2 + 1 = 101$$
   $$p_2 = x^2 + x - 1 = 112$$

   Das diese keine Nullstelle besitzen und ihr Grad nicht mindestens 4 ist, sind sie irreduzibel.

   Gemäß 18.17 bilden wir die Körper

   $$F_1 = Z_3[x]/(p_1)$$
   $$F_2 = Z_3[x]/(p_2)$$

   mit den erzeugenden Elementen

   $$a_1 = [x]_{(p_1)} = (001)_{(101)}$$
   $$a_2 = [x]_{(p_2)} = (001)_{(112)}$$

   (a) Zeigen Sie, dass jedes dieser Polynome über jeder Variante von GF(9) in Linearfaktoren zerfällt.

   Lösung:
   Direkt aus der Definition folgen

   $$p_1(a_1) = a_1^2 + 1 = ([x]_{(p_1)})^2 + [1]_{(p_1)} = [x^2 + 1]_{(p_1)})^2 = [0]_{(p_1)}$$
   $$p_2(a_2) = a_2^2 + a_2^1 - 1 = ([x]_{(p_2)})^2 + [x]_{(p_2)} - [1]_{(p_2)} = [x^2 + x - 1]_{(p_2)})^2 = [0]_{(p_2)}$$

   Man beachte, dass wir hier, damit wir überhaupt z.B. a_1 in p_1 einsetzen können, die Elemente von $\mathbb{Z}_3$ mit deren Äquivalenzklasse identifizieren. In diesem Sinn lassen sich die Polynome auch als definierende Gleichungen für ihre Nullstellen verstehen:

   $$a_1^2 + 1 = 0$$
   $$a_2^2 + a_2 - 1 = 0$$

   bzw.

   $$a_1^2 = -1 = 2$$
   $$a_2^2 = -a_2 + 1 = 2a_2 + 1$$

Die jeweils andere Nullstelle erhalten wir z.B. durch Abspalten des linearen Faktors. Zuerst für F_1:

$$\begin{array}{rl} (x^2 & +1) : (x - a_1) = x + a_1 \\ a_1 x & +1 \\ \hline & 0 \end{array}$$

Somit ist auch $-a_1$ eine Nullstelle von p_1. Dies ist auch deshalb klar, weil a_1 eine Wurzel von -1 (oder, was hier dasselbe ist, von 2) ist.
Probe: $(x - a_1)(x + a_1) = x^2 - a_1^2 = x^2 + 1 = p_1$.
Nun für F_2:

$$\begin{array}{rl} (x^2 + x & -1) : (x - a_2) = x + (a_2 + 1) \\ (a_2 + 1)x & -1 \\ \hline & 0 \end{array}$$

Also ist $-a_2 - 1 = 2a_2 + 2$ die zweite Nullstelle von p_2.
Probe: $(x - a_2)(x + a_2 + 1) = x^2 + (a_2 + 1 - a_2)x - a_2^2 - a_2 = x^2 + x - 1$.
Somit sehen wir, dass p_1 über F_1 und p_2 über F_2 in Linearfaktoren zerfallen. Also ist F_1 ein Zerfällungskörper von p_1 und F_2 einer von p_2 (im Sinne von 19.3)
Da wir wissen, dass F_1 und F_2 isomorph sind (mit einem Isomorphismus, welcher auf $\mathbb{Z}_3$ isomorph wirkt, 19.4), wissen wir auch, dass sie beide Polynome über beiden Körpern zerfallen müssen. Wir suchen explizit die Nullstellen von p_1 in F_2, am einfachsten durch Probieren:

$$\begin{aligned} (a_2 + 2)^2 &= a_2^2 + 4a_2 + 4 = 2a_2 + 1 + a_2 + 1 = 2 \\ (2a_2 + 1)^2 &= (-(a_2 + 2))^2 = 2 \end{aligned}$$

Probe: $(x - (a_2 + 2))(x - (2a_2 + 1)) = x^2 + 1$.
Ebenso findet man Nullstellen von p_2 in F_1.

(b) Bestimmen Sie in jeder Variante ein primitives Element und dessen Minimalpolynom. Ist letzteres maximalperiodisch?

Lösung:
Wegen $a_1^2 = 2$, und somit $a_1^4 = 1$, ist a_1 kein primitives Element von F_1.
a_2 dagegen ist bereits ein primitives Element von F_2, denn $a_2^4 = ((a_2)^2)^2 = (2a_2 + 1)^2 = 4a_2^2 + 4a_2 + 1 = a_2^2 + a_2 + 1 = (2a_2 + 1) + a_2 + 1 = 2$ (die Ordnung von a_2 muss ein Teiler von 8 sein).
p_2 ist das Minimalpolynom von a_2 (weil irreduzibel und $p_2(a_2) = 0$) und somit maximalperiodisch. p_1 dagegen nicht.
Um ein primitives Element von F_1 zu finden, können wir z.B. einfach eine Nullstelle von p_2 in F_1 verwenden.

(c) Geben Sie einen Isomorphismus zwischen beiden Varianten an.

Lösung:
Anmerkung:

Da F_1 über $\mathbb{Z}_3$ durch a_1 erzeugt ist, lässt sich jedes Element von F_1 als $p(a_1)$ darstellen, mit einem geeigneten Polynom $p \in \mathbb{Z}_3[x]$. Um einen Isomorphismus $h : F_1 \to F_2$ zu definieren, muss nur $h(a_1)$ festgelegt werden, da dann

$$h(p(a_1)) = p(h(a_1))$$

aus der Homomorphieeigenschaft folgt. Es ist unmittelbar ersichtlich, dass jede so definierte Funktion ein Homomorphismus ist. Gar nicht klar ist dagegen, dass dadurch überhaupt eine Funktion definiert wird, da die Darstellung der Elemente von F als $p(a_1)$ keineswegs eindeutig ist. Insbesondere ist $p_1(a_1) = 0$; daher muss auch $p_1(h(a_1)) = h(p_1(a_1)) = h(0) = 0$ sein. a_1 darf also nur auf andere Nullstellen von p_1 abgebildet werden, ansonsten wäre h nicht wohldefiniert. Tatsächlich führt jede derartige Wahl zu einer wohldefinierten Funktion, da aus $p(a_1) = q(a_1)$ folgt $(p-q)(a_1) = 0$, d.h. $p-q$ und p_1 haben eine gemeinsame Nullstelle; dies bedeutet, da p_1 irreduzibel ist, dass $p-q = r \cdot p_1$. Somit ist $p(h(a_1))-q(h(a_1)) = r(h(a_1)) \cdot p_1(a_1) = 0$.

$h(a_1)$ muss also eine Nullstelle von p_1 in F_2 sein. Wir haben zuvor schon eine solche gefunden und legen daher z.B. fest:

$$h(a_1) = 2a_2 + 1.$$

Die Umkehrfunktion $h^{-1} : F_2 \to F_1$ ist ebenfalls ein Isomorphismus und erfüllt (Umformen von $a_1 = 2h^{-1}(a_2) + 1$)

$$h^{-1}(a_2) = 2a_1 + 1.$$

(Eher zufällig dieselbe Formel) Auf diese Art finden wir auch leicht die Nullstellen von p_2 in F_1, da insbesondere $2a_1+1$ eine Nullstelle von p_2 in F_1 ist. Probe: $p_2(2a_1 + 1) = (2a_1 + 1)^2 + (2a_1 + 1) - 1 = 4a_1^2 + 4a_1 + 1 + 2a_1 + 1 - 1 = a_1^2 + 1 = 2 + 1 = 0$.

(d) Müssen bei jedem Isomorphismus zwischen Körpern alle primitiven Elemente auf primitive Elemente abgebildet werden?

Lösung:
Ist α ein primitives Element von F_1, dann ist $F_1 = \{0, 1, \alpha, \alpha^2, \alpha^3, \dots\}$. Ist weiters $h : F_1 \to F_2$ ein Isomorphismus, dann ist $F_2 = h(F_1) = \{h(0), h(1), h(\alpha), h(\alpha^2), h(\alpha^3), \dots\} = \{0, 1, h(\alpha), h(\alpha)^2, h(\alpha)^3, \dots\}$. Also ist $h(\alpha)$ ein primitives Element von F_2. In unserem Beispiel ist somit insbesondere $2a_1 + 1$ eine primitives Element von F_1.

(e) Gibt es einen Automorphismus von (irgendeiner Variante von) GF(9), welcher eine Nullstelle von $x^2 + 1$ auf eine Nullstelle von $x^2 + x + 1$ abbildet?

Lösung:
Dies ist nur möglich, wenn die beiden Polynome eine gemeinsame Nullstelle haben. Dies ist aber nicht möglich, weil sie teilerfremd sind, wie aus dem durch den Euklidischen Algorithmus berechneten ggT sofort ersichtlich.

2. Sei f irreduzibel über $\mathbb{Z}_2$, so wie in Beispiel 19.11.

(a) Bestimmen Sie alle Nullstellen von f in GF(16).

Lösung:
a, a^2, a^4, a^8

(b) Wieviele Automorphismen von GF(16) gibt es?

Lösung:

Ein Automorphismus ist durch das Bild von a bereits eindeutig bestimmt. Dieses muss eine Nullstelle von f sein. Dazu gibt es 4 Möglichkeiten.

(c) Hängt dies vom gewählten irreduziblen Polynom ab?

Lösung:

Kann nicht sein, weil alle GF(16) isomorph sind.

(d) Wieviele Isomorphismen gibt es zwischen 2 verschiedenen Varianten von GF(16)?

Lösung:

Genausoviele wie Automorphismen.