Bernhard Dietrich

Aufgabe 8.1

(i)

```
(x^7  - 5x^6                        + 3x^2       + 1) : (x^2 + 1)  =  x^5 - 5x^4 - x^3 + 5x^2 + x - 2  Rest  -x + 3
 x^7          + x^5
-------------------------------------------------------
      - 5x^6  - x^5                 + 3x^2       + 1
      - 5x^6          - 5x^4
-------------------------------------------------------
              - x^5  + 5x^4         + 3x^2       + 1
              - x^5          - x^3
-------------------------------------------------------
                       5x^4  + x^3  + 3x^2       + 1
                       5x^4         + 5x^2
                      ---------------------------------
                             x^3   - 2x^2       + 1
                             x^3           + x
                            ---------------------------
                                   - 2x^2  - x  + 1
                                   - 2x^2       - 2
                                  ---------------------
                                           - x  + 3
```

(ii)

```
(x^6                                + 2) : (x^2 + x + 1)  =  x^4 - x^3 + x - 1
 x^6  + x^5  + x^4
-------------------------------------------
      - x^5  - x^4                  + 2
      - x^5  - x^4  - x^3
-------------------------------------------
                x^3                 + 2
                x^3  + x^2  + x
               ---------------------------
                     - x^2  - x  + 2
                     - x^2  - x  - 1
                    -----------------------
                                   3 = 0 mod 3
```

(iii)

```
(x^10                - 1) : (x^4 - 1)  =  x^6 + x^2   Rest  x^2 + 2
 x^10  - x^6
 ──────────────────────
        x^6          - 1
        x^6  - x^2
        ──────────────
              x^2  - 1 = x^2 +2 mod 3
```

(iv)

```
(x^5                  +   x  - 2) : (x^3 + 3x - 1)  =  x^2 - 3   Rest  x^2 + 10x - 5
 x^5  + 3x^3  - x^2
 ──────────────────────────────
     - 3x^3  + x^2  +   x  - 2
     - 3x^3         -  9x  + 3
     ──────────────────────────
               x^2  + 10x  - 5
```

(v)

i	r_i	s_i	t_i	q_i
1	$x^7-5x^6+3x^2+1$	1	0	-
2	x^2+1	0	1	$x^5-5x^4-x^3+5x^2+x-2$
3	$-x+3$	1	$-x^5+5x^4+x^3-5x^2-x+2$	$-x-3$
4	10	$x+3$	$-x^6+2x^5+16x^4-2x^3-16x^2-x-7$	-

Die beiden Polynome sind Teilerfremd, also $\mathrm{ggT}(a,b)=1$

(vi)

i	r_i	s_i	t_i	q_i
1	$x^{10}-1$	1	0	-
2	x^4-1	0	1	x^6+x^2
3	x^2-1	1	$-x^6-x^2$	x^2+1
4	0	$-x^2-1$	$x^8+x^6+x^4+x^2+1$	-

$\mathrm{ggT}(a,b)=x^2-1$

Aufgabe 8.2

(i) Zu zeigen: $\deg(r_{i+1}) < \deg(r_i)$, für $1 \le i < 1$

Induktionsanfang: $\deg(r_1) = \deg(b)$

$\deg(r_2) = \deg(a - (a \text{ quo } b) \cdot b) = \deg(a \text{ rem } b)$

Induktionsvor.: $\deg(r_2) < \deg(r_1)$

$\deg(r_{i+1}) < \deg(r_i)$

Induktionsschritt: $i \to i+1$

$\deg(r_{i+2}) = \deg(r_i \text{ rem } r_{i+1})$

Nach IV gilt $r_{i+1} < r_i$, dann gilt auch $r_{i+2} < r_{i+1}$

(ii) Nach i gilt $\deg(r_{i+1}) < \deg(r_i)$. Außerdem ist bekannt, dass $\deg(r_1) = b$. Der Algorithmus hat also nach spätestens b Schritten den Grad 1 bzw. nach $b+1$ Schritten den Grad 0. Ist $\text{ggT}(a,b) = 1$, so wird dieser spätestens in diesem Schritt gefunden.

Der Algorithmus terminiert also nach höchstens $\deg(b)+1$ Durchläufen.

(iii) Zu zeigen: $g = \text{ggT}(r_i, r_{i+1}) = \text{ggT}(a,b)$, für alle $0 \le i < l$

Induktionsanfang: $i = 0$

$\text{ggT}(r_0, r_1) = \text{ggT}(a,b)$ (wahre Aussage, da $r_0 = a$ und $r_1 = b$)

Induktionsschritt: $i \to i+1$

$\text{ggT}(r_{i+1}, r_{i+2}) = \text{ggT}(r_{i+1}, r_{i+2} - q_i r_i)$

Mit $ggT(a,b) = ggT(b, a-b)$ folgt

$$\begin{aligned}\text{ggT}(r_{i+1}, r_{i+2}) &= \text{ggT}(q_i r_i, r_{i+1}) \\ &= \text{ggT}(r_i, r_{i+1}) \\ &\overset{\text{I.V.}}{=} \text{ggT}(a,b)\end{aligned}$$

(iv) Zu zeigen: $r_i = s_i a + t_i b$ und $g = sa + tb$, für alle $0 \le i < l$

Induktionsanfang: $i = 0$

$r_0 = 1 \cdot a + 0 \cdot b = a$

Induktionsschritt: $i \to i+1$

$$\begin{aligned}r_{i+1} &= r_{i-1} - q_i r_i \\ &= (s_{i-1} a + t_{i-1} b) - q_i (s_i a + t_i b) \\ &= (s_{i-1} a + t_{i-1} b) - q_i s_i a + q_i t_i b \\ &= s_{i-1} a - s_i a q_i + t_{i-1} b - t_i b q_i \\ &= a(s_{i-1} - s_i q_i) + b(t_{i-1} - t_i q_i) \\ &= a \cdot s_{i+1} + b \cdot t_{i+1}\end{aligned}$$

$$\Rightarrow r_i = s_i a + t_i b$$

(v) Zu zeigen $\mathrm{ggT}(a,b)=1 \Rightarrow sa \equiv 1 \bmod b$

$\mathrm{ggT}(a,b) = sa + tb = 1$

$\Rightarrow 1 = sa + tb$

$\Rightarrow -tb = sa - 1$

$\Rightarrow b \mid (sa-1)$

$\Rightarrow sa - 1 \equiv 0 \bmod b$

$\Rightarrow sa \equiv 1 \bmod b$

Aufgabe 8.3

(i) Beweis durch Widerspruch:
Annahme: Sei $f = \alpha x + \beta$ zerlegbar in $f = g \cdot h$
Aufgrund der Abgeschlossenheit (Bedingung für einen Körper) folgt aus $g \in \mathbb{F}$ und $h \in \mathbb{F}$, dass auch $g \cdot h \in \mathbb{F}$ ist. Aber f ist als $\mathbb{F}[x]$ in $\mathbb{F}$.
Also muss $f = \alpha x + \beta$ irreduzibel sein.

(ii)

(iii) $x^4 + 2x^2 + 1 = (x^2+1)^2$ hat in $\mathbb{R}[x]$ keine Nullstellen. (Nullstellen in $\mathbb{C}[x]$ sind $x_{1/2} = \pm i$)

(iv) $f \in \mathbb{F}[x]$ mit $\deg(f) = 2 \vee \deg(f) = 3$ ist zerlegbar $\Leftrightarrow$ f besitzt eine Nullstelle in $\mathbb{F}$

- „$\Rightarrow$“
  $f \in \mathbb{F}[x]$ mit $\deg(f) = 2 \vee \deg(f) = 3$ ist zerlegbar
  $\Rightarrow f = g \cdot h$ mit $g, h \in \mathbb{F}[x]$ und $\deg(g) + \deg(h) = def(f)$
  $\Rightarrow$ Betrachtung von zwei Fällen:
  1. $\deg(f) = 2 : \deg(g) = \deg(h) = 1$
  2. $\deg(f) = 3 : \deg(g) + \deg(h) = 3$
     $\Rightarrow \deg(g) = 1 \wedge \deg(h) = 2 \vee \deg(g) = 2 \wedge \deg(h) = 1$

  Aus den beiden Fällen folgt, dass mindestens eine Zerlegung den Grad 1 hat und somit die Zerlegung die Form $(x-a)$ hat, also hat f mindestens eine Nullstelle in $\mathbb{F}$.

- „$\Leftarrow$“
  f besitzt eine Nullstelle in $\mathbb{F} \Rightarrow f(x) = g(x) \cdot (x-a) \Rightarrow f$ ist zerlegbar.
  $g(x)$ hat Grad 1 oder 2.

■

α	β	γ	$x^3+\alpha x^2+\beta x+\gamma$	**Nullstelle(n)**
0	0	0	x^3	$f(0)=0$
0	0	1	x^3+1	$f(1)=2=0$ in $\mathbb{F}_2$
0	1	0	x^3+x	$f(1)=2=0$ in $\mathbb{F}_2$ und $f(0)=0$
0	1	1	x^3+x+1	Irreduzibel
1	0	0	x^3+x^2	$f(1)=2=0$ in $\mathbb{F}_2$ und $f(0)=0$
1	0	1	x^3+x^2+1	Irreduzibel
1	1	0	x^3+x^2+x	$f(0)=0$
1	1	1	x^3+x^2+x+1	$f(1)=4=0$ in $\mathbb{F}_2$

(v) Jedes Polynom z vom Grad $d \geq 1$ ist also nicht irreduzibel und hat d Nullstelen (laut iv). Klammert man nun einen Nullstellen-Linearfaktor, so erhält man ein Polynom mit Grad $d-1$. Somit lässt sich jedes Polynom als d Linearfaktoren schreiben.

Induktionsanfang: $\deg(z)=2$: Hat eine Nullstelle; ist nach iv als Produkt aus 2 Linearfaktoren scheibbar

Induktionsschritt: $d \to d+1$

Grad $d+1$: $d+1$ Linearfaktoren

Ein Polynom mit $\deg(z)+1$ ist nach dem Fundamentalsatz der Algebra nicht irreduzibel und hat also nach iv eine Nullstelle.

$\Rightarrow$ Polynom mit $\deg(z)+1=$ Polynom

mit $\deg(z)+$ Nullstelle als Linearfaktor $\overset{\text{I.V.}}{=} \deg(z)$ Linearfaktoren $+$ 1 Linearfaktor.

■

Aufgabe 8.4

(i) Annahme: die Funktion sei reduzibel (d.h. Produkt aus Linearfaktoren):

x^3+x+1 hat Nullstellen, aber:

$f(0)=1\neq 0$ (keine Nullstelle)

$f(1)=3 \text{ in } \mathbb{F}_2=1\neq 0$ (keine Nullstelle)

also nicht reduzibel $\Rightarrow$ irreduzibel.

(ii) Polynomdivision mit Rest durch $f(x)\,x^3+x+1$:

$\deg(f(x))=3$

mögliche Reste: alle Polynome aus $\mathbb{F}_2$ mit Grad kleiner als x^3+x+1

$\deg(f(x))=0$: $0,1$

$\deg(f(x))=1$: $a+1, a+0$

$\deg(f(x))=3$: $a^2+a+1, a^2+a+0, a^2+0, a^2+1$

Also: $\mathbb{F}_8=\{0,1,a^2,a^2+1,a^2+a,a^2+a+1,a,a+1\}$

(iii)

- $a\left(a^2+a+1\right)=a^3+a^2+a\equiv a^2+1 \bmod\left(a^3+a+1\right)$,
  denn $x^3+x^2+x=\left(x^3+x+1\right)1+x^2-1$, aber $a^2-1\equiv a^2+1 \bmod\left(a^3+a+1\right)$
  weil $-1\equiv 1$ in $\mathbb{F}_2$
- $a^2\left(a^2+a+1\right)=a^4+a^3+a^2\equiv 1 \bmod\left(a^3+a+1\right)$,
  denn $x^4+x^3+x^2=\left(x^3+x+1\right)\left(x+1\right)-2x-1$ aber $-2a-1\equiv 1 \bmod\left(a^3+a+1\right)$
  weil $-1\equiv 1\wedge 2a\equiv 0a$ in $\mathbb{F}_2$
- $a^{-1}\overset{\text{vgl. v}}{\equiv} a^6\equiv a^2+1 \bmod\left(a^3+a+1\right)$, denn $x^6=\left(x^3+x+1\right)\left(x^3-x-1\right)+x^2+2x+1$,
  aber $2a\equiv 0a$ in $\mathbb{F}_2$

(iv) $\mathbb{F}_8$ ist ein Körper, denn:

- Für die Multiplikation ist $\mathbb{F}_8$ eine Gruppe (abgeschlossen, inverses Element (vgl. vi), neutrales Element, assoziativ)
- Für die Addition ist $\mathbb{F}_8$ ebenfalls eine Gruppe (abgeschlossen, inverses Element (vgl. vi), neutrales Element, assoziativ)

(v) $z=ax+b$, $a,b\in\mathbb{F}_2$
mittels Pascal'schem Dreieck ergibt sich:
$z^7=a^7x^7+7a^6bx^6+21a^5b^2x^5+35a^4b^3x^4+35a^3b^4x^3+21a^2b^5x^2+7ab^6x+b^7$
wegen $a^s\equiv a, b^t\equiv b$ in $\mathbb{F}_2$:

$\equiv ax^7+7abx^6+21abx^5+35abx^4+35abx^3+21abx^2+7abx+b$

$\equiv ax^7+abx^6+abx^5+abx^4+abx^3+abx^2+abx+b$

weiteres Umformen mit Polynomdivision führt zu:

$\equiv a+ab\left(x^2+1\right)+ab\left(x^2+x+1\right)+ab\left(x^2+x\right)+ab\left(x+1\right)+abx^2+abx+b$

$\equiv a+4abx^2+4abx+3ab+b$

$z^7\equiv a+3ab+b$

a	b	$3ab$ in $\mathbb{F}_2$	$a+3ab+b$
0	0	0	0
0	1	0	0
1	0	0	1
1	1	$3\equiv 1$	$3\equiv 1$

Falls $a\neq 0\wedge b\neq 0$ gilt $z^3\equiv 1$

(vi) Zu zeigen: $z^{-1}=z^6$ für $z\neq 0$
$z^6\equiv z^{-1} \bmod\left(x^3+x+1\right)$ erweitert mit z: $z^7\equiv 1 \bmod\left(x^3+x+1\right)$ nach iv

(vii) $\mathbb{Z}_8$ ist kein Körper, da es nicht einmal im Integritätsbereich ist, da es noch andere Nullteiler gibt außer 0, z.B. 4.