Universität Konstanz
Fachbereich Mathematik und Statistik
Prof. Dr. Markus Schweighofer
Aaron Kunert / Sven Wagner

Wintersemester 2009/2010
Lösungsblatt 6
09.12.2009

Lineare Algebra I

Lösung 6.1:

Allgemeine Voraussetzung: Seien K ein Körper und $K[X]$ der Polynomring über K in der Unbestimmten X.

(a) Voraussetzung: Seien $p, q \in K[X]$.
Behauptung:

$$\deg(p+q) \leq \max\{\deg(p), \deg(q)\}, \tag{1}$$
$$\deg(p+q) = \max\{\deg(p), \deg(q)\}, \text{ falls } \deg(p) \neq \deg(q), \text{ und} \tag{2}$$
$$\deg(pq) = \deg(p) + \deg(q), \tag{3}$$

wobei hier $-\infty + d := -\infty =: d + (-\infty)$ für alle $d \in \mathbb{N}_0 \cup \{-\infty\}$ und $-\infty < d$ für alle $d \in \mathbb{N}_0$ gelte.
Beweis: Ist $p = 0$ oder $q = 0$, so folgen diese Behauptungen sofort aus den oben angebenen Regeln für den Umgang mit $-\infty$. Wir können also $p, q \neq 0$ annehmen. Sei $n = \deg(p)$ und $m = \deg(q)$. Es gilt, dass $n, m \in \mathbb{N}_0$, und wir können annehmen, dass $n \geq m$. Wir können somit p und q folgendermaßen schreiben:

$$p = \sum_{i=0}^{n} a_i X^i, \qquad q = \sum_{i=0}^{m} b_i X^i,$$

wobei $a_0, \ldots, a_n, b_0, \ldots, b_m \in K$ mit $a_n, b_m \neq 0$ sind. 1. Fall: Es gilt $n > m$. Setze $b_{m+j} := 0$ für $j \in \{1, \ldots, n-m\}$. Dann gilt

$$p + q = \sum_{i=0}^{n} (a_i + b_i) X^i,$$

und, da $a_n + b_n = a_n + 0 = a_n \neq 0$ ist, gilt $\deg(p+q) = n = \deg(p) = \max\{\deg(p), \deg(q)\}$. Somit haben wir in diesem Fall (1) gezeigt, aber auch gleichzeitig (2) vollständig bewiesen. 2. Fall: Es gilt $n = m$. Wieder haben wir

$$p + q = \sum_{i=0}^{n} (a_i + b_i) X^i.$$

Gilt $a_n + b_n \neq 0$, so ist $\deg(p+q) = n = \deg(p) = \deg(q) = \max\{\deg(p), \deg(q)\}$. Gilt allerdings $a_n + b_n = 0$, so ist aber $\deg(p+q) < n = \deg(p) = \deg(q) = \max\{\deg(p), \deg(q)\}$. Somit ist auch hier (1) gezeigt.

Wir müssen nun noch (3) zeigen. Mit den obigen Darstellungen von p und q gilt nach Definition des Produktes zweier Polynome

$$pq = \sum_{i=0}^{n+m} \Big(\sum_{j=0}^{i} a_j b_{i-j}\Big) X^i,$$

wenn man $a_{n+k} := 0$ für $k \in \{1, \dots, m\}$ und $b_{m+k} := 0$ für $k \in \{1, \dots, n\}$ setzt. Betrachten wir also den $(n+m)$-ten Koeffizienten: $\sum_{j=0}^{n+m} a_j b_{n+m-j}$. Ist $j > n$, so ist $a_j = 0$. Ist $n + m - j > m$, so ist $b_{n+m-j} = 0$. Es gilt aber $n + m - j > m$ genau dann, wenn $n - j > 0$ also $n > j$ ist. Somit ist $a_j b_{n+m-j} = 0$, wenn $j \neq n$ ist. Ist aber $j = n$, so ist $a_j b_{n+m-j} = a_n b_m \neq 0$, da $a_n, b_m \neq 0$ gilt. Zusammengefasst ist also der $(n+m)$-te Koeffizient von pq nicht 0, damit ist aber $\deg(pq) = n+m = \deg(p)+\deg(q)$.

(b) Voraussetzung: Seien $p, q \in K[X]$.
Behauptung: Aus $pq = 0$ folgt stets $p = 0$ oder $q = 0$. Beweis: Wir zeigen die Kontraposition: Gilt $p, q \neq 0$, so ist $pq \neq 0$. Dies sieht man folgendermaßen: Sind $p, q \neq 0$, so gilt $\deg(p), \deg(q) \in \mathbb{N}_0$. Mit (3) aus Aufgabnteil (a), folgt $\deg(pq) \in \mathbb{N}_0$. Also $\deg(pq) \neq -\infty$, und somit $pq \neq 0$.

(c) Voraussetzung: Sei $g \in K[X]$, und sei $(g) = \{pg \mid p \in K[X]\}$ das davon erzeugt Hauptideal in $K[X]$. Es bezeichne $\equiv_{(g)}$ die dazugehörige Kongruenzrelation auf $K[X]$, das heißt $p \equiv_{(g)} q \iff p - q \in (g)$ für alle $p, q \in K[X]$.
Behauptung: Sind $p, q \in K[X]$ mit $\deg(p) < \deg(g) > \deg(q)$ und $p \equiv_{(g)} q$, so gilt $p = q$.
Beweis: Seien also solche $p, q \in K[X]$ gegeben. Dann gilt mit (1) aus (a), dass $\deg(p - q) \leq \max\{\deg(p), \deg(q)\} < \deg(g)$. Da aber $p - q \in (g)$ gilt, gibt es ein $h \in K[X]$ mit $p - q = gh$. Also gilt mit (3) aus (a), dass $\deg(p - q) = \deg(g) + \deg(h)$ ist. Wegen $\deg(p - q) < \deg(g)$, ist dies nur möglich, wenn $\deg(h) = -\infty$, also $h = 0$, ist. Somit ist auch $p - q = 0$, das heißt $p = q$.

(d) Voraussetzung: Sei $g \in K[X]$ und $g \neq 0$. Sei $f \in K[X]$ mit $\deg(g) \leq \deg(f)$.
Behauptung: Es existiert ein $r \in K[X]$ mit $f \equiv_{(g)} r$ und $\deg(r) < \deg(f)$.
Beweis: Sei $\deg(f) = n$ und $\deg(g) = m$, und sei $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{i=0}^{m} b_i X^i$. Betrachte $r := f - \frac{a_n}{b_m} X^{n-m} g$. Es gilt

$$r = \sum_{i=0}^{n} a_i X^i - \sum_{i=n-m}^{n} \frac{a_n b_{i-n+m}}{b_m} X^i = \sum_{i=0}^{n-m-1} a_i X^i + \sum_{i=n-m}^{n} \Big(a_i - \frac{a_n b_{i-n+m}}{b_m}\Big) X^i.$$

Der n-te Koeffizient von r ist $a_n - \frac{a_n b_m}{b_m} = 0$, somit gilt $\deg(r) < n = \deg(f)$. Außerdem ist offensichtlich $f \equiv_{(g)} r$.

(e) Voraussetzung: Seien $f, g \in K[X]$ und $g \neq 0$.
Behauptung: Es existiert genau ein $r \in K[X]$ mit $f \equiv_{(g)} r$ und $\deg(r) < \deg(g)$.
Beweis: Existenz: Ist $\deg(f) < \deg(g)$, so setze $r := f$. Andernfalls finden wir nach Anwendung von (d) zunächst ein Polynom f_1 mit $f \equiv_{(g)} f_1$ und $\deg(f_1) < \deg(f)$. Wenden wir (d) auf f_1 an, so finden wir ein Polynom f_2 mit $f_1 \equiv_{(g)} f_2$ und $\deg(f_2) < \deg(f_1)$. Damit gilt aber auch $f \equiv_{(g)} f_2$. Da der Grad bei Anwendung von (d) immer kleiner wird, finden wir nach endlich vielen Schritten ein Polynom r mit $f \equiv_{(g)} r$ und $\deg(r) < \deg(g)$.
Eindeutigkeit: Seien r_1 und r_2 zwei Polynome mit $f \equiv_{(g)} r_i$ und $\deg(r_i) < \deg(g)$ für $i = 1, 2$. Dann gilt auch $r_1 \equiv_{(g)} r_2$, aber dann impliziert (c) $r_1 = r_2$.

(f) Voraussetzung: Seien $f, g \in K[X]$ und $g \neq 0$.
Behauptung: Es existiert genau ein Paar $(q, r) \in K[X] \times K[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$.
Beweis: Existenz: Nach (e) existiert genau ein Polynom r mit $f \equiv_{(g)} r$ und $\deg(r) < \deg(g)$. Insbesondere ist $f - r \in (g)$, d.h. es existiert ein $q \in K[X]$ mit $f - r = qg$, also $f = qg + r$. Die Eindeutigkeit von r ist damit auch schon gezeigt.

Eindeutigkeit: Seien (q_1, r) und (q_2, r) zwei solche Paare. Es gilt also $q_1 g + r = f = q_2 g + r$, und somit $q_1 g = q_2 g$. Damit gilt $(q_1 - q_2)g = 0$, was aber nach (b) $q_1 - q_2 = 0$ bedeutet, da $g \neq 0$ ist. Somit ist $q_1 = q_2$.

(g) Voraussetzung: Seien $f, g \in K[X]$ und $g \neq 0$.
Behauptung: Das Polynom r aus (e) ist der Rest der Polynomdivision von f durch g ist.
Beweis: Das wurde schon im Beweis von (f) gezeigt.

(h) Wir berechnen folgende Reste von Polynomdivisionen in $K[X]$:

- $(2X^3 + 2X^2 - 1)^{100} \bmod X^2 - 2$ für $K = \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. Wir schreiben hier etwas salopp n statt $\overline{n}^{(5)}$ für $n \in \mathbb{Z}$ (vgl. Übungsblatt 7).
  Sei $\equiv := \equiv_{(X^2-2)}$. Es gilt also $X^2 \equiv 2$. Damit ist

  $$2X^3 + 2X^2 - 1 \equiv 2 \cdot 2 \cdot X + 2 \cdot 2 - 1 = 4X + 3,$$

  und aus (g) folgt, dass $4X + 3 = 2X^3 + 2X^2 - 1 \bmod X^2 - 2$.
  Es ist, wegen $4^2 = 1$, $3^4 = 1$ und $5 = 10 = 0$ in $\mathbb{F}_5$,

  $$\begin{aligned}&(4X + 3)^5\\ &= 4^5X^5 + 5 \cdot 4^4 \cdot 3 \cdot X^4 + 10 \cdot 4^3 \cdot 3^2 \cdot X^3 + 10 \cdot 4^2 3^3 \cdot X^2 + 5 \cdot 4 \cdot 3^4 \cdot X + 3^5\\ &= 4X^5 + 3 \equiv 4 \cdot 2^2 \cdot X + 3 = X + 3.\end{aligned}$$

  Es ist $(X + 3)^5 = X^5 + 3^5 \equiv 4X + 3$. Außerdem gilt

  $$\begin{aligned}&(4X + 3)^4 = 4^4X^4 + 4 \cdot 4^3 \cdot 3 \cdot X^3 + 6 \cdot 4^2 \cdot 3^2 \cdot X^2 + 4 \cdot 4 \cdot 3^3 \cdot X + 3^4\\ &= X^4 + 3X^3 + 4X^2 + 2X + 1 \equiv 4 + 6X + 8 + 2X + 1 = 3X + 3 = 3(X + 1).\end{aligned}$$

  Somit ist

  $$(2X^3 + 2X^2 - 1)^{100} \equiv (4X + 3)^{5 \cdot 5 \cdot 4} = 3(X + 1),$$

  also $3(X + 1) = (2X^3 + 2X^2 - 1)^{100} \bmod X^2 - 2$.
- $(64X^6 + 144X^4 + 108X^2 + 27)^{473} \bmod 16X^4 + 24X^2 + 10$ für $K = \mathbb{R}$.
  Man rechnet zuerst

  $$\begin{array}{rrrl} & & & 64X^6 + 144X^4 + 108X^2 + 27 = \left(16X^4 + 24X^2 + 10\right)\left(4X^2 + 3\right) - 4X^2 - 3\\ -\,64X^6 & -\,96X^4 & -\,40X^2 & \\ \hline & 48X^4 & +\,68X^2 + 27 & \\ & -\,48X^4 & -\,72X^2 - 30 & \\ \hline & & -\,4X^2 & -\,3 \end{array}$$

  Also verkürzt sich die Aufgabe zu

  $$(-4X^2 - 3)^{473} \bmod 16X^4 + 24X^2 + 10.$$

  Allerdings ist $(-4X^2 - 3)^2 \bmod 16X^4 + 24X^2 + 10 = -1$. Somit ergibt sich

  $$(-4X^2 - 3)^{473} \equiv (-4X^2 - 3)^{4 \cdot 118 + 1} \equiv (-1)^{2 \cdot 118} \cdot (-4X^2 - 3) \equiv -4X^2 - 3.$$

  Also ist $(64X^6 + 144X^4 + 108X^2 + 27)^{473} \bmod 16X^4 + 24X^2 + 10 = -4X^2 - 3$.

- $\prod_{i=1}^{6}(X^i - \frac{1}{i}) \bmod X^7$ für $K = \mathbb{F}_7$. Wir schreiben auch hier n statt $\overline{n}^{(7)}$ für $n \in \mathbb{Z}$.
  Sei $\equiv := \equiv_{(X^7)}$. Es ist $2 \cdot 4 = 1$, $3 \cdot 5 = 1$ und $6 \cdot 6 = 1$ in $\mathbb{F}_7$. Außerdem ist $4 = -3$, $5 = -2$ und $6 = -1$ in $\mathbb{F}_7$. Also gilt

$$\prod_{i=1}^{6}(X^i - \frac{1}{i}) = (X+6)(X^2+3)(X^3+2)(X^4+5)(X^5+4)(X^6+1).$$

  Nun ist zunächst

$$(X+6)(X^6+1) = X^7 + 6X^6 + X + 6 \equiv 6X^6 + X + 6,$$

$$(X^3+2)(X^4+5) = X^7 + 2X^4 + 5X^3 + 10 \equiv 2X^4 + 5X^3 + 3$$

  und

$$(X^2+3)(X^5+4) = X^7 + 3X^5 + 4X^2 + 12 \equiv 3X^5 + 4X^2 + 5.$$

  Weiter ist

$$\begin{aligned}&(6X^6 + X + 6)(2X^4 + 5X^3 + 3)\\ &= 12X^{10} + 30X^9 + 18X^6 + 2X^5 + 17X^4 + 30X^3 + 3X + 18\\ &\equiv 4X^6 + 2X^5 + 3X^4 + 2X^3 + 3X + 4\end{aligned}$$

  und

$$\begin{aligned}&(4X^6 + 2X^5 + 3X^4 + 2X^3 + 3X + 4)(3X^5 + 4X^2 + 5)\\ &= 12X^{11} + 6X^{10} + 9X^9 + 22X^8 + 8X^7 + 41X^6 + 30X^5 + 15X^4 + 22X^3\\ &\quad + 16X^2 + 15X + 20\\ &\equiv 6X^6 + 2X^5 + X^4 + X^3 + 2X^2 + X + 6.\end{aligned}$$

  Damit ist $6X^6 + 2X^5 + X^4 + X^3 + 2X^2 + X + 6 = \prod_{i=1}^{6}(X^i - \frac{1}{i}) \bmod X^7$.

Lösung 6.2:

(a) Voraussetzung: Sei $\mathbb{F}_2 = \mathbb{Z}/(2) = \{0, 1\}$ der Körper mit zwei Elementen, und sei $\mathbb{F}_2[X]$ der Polynomring in einer Unbestimmten über $\mathbb{F}_2$. Sei $g := X^2 + X + 1 \in \mathbb{F}_2[X]$.
Behauptung:

(i) $\mathbb{F}_4 := \mathbb{F}_2[X]/(g) = \{\overline{0}, \overline{1}, \overline{X}, \overline{X+1}\}$.

(ii) $\mathbb{F}_4$ ist ein Körper mit vier Elementen. Stellen Sie dafür auch die Additions- und Multiplikationstabelle auf, wobei Sie $\overline{0}$ mit 0, $\overline{1}$ mit 1, $\overline{X}$ mit a und $\overline{X+1}$ mit b bezeichnen.

Beweis: Zu (i): Sei $f \in \mathbb{F}_2[X]$. Dann existier nach Aufgabe 6.1 (e) genau ein $r \in \mathbb{F}_2[X]$ mit $f \equiv_{(g)} r$ und $\deg(r) < \deg(g)$. Somit müssen wir nur noch die Restklassen von Polynomen mit Grad < 2 betrachten. Ein solches Polynom hat die Gestalt $a_0 + a_1 X$ mit $a_0, a_1 \in \mathbb{F}_2 = \{0, 1\}$. Dies sind aber gerade die Polynome 0, 1, X und $X + 1$.
Zu (ii): Aus Aufgabe 6.1 (c) folgt, dass die vier Kongruenzklassen $\overline{0}$, $\overline{1}$, $\overline{X}$ und $\overline{X+1}$ paarweise verschieden sind. $\mathbb{F}_4$ hat also genau vier Elemente. Da (g) ein Ideal von $\mathbb{F}_2[X]$ ist, ist $\mathbb{F}_4$ ein kommutativer Ring mit Nullelement $\overline{0}$ und Einselement $\overline{1}$. Setze außerdem $a := \overline{X}$ und $b := \overline{X+1}$.
Es gilt $x + x = 2x = 0$ für alle $x \in \mathbb{F}_4$. Außerdem gilt $1 + a = \overline{1} + \overline{X} = \overline{1+X} = b$,

$1 + b = \overline{1} + \overline{X+1} = \overline{X+2} = \overline{X} = a$ und $a + b = \overline{X} + \overline{X+1} = \overline{2X+1} = \overline{X}$. Wir erhalten also folgende Additionstabelle:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Nun betrachten wir die Produkte: Es ist

$$a^2 = \overline{X}^2 = \overline{X^2} = \overline{X^2 - g} = \overline{-X - 1} = \overline{X+1} = b,$$

$$b^2 = (\overline{X+1})^2 = \overline{(X+1)^2} = \overline{X^2 + 2X + 1} = \overline{X^2 + 1 - g} = \overline{-X} = \overline{X} = a$$

und

$$ab = \overline{X} \cdot \overline{X+1} = \overline{X(X+1)} = \overline{X^2 + X - g} = \overline{-1} = \overline{1} = 1.$$

Somit haben wir folgende Multiplikationtabelle (ohne die Zeile und Spalte der 0):

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Insbesondere sehen wir, dass jedes von 0 verschiedene Element multiplkativ invertierbar ist. Somit ist $\mathbb{F}_4$ ein Körper.

(b) Voraussetzung: Sei K ein beliebiger Körper mit vier Elementen.
Behauptung: K ist als kommutativer Ring isomorph zu $\mathbb{F}_4$.
Beweis: Wir bezeichnen die Elemente von K mit 0, 1, a und b. Die additive abelsche Gruppe $(K, +)$ hat also genau vier Elemente. Nach Aufgabe 3.2 (b) (bzw. deren Lösung) ist sie damit entweder isomorph zu $\mathbb{Z}/(4)$ oder $(\mathbb{Z}/(2)) \times (\mathbb{Z}/(2))$. Ersteres ist aber nicht möglich, da sonst $1 + 1 \neq 0$, aber $(1 + 1) \cdot (1 + 1) = 1 + 1 + 1 + 1 = 0$ wäre. Das kann aber in einem Körper nicht vorkommen. Somit ist $(K, +)$ isomorph zu $(\mathbb{Z}/(2)) \times (\mathbb{Z}/(2))$. Dies bedeutet aber nach Aufgabe 3.2 (b), dass die Additionstabelle folgendermaßen aussieht:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Da K ein Körper ist, hat die multiplikative abelsche Gruppe $K^\times$ genau drei Elemente: 1, a und b. Nach der Vorlesung gibt es aber bis auf Isomorphie genau eine abelsche Gruppe mit drei Elementen: $\mathbb{Z}/(3)$. Diese hat (multiplikativ geschrieben) die Multiplikationstabelle:

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Wir sehen also, dass die Additions- und die Multiplikationstabellen von $\mathbb{F}_4$ und K übereinstimmen. Somit ist $\mathbb{F}_4 \to K$, $0 \mapsto 0$, $1 \mapsto 1$, $\overline{X} \mapsto a$ und $\overline{X+1} \mapsto b$ ein Ringisomorphismus.

Lösung 6.3:

(a) Sei $a \in \mathbb{F}$. Wir betrachten die von a erzeugte Untergruppe $A = \langle a \rangle$ von $G := (\mathbb{F}, +)$. Als Menge ist

$$A = \left\{ \sum_{i=1}^{k} a \mid k \in \mathbb{N} \right\} \cup \left\{ \sum_{j=1}^{l} (-a) \mid l \in \mathbb{N} \right\} \cup \{0\}.$$

Da $A \subseteq G$ eine endliche Menge ist, ist insbesondere die Menge $\left\{ \sum_{i=1}^{k} a \mid k \in \mathbb{N} \right\}$ eine endliche Menge. Also gibt es $r > s$ in $\mathbb{N}$, so dass $\sum_{i=1}^{r} a = \sum_{i=1}^{s} a$ ist. Daraus folgt aber, dass $\sum_{i=1}^{r-s} a = 0$ ist. Da wir $r > s$ vorausgesetzt haben, ist $r - s \in \mathbb{N}$. Ist $a \neq 0$, so betrachten wir zu a die kleinste natürliche Zahl k mit $\sum_{i=1}^{k} a = 0$. (Die Existenz solch einer Zahl haben wir gerade nachgewiesen.)
Nun betrachtet man die Menge

$$\widetilde{A} := \left\{ \sum_{i=1}^{l} a \mid 1 \leq l \leq k \right\}.$$

Sicherlich ist $\widetilde{A} \subseteq \langle a \rangle$. Andererseits ist $\widetilde{A}$ auch eine Untergruppe von $(\mathbb{F}, +)$, die a enthält. In der Tat ist $0 \in \widetilde{A}$, dafür wählen wir $l = k$. Das Inverse von $\sum_{i=1}^{l} a$ mit $l < k$ ist gegeben durch $\sum_{i=1}^{k-l} a \in \widetilde{A}$. Aus dieser Überlegung folgt wegen $a \in \widetilde{A}$, dass $\widetilde{A} = \langle a \rangle$ ist. Nun überlegt man sich, dass alle Elemente $\sum_{i=1}^{l} a$ mit $1 \leq l \leq k$ verschieden sein müssen. Wäre $v < u$ mit $\sum_{i=1}^{u} a = \sum_{i=1}^{v} a$, so wäre $\sum_{i=1}^{u-v} a = 0$, aber $0 < u - v < k$. Allerdings war k als minimal mit dieser Eigenschaft vorausgesetzt, somit hätten wir einen Widerspruch. Insbesondere wissen wir nun, dass $\#\langle a \rangle = k$ gilt.
Weiter wissen wir aus der Vorlesung, dass

$$\#G = \#(G/\langle a \rangle) \cdot \#\langle a \rangle$$

gilt. Es gibt also eine natürliche Zahl $k' = \#(G/\langle a \rangle)$ mit $k' \cdot \#\langle a \rangle = k'k = m$. Damit folgt

$$\sum_{i=1}^{m} a = \sum_{i=1}^{k' \cdot k} = \sum_{j=1}^{k'} \underbrace{\left(\sum_{i=1}^{k} a \right)}_{=0} = 0.$$

Somit ist die Behauptung für alle $a \neq 0$ aus $G = (\mathbb{F}, +)$ gezeigt. Da sie für $a = 0$ aber offensichtlich ist, ist alles gezeigt.

(b) Dieser Beweis funktioniert analog zum letzten Beweis. Hier betrachten wir die abelsche Gruppe $G := (\mathbb{F} \setminus \{0\}, \cdot)$. Da $\mathbb{F}$ ein Körper ist, gilt $\#G = m - 1$. Ersetzt man also im obigen Beweis $+$ durch $\cdot$, 0 durch 1 und m durch $m - 1$, erhält man das gewünschte Ergebnis.

(c) Aus Aufgabenteil (b) folgt, dass die Nullstellen von $p := \prod_{a \in \mathbb{F}^\times} (X - a)$ auch Nullstellen von $q := X^{m-1} - 1$ sind. Nun ist aus der Vorlesung bekannt, dass man bei einem Polynom f mit Nullstelle α das Polynom $(X - \alpha)$ abspalten kann. Angenommen f

habe paarweise verschiedene Nullstellen α_i für $i = 1, \ldots, k$. Dann hat $g(X) := f(X)$ div $(X - \alpha_j)$ immer noch die Nullstellen α_i mit $i = 1, \ldots, k$ und $i \neq j$. Dies folgt aus der Gleichung $g(X) \cdot (X - \alpha_j) = f(X)$. Setzt man für X den Wert α_i mit $i \neq j$ ein, so ist die rechte Seite 0, aber $(\alpha_i - \alpha_j) \neq 0$. Wegen der Nullteilerfreiheit des Körpers muss also $g(\alpha_i) = 0$ sein. Also ist q durch jedes $(X - a)$ mit $a \in \mathbb{F}^\times$ teilbar. Da alle diese Elemente $a \in \mathbb{F}^\times$ paarweise verschieden sind, können wir obige Überlegung anwenden und erhalten, dass p durch q teilbar ist. Da beide Polynome denselben Grad haben, gibt es ein $c \in \mathbb{F}^\times$, so dass p div $q = c$ ist. Da beide Polynome den Leitkoeffizienten 1 haben, muss $c = 1$ sein, was die Gleichheit von p und q impliziert.

(d) Wir wissen schon für $p(X) = X^{m-1} - 1$, dass $p(a) = 0$ für alle $a \in \mathbb{F} \setminus \{0\}$ gilt. Man muss sich also nur noch überlegen, wie man die 0 als Nullstelle hinzufügt. Dafür betrachtet man das Polynom $g(X) := X \cdot p(X)$. Dieses hat eine Nullstelle an jedem Element aus $\mathbb{F}$.

Lösung 6.4:

(i) $(2 + 3\mathring{\iota})(1 - 5\mathring{\iota}) = 2 + 3\mathring{\iota} - 10\mathring{\iota} - 15\mathring{\iota}^2 = 2 - 7\mathring{\iota} + 15 = 17 - 7\mathring{\iota}$

(ii) $\dfrac{1}{\mathring{\iota}} = \dfrac{\mathring{\iota}}{\mathring{\iota} \cdot \mathring{\iota}} = \dfrac{\mathring{\iota}}{-1} = -\mathring{\iota}$

(iii) $\dfrac{1}{1 + \mathring{\iota}} = \dfrac{1 - \mathring{\iota}}{(1 + \mathring{\iota})(1 - \mathring{\iota})} = \dfrac{1 - \mathring{\iota}}{1 - \mathring{\iota}^2} = \dfrac{1 - \mathring{\iota}}{2} = \dfrac{1}{2} - \dfrac{1}{2}\mathring{\iota}$

(iv) $\dfrac{1 + \mathring{\iota}}{1 - \mathring{\iota}} = \dfrac{(1 + \mathring{\iota})(1 + \mathring{\iota})}{(1 - \mathring{\iota})(1 + \mathring{\iota})} = \dfrac{1 + 2\mathring{\iota} + \mathring{\iota}^2}{1 - \mathring{\iota}^2} = \dfrac{1 + 2\mathring{\iota} - 1}{2} = \dfrac{2\mathring{\iota}}{2} = \mathring{\iota}$

(v) $(1 + \mathring{\iota})^{16} = (2\mathring{\iota})^8 = (-4)^4 = 2^8 = 256$