

Lineare Algebra I, HWS 2014, Mannheim

## Ergänzungen in der großen Übung zu Kapitel 2

### Der Ring $\mathbb{Z}$ und seine Primzahlen

**Definition 2.16** (a) Seien  $a, b \in \mathbb{Z} - \{0\}$ .

$\text{kgV}(a, b) :=$  "kleinstes gemeinsames Vielfaches" =  $\min(n \in \mathbb{N} \mid a|n \text{ und } b|n)$ ,

$\text{ggT}(a, b) :=$  "größter gemeinsamer Teiler" =  $\max(n \in \mathbb{N} \mid n|a \text{ und } n|b)$ .

(b)  $p \in \mathbb{N}$  mit  $p \neq 1$  ist eine Primzahl, falls 1 und  $p$  seine einzigen Teiler in  $\mathbb{N}$  sind.

**Satz 2.17** Seien  $a, b \in \mathbb{Z} - \{0\}$ .

(a)  $a\mathbb{Z} \cap b\mathbb{Z} = \text{kgV}(a, b)\mathbb{Z}$ .

(b) Es gibt  $k, l \in \mathbb{Z}$  mit  $\text{ggT}(a, b) = ka + lb$ . Man kann  $k$  oder  $l$  in  $\mathbb{N}$  wählen.

(c) Sei nun  $p$  eine Primzahl mit  $p|ab$ . Dann gilt  $p|a$  oder  $p|b$ .

(d) Seien  $p_1, \dots, p_k$  und  $q_1, \dots, q_l$  Primzahlen mit

$$p_1 \cdot \dots \cdot p_k = q_1 \cdot \dots \cdot q_l.$$

Dann ist  $k = l$ , und es gibt eine Bijektion  $\sigma \in S_k$  mit

$$p_i = q_{\sigma(i)} \quad \text{für } i = 1, \dots, k.$$

Dies ist die Eindeutigkeit der Zerlegung einer natürlichen Zahl in Primzahlen. Sie ist NICHT selbstverständlich.

**Beweis:** (a)  $a\mathbb{Z}$  und  $b\mathbb{Z}$  sind Untergruppen von  $(\mathbb{Z}, +)$ , also ist auch  $a\mathbb{Z} \cap b\mathbb{Z}$  eine. Nach Satz 1.21 (b) existiert ein  $m \in \mathbb{N}$  mit  $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ .

Aus  $m \in a\mathbb{Z}$  und  $m \in b\mathbb{Z}$  folgt  $a|m$  und  $b|m$ , also  $m \geq \text{kgV}(a, b)$ .

Andererseits ist  $\text{kgV}(a, b) \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ , also  $\text{kgV}(a, b) \geq m$ .

Also ist  $\text{kgV}(a, b) = m$ .

(b) Die Menge  $\{ka + lb \mid k, l \in \mathbb{Z}\}$  ist eine Untergruppe von  $(\mathbb{Z}, +)$ . Nach Satz 1.21 (b) existiert ein  $m \in \mathbb{N}$  mit  $\{ka + lb \mid k, l \in \mathbb{Z}\} = m\mathbb{Z}$ , und es existieren  $k_0, l_0 \in \mathbb{Z}$  mit  $m = k_0a + l_0b$ . Mit

$$c := k_0 \frac{a}{\text{ggT}(a, b)} + l_0 \frac{b}{\text{ggT}(a, b)} \in \mathbb{N}$$

ist  $m = c \cdot \text{ggT}(a, b)$ , also  $m \geq \text{ggT}(a, b)$ .

Wegen  $a \in m\mathbb{Z}$  ( $\Leftarrow k = 1, l = 0$ ) und  $b \in m\mathbb{Z}$  ( $\Leftarrow k = 0, l = 1$ ) ist  $m$  ein Teiler von  $a$  und  $b$ , also  $m \leq \text{ggT}(a, b)$ . Es folgt  $m = \text{ggT}(a, b)$ .

Wenn man  $k_0$  und  $l_0$  abändert zu

$$k_1 = k_0 + \alpha \cdot \frac{b}{\text{ggT}(a, b)}, \quad l_1 = l_0 - \alpha \cdot \frac{a}{\text{ggT}(a, b)}$$

mit einem beliebigen  $\alpha \in \mathbb{Z}$ , gilt immer noch  $k_1 a + l_1 b = \text{ggT}(a, b)$ . Insbesondere kann man  $k_1 > 0$  oder  $l_1 > 0$  erreichen (aber meistens nicht beides zugleich).

(c) Annahme:  $p \nmid a$ . Zu zeigen:  $p \mid b$ .

Annahme und  $p$  Primzahl  $\implies \text{ggT}(a, p) = 1$ .

Aus (b) folgt, daß  $k, l \in \mathbb{Z}$  mit  $ka + lp = 1$  existieren. Dann ist

$$b = 1 \cdot b = (ka + lp) \cdot b = k(ab) + (lb)p.$$

Mit  $p \mid ab$  folgt  $p \mid b$ .

(d) Aus (c) und

$$p_1 \mid (p_1 \cdot \dots \cdot p_k) = q_1 \cdot (q_2 \cdot \dots \cdot q_l)$$

folgt  $p_1 \mid q_1$  oder  $p_1 \mid (q_2 \cdot \dots \cdot q_l)$ . Induktiv folgt:  $p_1$  teilt ein  $q_j$ .

Weil  $q_j$  eine Primzahl ist, ist  $p_1 = q_j$ . Daher ist

$$p_2 \cdot \dots \cdot p_k = q_1 \cdot \dots \cdot q_{j-1} \cdot q_{j+1} \cdot \dots \cdot q_l.$$

Induktiv folgen  $k = l$  und die Existenz von  $\sigma \in S_k$  mit  $p_i = q_{\sigma(i)}$ .

□

## Polynome

**Lemma/Definition 2.18** Sei  $R$  ein Ring.

(a) (Unsaubere Definition, mit der man aber gut arbeiten kann) Ein Polynom in einer Variablen  $t$  mit Koeffizienten in  $R$  ist ein Ausdruck der Gestalt

$$a_0 + a_1 t + \dots + a_n t^n \quad \text{mit } a_0, a_1, \dots, a_n \in R.$$

$t$  ist eine „Unbestimmte“.

Vorsicht: das  $n$  hier ist nicht eindeutig; es ist

$$a_0 + a_1 t + \dots + a_n t^n = a_0 + a_1 t + \dots + a_n t^n + 0 \cdot t^{n+1} + \dots + 0 \cdot t^{n+k}, \quad k \in \mathbb{N} \text{ beliebig.}$$

Das Nullpolynom ist das Polynom  $0 + 0 \cdot t + \dots + 0 \cdot t^n = 0$ .

(b) (Saubere Definition) Ein Polynom in einer Variablen ist eine Abbildung  $a : \mathbb{N}_0 \rightarrow R$ ,  $i \mapsto a(i) =: a_i$ , bei der nur endlich viele Zahlen  $i$  einen Wert

$a_i \neq 0$  haben. Nun kann man ein  $n \in \mathbb{N}$  wählen, so dass für alle  $i > n$   $a_i = 0$  ist und die Abbildung  $a$  wie in Teil (a) notieren, als  $f = a_0 + a_1t + \dots + a_nt^n$ . So kommt man zur unsaubereren, aber anschaulichen Definition in (a).

(c) (Definition) Der Grad eines Polynoms  $f(t) = a_0 + a_1t + \dots + a_nt^n$  mit  $f(t) \neq 0$  ist

$$\deg f(t) := \max\{k \mid a_k \neq 0\}.$$

Der Grad des Nullpolynoms  $0$  ist  $-\infty$ .

(d) Die Menge  $R[t]$  aller Polynome in einer Variablen  $t$  mit Koeffizienten in  $R$  ist zusammen mit den folgenden Verknüpfungen  $+$  und  $\cdot$  ein Ring, der „Polynomring“  $(R[t], +, \cdot)$ . Addition (z.B. für  $n \geq m$ ):

$$\begin{aligned} & (a_0 + a_1t + \dots + a_nt^n) + (b_0 + b_1t + \dots + b_mt^m) \\ := & (a_0 + b_0) + (a_1 + b_1)t + \dots + (a_n + b_n)t^n, \\ & \text{mit } b_{m+1} := 0, \dots, b_n := 0, \end{aligned}$$

Multiplikation:

$$\begin{aligned} & (a_0 + a_1t + \dots + a_nt^n) \cdot (b_0 + b_1t + \dots + b_mt^m) \\ := & c_0 + c_1t^1 + \dots + c_{n+m}t^{n+m}, \\ \text{mit} & \quad c_k := a_k b_0 + a_{k-1} b_1 + \dots + a_0 b_k, \\ \text{und} & \quad a_k := 0 \text{ für } k > n, \quad b_l := 0 \text{ für } l > m, \\ \text{also} & \quad c_0 = a_0 b_0, \quad c_1 = a_1 b_0 + a_0 b_1, \quad c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2, \dots \\ & \quad c_{n+m} = a_n b_m = a_{n+m} b_0 + \dots + a_n b_m + \dots + a_0 b_{n+m}. \end{aligned}$$

(e) Ist  $R$  ein kommutativer Ring, so auch  $R[t]$ . Hat  $R$  eine  $1$ , so auch  $R[t]$ .

(f) Ist  $R$  ein Körper und sind  $p(t), q(t) \in R[t] - \{0\}$ , so ist auch  $p(t)q(t) \in R[t] - \{0\}$ . Es ist  $\deg(p(t)q(t)) = \deg p(t) + \deg q(t)$ .

(g) Die Abbildung  $R \rightarrow R[t]$ ,  $a_0 \mapsto a_0$ , ist ein injektiver Ringhomomorphismus. Mit seiner Hilfe wird  $R$  mit dem Unterring von  $R[t]$  identifiziert, der aus den konstanten Polynomen besteht.

(h) Ist  $R$  kommutativ, so ist für jedes  $c \in R$  die Abbildung

$$\iota_c : R[t] \rightarrow R, \quad f(t) = a_0 + a_1t + \dots + a_nt^n \mapsto f(c) := a_0 + a_1c + \dots + a_nc^n$$

ein Ringhomomorphismus, ein „Einsetzungshomomorphismus“.

**Beweis:** (a)-(c) sind Definitionen.

(d) Aufgrund von Blatt 3 Aufgabe 4 ist  $(R[t], +)$  eine abelsche Gruppe (die Multiplikation die dort betrachtet wird ist NICHT die Multiplikation im

Polynomring). Wir müssen die Assoziativität der Multiplikation sowie das Distributivgesetz zeigen. Sei  $n, m, l \in \mathbb{N}_0$  mit  $m \geq l$ . Es gilt

$$\begin{aligned} & (a_0 + \dots + a_n t^n) \cdot ((b_0 + \dots + b_m t^m) + (c_0 + \dots + c_l t^l)) \\ &= (a_0 + \dots + a_n t^n) \cdot ((b_0 + \dots + b_m t^m) + (c_0 + \dots + c_m t^m)) \\ &= (d_0 + \dots + d_{m+n} t^{m+n}), \end{aligned}$$

$$\begin{aligned} & (a_0 + \dots + a_n t^n) \cdot (b_0 + \dots + b_m t^m) + (a_0 + \dots + a_n t^n) \cdot (c_0 + \dots + c_l t^l) \\ &= (a_0 + \dots + a_n t^n) \cdot (b_0 + \dots + b_m t^m) + (a_0 + \dots + a_n t^n) \cdot (c_0 + \dots + c_m t^m) \\ &= (f_0 + \dots + f_{m+n} t^{m+n}) \end{aligned}$$

mit  $c_{l+1} = \dots = c_m = 0$ . Es ist

$$\begin{aligned} d_k &= a_0 \cdot (b_k + c_k) + \dots + a_k \cdot (b_0 + c_0), \\ f_k &= a_0 b_k + \dots + a_k b_0 + a_0 c_k + \dots + a_k c_0. \end{aligned}$$

Es gilt  $d_k = f_k$  aufgrund des Distributivgesetzes in  $R$ . Der Beweis der Assoziativität der Multiplikation in  $R[t]$  ist ähnlich und lässt sich auf die Assoziativität der Multiplikation in  $R$  zurückführen.

(e) Es ist

$$\begin{aligned} (a_0 + a_1 t + \dots + a_n t^n) \cdot (b_0 + b_1 t + \dots + b_m t^m) &= c_0 + c_1 t + \dots + c_{n+m} t^{n+m}, \\ (b_0 + b_1 t + \dots + b_m t^m) \cdot (a_0 + a_1 t + \dots + a_n t^n) &= d_0 + d_1 t + \dots + d_{n+m} t^{n+m} \end{aligned}$$

mit

$$\begin{aligned} c_k &= a_k b_0 + \dots + a_0 b_k, \\ d_k &= b_k a_0 + \dots + b_0 a_k. \end{aligned}$$

Aufgrund der Kommutativität von  $R$  ist  $c_k = d_k$ .

(f) Es sei  $\deg p(t) = n \geq 0$ , also  $p(t) = a_0 + a_1 t + \dots + a_n t^n$  mit  $a_n \neq 0$ , und  $\deg q(t) = m \geq 0$ , also  $q(t) = b_0 + b_1 t + \dots + b_m t^m$  mit  $b_m \neq 0$ . Dann ist  $p(t)q(t) = a_0 b_0 + \dots + a_n b_m t^{n+m}$  mit  $a_n b_m \neq 0$  (Lemma 2.4 (d), hier braucht man die Voraussetzung  $R$  Körper). Also ist  $p(t)q(t) \neq 0$  und  $\deg p(t)q(t) = n + m$ .

(g) Klar.

(h) Sei  $f(t) := a_0 + \dots + a_n t^n$  und  $g(t) := b_0 + \dots + b_m t^m$  und  $n \geq m$ . Es ist

$$\begin{aligned} i_c(f(t) + g(t)) &= i_c((a_0 + b_0) + \dots + (a_n + b_n)t^n) = (a_0 + b_0) + \dots + (a_n + b_n)c^n, \\ i_c(f(t)) + i_c(g(t)) &= a_0 + \dots + a_n c^n + b_0 + \dots + b_n c^n, \end{aligned}$$

wobei  $b_{m+1} = \dots = b_n = 0$ . Die Homomorphie bzgl. " + " folgt dann aus dem Distributivgesetz in  $R$ . Weiter gilt

$$i_c(f(t) \cdot g(t)) = i_c(d_0 + \dots + d_{n+m} t^{n+m}) = d_0 + \dots + d_{n+m} c^{n+m}$$

mit  $d_k = a_k b_0 + \dots + a_0 b_k$  und

$$\begin{aligned} i_c(f(t)) \cdot i_c(g(t)) &= (a_0 + \dots + a_n c^n) \cdot (b_0 + \dots + b_m c^m) \\ &= a_0 b_0 + (a_1 c b_0 + a_0 b_1 c) + \dots + a_n c^n b_m c^m. \end{aligned}$$

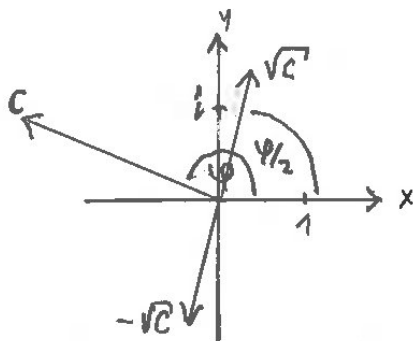
Die Homomorphie bzgl. „ $\cdot$ “ folgt aus dem Distributivgesetz und der Kommutativität von  $R$  (Man muss das Element  $c$  und die Koeffizienten  $b_0, \dots, b_m$  vertauschen).  $\square$

**Satz 2.19** (*Fundamentalsatz der Algebra; Beweis nicht in der linearen Algebra*)

Jedes Polynom  $f(t) \in \mathbb{C}[t]$  mit  $\deg f(t) \geq 1$  hat eine Nullstelle in  $\mathbb{C}$ , d.h. eine Zahl  $c \in \mathbb{C}$  existiert mit  $f(c) = 0$ .

**Beispiel 2.20** (i) Die analoge Aussage für  $\mathbb{R}$  statt  $\mathbb{C}$  ist falsch; das Polynom  $t^2 + 1$  hat keine reellen Nullstellen.

(ii) Das Polynom  $t^2 - c$  für ein  $c \in \mathbb{C} - \{0\}$  hat 2 Nullstellen in  $\mathbb{C}$ , von denen man eine  $\sqrt{c}$  nennen kann, z.B. die mit Argument in  $[0, \pi)$ ; dann ist die andere  $-\sqrt{c}$ . Ist  $c = |c| \cdot e^{i\varphi}$  mit  $\varphi \in [0, 2\pi)$ , so ist  $\pm\sqrt{c} = \pm\sqrt{|c|} \cdot e^{i\varphi/2}$ .



(iii) Das Polynom  $t^2 + pt + q$  mit  $p, q \in \mathbb{C}$  hat die beiden Nullstellen (manchmal fallen sie zusammen)

$$c_1 = -\frac{p}{2} + \frac{1}{2}\sqrt{p^2 - 4q}, \quad c_2 = -\frac{p}{2} - \frac{1}{2}\sqrt{p^2 - 4q}.$$

Es ist

$$(t - c_1)(t - c_2) = t^2 - (c_1 + c_2)t + c_1 c_2 = t^2 + pt + q.$$

(iv) Zusammen geben (ii) und (iii) einen Beweis von Satz 2.19 im Fall von Polynomen vom Grad 2.

(v) Sind  $p, q \in \mathbb{R}$ , so sind die Nullstellen von  $t^2 + pt + q$  reell  $\iff p^2 - 4q \geq 0$ .

**Satz 2.21** *Es sei  $K$  ein Körper.*

(a) (Polynomdivision mit Rest) *Es seien  $f(t), g(t) \in K[t]$  und  $\deg g(t) \geq 1$ . Dann gibt es eindeutige Polynome  $q(t)$  und  $r(t)$  mit  $\deg r(t) < \deg g(t)$  und*

$$f(t) = q(t)g(t) + r(t).$$

(b) *Sei  $f(t) \in K[t]$  ein Polynom mit  $\deg f(t) = n \geq 1$  und mit einer Nullstelle  $c \in K$ .*

*Dann gibt es ein eindeutig bestimmtes Polynom  $q(t) \in K[t]$  mit*

$$f(t) = (t - c) \cdot q(t).$$

*Es ist  $\deg q(t) = n - 1$ .*

(c) *Sind  $c_1, \dots, c_n, d_1, \dots, d_n \in K$  mit*

$$(t - c_1) \cdot \dots \cdot (t - c_n) = (t - d_1) \cdot \dots \cdot (t - d_n),$$

*so gibt es ein  $\sigma \in S_n$  mit  $c_i = d_{\sigma(i)}$  für  $i = 1, \dots, n$ .*

**Beispiel 2.22** zur Polynomdivision mit Rest.

$$f(t) = 2t^3 - t^2 + 1, \quad g(t) = t^2 + 1,$$

$$\begin{array}{r} (2t^3 - t^2 + 1) : (t^2 + 1) = 2t - 1 + (-2t + 2) : (t^2 + 1) \\ \underline{2t^3 \phantom{- t^2} + 2t} \\ -t^2 - 2t + 1 \\ \underline{-t^2 \phantom{- 2t} - 1} \\ -2t + 2 \end{array}$$

also ist  $q(t) = 2t - 1$  und  $r(t) = -2t + 2$ .

**Beweis von Satz 2.21:** (a) Zuerst die **Eindeutigkeit** von  $q(t)$  und  $r(t)$ : Sei  $f(t) = q_1(t)g(t) + r_1(t) = q_2(t)g(t) + r_2(t)$  mit  $\deg r_1(t) < \deg g(t)$  und  $\deg r_2(t) < \deg g(t)$ . Dann ist

$$(q_1(t) - q_2(t))g(t) = r_2(t) - r_1(t).$$

Wäre  $q_1(t) \neq q_2(t)$ , so wäre wegen Lemma/Definition 2.18 (f)

$$\deg((q_1(t) - q_2(t))g(t)) \geq \deg g(t) > \deg(r_1(t) - r_2(t)).$$

Widerspruch. Also ist  $q_1(t) = q_2(t)$  und  $r_1(t) = r_2(t)$ .

Nun die **Existenz** von  $q(t)$  und  $r(t)$ : Man führt den Beweis über vollständige Induktion nach  $\deg f(t) - \deg g(t)$ .

Induktionsanfang: Ist  $\deg f(t) < \deg g(t)$ , so ist  $q(t) = 0$  und  $r(t) = f(t)$ .

Induktionsschritt: Sei  $n = \deg f(t) \geq \deg g(t) = m$  und  $f(t) = a_n t^n + \dots + a_0$ ,  $g(t) = b_m t^m + \dots + b_0$ . Dann hat

$$f_2(t) := f(t) - \frac{a_n}{b_m} t^{n-m} g(t)$$

kleineren Grad als  $f(t)$ . Also gibt es nach Induktionsannahme  $q_2(t)$  und  $r_2(t)$  mit  $\deg r_2(t) < \deg g(t)$  und  $f_2(t) = q_2(t)g(t) + r_2(t)$ . Daher ist

$$f(t) = \left(\frac{a_n}{b_m} t^{n-m} + q_2(t)\right)g(t) + r_2(t).$$

Ende des Induktionsbeweises.

(b) Polynomdivision mit Rest gibt  $f(t) = q(t)(t - c) + r$  mit  $q(t) \in K[t]$  und  $r \in K$ . Wegen  $f(c) = 0$  ist  $r = 0$ . Wegen der Eindeutigkeit in a) ist  $q(t)$  eindeutig.

(c) Annahme:  $c_1 \notin \{d_1, \dots, d_n\}$ . Einsetzen von  $c_1$  für  $t$  gibt

$$\begin{aligned} 0 &= (c_1 - c_1) \cdot (c_1 - c_2) \cdot \dots \cdot (c_1 - c_n) \quad (\text{Lemma 2.4 (a)}) \\ &= (c_1 - d_1) \cdot \dots \cdot (c_1 - d_n) \neq 0 \quad (\text{Lemma 2.4 (d)}). \end{aligned}$$

Widerspruch. Also gibt es ein  $j$  mit  $c_1 = d_j$ .

Division durch  $(t - c_1)$  gibt

$$(t - c_2) \cdot \dots \cdot (t - c_n) = (t - d_1) \cdot \dots \cdot (t - d_{j-1})(t - d_{j+1}) \cdot \dots \cdot (t - d_n).$$

Mit vollständiger Induktion folgt die Behauptung.  $\square$

**Satz 2.23** (Anwendung von Satz 2.19 und Satz 2.21)

(a) Für jedes Polynom  $f(t) = a_0 + a_1 t + \dots + a_n t^n \in \mathbb{C}[t]$  mit  $\deg f(t) = n \geq 1$  (also  $a_n \neq 0$ ) gibt es (bis auf die Reihenfolge) eindeutige Zahlen  $c_1, \dots, c_n \in \mathbb{C}$  mit

$$f(t) = a_n \cdot (t - c_1) \cdot \dots \cdot (t - c_n).$$

Die Zahlen  $c_1, \dots, c_n$  sind die Nullstellen von  $f(t)$ . Man sagt: ein komplexes Polynom zerfällt in Linearfaktoren.

(b) Für jedes Polynom  $f(t) = a_0 + a_1 t + \dots + a_n t^n \in \mathbb{R}[t]$  mit  $\deg f(t) = n \geq 1$  gibt es (bis auf die Reihenfolge) eindeutige Zahlen  $c_1, \dots, c_k \in \mathbb{R}$  und (bis auf die Reihenfolge) eindeutige Polynome  $q_1(t), \dots, q_l(t) \in \mathbb{R}[t]$  mit

$$f(t) = a_n \cdot (t - c_1) \cdot \dots \cdot (t - c_k) \cdot q_1(t) \cdot \dots \cdot q_l(t)$$

und

$$q_j(t) = t^2 + \alpha_j t + \beta_j, \quad \alpha_j, \beta_j \in \mathbb{R}, \quad \alpha_j^2 - 4\beta_j < 0$$

( $\alpha_j^2 - 4\beta_j < 0$  sagt, daß  $q_j(t)$  keine reelle Nullstelle hat).

Es ist  $0 \leq k \leq n$  und  $0 \leq l \leq \frac{n}{2}$ . Es ist  $k + 2l = n$ .

Man sagt: ein reelles Polynom zerfällt in lineare und quadratische Faktoren.

**Beweis:** (a) Durch wiederholte Anwendung von Satz 2.19 und Satz 2.21 (b) bekommt man eine Zerlegung von  $f(t)$  in Linearfaktoren, mit Satz 2.21 c) ihre Eindeutigkeit.

(b) Ist  $c \in \mathbb{C}$  eine Nullstelle von  $f$ , so auch  $\bar{c}$ , denn wegen  $a_0, \dots, a_n \in \mathbb{R}$  ist

$$\begin{aligned} f(\bar{c}) &= a_0 + a_1 \cdot \bar{c} + \dots + a_n \cdot \bar{c}^n \\ &= \overline{a_0 + a_1 \cdot c + \dots + a_n \cdot c^n} \\ &= \overline{f(c)} = \overline{0} = 0. \end{aligned}$$

( $\bar{\cdot}$  ist ein Körperisomorphismus von  $\mathbb{C}$  auf sich selbst). Nach (a) ist  $f(t) = a_n(t - c_1) \cdot \dots \cdot (t - c_n)$  mit  $c_1, \dots, c_n \in \mathbb{C}$ . Die  $c_i$  seien so numeriert, daß  $c_1, \dots, c_k \in \mathbb{R}$ ,  $c_{k+1}, \dots, c_n \in \mathbb{C} - \mathbb{R}$ . Wegen der Rechnung oben und wegen Satz 2.21 (c) gibt es ein  $\sigma \in S_n$  mit  $\bar{c}_i = c_{\sigma(i)}$ . Diese Permutation bildet  $\{j \mid k < j \leq n, \Im(c_j) > 0\}$  bijektiv auf  $\{j \mid k < j \leq n, \Im(c_j) < 0\}$  ab. Es ist

$$(t - c_j)(t - \bar{c}_j) = t^2 - (c_j + \bar{c}_j)t + c_j\bar{c}_j \in \mathbb{R}[t],$$

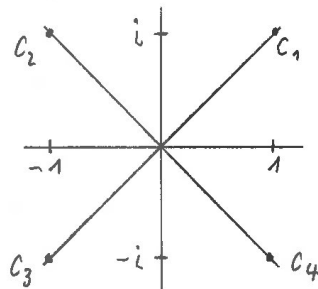
und dieses Polynom hat keine reelle Nullstelle, falls  $c_j \notin \mathbb{R}$ .

Man wählt eine Bijektion (für  $l$  geeignet)  $\tau : \{1, 2, \dots, l\} \rightarrow \{j \mid k < j \leq n, \Im(c_j) > 0\}$  und definiert

$$q_j(t) := (t - c_{\tau(j)})(t - \overline{c_{\tau(j)}}).$$

□

**Beispiel 2.24** Das reelle Polynom  $t^4 + 4$  hat die komplexen Nullstellen  $c_j := \sqrt{2}e^{2\pi i \frac{2j-1}{8}}$ ,  $j = 1, 2, 3, 4$ .



$$\begin{aligned} c_1 &= \sqrt{2} \cdot e^{2\pi i/8} = 1 + i \\ c_2 &= \sqrt{2} \cdot e^{2\pi i \cdot 3/8} = -1 + i \\ c_3 &= \sqrt{2} \cdot e^{2\pi i \cdot 5/8} = -1 - i \\ c_4 &= \sqrt{2} \cdot e^{2\pi i \cdot 7/8} = 1 - i \end{aligned}$$

Sie erfüllen  $\bar{c}_1 = c_4$ ,  $\bar{c}_2 = c_3$ . Daher ist

$$\begin{aligned} t^4 + 4 &= (t - c_1)(t - c_2)(t - c_3)(t - c_4) \\ &= (t^2 - (c_1 + c_4)t + c_1c_4)(t^2 - (c_2 + c_3)t + c_2c_3) \\ &= (t^2 - 2t + 2)(t^2 + 2t + 2). \end{aligned}$$