LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Fabien Morel
Dr. Andrei Lavrenov, Oliver Hendrichs, Katharina Novikov

Wintersemester 2024/25
6. Mai 2025

Lineare Algebra II – Lösungsskizzen zu Übungsblatt 1

Aufgabe 1.
Betrachten Sie die folgenden Polynome $f(x), g(x) \in \mathbb{R}[x]$ und dividieren Sie jeweils f mit Rest durch g.

1. $f(x) = x^6 + 3x^4 + x^3 - 2$, $g(x) = x^2 - 2x + 1$;
2. $f(x) = x^n - 1$, $g(x) = x - 1$, mit $n \in \mathbb{N} \setminus \{0\}$.

Lösung.

1. Erinnern wir uns an die schriftliche Division von Polynomen.

   Zuerst dividieren wir x^6 durch x^2 mit Rest. Der Quotient ist x^4 und wir rechnen zurück:

   $$x^4(x^2 - 2x + 1) = x^6 - 2x^5 + x^4.$$

   Jetzt subtrahieren wir dieses Polynom von $f(x)$. Dann müssen wir das Ergebnis $2x^5 + 2x^4 + x^3 - 2$ durch $g(x)$ mit Rest dividieren. Der Quotient von $2x^5$ durch x^2 ist $2x^3$ und

   $$2x^3(x^2 - 2x + 1) = 2x^5 - 4x^4 + 2x^3.$$

   Wir setzen diesen Algorithmus fort bis wir am Ende den Term $x^4 + 2x^3 + 6x^2 + 11x - 6$ erhalten und der Rest $10x - 19$ ist. Anders ausgedrückt gilt

   $$f(x) = (x^4 + 2x^3 + 6x^2 + 11x + 16)g(x) + (21x - 18)$$

2. Führen wir den ersten Schritt der schriftlichen Division aus:

   $$x^n - 1 = x^{n-1}(x - 1) + (x^{n-1} - 1).$$

   Es ist jetzt einfach durch Induktion zu beweisen, dass

   $$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1).$$

   Der Induktionsanfang $n = 1$ ist klar. Nach der Induktionsannahme haben wir

   $$x^{n-1} - 1 = (x - 1)(x^{n-2} + \ldots + x^2 + x + 1).$$

   Zusammen mit der ersten Gleichung erhalten wir die Forderung.

Aufgabe 2.

1. Sei K ein Körper und $f(x) \in K[x]$ ein Polynom vom Grad höchstens 3. Beweisen Sie, dass $f(x)$ irreduzibel ist, wenn und nur wenn $f(x)$ keine Nullstelle in K hat.

2. Geben Sie ein Beispiel eines Polynoms $f(x) \in \mathbb{R}[x]$ vom Grad 4 an, das keine Nullstellen in $\mathbb{R}$ hat, aber reduzibel ist.

Lösung.

1. Nehmen wir zuerst an, dass $f(x)$ eine Nullstelle $c \in K$ hat. Das ist nur möglich, wenn $f(x) = (x - c) \cdot g(x)$ für $g(x) \in K[x]$, aber dann ist $f(x)$ reduzibel.

   Nehmen wir zunächst an, dass $f(x)$ reduzibel ist. Dann $f(x) = g(x) \cdot h(x)$ für $g(x)$, $h(x) \in K[x]$ von Graden mindestens 1. Da $f(x)$ Grad höchstens 3 hat, ist entweder $g(x)$ oder $h(x)$ vom Grad 1. Somit hat $f(x)$ einen linearen Faktor $cx + d \in K[x]$, $c \neq 0$ und $-d/c$ ist eine Nullstelle.
2. Sei $f(x) = (x^2+1)^2$. Für jedes $c \in \mathbb{R}$ ist $(c^2+1)^2 \geq 1$ und deshalb hat $f(x)$ keine reelen Nullstellen.

Aufgabe 3.
Erinnern Sie sich, dass die Menge

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

ein Unterring von $\mathbb{C}$ ist (i ist die imaginäre Einheit). Dieser Ring heißt der Ring der gaußschen Zahlen oder Gaußscher Zahlring. Für $x = a + bi \in \mathbb{Z}[i]$ setzt man $N(x) = |x|^2 = a^2 + b^2 \in \mathbb{Z}$, wobei $|\ \ |$ die komplexe Norm ist.

Beweisen Sie, dass man gaußsche Zahlen mit Rest dividiern kann, d.h., für $x \in \mathbb{Z}[i]$, $y \in \mathbb{Z}[i] \setminus \{0\}$ gibt es q, $r \in \mathbb{Z}[i]$, so dass

$$x = y \cdot q + r \quad \text{und} \quad N(r) < N(y).$$

Mit anderen Worten beweisen Sie, dass $\mathbb{Z}[i]$ ist ein euklidischer Ring mit euklidischer Normfunktion N ist.
Hinweis: Dividieren Sie zuerst x durch y als komplexe Zahlen.

Lösung.
Sei $x/y = a + bi$ für a, $b \in \mathbb{R}$. Es gibt m, $n \in \mathbb{Z}$, so dass $|a - m| \leq \frac{1}{2}$ und $|b - n| \leq \frac{1}{2}$. Setzen wir $q := m + ni$. Dann

$$r := x - yq = y\left(\frac{x}{y} - q\right) = y \cdot \big((a - m) + i(b - n)\big),$$

und

$$N(r) = N(y) \cdot N\big((a-m)+i(b-n)\big) = N(y) \cdot \big((a-m)^2+(b-n)^2\big) \leq N(y)\left(\frac{1}{4} + \frac{1}{4}\right) \leq \frac{1}{2}N(y).$$

Aufgabe 4.
Sei $R = \mathbb{Z}[t]$ und $I = \{f(t) \mid f(0) \in 2\mathbb{Z}\} \subseteq R$ die Teilmenge aller Polynome mit geradem Absolutglied.

Beweisen Sie, dass I ein Ideal von R, aber kein Hauptideal ist. Mit anderen Worten es gibt kein Element $f_0(t) \in I$, das I als Ideal von R erzeugt.

Lösung.
Es ist klar, dass für $f(t)$, $g(t) \in I$ gilt $(f + g)(0) = f(0) + g(0) \in 2\mathbb{Z}$, so dass $f + g \in I$ und,

dass für $f(t) \in R$, $g(t) \in I$ gilt $(fg)(0) = f(0)g(0) \in 2\mathbb{Z}$, so dass $fg \in I$. Dann ist I in der Tat ein Ideal von R.

Nehmen wir jetzt an, dass es ein Element $f_0(t) \in I$ gibt, das I als Ideal erzeugt, d.h., für jedes $g(t) \in I$ gibt es $h(t) \in R$, so dass $g(t) = h(t)f_0(t)$.

Insbesondere $2 \in I$ und es gibt $h(t) \in R$, so dass $2 = h(t)f_0(t)$. Das ist aber nur möglich, wenn $h(t)$ and $f_0(t)$ Grad 0 haben, d.h. $h(t) = c \in \mathbb{Z}$ und $f_0(t) = d \in \mathbb{Z}$. Aber dann $d \,|\, 2$ in $\mathbb{Z}$, d.h. $d = \pm 1, \pm 2$. Aber, da $f_0(t) \in I$, ist es unmöglich, dass $d = \pm 1$. Deshalb $d = \pm 2$.

Da $t \in I$, haben wir auch, dass es $h'(t)$ gibt, so dass $t = h'(t)f_0(t) = d \cdot h'(t)$. Aber alle Koeffizienten von $d \cdot h'(t)$ sind gerade und deshalb ist die Gleichung $t = d \cdot h'(t)$ unmöglich.

Der Wiederspruch zeigt, dass $f_0(t)$ nicht existieren kann, mit anderen Worten I ist kein Hauptideal von R.