LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

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

Wintersemester 2024/25
13. Mai 2025

Lineare Algebra II – Lösungsskizzen zu Übungsblatt 2

Aufgabe 1.

1. Bestimmen Sie die Menge $\mathbb{Z}[i]^\times$ aller Einheiten des Gaußschen Zahlrings $\mathbb{Z}[i]$.
   Hinweis. Beweisen Sie zuerst, dass für jede Einheit $u \in \mathbb{Z}[i]^\times$ gilt $N(u) = 1$, wobei N wie in Aufgabe 3 von Übungsblatt 1 ist.
2. Beweisen Sie, dass für eine Primzahl $p \in \mathbb{Z}$ die folgenden Aussagen äquivalent sind:
   a) p ist die Summe zweier Quadrate, d.h., es gibt ganze Zahlen a, $b \in \mathbb{Z}$, so dass $p = a^2 + b^2$;
   b) p ist als Element von $\mathbb{Z}[i]$ reduzibel.

Lösung.

1. Erinnern wir uns daran, dass für $u = a + bi \in \mathbb{Z}[i]$ die Norm als $N(u) = a^2 + b^2 \in \mathbb{N}$ definiert ist. Wenn $u \in \mathbb{Z}[i]^\times$, gibt es $v \in \mathbb{Z}[i]$, so dass $uv = 1$. Aber dann
   $$N(u) \cdot N(v) = N(uv) = N(1) = 1.$$
   Da $N(u)$, $N(v) \in \mathbb{N}$, ist dies nur möglich, wenn $N(u) = 1 = N(v)$.
   Jetzt bestimmen wir alle Elemente $u = a + bi \in \mathbb{Z}[i]$ mit $N(u) = 1$. Offensichtlich ist $a^2 + b^2 = 1$ für ganze Zahlen a, b nur möglich, wenn entweder $a = 0$ und $b = \pm 1$ oder $b = 0$ und $a = \pm 1$. Mit anderen Worten gibt es nur vier Elemente: 1, -1, i und $-i \in \mathbb{Z}[i]$ mit Norm 1. Es ist klar, dass alle diese Elemente in $\mathbb{Z}[i]$ invertierbar sind: $1^2 = (-1)^2 = 1$ und $i(-i) = 1$. Es folgt $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
2. Nehmen wir zuerst an, dass p reduzibel in $\mathbb{Z}[i]$ ist, d.h. $p = xy$ für x, $y \in \mathbb{Z}[i] \setminus \{\pm 1, \pm i\}$. Dann haben wir auch
   $$p^2 = N(p) = N(x)N(y)$$
   und, da x, y nicht invertierbar sind, folgt $N(x)$, $N(y) \in \mathbb{N} \setminus \{0, 1\}$. Das ist nur möglich, wenn $N(x) = p = N(y)$. Aber $x = a + bi$ und $p = N(x) = a^2 + b^2$.
   Nehmen wir zunächst an, dass $p = a^2 + b^2$. Sei $x := a - bi$ und $y := a + bi$. Dann
   $$xy = (a - bi)(a + bi) = a^2 + b^2 = p.$$
   Aber $N(x) = N(y) = a^2 + b^2 \neq 0, 1$ und deshalb sind x, y nicht invertierbar.

Aufgabe 2.
Sei $n \in \mathbb{N} \setminus \{0\}$, so dass $2^n + 1$ eine Primzahl ist. Beweisen Sie, dass $n = 2^m$ für ein $m \in \mathbb{N}$.
Hinweis. Faktorisieren Sie $n = 2^m \cdot k$ für k ungerade.

Lösung.
Sei $n = 2^m \cdot k$ für k ungerade, $m \in \mathbb{N}$. Dann

$$2^n + 1 = 2^{2^m k} - (-1) = (2^{2^m})^k - (-1)^k.$$

Erinnern wir uns daran, dass für alle x, $y \in \mathbb{Z}$ gilt

$$x^k - y^k = (x - y)(x^{k-1} + x^{k-2}y + x^{k-3}y^2 + \ldots + xy^{k-2} + y^{k-1}).$$

Insbesondere, haben wir

$$2^n + 1 = (2^{2^m} + 1)(2^{2^m(k-1)} - 2^{2^m(k-2)} + 2^{2^m(k-3)} + \ldots + (-1)^{k-2}2^{2^m} + (-1)^{k-1}).$$

Da $2^{2^m} + 1 > 1$ und $p = 2^n + 1$ eine Primzahl ist, schliessen wir, dass

$$2^{2^m(k-1)} - 2^{2^m(k-2)} + 2^{2^m(k-3)} + \ldots + (-1)^{k-2}2^{2^m} + (-1)^{k-1} = 1.$$

Aber k ist ungerade und deshalb haben wir $(-1)^{k-1} = 1$ und, da $k > 1$ ist, haben wir auch

$$2^{2^m(k-1)} > 2^{2^m(k-2)}, \qquad 2^{2^m(k-3)} > 2^{2^m(k-4)}, \quad \ldots, \quad 2^{2^m \cdot 2} > 2^{2^m}.$$

Mit anderen Worten für $k > 1$ haben wir

$$2^{2^m(k-1)} - 2^{2^m(k-2)} + 2^{2^m(k-3)} + \ldots + (-1)^{k-2}2^{2^m} + (-1)^{k-1} > 1.$$

Dann kann k nur 1 gleich sein, d.h. $n = 2^m$.

Aufgabe 3.
Sei K ein Körper, $n, d \in \mathbb{N}$ und $A \in \mathrm{M}_n(K)$, so dass $A^d = 0$.

1. Beweisen Sie, dass $A^n = 0$.
   Hinweis. Benutzen Sie das Minimalpolynom $\mu_A(X)$ von A.
2. Bestimmen Sie das charakteristische Polynom $\chi_A(X) \in K[X]$ von A.
   Hinweis. Sie dürfen benutzen, dass es einen algebraisch abgeschlossen Körper E gibt, so dass K ein Unterkörper von E ist.

Lösung.

1. Erinnern wir uns daran, dass die Menge $I = \{P(X) \in K[X] \mid P(A) = 0\}$ ein Ideal von $K[X]$ ist, das vom Minimalpolynom $\mu_A(X)$ erzeugt wird. Wir nehmen an, dass der Leitkoeffizient von $\mu_A(X)$ gleich 1 ist. Da $A^d = 0$, schließen wir, dass X^d zu diesem Ideal I gehört und somit $X^d = \mu_A(X) \cdot h(X)$ für ein $h(X) \in K[X]$. Das ist nur möglich, wenn $\mu_A(X) = X^r$ für ein $r \leq d$. Aber dem Satz von Cayley–Hamilton folgern wir, dass $\chi_A(X)$ auch zu I gehört, und deshalb $\mu_A(X) \,|\, \chi_A(X)$. Da $\chi_A(X)$ Grad n hat, schließen wir, dass $r \leq n$. Aber $A^r = 0$ und deshalb auch $A^n = 0$.
2. Da K Unterkörper von E ist, können wir A als Element von $\mathrm{M}_n(E)$ betrachten. Aber da E algebraisch abgeschlossen ist, können wir $\chi_A(X)$ in ein Produkt von Grad 1 Polynomen faktorisieren:
   $$\chi_A(X) = (X - \lambda_1) \cdot \ldots \cdot (X - \lambda_n)$$
   für $\lambda_i \in E$. Diese λ_i sind genau alle Eigenwerte von A in E. Sei $v \neq 0$ ein Eigenvektor von A zu λ_i für ein i. Da $A^d = 0$, haben wir insbesondere $A^d v = 0$. Sei $k \geq 1$ minimal, so dass $A^k v = 0$. Aber dann
   $$0 = A^k v = A^{k-1}(Av) = A^{k-1}(\lambda_i v) = \lambda_i (A^{k-1} v).$$
   Da $A^{k-1}v \neq 0$, schließen wir, dass $\lambda_i = 0$. Da i beliebig war, haben wir
   $$\chi_A(X) = X^n.$$

Aufgabe 4.

1. Beweisen Sie, dass der Quotientring $\mathbb{Z}[X]/(X^2+1)$ isomorph zu $\mathbb{Z}[i]$ ist.
2. Beweisen Sie, dass für eine ganze Zahl $n \in \mathbb{Z}$ der Quotientring $\mathbb{Z}[i]/n\mathbb{Z}[i]$ isomorph zu $(\mathbb{Z}/n\mathbb{Z})[X]/(X^2+1)$ ist.
3. Beweisen Sie, dass für eine Primzahl $p \in \mathbb{Z}$ die folgenden Aussagen äquivalent sind:
   a) p ist die Summe zweier Quadrate, d.h., es gibt ganze Zahlen a, $b \in \mathbb{Z}$, so dass $p = a^2 + b^2$;
   b) -1 is ein Quadrat modulo p, d.h., es gibt $c \in \mathbb{Z}$, so dass $c^2 \equiv -1 \mod p$.

Lösung.

1. Betrachten wir zuerst die Abbildung $F\colon \mathbb{Z}[X] \to \mathbb{Z}[i]$, die $P(X)$ auf $P(i)$ schickt. Es ist klar, dass F ein Ringhomomorphismus ist. Es ist auch klar, dass $F(X^2+1) = i^2+1 = 0$ und deshalb ist die Abbildung

$$f\colon \mathbb{Z}[X]/(X^2+1) \to \mathbb{Z}[i],$$

die $[P(X)]$ nach $P(i)$ schickt wohldefiniert ($[P(X)]$ bezeichnet die Klasse von $P(X)$ modulo (X^2+1)). Es ist auch klar, dass f surjektiv ist. In der Tat, für jedes $a+bi \in \mathbb{Z}[i]$ haben wir $f([a+bX]) = a+bi$.

Nehmen wir jetzt an, dass $P(i) = 0$. Betrachten wir P als Polynom in $\mathbb{C}[X]$ und bemerken wir, dass $P(\bar{i}) = \overline{P(i)} = \bar{0} = 0$, da alle Koeffizienten von P rell sind (wobei $\bar{}$ die komplexe Konjugation ist). Da i und $\bar{i} = -i$ Nullstellen von P sind, schließen wir, dass

$$P(X) = (X-i)(X+i)Q(X)$$

für ein $Q(X) \in \mathbb{C}[X]$. Aber da $(X-i)(X+i) = X^2+1$, haben wir

$$P(X) = (X^2+1)Q(X).$$

Schreiben wir $Q(X) = a_sX^s + \ldots + a_1X + a_0$, $a_s \neq 0$. Dann

$$P(X) = a_sX^{s+2} + a_{s-1}X^{s+1} + (a_{s-2}+a_s)X^s + (a_{s-3}+a_{s-1})X^{s-1} + \ldots + (a_2+a_0)X^2 + a_1X + a_0.$$

Da $P[X] \in \mathbb{Z}[X]$, sind alle Koeffizienten von $P(X)$ ganz, insbesondere a_s und $a_{s-1} \in \mathbb{Z}$. Aber dann auch a_{s-2}, $a_{s-3} \in \mathbb{Z}$ und induktiv erhalten wir auf diese Weise, dass $a_i \in \mathbb{Z}$ für alle i. Mit anderen Worten $Q(X) \in \mathbb{Z}[X]$ und deshalb $[P(X)] = [0]$ in $\mathbb{Z}[X]/(X^2+1)$. Das beweist, dass f injektiv ist.

2. Es ist genug zu zeigen, dass $\big(\mathbb{Z}[X]/(X^2+1)\big)/(n)$ isomorph zu $(\mathbb{Z}/n\mathbb{Z})[X]/(X^2+1)$ ist.

Beweisen wir zuerst, dass $(\mathbb{Z}/n\mathbb{Z})[X] \cong \mathbb{Z}[X]/(n)$. Die Abbildung $G\colon \mathbb{Z}[X] \to (\mathbb{Z}/n\mathbb{Z})[X]$, die ein Polynom $\sum a_iX^i$ nach $\sum (a_i \mod n)X^i$ schickt, induziert die wohldefinierte Abbildung

$$g\colon \mathbb{Z}[X]/(n) \to (\mathbb{Z}/n\mathbb{Z})[X].$$

Ähnlich ist die Abbildung $h\colon (\mathbb{Z}/n\mathbb{Z})[X] \to \mathbb{Z}[X]/(n)$, die $\sum (a_i \mod n)X^i$ nach $[\sum a_iX^i]$ schickt, wohldefiniert (wobei $[\sum a_iX^i]$ die Klasse von $\sum a_iX^i$ in $\mathbb{Z}[X]/(n)$ bezeichnet). Es ist klar, dass diese Abbildungen zueinander inverse Ringhomomorphismen sind.

Beweisen wir jetzt, dass $\big(\mathbb{Z}[X]/(X^2+1)\big)/(n)$ isomorph zu $\big(\mathbb{Z}[X]/(X^2+1)\big)/(n)$ ist. Die kanonische Projektion

$$P\colon \mathbb{Z}[X] \to \big(\mathbb{Z}/[X]/(X^2+1)\big)/(n)$$

induziert die wohldefinierte Abbildung $p\colon \big(\mathbb{Z}[X]/(n)\big)/(X^2+1) \to \big(\mathbb{Z}/[X]/(X^2+1)\big)/(n)$, da $P(n) = 0$ und $P(X^2+1) = 0$. Ähnlich, induziert die kanonische Projektion

$$Q\colon \mathbb{Z}[X] \to \big(\mathbb{Z}[X]/(n)\big)/(X^2+1)$$

die wohldefinierte Abbildung $q\colon \big(\mathbb{Z}[X]/(X^2+1)\big)/(n) \to \big(\mathbb{Z}[X]/(n)\big)/(X^2+1)$. Es ist auch klar, dass diese Abbildungen zueinander inverse Ringhomomorphismen sind.

3. -1 ist ein Quadrat modulo p, wenn und nur wenn $X^2+1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ reduzibel ist. Wie Sie schon aus der Vorlesung wissen, ist $X^2+1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ reduzibel, wenn und nur wenn $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ kein Integritätsbereich ist. Aber $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1) \cong \mathbb{Z}[i]/(p)$ ist kein Integritätsbereich, wenn und nur wenn p reduzibel in $\mathbb{Z}[i]$ ist. Nach Aufgabe 1 ist dies möglich, wenn und nur wenn p die Summe zweier Quadrate ist.