Übungsblatt 4: Teilbarkeitslehre

Lassen Sie sich nicht durch die Menge der Aufgaben einschüchtern. Es gibt nur wenig schriftliche Aufgaben und wir halten die Menge der Votieraufgaben überschaubar.
Alle weiteren Aufgaben sind ein gutgemeinter Vorschlag: Wir möchten Sie ermutigen, sich über das Notwendigste hinaus mit Algebra zu beschäftigen.

1. Hauptidealringe und faktorielle Ringe

V 1.1. Welches sind die irreduziblen Elemente in $\mathbb{C}[X]$. Und in $\mathbb{R}[X]$?

Lösungshinweise: — *Aus dem Fundamentalsatz der Algebra folgt, dass sich jedes Polynom über $\mathbb{C}$ als ein Produkt von Linearfaktoren darstellen lässt. Damit sind die einzigen Kandidaten für irreduzible Polynome die linearen Polynome $p_z = X - z$ für ein $z \in \mathbb{C}$ (und alle assoziierten Polynome). Diese sind auch tatsächlich irreduzibel, denn aus $p_z = rs$ mit $r,s \in \mathbb{C}[X]$ folgt, dass $1 = \deg(p_z) = \deg(r) + \deg(s)$ und damit hat eines der Polynome Grad 0 und ist invertierbar.*
Um an die irreduziblen Elemente in $\mathbb{R}[X]$ zu kommen, muss man sich in Erinnerung rufen, dass wenn $z \in \mathbb{C}\backslash\mathbb{R}$ eine Nullstelle eines reellen Polynomes ist, auch $\overline{z}$ eine Nullstelle ist. Damit nimmt man zuerst die Zerlegung des Polynoms $p \in \mathbb{R}[X]$ in Linearfaktoren über $\mathbb{C}$ vor und sortiert dann die Linearfaktoren mit z und $\overline{z}$ zusammen. Diese ergeben multipliziert $q = (X-z)(X-\overline{z}) = X^2 - 2Re(z)X + |z|^2$, also ein Polynom in $\mathbb{R}[X]$. Dieses ist dann irreduzibel, denn jede echte Zerlegung $q = st$ in $\mathbb{R}[X]$ liefert wegen der Eindeutigkeit der Zerlegung in $\mathbb{C}[X]$ dann $s \sim X - z$ oder $s \sim X - \overline{z}$, was nicht sein kann, weil kein zu $X - z$ (bzw. $X - \overline{z}$) assoziiertes Element reell sein kann. Die irreduziblen Elemente sind also die linearen Polynome $X - r$ für ein $r \in \mathbb{R}$ und die quadratischen Polynome $X^2 + bX + c$ mit $b^2 - 4c < 0$ (echt komplexe Nullstellen!) und natürlich auch all ihre assoziierten Elemente. —

S 1.2. (3 Punkte) $\mathbb{Z}[X]$ ist kein Hauptidealring, denn z.B. $(2,X)$ ist kein Hauptideal.

Lösungshinweise: — *Wenn $(2,X)$ gleich einem Hauptideal (p) mit $p \in \mathbb{Z}[X]$ wäre, dann gäbe es Polynome $r,s \in \mathbb{Z}[X]$ mit mit $2 = rp$, $X = sp$. Da $\mathbb{Q}[X]$ ein faktorieller Ring ist und $2 \in \mathbb{Q}[X]^\times$, folgt aus der ersten Gleichung, dass $p \in \mathbb{Q}[X]^\times = \mathbb{Q}^\times$ liegt. Damit ist $p \in \{\pm 1, \pm 2\}$, da $p \in \mathbb{Z}[X]$. Aus der zweiten Gleichung folgern wir nun, dass $p = \pm 1$, da X in $\mathbb{Z}[X]$ nicht durch 2 teilbar ist. Damit wäre aber $(p) = \mathbb{Z}[X]$. Wir zeigen, dass $(2,X) \neq \mathbb{Z}[X]$ gilt. Sei $1 = 2r + Xs$ mit $r,s \in \mathbb{Z}[X]$, dann gilt in $\mathbb{Z}/_2[X]$ die Gleichung $1 = Xs$, was aus Gradgründen nicht sein kann. Damit folgt $1 \notin (2,X)$.*
Eine alternative Lösung sieht wie folgt aus:
Wir stellen fest, dass beim Multiplizieren zweier Polynome der konstante Term des Produkts als das Produkt der konstanten Terme der Faktoren gegeben ist. Es gibt $r,s \in \mathbb{Z}[X]$, so dass $2r + Xs = p$. Damit muss der konstante Term a_0 in p durch 2 teilbar sein. Wenn nun $a_0 \neq 0$, dann ist $X \notin (p)$, da aus der Gleichung $pq = X$ folgt, dass der konstante Term von q gleich 0 ist und man damit bei pq ein Vielfaches von $2X$ erhält. Wenn $a_0 = 0$, dann ist $2 \notin (p)$. Also erhalten wir stets einen Widerspruch. —

1.3. Der Polynomring $K[X]$ ist genau dann ein Hauptidealring, wenn K ein Körper ist.

Lösungshinweise: — *Dass für einen Körper K der Polynomring $K[X]$ ein Hauptidealring ist, wurde in der Vorlesung gezeigt. Dies folgt daraus, dass $K[X]$ sogar ein euklidischer Ring ist.*
Wenn andererseits $K[X]$ ein Hauptidealring ist, dann ist $K[X]$ nach Definition nullteilerfrei. Also ist K ein Integritätsring. Wir betrachten nun das Ideal (X,a) für ein $a \in K^*$. Dann ist $(X,a) = (p)$ für ein Polynom $p \in K[X]$ nach Voraussetzung. Aus $rp = a$ folgt mit der Gradfunktion, dass $\deg(p) = 0$ (K ist Integritätsring!). Also ist $p \in K^*$. Andererseits ist auch $sp = X$, was auf p teilt 1 führt und damit ist $p \in K^\times$. Damit gilt aber auch $1 = ra + sX$ mit $r,s \in K[X]$ oder anders: $ra = 1$ in $K[X]/(X) \cong K$. Also ist a in K invertierbar. —

2. Nicht-eindeutige Zerlegung in irreduzible Elemente

2.1. Für jedes $k \in \mathbb{N}$ ist $M_k = 1 + k\mathbb{N}$ ein Untermonoid von $(\mathbb{N}, \cdot)$. In $M_1 = \{1,2,3,4,\dots\}$ lässt sich jedes Element eindeutig in irreduzible Faktoren zerlegen. Gilt dies auch in $M_2 = \{1,3,5,7,\dots\}$? und in $M_3 = \{1,4,7,10,\dots\}$?

Lösungshinweise: — *In M_2 ist die Zerlegung eindeutig, da die Zerlegung mit der Zerlegung in $\mathbb{N}$ übereinstimmt. Im M_3 betrachten wir $100 = 10 \cdot 10 = 4 \cdot 25$. Die möglichen Faktoren 2 und 5 sind nicht in M_3 enthalten. Also sind $4, 10$ und 25 irreduzible Elemente. Damit ist die Zerlegung nicht eindeutig.* —

2.2. Selbst ein Polynomring kann nicht-faktorielle Unterringe haben:

(a) Man zeige, dass $K := \{ P \in \mathbb{Q}[X] \mid P'(0) = 0 \}$ ein Unterring von $\mathbb{Q}[X]$ ist. Es ist $K = \mathbb{Q}[X^2, X^3]$ der von $\{X^2, X^3\}$ über $\mathbb{Q}$ erzeugte Unterring.

(b) Man bestimme die Gruppe $K^\times$ der in K invertierbaren Elemente.

(c) Lässt sich jedes Element in K als Produkt irreduzibler Faktoren schreiben?

(d) Sind die Polynome X^2 und X^3 im Ring K irreduzibel? Sind sie prim?

(e) In K bestimme man alle Zerlegungen von X^6 und X^7 in irreduzible Faktoren.

(f) Man gebe $P, Q \in K$ an, die in K keinen größten gemeinsamen Teiler haben.

Lösungshinweise: — *Die wesentliche Idee ist alle Aussagen zuerst in $\mathbb{Q}[X]$ zu betrachten und dann zu schauen, ob diese auch in K gelten...*

(a) *Die Ringeigenschaften rechnet man direkt nach. Die Gleichung $P'(0) = 0$ ist äquivalent dazu, dass der lineare Term des Polynoms verschwindet. Der Ring $\mathbb{Q}[X^2, X^3]$ enhält alle Potenzen von X außer X^1, da die Menge $\{2,3\}$ im Monoid $(\mathbb{N}, +)$ alle Zahlen außer der 1 erzeugt. Also ist $K = \mathbb{Q}[X^2, X^3]$*

(b) *Es gilt $\mathbb{Q}^\times \subset K^\times \subset \mathbb{Q}[X]^\times = \mathbb{Q}^\times$. Also $K^\times = \mathbb{Q}^\times$.*

(c) *Die Gradfunktion auf $\mathbb{Q}[X]$ ist natürlich auch auf der Teilmenge K vorhanden. Diese nimmt nur Werte in $\mathbb{N} \cup \{-\infty\}$ an und damit geht der Beweis der Existenz einer Zerlegung ebenso durch wie in $\mathbb{Q}[X]$.*

(d) *Die beiden Polynome sind irreduzibel, denn bei der Zerlegung in $\mathbb{Q}[X]$ erhält man stets das Polynom X, welches aber nicht in K liegt. X^2 ist nicht prim, da X^2 den Term $X^3 \cdot X^3$ teilt, aber keinen der beiden Faktoren. Ebenso ist X^3 nicht prim, da X^3 das Produkt $X^4 \cdot X^4$ teilt, aber nicht X^4.*

(e) *$X^6 = X^2 \cdot X^2 \cdot X^2 = X^3 \cdot X^3$ sind alle Zerlegungen (bis auf Einheiten) und $X^7 = X^2 \cdot X^2 \cdot X^3$ hat nur eine Zerlegung.*

(f) *Die beiden Polynome aus Teil (e) haben keinen ggT, denn die Menge der Teiler von X^6 ist $\{1, X^2, X^3, X^4, X^6\}$ (bis auf Einheiten) und die Teiler von X^7 sind $\{1, X^2, X^3, X^4, X^5, X^7\}$. Der einzige Kandidat für den ggT ist X^4. Aber um ggT zu sein, muss der gemeinsame Teiler X^3 auch ein Teiler von X^4 sein, was nicht der Fall ist. Also gibt es keinen ggT.*

—

3. Keine Zerlegung in irreduzible Elemente

Es ist nicht einfach, einen Ring zu finden, in dem sich manche Elemente nicht als Produkt von irreduziblen Elementen schreiben lassen. Hier eines der einfachsten Beispiele:

Wir schreiben das Monoid $(\mathbb{Q}_{\geq 0}, +)$ multiplikativ als $M = \{X^a \mid a \in \mathbb{Q}_{\geq 0}\}$ mit $X^a \cdot X^b = X^{a+b}$. Sei $R = \mathbb{C}M$ der Monoidring über dem Körper $\mathbb{C}$ der komplexen Zahlen: Jedes Element schreibt sich eindeutig als eine Summe $a_1 X^{e_1} + \cdots + a_n X^{e_n}$ der Länge $n \in \mathbb{N}$ mit Koeffizienten $a_1, \dots, a_n \in \mathbb{C}^*$ und Exponenten $0 \leq e_1 < \cdots < e_n$ in $\mathbb{Q}$.

3.1. (a) Für jedes $n \in \mathbb{N}$, $n \geq 1$, ist $\mathbb{C}[X^{1/n}] \subset R$ ein Polynomring in $X^{1/n}$ über $\mathbb{C}$.

(b) Jede endliche Familie $P_1, \dots, P_k \in R$ liegt in einem Polynomring $\mathbb{C}[X^{1/n}] \subset R$.

(c) Man bestimme die Gruppe $R^\times$ der in R invertierbaren Elemente.

(d) Man bestimme alle irreduziblen Elemente in R. Ist R faktoriell?

Lösungshinweise: —

(a) *Der Ring $\mathbb{C}[X^{1/n}]$ genügt offenbar der Definition eines Polynomringes, wenn man zeigen kann, dass es wirklich ein Ring ist. Dies folgt aber aus den Rechengesetzen für Potenzen und Brüche. Addieren von positiven Brüchen, deren Nenner ein Teiler von n ist, liefert wieder einen solchen Bruch. Diese bilden ein Untermonoid in $(\mathbb{Q}_{\geq 0},+)$, der zu $(\mathbb{N},+)$ isomorph ist.*

(b) *In einer endlichen Familie von Polynomen tauchen nur endlich viele Brüche als Potenzen von Monomen auf. Diese kann man alle auf einen gemeinsamen Nenner n bringen und erhält damit die Aussage.*

(c) *Es gelte $pq = 1$ in R. Dann gilt $pq = 1$ in $\mathbb{C}[X^{1/n}]$ für ein geeignetes $n \in \mathbb{N}$ nach Teil (b). In einem Polynomring sind aber nur die Körperelemente invertierbar, also sind $p,q \in \mathbb{C}$. Insgesamt folgt $R^\times = \mathbb{C}$.*

(d) *In R gibt es keine irreduziblen Elemente. Denn wir befinden uns über dem Körper $\mathbb{C}$ und jedes Polynom zerfällt in Linearfaktoren. Aber ein Linearfaktor $Y - \alpha$ in der Variablen $Y = X^{1/n}$, stellt ein quadratisches Polynom $Z^2 - \alpha$ in der Variablen $Z = X^{1/2n}$ dar, welches dann wieder faktorisiert. Damit kann R natürlich nicht faktoriell sein.*

—

4. Der Ring $\mathbb{Z}[i]$ der Gauss'schen Zahlen

S 4.1. (6 Punkte)

(a) Die Menge $\mathbb{Z}[i] = \{\, a+bi \mid a,b \in \mathbb{Z} \,\}$ ist ein Unterring von $\mathbb{C}$.

(b) Die Norm $N(z) = z\bar{z}$ ist ein Monoidhomomorphismus $N\colon (\mathbb{Z}[i],\cdot) \to (\mathbb{N},\cdot)$ mit $N(z) = 0 \Leftrightarrow z = 0$ und $N(z) = 1 \Leftrightarrow z \in \mathbb{Z}[i]^\times$. Man bestimme $\mathbb{Z}[i]^\times$.

(c) Wenn $N(z)$ irreduzibel in $\mathbb{N}$ ist, dann ist z irreduzibel in $\mathbb{Z}[i]$.

(d) Der Ring $\mathbb{Z}[i]$ ist euklidisch bezüglich der Norm N. *Hinweis:* Zu $a,b \in \mathbb{Z}[i], b \neq 0$, approximiere man $\frac{a}{b} \in \mathbb{C}$ durch ein $q \in \mathbb{Z}[i]$ mit $|\frac{a}{b} - q|^2 \leq \frac{1}{2}$.

Lösungshinweise: —

(a) *Man muss die Abgeschlossenheit unter Subtraktion und Multiplikation nachweisen, ebenso wie $1 \in Z[i]$. Dies folgt aber alles direkt aus $i^2 = -1 \in \mathbb{Z}$ und der Tatsache, dass $\mathbb{Z}$ ein Ring ist.*

(b) *Es ist $N(zw) = zw\overline{zw} = z\bar{z}w\bar{w} = N(z)N(w)$ und $N(1) = 1\bar{1} = 1$, was zu zeigen war. $N(z) = z\bar{z} = |z|^2 = 0$ liefert die Äquivalenz $N(z) = 0 \Leftrightarrow z = 0$. Wenn $N(z) = 1$ ist, schreiben wir $z = a+bi$ mit $a,b \in \mathbb{Z}$. Dann folgt $1 = |z|^2 = a^2 + b^2$. Dies hat die Lösungen $a = \pm 1, b = 0$ und $a = 0, b = \pm 1$. Also sind die Elemente mit Norm 1 gleich $\{1,-1,i,-i\}$. Diese sind offenbar auch invertierbar. Jedes invertierbare Element hat umgekehrt auch Norm 1. Denn aus $1 = zw$ folgt $1 = N(1) = N(zw) = N(z)N(w)$ und damit $N(z) = N(w) = 1$.*

(c) *Sei $z = rs$ mit $r,s \in \mathbb{Z}[i]$, dann ist $N(z) = N(r)N(s)$. Nach Voraussetzung ist $N(z)$ irreduzibel, also ist $N(r) = 1$ oder $N(s) = 1$. Nach Teil (b) folgt, dass r oder s invertierbar sind und damit ist z irreduzibel.*

(d) *Betrachte $a,b \in \mathbb{Z}[i], b \neq 0$. Dann ist $\frac{a}{b} = x+iy \in \mathbb{C}$. Es gibt $u,v \in \mathbb{Z}$ mit $|x-u| \leq \frac{1}{2}$ und $|y-v| \leq \frac{1}{2}$. Setze $q = u+iv$. Damit ist dann $|\frac{a}{b} - q|^2 = |x+iy-u+iv|^2 = (x-u)^2 + (y-v)^2 \leq \frac{1}{2}$. Umstellen der Gleichung liefert $|a-qb|^2 \leq \frac{|b|^2}{2}$. Setzen wir also $r = a-qb$, so ist $a = qb+r$ und $N(r) = |r|^2 \leq \frac{|b|^2}{2} < N(b)$, was zu zeigen war.*

—

Dass der Ring $\mathbb{Z}[i]$ euklidisch ist, hat erstaunliche Konsequenzen für Primzahlen in $\mathbb{Z}$:

S 4.2. (2 Punkte) Jede Primzahl $p \in \mathbb{Z}$ lässt sich auf höchstens eine Art als Summe von zwei Quadraten schreiben, das heißt, aus $p = a^2 + b^2 = c^2 + d^2$ folgt $\{a^2, b^2\} = \{c^2, d^2\}$. *Hinweis:* Man betrachte $p = (a+ib)(a-ib) = (c+id)(c-id)$ in $\mathbb{Z}[i]$.

Lösungshinweise: — *Nehmen wir an, dass $p = (a+ib)(a-ib) = (c+id)(c-id)$ in $\mathbb{Z}[i]$. Dann folgt durch Anwenden der Norm, dass $N(a \pm bi) = N(c \pm di) = p$. Aus Aufgabe 4.1 (c) wissen wir nun, dass die vier Faktoren irreduzibel sind. Wegen der Eindeutigkeit der Zerlegung in irreduzible Elemente in $\mathbb{Z}[i]$, muss also $a+bi = \varepsilon(c \pm di)$ und $a-bi = \mu(c \mp di)$ mit Einheiten $\varepsilon, \mu \in \mathbb{Z}[i]$ gelten. Die Einheiten sind aber $\{1, -1, i, -i\}$, so dass man erhält, dass $a = \pm c, b = \pm d$ oder $a = \pm d, b = \pm c$ gilt. Auf jeden Fall ist $\{a^2, b^2\} = \{c^2, d^2\}$.* —

Für die Primzahl 2 gilt $2 = 1^2 + 1^2$. Für die Primzahlen $3, 7, 11, \ldots$ gibt es keine solche Zerlegung. Andererseits gilt $5 = 1^2 + 2^2$ und $13 = 2^2 + 3^2$ und $17 = 1^2 + 4^2, \ldots$.

Satz (Zwei-Quadrate-Satz von Fermat) *Die Primzahlen $p \in \mathbb{N}$ mit $p \equiv 3 \pmod 4$ lassen sich nicht als Summe von zwei Quadraten schreiben. Zu jeder Primzahl $p \in \mathbb{N}$ mit $p \equiv 1 \pmod 4$ existiert genau ein Paar $a < b$ in $\mathbb{N}$ sodass $p = a^2 + b^2$.*

V 4.3. Für $p \equiv 3 \pmod 4$ ist $p = a^2 + b^2$ schon modulo 4 unmöglich.

Lösungshinweise: — *Modulo 4 gilt stets $a^2 \in \{0, 1\}$. Die Summe zweier Quadrate kann also nie kongruent 3 modulo 4 sein.* —

Im Folgenden sei $p \in Z$ eine Primzahl mit $p \equiv 1 \pmod 4$.

V 4.4. (a) Es gibt $\xi \in \mathbb{Z}/_p$ mit $\xi^2 = -1$. *Hinweis:* In $\mathbb{Z}/_p$ vergleiche man $1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$ und $\frac{p+1}{2} \cdots (p-2) \cdot (p-1)$ und berechne ihr Produkt.

(b) Aus $p \mid q^2 + 1$ in $\mathbb{Z}$ folgt $p \mid (q+i)(q-i)$ in $\mathbb{Z}[i]$. Ist p prim?

(c) In $\mathbb{Z}[i]$ zerfällt p in zwei irreduzible Faktoren, $p = (a+ib)(a-ib)$.

Lösungshinweise: —

(a) *Das zweite Produkt im Hinweis enthält gerade die negativen Faktoren des ersten Produktes. Sie sind also gleich bis auf einen Faktor $(-1)^n$, wobei n = Anzahl der Faktoren ist. Da $p \equiv 1 \pmod 4$ gilt, ist die Anzahl der Elemente ungleich 0 durch 4 teilbar. Dies ist aber $2n$, so dass n selbst gerade sein muss. Also sind die beiden Produkte gleich und wir setzen diese Zahl als das gesuchte ξ. Wir müssen also nur noch zeigen, dass $\xi^2 = 1 \cdot 2 \cdots (p-2) \cdot (p-1) = -1$ gilt. Dazu beachte man, dass zu jedem Element auch sein Inverses in dem Produkt auftaucht. Diese kürzen sich, es sei denn, das Element ist selbstinvers, löst also die Gleichung $x^2 = 1$. Diese Gleichung hat im Körper $\mathbb{Z}/_p$ höchstens zwei Lösungen und diese können wir sofort angeben: $\{1, -1\}$. Also ist das obige Produkt gleich dem Produkt aus 1 und -1, was wir zeigen wollten.*

(b) *Eine Primzahl $p \equiv 1 \pmod 4$ ist in $\mathbb{Z}[i]$ nicht prim. Denn aus Teil (a) folgt, dass $p \mid (q+i)(q-i)$ für ein $q \in \mathbb{Z}$, aber p teilt keinen der Faktoren, da es dann den Real- und Imaginärteil teilen würde, also insbesondere $p \mid 1$, was nicht sein kann.*

(c) *Wenn p nicht prim ist, ist p im euklidischen Ring $\mathbb{Z}[i]$ auch nicht irreduzibel und zerfällt in $\mathbb{Z}[i]$ in irreduzible Faktoren. Wenn $p = rs$, dann gilt aber, dass $N(r)N(s) = N(p) = p^2$, so dass jeder nichttriviale Faktor von p die Norm p haben muss. Damit zerfällt p also in zwei irreduzible Faktoren. Diese müssen zueiander konjugiert sein, damit ihr Produkt reell ist.*
Daraus folgt nun durch Anwenden der Norm der Zwei-Quadrate-Satz.

—

5. Die Ringe $\mathbb{Z}[i\sqrt{2}]$ und $\mathbb{Z}[i\sqrt{3}]$

5.1. (a) Für $\xi = i\sqrt{2}$ ist $\mathbb{Z}[\xi] = \{\, a+b\xi \mid a,b \in \mathbb{Z} \,\}$ ein Unterring von $\mathbb{C}$.
Man zeichne das Gitter $\mathbb{Z}[\xi]$ in der komplexen Ebene und bestimme $\mathbb{Z}[\xi]^\times$.
(b) Jede komplexe Zahl $q \in \mathbb{C}$ erlaubt eine Näherung $z \in \mathbb{Z}[\xi]$ mit $|q-z|^2 \leq \frac{3}{4}$.
Man folgere daraus, dass $\mathbb{Z}[\xi]$ ein euklidischer Ring ist bezüglich $N(z) = z\bar{z}$.

Lösungshinweise: — *Diese Aufgabe löst man analog zur Aufgabe 4.1. Die Einheiten sind nur* 1 *und* -1. *Hier kann man in y-Richtung nur bis auf* $\frac{\sqrt{2}}{2}$ *approximieren, so dass man nur* $|q-z|^2 \leq \frac{3}{4}$ *erhält.* **—**

5.2. (a) Für $\xi = i\sqrt{3}$ ist $\mathbb{Z}[\xi] = \{\, a+b\xi \mid a,b \in \mathbb{Z} \,\}$ ein Unterring von $\mathbb{C}$.
Man zeichne das Gitter $\mathbb{Z}[\xi]$ in der komplexen Ebene und bestimme $\mathbb{Z}[\xi]^\times$.
(b) Jede komplexe Zahl $q \in \mathbb{C}$ erlaubt eine Näherung $z \in \mathbb{Z}[\xi]$ mit $|q-z|^2 \leq 1$.
Warum bricht die Konstruktion einer euklidischen Division hier zusammen?
(c) Man zähle die kleinsten Werte der Norm $N\colon \mathbb{Z}[\xi] \to \mathbb{N}$, $N(z) = z\bar{z}$, auf und folgere daraus, dass jedes Element $z \in \mathbb{Z}[\xi]$ mit $N(z) = 4$ irreduzibel ist.
(d) Man betrachte $2 \cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3})$. Ist $\mathbb{Z}[i\sqrt{3}]$ faktoriell?

Lösungshinweise: —

(a)+(b) *Dieser Teil geht wie bei den vorherigen Aufgaben und* $\mathbb{Z}[i\sqrt{3}]^\times = \{1,-1\}$. *Hier erhält man nun aber nur* $|q-z|^2 \leq 1$, *was nicht zu* $N(r) < N(b)$ *führt, wenn man die Konstruktion von Aufgabe 4 benutzt.*

(c) *Es ist* $N(a+b\xi) = a^2+3b^2$. *Damit nimmt die Norm nur die Werte* $\{0,1,3,4,7,9,12,\ldots\}$ *an. Ein Element mit Norm* 4 *ist also irreduzibel, da die Faktoren sonst Norm* 2 *haben müssten.*

(d) *Der Term* $2 \cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3})$ *zeigt zwei verschiedene Zerlegungen der* 4 *in irreduzible Faktoren (nach (c)). Damit ist* $\mathbb{Z}[i\sqrt{3}]$ *nicht faktoriell.*

—

6. Euklidischer Algorithmus

6.1. Die Ringe $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[X]$ sind euklidisch. Man berechne:

(a) $\operatorname{ggT}(24087, 33411)$ in $\mathbb{Z}$, (b) $\operatorname{ggT}(5+3i, 13+8i)$ in $\mathbb{Z}[i]$,

(c) $\operatorname{ggT}(X^5+X^4+X^3+X^2+X+1, X^4-X^3-X+1)$ in $\mathbb{Q}[X]$.

Lösungshinweise: — *Wir geben jeweils einen Repräsentanten aus der Menge der GGT an.*

(a) $\operatorname{ggT}(24087, 33411) = 777$
(b) $\operatorname{ggT}(5+3i, 13+8i) = 1$
(c) $\operatorname{ggT}(X^5+X^4+X^3+X^2+X+1, X^4-X^3-X+1) = X^2+X+1$

—

6.2. Prüfen Sie, ob die folgenden Gleichungen in $\mathbb{Z}^2$ lösbar sind und bestimmen Sie gegebenenfalls alle Lösungen.

(a) $320x - 18y = 2$, (b) $102x - 15y = 5$, (c) $101x - 15y = 5$.

Lösungshinweise: — *Im Teil (b) ist* 3 *stets ein Teiler der linken Seite, aber nicht der rechten. Die Gleichung hat also keine Lösung.*

In den beiden anderen Fällen liefert die Anwendung des euklidischen Algorithmus jeweils eine spezielle Lösung $(x_0, y_0) \in \mathbb{Z}^2$, *indem man zuerst die Gleichung* $ax+by = ggT(a,b)$ *löst.*

Dies ist in Teil (a) zum Beispiel $(4, 71)$ *und in Teil (c) z.B.* $(-5, -34)$.

Die anderen Lösungen erhält man ähnlich wie bei linearen Gleichungssystemen, indem man die "homogene" Gleichung löst. Zum Beispiel: $320x = 18y$. *Zerlegt man die beiden Faktoren, so ergibt sich* $2^6 \cdot 5x = 2 \cdot 3^2 y$. *Die eindeutige Zerlegung in Primzahlen liefert, dass* y *von* $2^5 \cdot 5$ *und* x *von* 3^2 *geteilt wird. Also* $y = 160u, x = 9v$. *Damit wird die Gleichung zu* $9 \cdot 320v = 160 \cdot 18u$. *Nach Kürzen der Faktoren ergibt sich* $u = v$.
Also sind alle Lösungen gegeben durch $(4,71) + k(9,160)$ *mit* $k \in \mathbb{Z}$.
In Teil (c) ergibt sich $(-5,-34) + k(15,101)$ *mit* $k \in \mathbb{Z}$. —

6.3. Sei $n = 582$ und $a = 115$. Man bestimme a^{-1} in $\mathbb{Z}/_n$.

Lösungshinweise: — *Wir müssen die Gleichung* $ax = 1$ *in* $\mathbb{Z}/_n$ *lösen, oder anders ausgedrückt die Gleichung* $ax + ny = 1$ *in* $\mathbb{Z}^2$. *Dazu verwenden wir den euklidischen Algorithmus. Es gilt*

$$582 = 5 \cdot 115 + 7, \qquad 115 = 16 \cdot 7 + 3 \quad \textit{und} \quad 7 = 2 \cdot 3 + 1$$

Rückwärts einsetzen liefert

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (115 - 16 \cdot 7) = -2 \cdot 115 + 33 \cdot 7 = -2 \cdot 115 + 33 \cdot (582 - 5 \cdot 115) = 33 \cdot 582 - 167 \cdot 115$$

Also ist $a^{-1} = -167 = 415$. —

6.4. Man wende den (erweiterten) euklidischen Algorithmus auf das folgende Problem an.

(a) Zu den Polynomen $P = X^2 + 1$ und $Q = X^3 - 2$ in $\mathbb{Q}[X]$ bestimme man $T = \operatorname{ggT}(P,Q)$ in $\mathbb{Q}[X]$ sowie $U, V \in \mathbb{Q}[X]$ sodass $T = UP + VQ$.

(b) Man vereinfache $\frac{X^3+1}{(X^2+1)(X^3-2)}$ zu $A + \frac{B}{X^2+1} + \frac{C}{X^3-2}$ und bestimme hierzu $A, B, C \in \mathbb{Q}[X]$ so, dass $\deg B < 2$ und $\deg C < 3$.

Lösungshinweise: — *Der euklidische Algorithmus liefert* $5 = [-X^2 + 2X + 1](X^2 + 1) + [X - 2](X^3 - 2)$. *Dividiert man nun diese Gleichung durch* $5(X^2+1)(X^3-2)$ *und multipliziert mit* (X^3+1), *erhält man eine Zerlegung, die allerdings die Forderungen* $\deg B < 2$ *und* $\deg C < 3$ *noch nicht erfüllt. Dazu muss man in jedem Faktor eine Division mit Rest durchführen und erhält insgesamt:*
$\frac{X^3+1}{(X^2+1)(X^3-2)} = \frac{1}{5}\frac{3X-1}{X^2+1} - \frac{3}{5}\frac{X^2-2X-1}{X^3-2}$ —