Lineare Algebra 2, SS06
M. Hortmann

Blatt 2

Aufgabe 1

a) 2 ist im Ring der Gaußschen Zahlen $\mathbb{Z}[i]$ nicht unzerlegbar, denn es gilt ja $2=(1+i)(1-i)$.
Man finde durch Probieren heraus, ob für $3,5,7,11,13,17,19,23,29,31\in\mathbb{Z}[i]$ Produkzerlegungen in Nicht-Einheiten existieren und stelle danach eine Vermutung auf, welche unzerlegbaren Elemente von $\mathbb{Z}$ auch unzerlegbar in $\mathbb{Z}[i]$ sind.

b) (Freiwillige Sonderaufgabe): man stelle dieselbe Untersuchung für $\mathbb{Z}[\omega]$ an.

Aufgabe 2

Sei *R* ein Integritätsring.

Sind $a,b,c\in R$, $a,b,c\neq 0$ und gilt $c \mid a$ und $c \mid b$, so nennt man *c* einen gemeinsamen Teiler von *a* und *b* . Auf Idealebene bedeutet dies: $<a>\subset<c>$ und $<b>\subset<c>$. Ein solcher Teiler *d* heißt *größter gemeinsamer Teiler* , wenn für jeden gemeinsamen Teiler *c* von *a*,*b* gilt: $c \mid d$. Natürlich teilt eine Einheit jedes Element von *R* . Ist eine Einheit größter gemeinsamer Teiler zweier Elemente, so nennt man diese *teilerfremd* .

a) Zeigen Sie: Ist *d* größter gemeinsame Teiler von *a*,*b* , so ist *d'* genau dann größter gemeinsamer Teiler von *a*,*b* , wenn *d* und *d'* assoziiert sind, d.h. wenn $d=\epsilon d'$ mit einer Einheit $\epsilon\in R$.

Obwohl also ein größter gemeinsamer Teiler ist nur bis auf Assoziiertheit eindeutig bestimmt ist, benutzt man die Schreibweise $d=\mathrm{ggT}(a,b)$.

b) Zeigen Sie: *d* ist genau dann größter gemeinsamer Teiler von *a*,*b* , wenn auf der Idealebene $<d>=<a,b>$, wobei wie üblich $<a,b>:=\{ra+sb \mid r,s\in R\}$

Man kann also nur in Hauptidealringen von der Existenz eines größten gemeinsamen Teilers beliebiger Elemente ausgehen.

Aufgabe 3

Man nennt einen Integritätsring *R euklidisch* , wenn es eine Abbildung $d: R-\{0\}\to\mathbb{N}$ gibt mit der Eigenschaft $\forall a,b\in R, b\neq 0 \;\; \exists q,r\in R: a=qb+r$ mit $r=0$ oder $d(r)<d(b)$.

Setzt man z.B. In $\mathbb{Z}$ $d(n):=|n|$, so handelt es sich bei obiger Formel um die bekannte "Division mit Rest". Wie $\mathbb{Z}$ sind auch $\mathbb{Z}[i]$ und $\mathbb{Z}[\omega]$ Unterringe von $\mathbb{C}$; damit die Abbildung d ganzzahlige Werte erhält, wählt man hier $d(z)=|z|^2=z\bar{z}$. Auch der Polynomring $K[X]$ über einem Körper wird zu einem Euklidischen Ring, wenn man $d(f)=\mathrm{grad}(f)$ setzt. Den Divisionsalgorithmus mit Rest für Polynome lernt man i.a. in der Schule.

In der Schule lernt man ebenfalls den größten gemeinsamen Teiler zweier natürlicher Zahlen *a,b* zu bestimmen, indem man die eindeutigen Primfaktorzerlegungen $a=\prod_p p^{\alpha_p}$, $b=\prod_p p^{\beta_p}$ ausrechnet, dann $\gamma_p:=\min\{\alpha_p,\beta_p\}$ setzt, so daß $c:=\prod_p p^{\gamma_p}$ der größte gemeinsame Teiler von *a,b* wird.

Dieser Algorithmus setzt voraus, daß man die obigen Primfaktorzerlegungen tatsächlich finden kann, was für hinreichend große Zahlen schnell schwierig bis unmöglich wird.

In einem Euklidischen Ring gibt es eine viel effektivere Methode, einen größten gemeinsamen Teiler zu finden:

Euklidischer Algorithmus

Man konstruiert rekursiv eine Folge (r_n) , indem man $r_0:=a$, $r_1:=b$ setzt , dann eine Division mit Rest ausführt und so das nächste Folgenglied bestimmt: $r_{n-1}=q_n r_n+r_{n+1}$.

Da $1\leqslant d(r_n)<\ldots<d(r_1)$, muß der Rest r_{n+1} in obiger Division irgendwann Null werden. Dann ist $r_n=\mathrm{ggT}(a,b)$! Man bricht also die Folge (r_n) ab, sobald ein Folgenglied Null wird. Das Folgenglied davor ist dann der gesuchte ggT.

a) Man bestimme auf diese Weise ggT(128535,79439) in $\mathbb{Z}$.
b) Ebenso in $\mathbb{Z}[i]$: ggT(293+382i,181+235i)

Erweiterter Euklidischer Algorithmus

Wie man in 2b) sieht, muß es eine Darstellung $ra+sb=\mathrm{ggT}(a,b)$ geben. In einem Euklidischen Ring kann man eine solche relativ einfach finden:

In der obigen Rekursion entsteht neben der Restefolge (r_n) auch die Quotientenfolg (q_n)

Man setze $s_0:=1,\ s_1:=0,\ t_0:=0,\ t_1:=1$ und nun analog zur Kontrunktion von r_{n+1} rekursiv $s_{n+1}:=s_{n-1}-q_n s_n$ und $t_{n+1}:=t_{n-1}-q_n t_n$. Durch Induktion beweist man sehr einfach

$$r_n=s_n r_0+t_n r_1=s_n a+t_n b$$

und hat daher für denjenigen Index *n* , für den $r_n=\mathrm{ggT}(a,b)$: $\mathrm{ggT}(a,b)=s_n\cdot a+t_n\cdot b$

Man bestimme demgemäß
c) eine ganzzahlige Lösung der Gleichung $\mathrm{ggT}(128535,79439)=128535\mathrm{x}+79439\mathrm{y}$
d) Eine Lösung von $\mathrm{ggT}(293+382\mathrm{i},181+235\mathrm{i})=x\cdot(293+382\mathrm{i})+y\cdot(181+235\mathrm{i})$ in $\mathbb{Z}[i]$.