Rückblick: Ringtheorie

- Definition der Ringe (additive abelsche Gruppe, multiplikatives abelsches Monoid, Distributivgesetz)
- Grundbegriffe: Ringhomomorphismus, Einheit, Nulteiler, Charakteristik, Integritätsbereich, Körper
- Definition der Teilringe (Ringeigenschaft), von einer Teilmenge $A \subseteq \tilde{R}$ über R erzeugter Teilring $R[A]$
- Ideale und ihre Erzeugendensysteme (Nullideal, Einheitsideal, Hauptideal, Primideal, maximales Ideal)
- Teilbarkeitsbegriff und Beziehung zur Idealtheorie

Rückblick: Ringtheorie

- Definition der Faktorringe R/I
  (für einen Ring R und ein Ideal $I \subseteq R$)
- Konstruktion von Ringerweiterungen durch Monomorphismen
  (Anwendungen: komplexe Zahlen, Quotientenkörper, Polynomringe)
- euklidische Ringe (Ringe mit Division mit Rest)
- neu: faktorielle Ringe
  (Ringe mit eindeutiger Primfaktorzerlegung)

Definition (12.1)

Die Normfunktion $N : \mathbb{C} \to \mathbb{R}_+$ ist definiert durch

$$N(z) \quad = \quad z\bar{z} \quad = \quad |z|^2 \quad \text{für alle} \quad z \in \mathbb{C}.$$

Die wichtigste Eigenschaft der Normfunktion ist die Multiplikativität: Für alle $z, w \in \mathbb{C}$ gilt $N(zw) = N(z)N(w)$.

Die Normfunktion auf den quadratischen Teilringen

Lemma (12.2)

Sei $d \in \mathbb{N}$. Schränkt man die Normfunktion auf die Elemente des Rings $\mathbb{Z}[\sqrt{-d}]$ bzw. $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$ ein, so erhält man ausschließlich Werte in $\mathbb{N}_0$. Genauer gilt:

(i) Ist $\alpha \in \mathbb{Z}[\sqrt{-d}]$, $\alpha = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$, dann ist

$$N(\alpha) = a^2 + db^2.$$

(ii) Gilt $(-d) \equiv 1 \mod 4$, $R = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})]$ und ist $\alpha = \frac{1}{2} + \frac{1}{2}b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$, $a \equiv b \mod 2$, dann ist

$$N(\alpha) = \tfrac{1}{4}a^2 + \tfrac{1}{4}db^2.$$

Sind α, β im Fall (i) oder (ii) jeweils Elemente des Rings R und gilt $\alpha \mid \beta$, dann ist $N(\alpha)$ ein Teiler von $N(\beta)$ im Ring $\mathbb{Z}$.

Definition der euklidischen Ringe

Definition (12.3)

Eine Höhenfunktion auf einem Integritätsbereich R ist eine Abbildung $h : R \setminus \{0_R\} \to \mathbb{N}$ mit der folgenden Eigenschaft: Sind $a, b \in R$, $b \neq 0_R$, dann gibt es Elemente $q, r \in R$, so dass die Gleichung

$$a \quad = \quad qb + r$$

erfüllt ist und außerdem entweder $r = 0_R$ oder $h(r) < h(b)$ gilt. Ein euklidischer Ring ist ein Integritätsbereich, auf dem eine Höhenfunktion existiert.

Beispiele für euklidische Ringe

Proposition (12.4)

(i) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein euklidischer Ring, denn die Abbildung $h : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ gegeben durch $h(a) = |a|$ ist eine Höhenfunktion auf diesem Ring.

(ii) Sei K ein Körper. Dann ist der Polynomring $K[x]$ ein euklidischer Ring mit der Höhenfunktion gegeben durch die Gradabbildung, also $h(f) = \mathrm{grad}(f)$ für alle $f \in K[x] \setminus \{0_K\}$.

(iii) Der Ring $\mathbb{Z}[i]$ ist ein euklidischer Ring, wobei eine Höhenfunktion durch die auf $\mathbb{Z}[i] \setminus \{0\}$ eingeschränkte Normfunktion gegeben ist.

wichtiger Hinweis:
Die meisten quadratischen Zahlringe sind keine euklidischen Ringe, zum Beispiel $\mathbb{Z}[\sqrt{-3}]$ und $\mathbb{Z}[\sqrt{-5}]$ nicht.

Euklidische Ringe sind Hauptidealringe

Erinnerung:
Ein Hauptidealring ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

Satz (12.8)

Jeder euklidische Ring R ist ein Hauptidealring.

Also sind insbesondere $\mathbb{Z}$, $\mathbb{Z}[i]$ und Polynomringe über Körpern Hauptidealringe.

Beispiel für einen Nicht-Hauptidealring

Nicht jeder Integritätsbereich ist ein Hauptidealring.

Proposition (12.9)

Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring, denn beispielsweise ist das Ideal $\mathfrak{p} = (3, 1 + 2\sqrt{-5})$ kein Hauptideal.

Beweis von Proposition 12.9:

Beh.: Das Ideal $\mathfrak{p} = (3, 1+2\sqrt{-5})$ ist <u>kein</u> Hauptideal im Ring $R = \mathbb{Z}[\sqrt{-5}]$.

Ang.: $\alpha \in R$ ist ein Element mit $\mathfrak{p} = (\alpha)$. $\rightarrow$

$(3, 1+2\sqrt{-5}) = (\alpha) \rightarrow 3 \in (\alpha)$ und $1+2\sqrt{-5} \in (\alpha)$

$\rightarrow \alpha \mid 3$ und $\alpha \mid (1+2\sqrt{-5}) \rightarrow N(\alpha) \mid N(3)$, $N(\alpha)$ teilt $N(1+2\sqrt{-5})$ $\quad N(3) = 3^2 = 9$, $N(\alpha) = 1^2 + 2^2 \cdot 5 = 21$

$\rightarrow N(\alpha) \mid ggT(9, 21) \rightarrow N(\alpha) \mid 3 \underset{N(\alpha) \in \mathbb{N}}{\Rightarrow} N(\alpha) \in \{1, 3\}$

1. <u>Fall</u>: $N(\alpha) = 3$ Schreibe $\alpha = a + b\sqrt{-5}$ mit $a, b \in \mathbb{Z}$

$\Rightarrow a^2 + 5b^2 = 3 \xrightarrow{b=0} a^2 = 3$ $\lightning$ da 3 kein Quadrat in $\mathbb{Z}$

2. Fall $N(\alpha) = 1 \Rightarrow \alpha\bar{\alpha} = 1 \Rightarrow 1 \in (\alpha) \Rightarrow 1 \in p$

$\rightarrow \exists \beta, \gamma \in R$ mit $1 = \beta \cdot 3 + \gamma \cdot (1 + 2\sqrt{-5})$ (*)

Schreibe $\beta = c + d\sqrt{-5}$, $\gamma = u + v\sqrt{-5}$ mit $c, d, u, v \in \mathbb{Z}$

$\Rightarrow 1 = (c + d\sqrt{-5}) \cdot 3 + (u + v\sqrt{-5}) \cdot (1 + 2\sqrt{-5}) =$

$(3c + u - 10v) + (3d + v + 2u) \cdot \sqrt{-5}$

Summe der Koeff.: $3c + 3u + 3d - 9v$, ist durch 3 teilbar, aber: $1 = 1 + 0\sqrt{-5}$, nicht durch 3 teilbar

Jedes Element in R hat eine eindeutige Darstellung der Form $r + s\sqrt{-5}$ mit $r, s \in \mathbb{Z}$. Also gibt es keine Elemente $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$, die (*) erfüllen.

Definition der irreduziblen Elemente

Definition (12.10)

Sei R ein Ring. Ein Element $p \in R$ wird irreduzibel genannt, wenn p weder eine Einheit noch Null ist und die Implikation

$$p = ab \quad \Rightarrow \quad a \in R^\times \text{ oder } b \in R^\times$$

für alle $a, b \in R$ erfüllt ist. Nichteinheiten ungleich Null, die nicht irreduzibel sind, bezeichnen wir als reduzible Ringelemente.

Definition der Primelemente

Definition (12.11)

Sei R ein Ring. Ein Element $p \in R$ heißt Primelement, wenn p weder eine Einheit noch Null ist und außerdem die Implikation

$$p \mid (ab) \quad \Rightarrow \quad p \mid a \quad \text{oder} \quad p \mid b \qquad \text{für alle } a, b \in R \text{ erfüllt ist.}$$

Satz (12.12)

In einem Integritätsbereich ist jedes Primelement irreduzibel.

Beweis von Satz 12.12:

geg.: Integritätsbereich R, $p \in R$ sei ein Primelement, z.zg.: p ist irreduzibel

p Primelement $\Rightarrow p \neq 0_R$, $p \notin R^\times$

Seien $a, b \in R$ mit $p = a \cdot b$ z.zg.:

$a \in R^\times$ oder $b \in R^\times$

$p = a \cdot b \rightarrow p \cdot 1_R = a \cdot b \rightarrow p \mid ab \overset{p \text{ prim}}{\Rightarrow} p \mid a$ oder $p \mid b$.

O.B.d.A. $p \mid a \Rightarrow \exists c \in R: a = pc$

einsetzen $\rightarrow p = pcb \overset{\text{Kürzungsregel}}{\Rightarrow} 1_R = cb$

$\rightarrow b \in R^\times$.

□

Irreduzibilität als Eigenschaft der Assoziiertenklasse

Notation:
Die Schreibweise $p \sim q$ bedeutet, dass zwei Ringelemente p und q zueinander assoziiert sind.

Proposition (12.13)

Sei R ein Integritätsbereich, und seien $p, q \in R$ mit $p \sim q$.

(i) Ist p irreduzibel, dann gilt dasselbe für q.

(ii) Ist p ein Primelement, dann ist auch q ein Primelement.

Proposition (12.14)

Im Ring $\mathbb{Z}$ der ganzen Zahlen sind die irreduziblen Elemente genau die Zahlen der Form $\pm p$, wobei p die Primzahlen durchläuft.

Beweis von Prop. 12.13 (ii)

geg.: Int.-bereich R, $p, q \in R$ mit $p \sim q$

Vor.: p ist prim z.zg.: q ist prim

$p \sim q \Rightarrow \exists \varepsilon \in R^\times$ mit $q = \varepsilon p$ ($\Rightarrow p = \varepsilon^{-1} q$)

zu überprüfen (1) $q \neq 0_R$, $q \notin R^\times$

(2) $\forall a, b \in R: q \mid ab \rightarrow q \mid a$ oder $q \mid b$

zu (1) Ang. $q = 0_R \Rightarrow p = \varepsilon^{-1} \cdot 0_R = 0_R$ ↯

Ang. $q \in R^\times \rightarrow p = \varepsilon^{-1} q \in R^\times$ ↯

zu (2) Seien $a, b \in R$ mit $q \mid ab \Rightarrow \exists c \in R$

$ab = cq \rightarrow ab = c\varepsilon p \rightarrow p \mid ab \overset{p \text{ prim}}{\Rightarrow}$

$p \mid a$ oder $p \mid b$, o.B.d.A. $p \mid a \rightarrow \exists d \in R$

□

mit $a = d\rho = d\varepsilon^{-1} q \Rightarrow q \mid a$. $\square$

2

3

1

$\Rightarrow$

Irreduzible Elemente in $\mathbb{Z}[\sqrt{-d}]$

Proposition (12.15)

Sei $d \in \mathbb{N}$, $R = \mathbb{Z}[\sqrt{-d}]$ und $\alpha \in R$ beliebig.

(i) Das Element α ist genau dann eine Einheit in R, wenn $N(\alpha) = 1$ ist.

(ii) Ist $N(\alpha)$ eine Primzahl, dann ist α in R irreduzibel.

(iii) Gilt $N(\alpha) = p^2$ mit einer Primzahl p, und besitzt die Gleichung $a^2 + db^2 = p$ keine Lösung mit $a, b \in \mathbb{Z}$, dann ist α ebenfalls ein irreduzibles Element.

Folgerung (12.16)

Sei $d \in \mathbb{N}$. Für die Einheitengruppe von $R = \mathbb{Z}[\sqrt{-d}]$ gilt $R^\times = \{\pm 1, \pm\sqrt{-1}\}$, falls $d = 1$ ist, ansonsten $R^\times = \{\pm 1\}$.

Anwendung:

Das Element $2 \in \mathbb{Z}[\sqrt{-3}]$ ist irreduzibel, aber nicht prim.

Beweis von Prop. 12.15

geg: $d \in \mathbb{N}$, $R = \mathbb{Z}[\sqrt{-d}]$, N Normfkt., $\alpha \in R$

zu i) Beh.: $\alpha \in R^\times \Leftrightarrow N(\alpha) = 1$

„$\Rightarrow$" $\alpha \in R^\times \to \exists \beta \in R$ mit $\alpha\beta = 1 \Rightarrow$

$N(\alpha)\,N(\beta) = N(\alpha\beta) = N(1) = 1$ $\overset{N(\alpha), N(\beta) \in \mathbb{N}}{\Rightarrow}$ da $\alpha, \beta \neq 0$

$N(\alpha) = N(\beta) = 1$ „$\Leftarrow$" $N(\alpha) = 1 \Rightarrow \alpha\bar{\alpha} = 1 \overset{\bar{\alpha} \in R}{\Rightarrow} \alpha \in R^\times$

zu ii) Vor.: $p = N(\alpha)$ ist Primzahl z.zg.: α ist irreduzibel

Es ist $\alpha \neq 0$ (sonst $p = N(\alpha) = 0$), $\alpha \notin R^\times$ (sonst $p = N(\alpha) = 1$ nach (i)). Seien $\beta, \gamma \in R$ mit $\alpha = \beta\gamma$.

z.zg.: $\beta \in R^\times$ oder $\gamma \in R^\times$. $N(\beta)\,N(\gamma) = N(\alpha) = p$

$N(\beta), N(\gamma) \in \mathbb{N}$, p Primzahl $\Rightarrow N(\beta) = 1$ oder $N(\gamma) = 1$

$\overset{i)}{\Rightarrow} \beta \in R^\times$ oder $\gamma \in R^\times$

zu iii) Vor. $N(\alpha) = p^2$, wobei $p \in \mathbb{N}$ Primzahl, es gibt keine $a, b \in \mathbb{Z}$ mit $p = a^2 + d b^2$.

Es ist $\alpha \neq 0$ und $\alpha \notin R^\times$, da sonst $N(\alpha) \in \{0, 1\}$, siehe oben

Seien $\beta, \gamma \in R$ mit $\alpha = \beta\gamma \Rightarrow p^2 = N(\alpha) = N(\beta\gamma) =$

$N(\beta)\, N(\gamma)$. Ang. $\beta, \gamma \notin R^\times \overset{i)}{\Rightarrow} N(\beta), N(\gamma) > 1$

$\Rightarrow$ neu $N(\beta) = N(\gamma) = p$ aber: Schreibe $\beta = a + b\sqrt{-d}$ mit $a, b \in \mathbb{Z}$. Dann folgt $p = N(\beta) = a^2 + d b^2$ $\lightning$ zur Vor.

□

Beh. (1) 2 ist irreduzibel in $\mathbb{Z}[\sqrt{-3}]$

(2) 2 ist kein Primelement in $\mathbb{Z}[\sqrt{-3}]$

zu (1) $N(2) = N(2+0\sqrt{-3}) = 2^2 + 0^2 \cdot 3 = 2^2$

(Primzahlquadrat) Ang. $\exists a,b \in \mathbb{Z}$ mit $a^2+3b^2 = 2$

$\overset{b=0}{\Rightarrow}$ $a^2 = 2$ ↯ (da 2 kein Quadrat in $\mathbb{Z}$)

Prop. 12.15 (iii) $\Rightarrow$ 2 irreduzibel in $\mathbb{Z}[\sqrt{-3}]$

zu (2) Es gilt $2 \cdot 2 = 4 = (1+\sqrt{-3})(1-\sqrt{-3})$

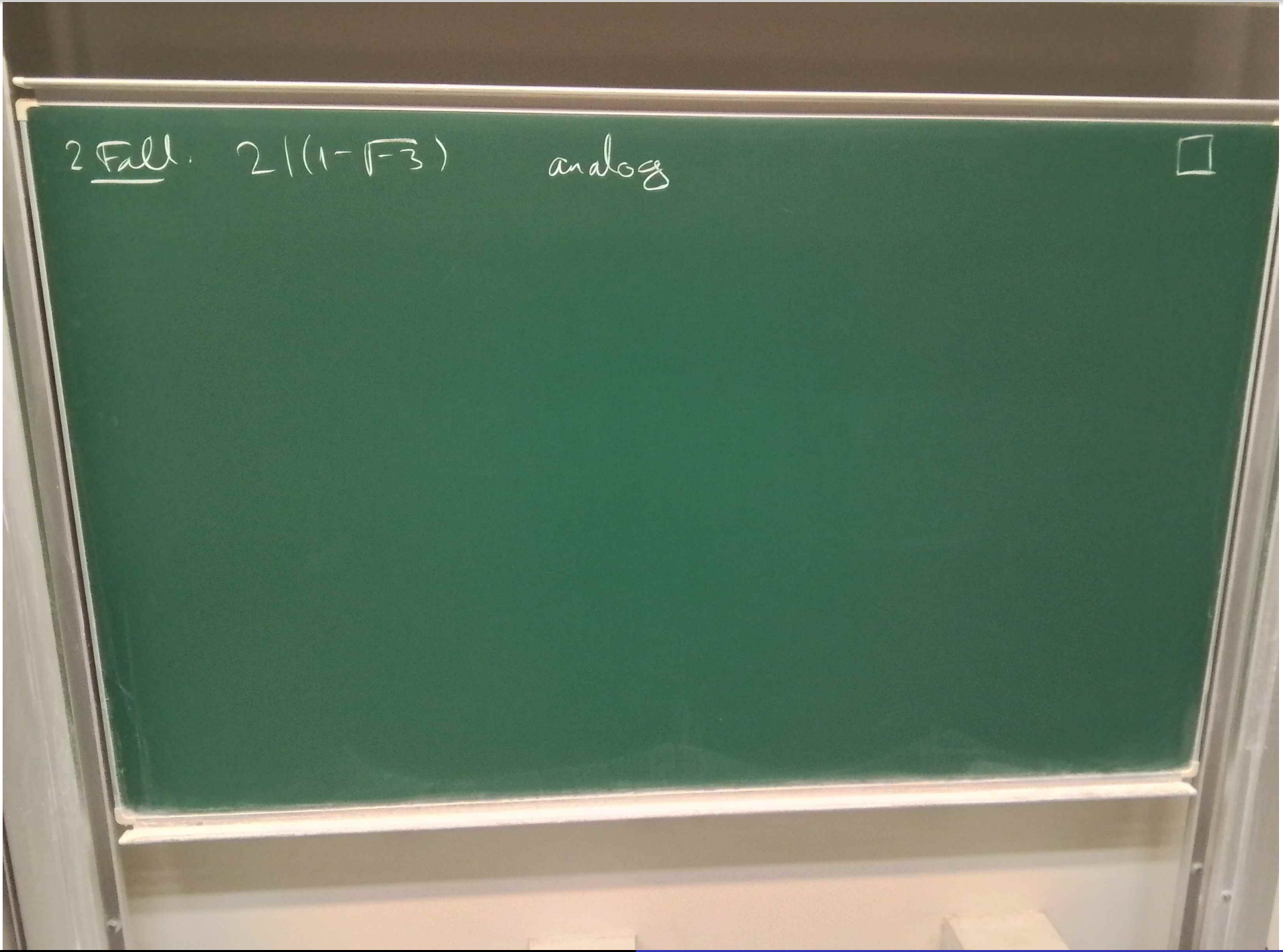
$\rightarrow 2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$ Ang. 2 ist prim. $\Rightarrow$

$2 \mid (1+\sqrt{-3})$ oder $2 \mid (1-\sqrt{-3})$

1. Fall: $2 \mid (1+\sqrt{-3}) \Rightarrow \exists \gamma \in \mathbb{Z}[\sqrt{-3}]$ mit

$1+\sqrt{-3} = 2\gamma \Rightarrow \gamma = \frac{1}{2}(1+\sqrt{-3})$ ↯ da

$\frac{1}{2}(1+\sqrt{-3}) \notin \mathbb{Z}[\sqrt{-3}]$


2 Fall. $2 \mid (1-\sqrt{-3})$ analog
□

Ideale in Hauptidealringen

Proposition (12.17)

Sei R ein Integritätsbereich und $p \in R$, $p \neq 0_R$. Genau dann ist p ein Primelement in R, wenn das Hauptideal (p) ein Primideal ist.

Satz (12.18)

Sei R ein Hauptidealring, aber kein Körper, und $p \in R$. Dann sind die folgenden Aussagen äquvialent.

(i) Das Element p ist prim.

(ii) Das Element p ist irreduzibel.

(iii) Das Ideal (p) ist maximal.

(iv) Das Ideal (p) ist ein Primideal, und es gilt $p \neq 0_R$.

Beweis von Prop. 12.17:

ggg: Integritätsbereich R, $p \in R \setminus \{0_R\}$

Beh: p ist prim $\Leftrightarrow$ (p) ist Primideal

„$\Rightarrow$" zu überprüfen (1) $(p) \neq (1_R)$

(2) $\forall a, b \in R: ab \in (p) \Rightarrow a \in (p)$ oder $b \in (p)$

zu (1) Ang. $(p) = (1_R) \Rightarrow 1_R \in (p) \Rightarrow \exists c \in R$ mit $1_R = pc \Rightarrow p \in R^\times$ ↯ zu p prim.

zu (2) Seien $a, b \in R$ mit $ab \in (p) \Rightarrow$ $\exists c \in R$ mit $ab = pc \Rightarrow p \mid ab \overset{p \text{ prim}}{\Rightarrow}$ $p \mid a$ oder $p \mid b$, o.B.d.A. $p \mid a \Rightarrow \exists d \in R$ mit $a = d \cdot p \Rightarrow a \in (p)$

„⇐": zu überprüfen: (3) $p \neq 0_R$, $p \notin R^\times$

(4) $\forall a,b \in R: p \mid ab \Rightarrow p \mid a$ oder $p \mid b$

zu (3) $p \neq 0_R$ gilt nach Vor. Ang. $p \in R^\times$.

$\Rightarrow \exists c \in R$ mit $1_R = c \cdot p \Rightarrow 1_R \in (p)$

$\Rightarrow (p) = (1_R)$ ↯ zu Vor.

zu (4) Seien $a,b \in R$ mit $p \mid ab$. $\Rightarrow \exists c \in R$ mit

$ab = c \cdot p \Rightarrow ab \in (p) \overset{\text{Vor.}}{\Rightarrow} a \in (p)$ oder $b \in (p)$,

o.B.d.A. $a \in (p) \Rightarrow \exists d \in R$ mit $a = d \cdot p \Rightarrow p \mid a$.

Bem.: In jedem Integritätsbereich R ist (0_R) ein Primideal, aber 0_R ist kein Primelement. □

Beweis von Satz 12.18.

geg R Hauptidealring, aber kein Körper, $p \in R$

„(i) $\Rightarrow$ (ii)" folgt aus Satz 12.12, da R ein Integritätsbereich ist

„(ii) $\Rightarrow$ (iii)" Vor.: p ist irred., z.zg.: (p) ist maximal

Es gilt $(p) \neq (1_R)$, da sonst $p \in R^\times$ ↯

Ang., es gibt ein Ideal I mit $(p) \subsetneq I \subsetneq (1_R)$

I Hauptideal $\Rightarrow \exists\, m \in R$ mit $I = (m)$

$(m) \subsetneq (1_R) \Rightarrow m \notin R^\times$ $\quad (p) \subseteq (m) \Rightarrow$

$p \in (m) \Rightarrow \exists\, c \in R$ mit $p = mc$ Ang

$c \in R^\times \Rightarrow m = c^{-1} p \Rightarrow m \in (p) \Rightarrow (m) \subseteq (p)$

$\Rightarrow$ gesamt $(p) = (m)$ $\lightning$ also: $p = mc$ mit $m, c \notin R^*$ $\lightning$ zur Irreduzibilität von p.

„(iii) $\rightarrow$ (iv)" Vor.: (p) maximal bereits bekannt: Jedes maximale Ideal ist ein Primideal.

Ang. $p = 0_R \rightarrow (0_R)$ ist max. Ideal $\Rightarrow$ $(0_R), (1_R)$ sind die einzigen Ideale in R, und $(0_R) \neq (1_R) \Rightarrow R$ ist Körper $\lightning$ zur Vor.

„(iv) $\Rightarrow$ i)" Vor.: (p) ist Primideal, $p \neq 0_R$ z.zg.: p ist Primelement. Dies folgt direkt aus Prop. 12.17.

(p), a.

□ □