Definition (9.1)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, genannt Addition und Multiplikation, so dass die folgenden Bedingungen erfüllt sind:

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(ii) Das Paar $(R, \cdot)$ ist ein kommutatives Monoid.

(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Definition der Ringhomomorphismen

Definition (9.2)

Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe. Eine Abbildung $\phi : R \to S$ heißt Ringhomomorphismus von $(R, +_R, \cdot_R)$ nach $(S, +_S, \cdot_S)$, wenn die Gleichung $\phi(1_R) = 1_S$ gilt und außerdem

$$\phi(a +_R b) = \phi(a) +_S \phi(b) \quad \text{und} \quad \phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$$

für alle $a, b \in R$ erfüllt ist.

Satz (9.3)

Für jeden Ring R existiert ein eindeutig bestimmter Ringhomomorphismus $\mathbb{Z} \to R$.

Beweis von Satz 9.3

geg ein Ring R. z.zg: Existenz und Eindeutigkeit eines Hom. $\mathbb{Z} \to R$

Existenz: Gruppentheorie $\Rightarrow$ Es gibt einen und bel. Gruppenhom. φ von $(\mathbb{Z}, +)$ nach $(R, +)$, der den Erzeuger 1 der zyklischen Gruppe $(\mathbb{Z}, +)$ auf 1_R abbildet (siehe § 3). Es gilt dann also $\varphi(m+n) = \varphi(m) + \varphi(n)$ $\forall m, n \in \mathbb{N}$, außerdem $\varphi(1) = 1_R$. noch z.zg: $\varphi(m \cdot n) = \varphi(m)\varphi(n)$ $\forall m, n \in \mathbb{Z}$. Zeige dies durch vollständige Ind. zunächst für $m \in \mathbb{Z}$

und $n \in \mathbb{N}_0$.

Ind.-Anf. Sei $m \in \mathbb{Z}$. $\varphi(m \cdot 0) = \varphi(0) = 0_R = \varphi(m) \cdot 0_R$ (φ Gruppenhom. $(\mathbb{Z},+) \to (R,+)$)
$= \varphi(m) \cdot \varphi(0)$

Ind.-schritt: Sei $m \in \mathbb{Z}$, $n \in \mathbb{N}_0$, setze die Gl. für n voraus.

$\varphi(m \cdot (n+1)) = \varphi(mn + m) = \varphi(mn) + \varphi(m) \overset{\text{Ind.-V.}}{=} \varphi(m)\varphi(n)$
$+ \varphi(m) \cdot 1_R = \varphi(m)\varphi(n) + \varphi(m)\varphi(1) = \varphi(m)(\varphi(n) + \varphi(1))$
$= \varphi(m) \cdot \varphi(n+1)$

Für jedes $n \in \mathbb{N}$ gilt auch $\varphi(m(-n)) = \varphi(-(mn)) \overset{\varphi \text{ Gruppenhom.}}{=} -\varphi(mn) \overset{\text{s.o.}}{=} -\varphi(m)\varphi(n) = \varphi(m)(-\varphi(n)) = \varphi(m)\varphi(-n)$

Also gilt $\varphi(mn) = \varphi(m)\varphi(n)$ für alle $m, n \in \mathbb{Z}$

Eindeutigkeit: folgt aus der Tatsache, dass φ als Gruppenhom. $(\mathbb{Z},+) \to (R,+)$ durch $\varphi(1)$ bereits eindeutig festgelegt ist. $\square$

Einheiten und Nullteiler

Definition (9.4)

Sei R ein Ring.

(i) Ein Element $a \in R$ heißt Einheit, wenn ein $b \in R$ mit $ab = 1_R$ existiert. Die Menge der Einheiten von R bezeichnen wir mit $R^\times$.

(ii) Man nennt es Nullteiler, wenn ein Element $b \in R$, $b \neq 0_R$ mit $ab = 0_R$ existiert.

Die Einheiten eines Rings R bilden eine Gruppe $R^\times$, die sogenannte Einheitengruppe.

Integritätsbereiche und Körper

Definition (9.5)

Ein Ring R mit 0_R als einzigem Nullteiler heißt Integritätsbereich.
Gilt $R^\times = R \setminus \{0_R\}$, dann ist R ein Körper.

Eigenschaften von Nullteilern und Einheiten

Lemma (9.6)

(i) Ein Element a in einem Ring R kann nicht zugleich Nullteiler und Einheit sein.

(ii) Jeder Körper ist ein Integritätsbereich.

(iii) In jedem Integritätsbereich R gilt die Kürzungsregel: Sind $a, b, c \in R$ mit $c \neq 0_R$, dann folgt aus $ac = bc$ die Gleichung $a = b$.

Die Injektivität der Körperhomomorphismen

Proposition (9.7)

Ein Körperhomomorphismus $\phi : K \to L$ ist stets injektiv.

Ein Ringhomomorphismus zwischen zwei Körpern wird auch Körperhomomorphismus genannt.

Beweis von Prop. 9.7

Sei $\phi : K \to L$ ein Körperhomomorphismus. Dann ist ϕ insb. ein Gruppenhom. $(K, +) \to (L, +)$. Für die Injektivität genügt es somit z.Zg., dass $\ker(\phi) \subseteq \{0_K\}$ gilt. Sei also $a \in \ker(\phi)$, ang. $a \neq 0_K$.

Grund 2.39., dass $\ker(\phi) \subseteq \{0_K\}$ gilt.

Dann existiert das Kehrwert $a^{-1} \in K^\times$, und

$1_L = \phi(1_K) = \phi(a \cdot a^{-1}) = \phi(a) \cdot \phi(a^{-1}) =$

$0_L \cdot \phi(a^{-1}) = 0_L$. Dies ist unmöglich, da L

ein Körper ist. $\lightning$ Also muss $a = 0_K$ gelten. $\square$

Die Charakteristik eines Rings

Definition (9.8)

Sei R ein Ring. Die Charakteristik eines Rings R ist definiert durch

$$\operatorname{char}(R) \quad = \quad \begin{cases} n & \text{falls } n \in \mathbb{N} \text{ minimal mit } n \cdot 1_R = 0_R \text{ ist,} \\ 0 & \text{falls } n \cdot 1_R \neq 0_R \text{ für alle } n \in \mathbb{N} \text{ gilt.} \end{cases}$$

Proposition (9.9)

Sei R ein Integritätsbereich. Dann ist die Charakteristik $\operatorname{char}(R)$ entweder gleich Null oder eine Primzahl.

Definition der Teilringe

Definition (9.10)

Sei R ein Ring. Eine Teilmenge $S \subseteq R$ wird Teilring von R genannt, wenn $1_R \in S$ gilt und mit $a, b \in S$ jeweils auch die Elemente $a - b$ und ab in S liegen.

Man bezeichnet einen Ring R als Erweiterungsring eines anderen Rings S, wenn S ein Teilring von R ist. Das Paar (S, R) bezeichnet man in diesem Fall als Ringerweiterung. Durch die Schreibweise $R|S$ wird ausgedrückt, dass (S, R) eine Ringerweiterung ist.

Teilringe sind Ringe

Satz (9.11)

Sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$ ein Teilring. Dann ist die Menge S unter den Verknüpfungen $+$ und $\cdot$ abgeschlossen. Bezeichnen wir mit $+_S$ und $\cdot_S$ die auf S eingeschränkten Verknüpfungen, dann ist $(S, +_S, \cdot_S)$ ein Ring.

Beweis von Satz 9.11:

geg.: Ring $(R, +, \cdot)$, $S \subseteq R$ Teilring,
d.h. $1_R \in S$, $\forall a, b \in S: a - b, a \cdot b \in S$
Abgeschlossenheit von S bzgl. $\cdot$ ist klar.
Voraussetzung gegeben
Nachweis der Abgeschlossenheit bzgl.
Addition: Seien $a, b \in S$, z.zg.: $a + b \in S$.

$a \in S \Rightarrow 0_R = a - a \in S$

$0_R \in S, b \in S \Rightarrow -b = 0_R - b \in S$

$a, -b \in S \Rightarrow a + b = a - (-b) \in S$

$0_R \in S, b \in S \Rightarrow -b = 0_R - b \in S$

Seien $+_S$ und $\cdot_S$ die Verknüpfungen auf S gegeben durch die Einschränkungen von $+$ und $\cdot$ zu überprüfen: (1) $(S, +_S)$ ist abelsche Gruppe

(2) $(S, \cdot_S)$ ist abelsches Monoid

(3) $\forall a, b, c \in S: a \cdot_S (b +_S c) = a \cdot_S b +_S a \cdot_S c$

Alle Eigenschaften werden von $(R, +, \cdot)$ geerbt!

Zum Beispiel in (3): Seien $a, b, c \in S$.

$a \cdot_S (b +_S c) = a \cdot (b + c) = a \cdot b + a \cdot c$

$= a \cdot_S b +_S a \cdot_S c$.

□

Durchschnitte von Teilringen sind Teilringe

Lemma (9.12)

Sei $(R, +, \cdot)$ ein Ring, und sei $(S_i)_{i \in I}$ eine Familie von Teilringen. Dann ist auch $S = \bigcap_{i \in I} S_i$ ein Teilring von R.

Definition der Teilkörper

Definition (9.13)

Sei K ein Körper. Eine Teilmenge $F \subseteq K$ wird Teilkörper von K genannt, wenn $1_K \in F$ gilt, für alle $a, b \in F$ auch die Elemente $a - b$ und ab in F liegen und für jedes $a \in F$, $a \neq 0_K$ auch $a^{-1} \in F$ gilt.

- Es ist leicht zu sehen, dass der durch F definierte Ring ein Körper ist.
- Die Begriffe Erweiterungskörper und Körpererweiterung sind in genauer Analogie zu den Ringen definiert.

Definition des Primkörpers

Lemma (9.14)

Sei K ein Körper und $(F_i)_{i \in I}$ eine beliebige Familie von Teilkörpern. Dann ist auch $F = \bigcap_{i \in I} F_i$ ein Teilkörper von K.

Folgerung (9.15)

Ist K ein Körper und ist $(F_i)_{i \in I}$ die Familie aller Teilkörper von K, dann nennt man $P = \bigcap_{i \in I} F_i$ den Primkörper von K. Es handelt sich um den bezüglich Inklusion kleinsten Teilkörper von K.

- Es ist $\mathbb{Q}$ der gemeinsame Primkörper von $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.
- Der Körper $\mathbb{F}_p$ ist jeweils sein eigener Primkörper.
- Wir werden später sehen, dass der Primkörper jedes Körpers isomorph zu $\mathbb{Q}$ oder zu $\mathbb{F}_p$ für eine Primzahl p ist.

Definition des erzeugten Teilrings

Satz (9.16)

Sei $\tilde{R}|R$ eine Ringerweiterung und $A \subseteq \tilde{R}$ eine beliebige Teilmenge. Dann gibt es einen eindeutig bestimmten Teilring $R[A]$ von $\tilde{R}$ mit den folgenden beiden Eigenschaften.

(i) Es gilt $R[A] \supseteq R \cup A$.

(ii) Ist R' ein weiterer Teilring von $\tilde{R}$ mit $R' \supseteq R \cup A$, dann folgt $R' \supseteq R[A]$.

Damit ist $R[A]$ also der kleinste Teilring von $\tilde{R}$, der $R \cup A$ enthält. Man nennt ihn den von A über R erzeugten Teilring.

Konvention zur Verwendung des Wurzelzeichens:

Sei $d \in \mathbb{R}$.

- Ist $d \geq 0$, dann bezeichnet $\sqrt{d}$ die nicht-negative Quadratwurzel von d, d.h. das eindeutig bestimmte $x \in \mathbb{R}_+$ mit $x^2 = d$.
- Ist $d < 0$, dann bezeichnet $\sqrt{d}$ die (eind. best.) Quadratwurzel in $\mathbb{C}$ mit positivem Imaginärteil, z.B. $\sqrt{-3} = i\sqrt{3}$.

Achtung: Es gilt im Allg. nicht $\sqrt{ab} = \sqrt{a} \cdot \sqrt{b}$ für alle $a, b \in \mathbb{R}$. z.B. $a = -3$, $b = -5$

Dann ist $\sqrt{ab} = \sqrt{15}$, aber $\sqrt{-3} \cdot \sqrt{-5} = (i\sqrt{3}) \cdot (i\sqrt{5}) = -\sqrt{15}$.

Beispiel: Quadratische Zahlringe

Satz (9.17)

Sei $d \in \mathbb{Z}$ und $\sqrt{d} \in \mathbb{C}$ wie oben definiert.

(i) Es gilt $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

(ii) Ist $d \equiv 1 \mod 4$, dann gilt
$\mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})] = \{\frac{1}{2}a + \frac{1}{2}b\sqrt{d} \mid a, b \in \mathbb{Z}, a \equiv b \mod 2\}$.

Die Ringe dieser Form bezeichnen wir als quadratische Zahlringe.

Beweis von Satz 9.17 (i)

Sei $d \in \mathbb{Z}$ und $S = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$. Für den Nachweis von $\mathbb{Z}[\sqrt{d}] = S$ müssen wir überprüfen

(0) S ist Teilring von $\mathbb{C}$ (1) $S \supseteq \mathbb{Z} \cup \{\sqrt{d}\}$

(2) Ist R ein bel. Teilring von $\mathbb{C}$ mit $R \supseteq \mathbb{Z} \cup \{\sqrt{d}\}$ dann folgt $R \supseteq S$.

zu (0) überprüfe (i) $1 \in S$ (ii) $\forall \alpha, \beta \in S : \alpha - \beta, \alpha\beta \in S$

zu (i) klar, da $1 = 1 + 0\sqrt{d}$ (und $1, 0 \in \mathbb{Z}$)

zu (ii) Seien $\alpha, \beta \in S \rightarrow \exists r, s, t, u \in \mathbb{Z}$ mit

$\alpha = r + s\sqrt{d}$, $\beta = t + u\sqrt{d} \Rightarrow \alpha - \beta = (r - t) + (s - u)\sqrt{d}$

$\Rightarrow \alpha - \beta \in S$ (da $r - t, s - u \in \mathbb{Z}$) ebenso: $\alpha \cdot \beta =$

$(r + s\sqrt{d}) \cdot (t + u\sqrt{d}) = rt + st\sqrt{d} + ru\sqrt{d} + su(\sqrt{d})^2 =$

$(rt+sud)+(st+ru)\sqrt{d} \in S$ (da

$rt+sud \in \mathbb{Z}$ und $st+ru \in \mathbb{Z}$)

zu (1) Für jedes $a \in \mathbb{Z}$ gilt $a = a+0\cdot\sqrt{d} \in S$,

außerdem $\sqrt{d} = 0+1\cdot\sqrt{d} \in S$, insgesamt

$\mathbb{Z} \cup \{\sqrt{d}\} \subseteq S$.

zu (2) Sei R ein Teilring von $\mathbb{C}$ mit der

Eigenschaft $R \supseteq \mathbb{Z} \cup \{\sqrt{d}\}$.

z.Zg.: $S \subseteq R$ Sei $\alpha \in S$ $\Rightarrow$

$\exists a, b \in \mathbb{Z}$ mit $\alpha = a+b\sqrt{d}$.

$a, b \in \mathbb{Z}$, $\mathbb{Z} \subseteq R \Rightarrow a, b \in R$

$\sqrt{d} \in R$, $a, b \in R$, R ist ein Teilring von $\mathbb{C}$,

damit abgeschlossen unter Addition (!) und Multiplikation. Daraus folgt $b\sqrt{d} \in R$ und $\alpha = a + b\sqrt{d} \in R$ $\square$

Von einem Element erzeugte Teilringe

Proposition (9.18)

Sei $\tilde{R} \mid R$ eine Ringerweiterung und $c \in \tilde{R}$. Dann gilt

$$R[c] = \left\{ f(c) \;\middle|\; f \in R[x] \right\}.$$

Beispiel zu Prop. 9.18:

$\mathbb{Z}[\pi] = \{ f(\pi) \mid f \in \mathbb{Z}[x] \}$

typische Elemente: $3+\pi$, $5-\pi+7\pi^2$, ...

ebenso: $\mathbb{Z}[\sqrt{2}] = \{ f(\sqrt{2}) \mid f \in \mathbb{Z}[x] \}$ (*)

$5-\sqrt{2}+7(\sqrt{2})^2 = 19-\sqrt{2}$

Allgemein ist leicht zu sehen, dass die Menge (*) genau mit $\{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$ übereinstimmt:

Sei: $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x] \Rightarrow f(\sqrt{2}) =$

$\sum_{k=0}^{n} a_k (\sqrt{2})^k = \sum_{k=0}^{n} a_k c_k$, $c_k = \begin{cases} 2^l & \text{falls } k = 2l \text{ gerade} \\ 2^l\sqrt{2} & \text{falls } k = 2l+1 \text{ ungerade} \end{cases}$