# Ringe und Module

Im folgenden sind alle Ringe frei wählbar (nicht notwendigerweise kommutativ)

DEFINITION (1.1): Seien $R, S$ zwei Ringe. Eine Abbildung $f: R \to S$ heißt Ringhomomorphismus, wenn für alle $x, y \in R$ gilt

(1) $f(x+y) = f(x) + f(y)$,

(2) $f(xy) = f(x) \cdot f(y)$.

DEFINITION (1.2): Eine nichtleere Teilmenge $S$ eines Ringes $(R, +, \cdot)$ heißt Teilring, wenn

(1) $S$ ist Untergruppe von $(R, +)$

(2) $S$ ist bezüglich Multiplikation abgeschlossen.

SATZ (1.3): Seien $R, S$ zwei Ringe und die Abbildung $f: R \to S$ ein Ringhomomorphismus, dann ist $Bild(f)$ Teilring von $S$ .

BEWEIS: Wir zeigen die Bedingungen (1) und (2) der Definition (1.2)

(1) (UG1) $0 \in Bild(f)$ , da $f(0) = 0$

(UG2) Abgeschlossenheit bezüglich Addition:

Seien $f(x), f(y) \in Bild(f)$ Dann ist $f(x+y) = f(x) + f(y)$ nach der Bedingung (1) aus der Definition (1.1), und es ist offensichtlich, dass $f(x) + f(y)$ in $Bild(f)$ liegt.

(UG3) Existenz des Inversen bezüglich Addition:

Sei $f(x) \in Bild(f)$ . Wir zeigen dass $f(-x)$ ein Inverses zu $f(x)$ ist:

$0 = f(0) = f(x + (-x)) = f(x) + f(-x)$ .

(2) Seien $f(x), f(y) \in Bild(f)$ . Dann gilt $f(x) \cdot f(y) = f(xy)$ nach Bedingung (2) der Definition (1.1), und es ist offensichtlich, dass $f(x) \cdot f(y)$ in $Bild(f)$ liegt.

❑

DEFINITION (1.4):

Ein Ideal $a$ in einem Ring ist eine Untergruppe der additiven Gruppe von $R$ derart das $Ra \subseteq a$ , $aR \subseteq a$ .

DEFINTION (1.5):

Eine Teilmenge $I \subseteq R$ heißt *linkes Ideal* in $R$ , wenn $I \neq \emptyset$ und

(i) $x, y \in I \Rightarrow x + y \in I$

(ii) $x \in I \text{ und } r \in R \Rightarrow r \cdot x \in I$

NOTATION (1.6):
Wir schreiben $a \lhd R$ um zu verdeutlichen das $a$ ein Ideal in $R$ ist. In der Tat gilt, wenn ein Ideal $a$ 1 enthält, dann enthält $a$ alle $x \in R$ .
Wenn $R$ 1 enthält und $1 \in a$ , dann gilt $a = R$ . Jedes Ideal verschieden von $R$ heißt *echt.*
Beispiel: $2\mathbb{Z}$ ist Ideal in $\mathbb{Z}$ .

DEFINITION (1.7):
Sei $f : R \to S$ ein Ringhomomorphismus, dann heißt die Menge

$$Kern(f) = \{x \in R : f(x) = 0\}$$

Kern von f.

SATZ (1.8): $Kern(f)$ ist ein Ideal in $R$ und eine Untergruppe von $(R, +)$ .

BEWEIS:
Der Kern ist eine Untergruppe von $(R, +)$ , zeige

(UG1) $0 \in Kern(f)$ , da $f(0) = 0$ .

(UG2) Abgeschlossenheit bezüglich Addition:
Seien $x, y \in Kern(f)$ , das heißt $f(x) = 0, f(y) = 0$ , dann gilt mit der Bedingung (1) aus der Definition (1.1): $0 = 0 + 0 = f(x) + f(y) = f(x + y)$ , somit liegt auch $x + y$ im $Kern(f)$ .

(UG3) Existenz des Inversen bezüglich Addititon:
Sei $x \in Kern(f)$ . Zeige, dass $-x \in Kern(f)$ das Inverse von $x$ bezüglich Addition ist. Mit der Bedingung (1) aus der Definition (1.1) gilt: $0 = f(0) = f(x + (-x)) = f(x) + f(-x)$ , somit ist $-x \in Kern(f)$ .

Der Kern ist ein Ideal in $R$

(i) Da der $Kern(f)$ eine Untergruppe ist, gilt die Abgeschlossenheit bezüglich Addition.

(ii) Wenn $a \in Kern(f)$ , dann ist $f(a) = 0$ und es gilt für alle $x \in R$ , $f(ax) = f(a) \cdot f(x) = 0$ und $f(xa) = f(x) \cdot f(a) = 0$ (zeig beide Seiten weil $R$ nicht unbedingt kommutativ ist) somit sind $ax, xa \in Kern(f)$ . ❑

DEFINITION (1.9):
Sei $R$ ein Ring und $a$ ein Ideal in $R$ , dann bezeichne mit $R/a = \{r + a : r \in R\}$ die Menge der *Nebenklassen* von $a$ in $R$ . Nach Definition sind zwei Nebenklassen $r_1 + a$ und $r_2 + a$ gleich, nur dann wenn $r_1 - r_2$ in $a$ liegt.

DEFINTION (1.10):
Wir definiere die Multiplikation bzw die Addition bezüglich $R/a = \{r + a : r \in R\}$ :

$\cdot : (r_1 + a) \cdot (r_2 + a) = r_1 r_2 + a$

$+ : (r_1 + a) + (r_2 + a) = r_1 + r_2 + a$ , wobei $r_1, r_2 \in R$

SATZ (1.11): Die Menge $R/a$ bezüglich der Addition und der Multiplikation ist ein Ring.

BEWEIS: Zeige, dass $R/a$ ein Ring ist. Sei im folgenden $r_1, r_2, r_3, r \in R$ .

(i) Assoziativität bezüglich Addition:

$$(r_1+a)+[(r_2+a)+(r_3+a)]=(r_1+a)+(r_2+r_3+a)$$
$$=r_1+r_2+r_3+a=(r_1+r_2+a)+(r_3+a)=[(r_1+a)+(r_2+a)]+(r_3+a)$$

(ii) Existenz eines Nullelementes bezüglich Addition: Zeige $0$ ist Nullelement.

$$(r+a)+(0+a)=r+0+a=r+a=0+r+a=(0+a)+(r+a)$$

(iii) Kommutativität bezüglich Addition:

$$(r_1+a)+(r_2+a)=r_1+r_2+a=r_2+r_1+a=(r_2+a)+(r_1+a)$$

(iv) Existenz eines inversen Elementes bezüglich Addition: Zeige $-r$ ist Inverses. $(r+a)+((-r)+a)=r+(-r)+a=a=(-r)+(r)+a=((-r)+a)+(r+a)$

(v) Assoziativität bezüglich der Multiplikation:

$$(r_1+a)[(r_2+a)(r_3+a)]=(r_1+a)(r_2r_3+a)=r_1r_2r_3+a$$
$$=(r_1r_2+a)(r_3+a)=[(r_1+a)(r_2+a)](r_3+a)$$

Zusätzlich ist der Ring der Nebenklassen kommutativ:

(vi) Kommutativität bezüglich der Multiplikation:

$$(r_1+a)(r_2+a)=r_1r_2+a=r_2r_1+a=(r_2+a)(r_1+a)$$ ❑

BEMERKUNG (1.12):

$R/a$ ist wieder eine Gruppe, abelsch genauso wie die additive Gruppe von $R$ und der Homomorphismus $\lambda: R \to R/a$ ist ein Gruppenhomomorphismus.
Wir zeigen nun das eine Multiplikation so auf den Nebenklassen definiert werden kann, das $R/a$ zu einem Ring und die Abbildung $\lambda$ zu einem Ringhomomorphismus wird. In der Tat gibt es genau einen Weg dies zu tun.
Sei $x, y \in R$ , dann sind $\lambda(x), \lambda(y)$ Nebenklassen von $a$ , deren Produkt $\lambda(x)\cdot\lambda(y)=\lambda(xy)$ erfüllen muss, z.B.

$$(x+a)(y+a)=xy+a \quad (2)$$

Diese Gleichung sagt uns wie wir fortfahren müssen: Bei gegebenen Nebenklassen $\alpha, \beta$ ,wählen wir $x \in \alpha, y \in \beta$ und nehmen als Pordukt von $\alpha \, und \, \beta$ die Nebenklasse $xy+a$ . Um sicher zu gehen, dass diese Multiplikation wohldefiniert ist müssen wir zeigen, das die Multiplikation unabhängig von der Wahl von $x \, und \, y$ in ihren zugehörigen Nebenklassen ist.
BEWEIS: Seien $x', y'$ anders gewählte Elemente, dann ist $x'=x+u, y'=y+v$ , wobei $u, v \in a$ , und es folgt

$$x'y'=(x+u)\cdot(y+v)=xy+xv+uy+uv=xy+xv+u(y+v)=xy+xv+uy' .$$

Da $a$ ein Ideal ist, $xv+uy' \in a$ und daher liegt $x'y'$ in der selben Nebenklasse wie $xy$ ; folglich ist das Produkt (2) in der Tat wohldefiniert.
Nun ist es ein leichtes das Assoziativgesetz und die Distributivgesetze zu beweisen.
Demnach ist $R/a$ ein Ring; wenn $R$ kommutativ ist, dann auch $R/a$ .
Der Kern ist natürlich $a$ .

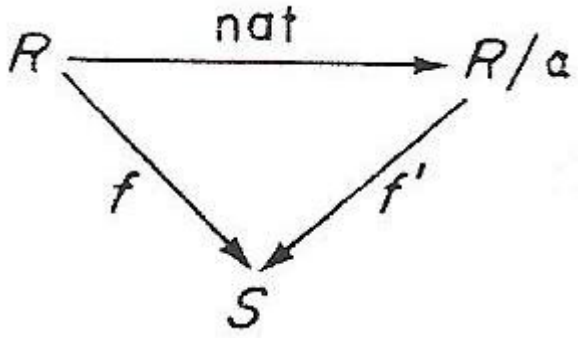
THEOREM 1(1.13):
Gegeben sei ein Ringhomomophismus $f: R \to S$ , sein Bild ist ein Teilring von $S$ und sein Kern ist ein Ideal von $R$ . Umgekehrt ist ein Ideal $a$ von $R$ gegeben, dann kann eine Ringstruktur auf der Menge der Nebenklassen $R/a$ definiert werden, in der art, dass die natürliche Abbbildung von $R$ nach $R/a$ ein Homomorphismus mit Kern $a$ ist. Weiterhin, wenn $R$ kommutativ ist, so auch $R/a$ . ■

DEFINITION (1.14):
Der Ring $R/a$ wird *Restklassenring* oder *Quotientenring* von $R$ für das Ideal $a$ genannt.

**Faktortheorem für Ringe (1.15)**
Gegeben seien $f: R \to S$ ein Ringhomomorphismus und $a \lhd R$ mit $a \subseteq Kern(f)$ , dann gibt es eine eindeutige Abbildung $f': R/a \to S$ , wie die Abbildung zeigt.

$$f' \text{ ist ein injektiver Ringhomomorphismus} \Leftrightarrow a = Kern(f)$$

■




**Erstes Isomorphismentheorem (1.16)**
Gegeben sei ein Ringhomomorphismus $f: S \to R$ , dann gilt

$$S/Kern(f) \cong Bild(f)$$

■

**Zweites Isomorphismentheorem (1.17)**
Sei $R$ ein Ring, $S$ ein Teilring und $A \lhd R$ ein Ideal, dann ist $A \cap S \lhd S$ und es gibt einen Isomorphismus

$$S/(S \cap A) \cong (S + A)/A \quad . \quad ■$$

BEWEIS :

1. zeige $A \cap S \lhd S$
2. beweise $S/(S \cap A) \cong (S + A)/A$

zu 1. Nutze die Bedingungen von $A \lhd R$ und vom Teilring $S$ .

(i) $x, y \in A \cap S \Rightarrow x, y \in A$ *und* $x, y \in S \Rightarrow x + y \in A$ *und* $x + y \in S \Rightarrow x + y \in A \cap S$
wobei $x + y \in A$ , weil $A \lhd R$ und $x + y \in S$ , weil $S$ Teilring ist und deswegen unter Addition abgeschlossen ist

(ii) $x \in A \cap S,\ s \in S \Rightarrow x \in A$ *und* $x \in S, s \in S \Rightarrow sx \in A$ *und* $sx \in S \Rightarrow sx \in A \cap S$
wobei $sx \in S$ , weil $S$ Teilring ist und somit abgeschlossen gegenüber

Multiplikation und $sx \in A$ , weil $A \lhd R$ und $S \subseteq R$ .
zu 2. Benutze das erste Isomorphismentheorem (10.1.10): Konstruiere eine Abbildung $f : S \to (S+A)/A$ mit $s \mapsto s+A$ und mit (10.1.10) gilt:
$S/S \cap A \cong (S+A)/A$ , wobei $S \cap A = Kern(f)$ und $(S+A)/A = Bild(f)$ seien.

$f$ ist Ringhomomorphismus, weil folgendes gilt:

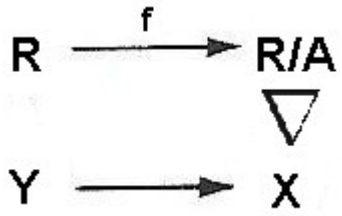
- $\forall s, x \in S : f(s)+f(x) = (s+A)+(x+A) = s+x+A = f(s+x)$
- $\forall s, x \in S : f(sx) = sx+A = (s+A)\cdot(x+A) = f(s)\cdot f(x)$
- $f(1) = 1+A$

Zeige nun $Bild(f) = (S+A)/A$ :Ein beliebiges Element von $(S+A)/A$ sieht wie folgend aus $(s+a)+A, wobei\ s \in S\ und\ a \in A$ dann gilt, aber auch $(s+a)+A = s+A = f(s)$ , somit ist ganz $(S+A)/A$ das $Bild(f)$ .
Weiterhin müssen wir noch zeigen, dass $Kern(f) = S \cap A$ :
$Kern(f) = \{s \in S : f(s) = 0+A\}$ somit sind alle $s \in S \cap A$ im $Kern(f)$ . ❑

**Drittes Isomorphismentheorem (1.18)**
Sei $R$ ein Ring und $a \lhd R$ . Dann entsprechen Teilringe (und Ideale) von $R/a$ in einer natürlichen Weise mit Teilringen ( und Idealen) von $R$ die $a$ enthalten und, wenn $b \supseteq a$ ein Ideal von $R$ ist entspricht das Ideal $b/a$ von $R/a$ diesem, dann

$$R/a/b/a \cong R/b \ . \quad \blacksquare$$

ERKLÄRUNG:
Sei $A \lhd R$ und $X \lhd R/A$ , dann entspricht $Y \lhd R$ dem Ideal $X$ auf folgende Weise (wobei $A \subseteq Y$ )




Nach der Definition, sei $Y$ ein Urbild von $X$ , also $Y = \{x \in R : f(x) \in X\}$
Zeigen wir $Y \lhd R$ :

$$x_1, x_2 \in Y \Rightarrow f(x_1), f(x_2) \in X$$

1. $Da\ X \lhd R/A\ ist\ gilt\ X \ni f(x_1)+f(x_2) = f(x_1+x_2) \Rightarrow x_1+x_2 \in Y$
2. $x \in Y, r \in R \Rightarrow f(xr) = f(x)\cdot f(r) \in X \Rightarrow xr \in Y \quad wobei\ f(x) \in X,\ f(r) \in R/A$

DEFINITION (1.19):
Ein Ideal von $R$ heißt *maximal* , wenn es maximal unter all den geeigneten Idealen ist.

DEFINITION (1.20):
Ein nicht tirvialer Ring $R$ , der keine Ideale außer $R$ und $0$ besitzt heißt *einfach*.

THEOREM 2 (1.21):
Sei $R$ ein Ring und $a$ ein Ideal in $R$, dann gilt

$$a \text{ ist maximal} \Leftrightarrow R/a \text{ ist einfach}$$

■

KOROLLAR (1.22):
Wenn $R$ ein kommutativer Ring ist und $a$ ein Ideal in $R$, dann gilt

$$a \text{ ist maximal} \Leftrightarrow R/a \text{ ist ein Körper}$$

■

DEFINITION UND NOTATION (1.23):
Im allgemeinen Ring $R$ sei eine Menge $\{a_i\}$ von Idealen in $R$ gegeben, der Schnitt $\cap a_i$ ist dann auch ein Ideal. Besonders wenn $X$ eine Teilmenge von $R$ ist, dann ist dieser Durchschnitt der Ideale , der $X$ enthält auch ein Ideal, das schwächste Ideal enthält $X$. Dieses Ideal erhalten wir auf eine genaue Art und Weise wie die Menge aller endlichen Summen

$$\alpha_1 x_1 \beta_1 + \cdots + \alpha_r x_r \beta_r \quad \text{, wobei } x_i \in X, \alpha_i, \beta_i \in R .$$

Es wird bezeichnet mit $RXR$ und genannt das *von X erzeugte Ideal*. Wenn $R$ kommutativ ist und $X$ endlich ist, sagt man $X = \{x_1, \ldots, x_r\}$, das von $X$ erzeugte Ideal besteht aus den Ausdrücken $x_1\alpha_1 + \cdots + x_r\alpha_r (\alpha_i \in R)$. In diesem Fall bezeichnen wir es mit $XR$ oder $\sum x_i R$, oder sogar $(x_1, \ldots, x_r)$. Besonders das von $x \in R$ erzeugte Ideal wird schrieben als $(x)$.

**10.2 Module über einem Ring**
Module sind einfache Verallgemeinerungen von abelschen Gruppen und Vektorräumen.

DEFINITION (2.1):
Es sei $R = (R, +, \bullet)$ ein Ring und sei $M = (M, +)$ eine abelsche Gruppe. Dann heißt $M$ zusammen mit einer äußeren Verknüpfung

$$\bullet : R \times M \to M$$
$$(\alpha, x) \mapsto \alpha \bullet x$$

ein $R$ *-Linksmodul,* wenn gilt

(M1) $(\alpha+\beta)\cdot x = \alpha\cdot x + \beta\cdot x$ (Distributivgesetz)
(M2) $\alpha\cdot(x+y) = \alpha\cdot x + \alpha\cdot y$
(M3) $(\alpha\cdot\beta)\cdot x = \alpha\cdot(\beta\cdot x)$ (Assoziativgesetz) $\forall \alpha, \beta \in R \text{ und } x, y \in M$

Analog gilt dies für $R$ *-Rechtsmodule* mit der äußeren Verknüpfung

$$\bullet : M \times R \to M$$
$$(x, \alpha) \mapsto x\cdot\alpha$$

NOTATION (2.2):
Sei $M$ ein Modul, dann bezeichnen wir ein $R$ - Linksmodul mit ${}_RM$ und entsprechend ein $R$ -Rechtsmodul mit $M_R$ .

DEFINTION (2.3):
Sei ${}_RM$ ein $R$ - Linksmodul und eine äußere Verknüpfung $\bullet : R \times M \to M$ . Eine nicht leere Menge $U \subseteq M$ heißt *Untermodul* von $M$ , wenn gilt:

(U1) $U$ ist Untergruppe von $(M, +)$ ,
(UG1) $0 \in U$
(UG2) $\forall\, x, y \in U \Rightarrow x + y \in U$
(UG3) $\forall\, x \in U \; \exists - x \in U$
(U2) $u \in U \text{ und } \alpha \in R \Rightarrow \alpha \cdot u \in U$ für Rechtsmodul $u \in U \text{ und } \alpha \in R \Rightarrow u \cdot \alpha \in U$

BEISPIELE (2.4):
(i) Jede abelsche Gruppe kann als ein $\mathbb{Z}$ -Modul angesehen werden; um mit n $(\geq 0)$ auf a zu arbeiten, addieren wir a n-mal zu sich selbst:

$$na = a + a + \cdots + a \qquad (n \text{ Terme } a), \qquad (1)$$

und für $n < 0$ , definieren wir $na$ mit $-(-n)a$ . Wir beachten, dass in diesem Fall Untermodul und Untergruppe das selbe sind:
Jedes Untermodul ist offenbar auch eine Untergruppe und umgekehrt enthält eine Untergruppe mit einem Element $a$ auch $na$ und $-na$ , und somit ein $\mathbb{Z}$ -Untermodul. Demnach können alle Ergebnisse, die für Module bewiesen wurden automatisch auch für abelsche Gruppen verwendet werden.

(ii) DEFINITIONEN UND BEMERKUNGEN (2.4.1):
Wenn $R$ ein beliebiger Ring ist, dürfen wir $R$ als ein $R$ -Rechtsmodul in Bezug auf die Multiplikation in $R$ ansehen. Wir bezeichnen das $R$ -Rechtsmodul mit $R_R$ .
Die Untermodule von $R_R$ heißen *rechte Ideale von* $R$ ;ein rechtes Ideal $a$ ist also eine Untergruppe der additiven Gruppe von $R$ , die $aR \subseteq a$ erfüllt.
Wir können $R$ auch als ein $R$ -Linksmodul unter der Multiplikation in $R$ ansehen. Wir schreiben dies so ${}_RR$ und die Untermodule von ${}_RR$ nennen wir *Linksideale.*
Ideale werden manchmal *zweiseitig* genannt im Gegensatz zu Links- und Rechtsidealen, die *einseitig* heißen.
Im kommutativen Fall verschwindet der Unterschied zwischen links-, rechts- und zweiseitigen Idealen und wir können ohne Risiko der Mehrdeutigkeit von Idealen sprechen.
(iii) Seien $R$ und $R^o$ Ringe, $R^o$ ist ein Ring mit der selben additiven Gruppenstruktur wie $R$ , aber mit der Multiplikation

$$a \circ b = ba \; .$$

Für einen kommutativen Ring ist da kein Unterschied zwischen $R$ und $R^o$, sie sind identisch unter der Abbildung, welche die grundlegenden Mengen identifiziert.
Gegeben sein ein Ring $R$, ein $R$-Linksmodul $M$ wird immer angesehen als ein $R^o$-Rechtsmodul, im ursprünglichem Sinne:
Wir definieren $x.a = ax (x \in M, a \in R)$; dann haben wir $(x.a).b = b(ax) = (ba)x = x.(ba) = x.(a \circ b)$, was uns zeigt das $M$ tatsächlich ein rechtes $R^o$-Modul ist. Auf die selbe Art wird das rechte $R$-Modul als linkes $R^o$-Modul angesehen.

(iv) Sei $R$ ein Ring, der frei wählbar sein kann, aber ist festgelegt durch die folgenden Bedingungen. Wenn $M, N$ beliebige $R$-Rechtsmodule sind und $f: M \to N$ ein Homomorphismus ist, ist er ein Homomorphismus von abelschen Gruppen mit $f(xa) = f(x)a \quad (x \in M, a \in R)$.
BEMERKUNG: $Kern(f), Bild(f)$ sind Untermodule jeweils von $M$ und $N$ sind.
BEWEIS: Zeige, dass $Kern(f), Bild(f)$ Untermodule jeweils von $M$ und $N$ sind.
(U1) (UG1) $0 \in Kern(f), da\ 0 = f(x) \cdot 0 = f(x0) = f(0), wobei\ x \in M, 0 \in R$
(UG2) $x, y \in Kern(f) \Rightarrow f(x) = 0, f(y) = 0:$
$0 = f(x) + f(y) = f(x+y) \Rightarrow x + y \in Kern(f)$
(UG3) $0 = f(0) = f(x-x) = f(x) + f(-x) \Rightarrow \exists -x \in Kern(f)$
(U2) mit der Bedingung von oben ist dies klar.
Für den Fall $Bild(f)$ ist Untermodul von $N$ geht der Beweis analog. ❑

DEFINITION (2.4.2):
Eine Folge von $R$-Modulen und Homomorphismen

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

gilt als *exakt in* $M_i$, wenn $Kern(f_i) = Bild(f_{i-1})$; die Folge wird dann *exakt* genannt wenn sie exakt in jedem Modul ist.

ANWENDUNG: *Homomorphismus* $f: M \to N$ *ist injektive* $\Leftrightarrow$

$$0 \to M \xrightarrow{f} N$$

*exakt ist*
*Homomorphismus* $f: M \to N$ *ist surjektive* $\Leftrightarrow$

$$M \xrightarrow{f} N \to 0$$

*exakt ist*

Während die Exaktheit von

$$0 \to M \xrightarrow{f} N \to 0$$

bedeutet, dass $f$ ein Isomorphismus ist.
Sei eine 3-Term exakte Folge gegeben (1)

$$0 \to M' \xrightarrow{\lambda} M \xrightarrow{\mu} M'' \to 0,$$

auch *kurze exakte Folge* genannt . Wenn in (1) $Bild(\lambda)=Kern(\mu)$ eine direkter Summand von $M$ ist, also $M=Bild(\lambda)\oplus A$ , wird die exakte Folge als *split* oder *exakt split* bezeichnet.

$$0 \to 3\mathbb{Z} \xrightarrow{id} \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \to 0$$

BEISPIEL:
Dies ist ein Beispiel für eine nicht split exakte Folge. Die Aussage ist hier, dass $3\mathbb{Z}$ kein direkter Summand von $\mathbb{Z}$ ist.

$$3\mathbb{Z}\oplus A\neq\mathbb{Z}$$

Dies folgt aus dem folgenden Satz.
SATZ:
$\mathbb{Z}$ kann nicht durch eine direkte Summe von zwei Untergruppen dargestellt werden: $\mathbb{Z}\neq A_1\oplus A_{2,}\, wobei\, A_1, A_2\neq 0$

BEWEIS:

- $A_{1,}A_2$ sind unendlich, da jede Untergruppe ungleich Null von $\mathbb{Z}$ unendlich ist und die Form $x\mathbb{Z}$ hat
- Der Schnitt von $A_1$ und $A_2$ besteht nicht nur aus $\{0\}$ ,denn $A_1=x_1\mathbb{Z}$ , $A_2=x_2\mathbb{Z}$ somit gilt $A_1\cap A_2=x_1\mathbb{Z}\cap x_2\mathbb{Z}$ und damit ist $x_1x_2\in A_1\cap A_{2,}\, wobei\, x_1x_2\neq 0$ . ❑

## 10.3 Kartesisches Produkte und Direkte Summen

ERKLÄRUNG:
Bezeichne das *Kartesische Produkt* mit $\prod_{i\in I} X_i$ und die *Direkte Summe* mit $\oplus_{i\in I} X_i$, wenn $i$ endlich ist sind Kartesisches Produkt und Direktes Summe das Selbe.

$$X_1 \oplus \cdots \oplus X_n = \{(x_1, \ldots, x_n) : x_i \in X_i\}$$

Falls $i$ unendlich ist, d.h. $\ldots, X_{-1}, X_0, X_1, \ldots$ Unterscheiden sich die Beiden wie folgend

$$\prod_{i\in I} X_i = \{(\ldots, x_{-1}, x_0, x_1, \ldots) : x_i \in X_i\}$$
$$\oplus_{i\in I} X_i = \{(0,\ldots,0, x_{-3}, 0, \ldots, 0, x_2, 0, \ldots, 0, x_9, 0, \ldots, 0) : x_i \in X_i\}$$

(d.h. die Menge aller $\infty$ Tupel, die nur eine endliche Anzahl von Elementen ungleich Null enthält)

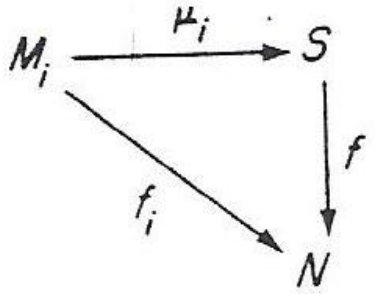
Gegeben sei eine Familie $(M_i)(i\in I)$ (d.h. Zum Beispiel gilt $M_1 = M_2$ )(nicht endlich) von Modulen, alle über dem selben Ring $R$, wir definieren eine Modulstruktur auf der theoretischen Menge des Kartesischen Produkts $P = \prod M_i$, durch das Ausführen aller Operationen komponentenweise. Also wenn $x = (x_i)$ ein typisches Element von $P$ ist, dann gilt

$$x + y = (x_i + y_i), \qquad xr = (x_i r) \qquad (r \in R),$$

und die kanonische Projektion $\varepsilon_i : x \mapsto x_i$ ist ein Homomorphismus von $P \to M_i$.

SATZ (3.1):
Gegeben sei eine Menge $(M_i)(i\in I)$ von $R$-Modulen, es existiert ein $R$-Modul $S$ mit Homomorphismen $\mu_i : M_i \to S$, so dass für jede Menge von Homomorphismen $f_i : M_i \to N$ ein eindeutiger Homomorphismus $f : S \to N$ existiert, so dass

$$f_i = f(\mu_i) \qquad \textit{für alle } i \in I. \qquad (1)$$

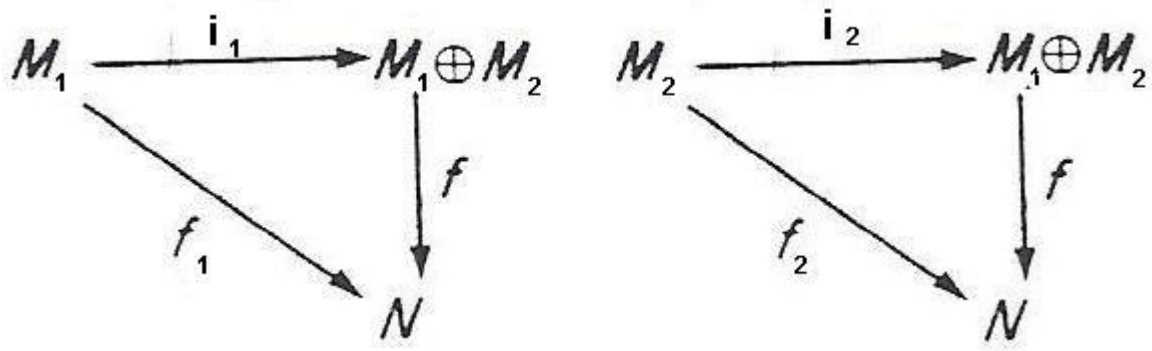



Um ein solches Modul $S$ zu finden, wird unser erster Versuch sein die direkte Summe und als Homomorphismus $\mu_i$, nimm die Einbettung $i_i(v) = (\ldots, v, \ldots)$ wobei dieses $v$ an der $i$-ten Stele im Tupel steht. Das Auffinden der Abbildung $f$ ist schwierig, es sei denn das die Index-Menge endlich ist, dann kann $f$ wie folgend definiert werden

$$f(\ldots, v_i, v_{i+1}, v_{i+2}, \ldots) = \sum f_i(v_i)$$

ERKLÄRUNG:
Sei nun $M_1, M_2$ gegeben und $i_1(m_1)=(m_1,0)$ *und* $i_2(m_2)=(0,m_2)$ sind Einbettungen in die direkte Summe $M_1 \oplus M_2$ . Dann ist die Funktion $f$ definiert mit

$$f(m_1, m_2)=f_1(m_1)+f_2(m_2)$$




Prüfe nach ob das Diagramm kommutiert.

$f_1(m_1)=f(i_1(m_1))=f((m_1,0))=f_1(m_1)+f_2(0)=f_1(m_1)$
$f_2(m_2)=f(i_2(m_2))=f((0,m_2))=f_1(0)+f_2(m_2)=f_2(m_2)$

PROPOSITION 1 (3.2):
Sei $R$ ein beliebiger Ring und $M$ ein $R$ -Modul.

$(M_i)$ *Menge von Untermodulen von M unabhängig* $\Leftrightarrow \sum x_i=0 \Rightarrow x_i=0 \; \forall i \in I$

Wobei aber endlich viele Elemente $x_i \in M_i$ nich-Null sind. ■

BEMERKUNGEN (3.3):
Beachten wir den Fall von einer endlichen Menge von Modulen $M_1,\ldots,M_n$ wo, die direkte Summe und das kartesische Produkt übereinstimmen und beide bezeichnet werden mit $M=\oplus_{i\in I} M_i$ . Wir haben die kanonische Injektion $\mu_i: M_i \to M$ und Projektionen $\varepsilon_i: M \to M_i$ und es ist leicht erkennbar, dass sie den folgenden Gleichungen genügen

$$\sum \mu_i(\varepsilon_i(x))=x \quad \sum \mu_i \varepsilon_i = 1_M \;, \quad \varepsilon_j(\mu_i(x))=\delta_{ij} id_M(x)=\delta_{ij} x \quad \varepsilon_i \mu_i = 1_M \;. \qquad (1)$$

Wenn wir die $\varepsilon$ s und die $\mu$ s als eine Zeile beziehungsweise als Spalte schreiben,

$$\varepsilon=(\varepsilon_1,\ldots,\varepsilon_n)^T \;, \qquad \mu=(\mu_1,\ldots,\mu_n) \;, \qquad (2)$$

können wir die Gleichungen (1) kürzer in Matrixschreibweise darstellen:

$$\mu\varepsilon = 1_M \;, \quad \varepsilon\mu=\begin{pmatrix}\varepsilon_1\\ \vdots \\ \varepsilon_n\end{pmatrix}(\mu_1,\ldots,\mu_n)=\begin{pmatrix}\varepsilon_1\mu_1 & \cdots & \varepsilon_1\mu_n \\ \vdots & & \vdots \\ \varepsilon_n\mu_1 & \cdots & \varepsilon_n\mu_n\end{pmatrix}=\begin{pmatrix}1_{M_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1_{M_n}\end{pmatrix} \;. \qquad (3)$$

Dies bringt uns zu einer anderen Charakterisierung der direkten Summe von endlichen Familien von Modulen.

PROPOSITION 2 (3.4):
Sein $R$ ein beliebiger Ring und $M, M_1, \ldots, M_n$ $R$-Module mit Homomorphismen $\mu_i: M_i \to M, \varepsilon_i: M \to M_i$ und seien $\varepsilon$ und $\mu$ wie in (2), dann $M$ *ist kartesisches Produkt (direkte Summe) von* $M_i \Leftrightarrow \varepsilon, \mu(3)$ *genügen* .

## 10.4 Freie Module

DEFINITION (4.1):
Sei $M$ ein Rechtsmodul über einen Ring $R$ . $M$ heißt *freies Modul* , wenn es eine Teilmenge $X \subseteq M$ gibt, sodass

(i) $\forall\, m \in M$ *existieren* $x_1, \ldots, x_n \in X$ *und* $r_1, \ldots, r_n \in R$ *, so dass* $m = x_1 r_1 + \ldots + x_n r_n$

(ii) *Die Elemente von X sind unabhängig über R ,* $d.h.\ x_1 r_1 + \ldots + x_n r_n \Rightarrow r_1 = \ldots = r_n = 0$ , wobei $n \in \mathbb{N}$

DEFINITIONEN UND BEMERKUNGEN (4.2):
Sei $R$ ein beliebiger Ring und $M$ ein $R$-Rechtsmodul. Wenn wir eine Teilmenge $X$ von $M$ gegeben haben, dann verstehen wir unter dem *Untermodul erzeugt von* $X$ , das kleinste Untermodul mit $X$ enthaltend, bezeichnet mit $XR$ oder $\langle X \rangle$ . In der Tat ist es nicht schwierig zu erkennen, dass die Menge aller endlichen linear Kombinationen in $X$ ,

$$XR = \{\sum x_i a_i \,|\, x_i \in X, a_i \in R\}$$

ein Untermodul mit $X$ enthaltend ist und natürlich enthält jedes Untermodul von $M$ $X$ und ebenfalls auch $XR$ , so dass $XR$ allerdings das kleinste Untermodul mit $X$ enthaltend ist. Wenn $XR = M$ nennen wir $X$ eine *erzeugende oder aufspannende Menge von* $M$ und sage weiterhin , dass $M$ der $Spann(X)$ ist.

BEMERKUNG (4.3):
Unter einer Basis von einem $R$-Modul $M$ versteht man eine Menge von Elementen, die linear unabhängig und $Spann(X)$ sind. Natürlich hat nicht jedes Modul eine Basis, z.B. eine zyklische Gruppe angesehen als ein $\mathbb{Z}$-Modul hat eine Basis genau dann wenn es endlich ist.

BEMERKUNGEN (4.4):
Im allgemeinen wird ein gegebenes freies Modul verschiedene Basen besitzen und der Wechsel von Basis ist einfach beschrieben durch Matrizen. Folglich wenn ein freies $R$-Rechtsmodul $M$ zwei endliche Basen $e_1, \ldots, e_m; f_1, \ldots, f_n$ besitzt, kann jede ausgedrückt werden durch eindeutige Terme der Anderen

$$f_\lambda = \sum e_i a_{i\lambda} \quad , \quad e_i = \sum f_\lambda b_{\lambda i} \quad , \quad (1)$$

wobei $i = 1, \ldots, m$ und $\lambda = 1, \ldots, n$ . Natürlich können wir in diesem Abschnitt nicht annehmen, dass $m = n$ ; bald sollten wir aber zeigen, dass in freien Modulen über einem kommutativen Ring alle Basen die selbe Anzahl an Elementen haben.
Von (1) bekommen wir bei Elimination der $f$ s,

$$e_i = \sum e_j a_{j\lambda} b_{\lambda i} \quad , \quad i, j = 1, \ldots., m; \lambda = 1, \ldots, n$$

folglich bei der linearen Unabhängigkeit der $e$ s finden wir $\sum a_{j\lambda} b_{\lambda i} = \delta_{ji}$ , das heißt beim Schreiben der Koeffizienten als eine Matrix : $A=(a_{i\lambda})$ , $B=(b_{\lambda i})$ , haben wir

$$AB = I_m \ ,$$

wobei $I_m$ die Einheitsmatrix der Größe $m$ ist. Bei Symmetrie gilt $BA = I_n$ . Folglich nehmen wir an , dass $m=n$ , wir sehen, dass der Wechsel von einer Basis eines freien Moduls zu einer Anderen beschrieben ist durch ein Paar selbstinverser Matrizen. Jetzt überprüfen wir, dass $m$ und $n$ tatsächlich gleich sind.

PROPOSITON 1 (4.5):
Sei $M$ ein freies Modul über einen nicht trivialen kommutativen Ring $R$ mit Eins, dann sind alle Basen von $M$ endlich, mit der selben Anzahl an Elementen.

BEWEIS (4.6):
Seien $\{e_1,\dots,e_m\}$ und $\{f_1,\dots,f_n\}$ zwei Basen von $M$ . Dann ist $m=n$ .
Man kann $f_1,\dots,f_n$ wie folgend darstellen

$$\begin{aligned} f_1 &= e_1 a_{1,1} + \dots + e_m a_{1,m} \\ &\vdots \\ f_n &= e_1 a_{n,1} + \dots + e_m a_{n,m} \end{aligned} \quad \text{, wobei } a_{i,j} \text{ } \textit{für } i=1,\dots,n, \ j=1,\dots,m \text{ } \textit{beliebig aber fest}$$

Durch umschreiben in Matrixschreibweise erhält man,

$$(f_1,\dots,f_n)=(e_1,\dots,e_m)\begin{pmatrix} a_{1,1} & \cdots & a_{n,1} \\ \vdots & \vdots & \vdots \\ a_{1,m} & \cdots & a_{n,m} \end{pmatrix} \quad \text{, sei} \quad A=\begin{pmatrix} a_{1,1} & \cdots & a_{n,1} \\ \vdots & \vdots & \vdots \\ a_{1,m} & \cdots & a_{n,m} \end{pmatrix}$$

$$(e_1,\dots,e_m)=(f_1,\dots,f_n)\begin{pmatrix} b_{1,1} & \cdots & b_{m,1} \\ \vdots & \vdots & \vdots \\ b_{1,n} & \cdots & b_{m,n} \end{pmatrix} \quad \text{, sei} \quad B=\begin{pmatrix} b_{1,1} & \cdots & b_{m,1} \\ \vdots & \vdots & \vdots \\ b_{1,n} & \cdots & b_{m,n} \end{pmatrix}$$

setzte jetzt ein, damit ergibt sich

$$(f_1,\dots,f_n)=(f_1,\dots,f_n)\begin{pmatrix} b_{1,1} & \cdots & b_{m,1} \\ \vdots & \vdots & \vdots \\ b_{1,n} & \cdots & b_{m,n} \end{pmatrix}\begin{pmatrix} a_{1,1} & \cdots & a_{n,1} \\ \vdots & \vdots & \vdots \\ a_{1,m} & \cdots & a_{n,m} \end{pmatrix}$$

und $BA=\begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \vdots & \vdots \\ c_{n,1} & \cdots & c_{n,n} \end{pmatrix}$ , somit ist

$$\begin{aligned} f_1 &= f_1 c_{1,1} + \dots + f_n c_{n,1} \\ &\vdots \quad \vdots \\ f_n &= f_1 c_{1,n} + \dots + f_n c_{n,n} \end{aligned}$$ dies ist erfüllt durch die Matrix

$$BA=\begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \vdots & \vdots \\ c_{n,1} & \cdots & c_{n,n} \end{pmatrix}=\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Sei nun $n>m$ , dann erweitere die Matrix $B$ um $n-m$ Spalten und die Matrix

$A$ ebenfalls um $n-m$ Zeilen von Nullen:

$$B_1=(B\,0) \quad , \quad A_1=\begin{pmatrix} A \\ 0 \end{pmatrix} \ ,$$

somit gilt

$$B_1 A_1=\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

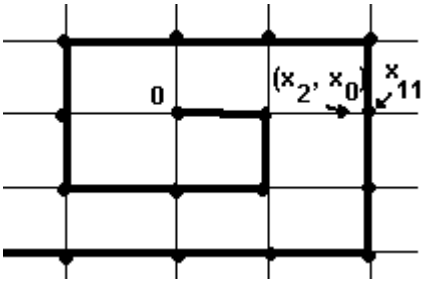
Dann ist $B_1 A_1=BA=I$ , folglich $det(B_1).det(A_1)=det(B_1 A_1)=1$ , aber $det(B_1)=0$ , $det(A_1)=0$ , weil $A_1$ eine Nullzeile und $B_1$ eine Nullspalte hat, das ist ein Widerspruch ( weil $1\neq 0$ in $R$ ist ). ■

BEMERKUNG:
Dieses Ereignis kann erweitert werden zu freien Modulen, die nicht endlich erzeugt sind und für diese Module haben alle Basen die selbe Kardinalität für alle Ringe ohne Ausnahme.

**BEISPIELAUFGABE:**
Modulbasen haben durchaus verschiedene Mächtigkeiten.
Ziel: Konstruiere einen Ring $R$ , so dass $R\cong R\oplus R$ ist. Danach betrachten wir $R$ und $R\oplus R$ als $R$ -Module. Das zeigt, dass $R\cong R\oplus R$ zwei verschiedene Dimensionen hat, nämlich $1$ und $2$ über $R$ .

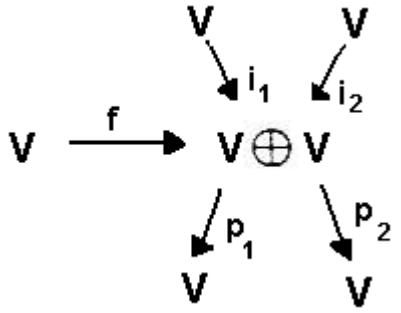
Allgemein: Sei $V$ ein Vektorraum über $K$ mit der Basis $\{x_i : i\in\mathbb{Z}\}$ und $W=V\oplus V$ ebenfalls ein Vektorraum mit Basis $\{(x_i, x_j) : i, j\in\mathbb{Z}\}$ . Da $V$ und $W$ gleich große Mengen sind, gibt es einen Isomorphismus $f: V\to W=V\oplus V$ .

(zu Erklärung:




)

Definiere nun zwei Einbettungen und zwei Projektionen, so dass folgendes gilt:




wobei $i_1(v)=(v,0),\ i_2(v)=(0,v)$ *und* $p_1((v_1,v_2))=v_1,\ p_2=((v_1,v_2))=v_2$

<u>Speziell für $R$ :</u>
Nun definiere $R=End(V)=Hom(V,V)=alle\,linearen\,Abb.\,von\,V\,nach\,V$ , somit ist $R$ ein Ring . Zeige nun noch das ein Ringisomorphismus $\varphi$ existiert mit
$\varphi: R\oplus R\to R$ mit
$$\varphi(r_1\oplus r_2)(v)=r_1\,p_1\,f(v)+r_2\,p_2\,f(v)\quad\in V \text{ , wobei } r_1,r_2\in R$$

Zur Erklärung: $\varphi(r_1\oplus r_2)\in R$ und $\varphi(r_1\oplus r_2)(v)\in V$ , weil
$$\varphi(r_1\oplus r_2)(v)=\underbrace{r_1\,\underbrace{p_1\,\underbrace{\underbrace{f(v)}_{V\oplus V}}_{V}}_{V}}_{V}+\underbrace{r_2\,\underbrace{p_2\,\underbrace{\underbrace{f(v)}_{V\oplus V}}_{V}}_{V}}_{V}\in V$$

Beweis:
Zeige 1) $\varphi((r_1\oplus r_2)+(r_1'\oplus r_2'))=\varphi(r_1\oplus r_2)+\varphi(r_1'\oplus r_2')$ , wobei $r_1,r_2,r_1',r_2'\in R$
2) $\varphi(r(r_1\oplus r_2))=r\,\varphi(r_1\oplus r_2)$ , wobei $r,r_1,r_2\in R$
3) $Kern(\varphi)=0\Rightarrow Injektivität$
4) $Bild(\varphi)=R\Rightarrow Surjektivität$

zu 1)
$\varphi(r_1\oplus r_2)(v)+\varphi(r_1'\oplus r_2')(v)=r_1\,p_1\,f(v)+r_2\,p_2\,f(v)+r_1'\,p_1\,f(v)+r_2\,p_2\,f(v)$
$\Leftrightarrow\quad \varphi(r_1\oplus r_2)(v)+\varphi(r_1'\oplus r_2')(v)=(r_1+r_1')\,p_1\,f(v)+(r_2+r_2')\,p_2\,f(v)$
$\Leftrightarrow\quad \varphi(r_1\oplus r_2)(v)+\varphi(r_1'\oplus r_2')(v)=\varphi(r_1+r_1'\oplus r_2+r_2')(v)$
$\Leftrightarrow\quad \varphi(r_1\oplus r_2)(v)+\varphi(r_1'\oplus r_2')(v)=\varphi((r_1\oplus r_2)+(r_1'\oplus r_2'))(v)$
zu 2)
$\varphi(r(r_1\oplus r_2))(v)=\varphi(r\,r_1\oplus r\,r_2)(v)=r\,r_1\,p_1\,f(v)+r\,r_2\,p_2\,f(v)=r[r_1\,p_1\,f(v)+r_2\,p_2\,f(v)]$
$\Leftrightarrow\quad \varphi(r(r_1\oplus r_2))(v)=r\,\varphi(r_1\oplus r_2)(v)$

zu 3) $Kern(\varphi)=\{(r_1\oplus r_2):\ \varphi(r_1\oplus r_2)=e\ \in R\}=\{(r_1\oplus r_2):\ \varphi(r_1\oplus r_2)(v)=0\ \in V\}$

somit folgt $\varphi(r_1(v_1)+r_2(v_2))=0 \quad\Leftrightarrow\quad r_1(v_1)+r_2(v_2)=0$

wenn $v_1=0 \Rightarrow r_2(v_2)=0 \Rightarrow r_2=0 \ \forall v_2\in V$

wenn $v_2=0 \Rightarrow r_1(v_1)=0 \Rightarrow r_1=0 \ \forall v_1\in V$

Dann ist nur für $r_1=0$ und $r_2=0 \quad \varphi(r_1\oplus r_2)(v)=0$

Damit ist $Kern(\varphi)=\{(0\oplus 0)\}$

zu 4) Sei $r\in R$ beliebiges Element , dann finde $r_1, r_2\in R$ , so dass $\varphi(r_1\oplus r_2)=r$ .

Setzte $r_1=r\,f^{-1}\,i_1$ und $r_2=r\,f^{-1}\,i_2$

$$\varphi(r_1\oplus r_2)(v)=r\,f^{-1}\,i_1\,p_1\,f(v)+r\,f^{-1}\,i_2\,p_2\,f(v)=r[f^{-1}(v_1,0)+f^{-1}(0,v_2)]=r[f^{-1}(v_1,v_2)]=r(v)$$

❑