Kommutative Algebra

Vorlesung von
Prof. Dr. Niko Naumann
im Sommersemester 2012
Überarbeitung und Textsatz in LyX von
Andreas Völklein

Stand: 9. Mai 2012

ACHTUNG

Diese Mitschrift ersetzt *nicht* die Vorlesung.
Es wird daher *dringend* empfohlen, die Vorlesung zu besuchen.

Copyright Notice

Disclaimer of Warranty

Limitation of Liability

Links

Der Text der „GNU Free Documentation License" kann auch auf der Seite

`https://www.gnu.org/licenses/fdl-1.3.de.html`

nachgelesen werden.
Eine transparente Kopie der aktuellen Version dieses Dokuments kann von

`https://github.com/andiv/KomAlg`

heruntergeladen werden.

Literatur

- Michael Francis Atiyah, Ian G. Macdonald: *Introduction to commutative algebra*, Westview Press, 1994; ISBN: 0-201-40751-5
- David Eisenbud: *Commutative algebra with a view toward algebraic geometry*, Springer, 2004; ISBN: 3-540-94269-6
- Hideyuki Matsumura: *Commutative ring theory*, Cambridge University Press, 2005 ISBN: 0-521-36764-6
- Nicolas Bourbaki: *Commutative algebra*, Springer, 1991 ISBN: 3-540-64239-0

Inhaltsverzeichnis

1 Ringe und Ideale

1.1 **Definition** (Ring, Ringhomomorphismus)

i) Ein (*unitärer*, *kommutativer*) *Ring* ist ein Tupel $(A, +, \cdot, 0, 1)$ mit den Eigenschaften:

a) $(A, +, 0)$ ist eine abelsche Gruppe.

b) Für alle $x,y,z \in A$ gelten:

$$\begin{aligned} (xy)\,z &= x\,(yz) && \text{(Assoziativität)} \\ x\,(y+z) &= xy + xz && \text{(Distributivität)} \\ xy &= yx && \text{(Kommutativität)} \\ x \cdot 1 &= x && \text{(neutrales Element)} \end{aligned}$$

ii) Sind A und B Ringe, so ist ein *Ringhomomorphismus* (*von A nach B*) (Abkürzung: Ringhom.) eine Abbildung $f : A \to B$, sodass für alle $x,y \in A$ gilt:

a) $f(x+y) = f(x) + f(y)$

b) $f(xy) = f(x)\,f(y)$

c) $f(1) = 1$

Aus a) folgt direkt $f(0) = 0$, da Ringe additive Gruppen sind.

Aus b) folgt aber nicht c), da Ringe im Allgemeinen keine multiplikativen Gruppen sind.

1.2 Beispiel

i) Bekannte Ringe sind $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[\mathbf{i}] = \left\{a + b\mathbf{i} \middle| a,b \in \mathbb{Z}\right\} \subseteq \mathbb{C}$, der Polynomring $A[X]$ eines Rings A und der Produktring $A \times B$ der Ringe A und B.

ii) Für jeden Ring A existiert genau ein Ringhomomorphismus $\mathbb{Z} \to A$.

Für jeden Ring A ist die Abbildung von Mengen

$$\begin{aligned} \left\{f : \mathbb{Z}[X] \to A \middle| f \text{ ist Ringhom.}\right\} &\xrightarrow{\sim} A \\ f &\mapsto f(X) \end{aligned}$$

bijektiv. (Die Ringhomomorphismen f sind die Einsetzungshomomorphismen.)

1.3 Definition (Unterring)

Sei A ein Ring.
Eine Teilmengen $B \subseteq A$ heißt *Unterring* (*von* A), wenn für alle x,$y \in B$ gilt:

i) $x - y \in B$, $x \cdot y \in B$

ii) $1 \in B$

In diesem Fall ist $\left(B, + \big|_{B\times B}, \cdot \big|_{B\times B}, 0, 1\right)$ wieder ein Ring.

1.4 Beispiel

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sind Unterringe, nicht aber $\mathbb{N} \subseteq \mathbb{Z}$.

1.5 Definition und Bemerkung (Ideal, Quotientenring)

Sei A ein Ring.

i) Eine Teilmenge $I \subseteq A$ heißt *Ideal* (*von* A), falls folgende Eigenschaften gelten:

   a) $I \subseteq (A, +, 0)$ ist eine Untergruppe.
   b) Für alle $x \in A$ und $y \in I$ gilt $xy \in I$.

ii) Ist $I \subseteq A$ ein Ideal, so ist die für alle x,$y \in A$ durch

$$x \equiv y \mod I \qquad :\Leftrightarrow \qquad x - y \in I$$

   (lies: „*x ist kongruent zu y modulo I*“) auf A definierte Relation eine Äquivalenzrelation und es existiert genau eine Ringstruktur ${}^{A}\!/_{I}$, sodass die kanonische Abbildung

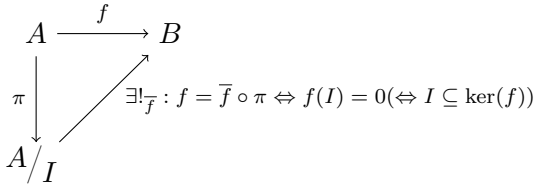
$$\begin{aligned} \pi : A &\to {}^{A}\!/_{I} \\ x &\mapsto \pi(x) := [x] := (x \mod I) \end{aligned}$$

   ein Ringhomomorphismus ist.
   Es gilt $\ker(\pi) = I$. Der Ring ${}^{A}\!/_{I}$ heißt *Quotientenring* (*von* A *bezüglich* I).

iii) Sind $I \subseteq A$ ein Ideal und B ein Ring, so ist die Abbildung

$$\begin{aligned} \left\{\overline{f} : {}^{A}\!/_{I} \to B \middle| \overline{f} \text{ ist Ringhom.}\right\} &\xrightarrow{\sim} \left\{f : A \to B \middle| f \text{ ist Ringhom.}, f(I) = 0\right\} \\ \overline{f} &\mapsto \overline{f} \circ \pi \end{aligned}$$

   bijektiv.
   Skizze:



   (universelle Eigenschaft des Quotientenrings)

1.6 **Beispiel** (Kern, Bild)

i) Ist $f : A \to B$ ein Ringhomomorphismus, so ist der *Kern*

$$\ker(f) := \{x \in A | f(x) = 0\} \subseteq A$$

ein Ideal und das *Bild*

$$\operatorname{im}(f) := \{f(x) | x \in A\} \subseteq B$$

ein Unterring.
(Ist $B \subseteq A$ ein Unterring, so ist $\iota : B \hookrightarrow A$ ein Ringhomomorphismus mit $\operatorname{im}(\iota) = B$.)

ii) Sind A ein Ring und $n \in \mathbb{N}_{>0}$, so gilt:

$$\left|\left\{f : {}^{\mathbb{Z}}/_{n\mathbb{Z}} \to A \text{ ist Ringhom.}\right\}\right| = \begin{cases} 1 & \text{falls } \underbrace{1 + \ldots + 1}_{n\text{-mal}} = 0 \text{ in } A \\ 0 & \text{sonst} \end{cases}$$

(Verwende 1.2 ii) und 1.5 iii) mit $I = n\mathbb{Z} \subseteq A = \mathbb{Z}$.)

1.7 **Proposition** (Ideale des Quotientenrings)

Seien A ein Ring, $I \subseteq A$ ein Ideal und $\pi : A \to {}^{A}/_{I}$ der kanonische Ringhomomorphismus. Dann ist die Abbildung

$$\begin{aligned} \Phi : M := \{J | J \subseteq A \text{ Ideal mit } I \subseteq J\} &\xrightarrow{\sim} N := \left\{\overline{J} | \overline{J} \subseteq {}^{A}/_{I} \text{ Ideal}\right\} \\ J &\mapsto \Phi(J) := \pi(J) \end{aligned}$$

wohldefiniert und bijektiv und erfüllt:
Für alle Ideale J_1,$J_2 \subseteq A$ mit $I \subseteq J_1$,J_2 gilt:

$$J_1 \subseteq J_2 \Leftrightarrow \Phi(J_1) \subseteq \Phi(J_2)$$

Man sagt, die Bijektion Φ ist ordnungserhaltend.

Beweis

Ist $J \in M$, so ist $\Phi(J) = \pi(J) \subseteq {}^{A}/_{I}$ als Bild des Ringhomomorphismus π ein Unterring von ${}^{A}/_{I}$ und somit ist insbesondere $(\pi(J), +, 0)$ eine Untergruppe.
Seien $\overline{x} \in {}^{A}/_{I}$ und $\overline{y} \in \Phi(J)$ gegeben. Wegen $\Phi(J) = \pi(J)$ und ${}^{A}/_{I} = \pi(A)$ gibt es ein $x \in A$ und ein $y \in J$ mit $\overline{x} = \pi(x)$ und $\overline{y} = \pi(y)$.

$$\overline{x} \cdot \overline{y} = \pi(x)\pi(y) = \pi(xy)$$

Da J ein Ideal ist, folgt aus $y \in J$ und $x \in A$ schon $xy \in J$. Daher ist $\overline{x} \cdot \overline{y} = \pi(xy) \in \pi(J)$, weswegen $\pi(J)$ ein Ideal ist. Also ist Φ wohldefiniert.

Betrachte die Abbildung:

$$\begin{aligned}\Psi : N &\to M \\ \overline{J} &\mapsto \pi^{-1}\left(\overline{J}\right)\end{aligned}$$

Seien $\overline{J} \subseteq {}^{A}\!/_{I}$ ein Ideal und $a,b \in \Psi\left(\overline{J}\right) = \pi^{-1}\left(\overline{J}\right)$, das heißt $\pi(a), \pi(b) \in \overline{J}$. Dann gilt:

$$\pi(a-b) = \underbrace{\pi(a)}_{\in \overline{J}} - \underbrace{\pi(b)}_{\in \overline{J}} \overset{\overline{J} \text{ Ideal}}{\in} \overline{J}$$

Also ist $a - b \in \pi^{-1}\left(\overline{J}\right)$ und somit $\left(\Psi\left(\overline{J}\right), +, 0\right)$ eine Untergruppe von A.
Seien $x \in A$ und $y \in \Psi\left(\overline{J}\right)$, das heißt $\pi(y) \in \overline{J}$, so gilt:

$$\pi(x \cdot y) = \pi(x)\underbrace{\pi(y)}_{\in \overline{J}} \overset{\overline{J} \text{ Ideal}}{\in} \overline{J}$$

Also ist $xy \in \Psi\left(\overline{J}\right)$ und daher $\Psi\left(\overline{J}\right) \subseteq A$ ein Ideal.
Da für alle Ideale $\overline{J} \in {}^{A}\!/_{I}$ schon $0 \in \overline{J}$ gilt, folgt $\pi^{-1}\left(\overline{J}\right) \supseteq \pi^{-1}(0) = \ker(\pi) = I$. Daher ist Ψ wohldefiniert. Nun gilt:

$$\begin{aligned}(\Phi \circ \Psi)\left(\overline{J}\right) &= \left(\pi \circ \pi^{-1}\right)\left(\overline{J}\right) \overset{\pi \text{ surjektiv}}{=} \overline{J} \\ (\Psi \circ \Phi)(J) &= \left(\pi^{-1} \circ \pi\right)(J) = \left\{a + b \middle| a \in J, b \in I\right\} \overset{I \subseteq J}{=} J\end{aligned}$$

Somit ist Ψ die Umkehrabbildung zu Φ, weswegen Φ bijektiv ist.
Zeige nun $J_1 \subseteq J_2 \Leftrightarrow \Phi(J_1) \subseteq \Phi(J_2)$:
„$\Rightarrow$“: Seien $J_1 \subseteq J_2$, und $\overline{x} \in \Phi(J_1) = \pi(J_1)$. Dann gibt es ein $x \in J_1$ mit $\overline{x} = \pi(x)$ und wegen $J_1 \subseteq J_2$ gilt $x \in J_2$. Daher ist $\overline{x} = \pi(x) \in \pi(J_2) = \Phi(J_2)$. Also gilt $\Phi(J_1) \subseteq \Phi(J_2)$.
„$\Leftarrow$“: Seien $\Phi(J_1) \subseteq \Phi(J_2)$ und $x \in J_1$. Dann ist $\overline{x} \in \pi(J_1) = \Phi(J_1) \subseteq \Phi(J_2)$ und daher gibt es ein $\tilde{x} \in J_2$ mit $\pi(\tilde{x}) = \overline{x}$. Also ist $x - \tilde{x} = a \in I$. Wegen $I \subseteq J_2$ folgt somit $x = \tilde{x} + a \in J_2$. Also gilt $J_1 \subseteq J_2$. $\square_{1.7}$

1.8 Beispiel

Die Ideale des Ringes ${}^{\mathbb{Z}}\!/_{6\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \ldots, \overline{5}\right\}$ sind genau die Hauptideale:

$$\left(\overline{0}\right), \left(\overline{3}\right), \left(\overline{2}\right), \left(\overline{1}\right) \subseteq {}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$$

1.9 **Definition** (Nullteiler, Integritätsring)

i) Sei A ein Ring. Ein Element $x \in A$ heißt genau dann *Nullteiler*, wenn es ein $x \in A \setminus \{0\}$ mit $xy = 0$ gibt.

ii) Ein *Integritätsring* (Abkürzung: IR) ist ein Ring $A \neq \{0\}$, in dem $0 \in A$ der einzige Nullteiler ist.

1.10 Beispiel

i) $\mathbb{Z}$ ist ein Integritätsring.

ii) Ist A ein Integritätsring, so ist auch $A[X]$ ein Integritätsring. (Gradformel!)

iii) Der Ring $A := {}^{\mathbb{Z}[X]}\!/_{\left(X^2\right)}$ ist kein Integritätsring, denn für $\overline{X} := \left(X \mod \left(X^2\right)\right)$ gilt $\overline{X} \neq 0$, aber auch $\overline{X} \cdot \overline{X} = 0$, weswegen $\overline{X} \in A$ ein Nullteiler ist.
Auch ${}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$ ist kein Integritätsring, denn $\underbrace{\overline{2}}_{\neq\overline{0}} \cdot \underbrace{\overline{3}}_{\neq\overline{0}} = \overline{0}$.

1.11 Definition (nilpotent)

Sei A ein Ring. Ein $x \in A$ heißt genau dann *nilpotent*, wenn es ein $n \in \mathbb{N}_{>0}$ gibt mit $x^n = 0$.

1.12 Beispiel

i) Ist $0 \neq x \in A \neq \{0\}$ nilpotent, so ist x ein Nullteiler, denn für $N := \min\left\{n \in \mathbb{N}_{>0} \middle| x^n = 0\right\}$ gilt $N \geq 1$ und wegen der Minimalität von N ist $x^{N-1} \neq 0$. Also folgt aus

$$0 = x^N = \underbrace{x}_{\neq 0} \cdot \underbrace{x^{N-1}}_{\neq 0}$$

schon, dass x ein Nullteiler ist.

ii) In dem Produktring $A := \mathbb{Z} \times \mathbb{Z}$ ist $x := (1,0)$ ein Nullteiler, da $x \cdot (0,1) = (0,0) = 0$ gilt, aber nicht nilpotent, denn für alle $n \in \mathbb{N}_{>0}$ gilt:

$$x^n = (1,0)^n = (1^n,0^n) = (1,0) = x \neq 0$$

1.13 Definition und Bemerkung (Einheit, Einheitengruppe)

Sei A ein Ring. Ein $x \in A$ heißt genau dann *Einheit* (*in* A), wenn es ein $y \in A$ mit $xy = 1$ gibt. Die Menge $A^* = \left\{x \in A \middle| x \text{ ist Einheit}\right\}$ der Einheiten ist eine kommutative Gruppe bezüglich der Multiplikation und heißt *die Einheitengruppe von* A.
(Beachte: $\{0\}^* = \{0 = 1\}$)

1.14 Beispiel

i) $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

ii) $\mathbb{Z}[\mathbf{i}]^* = \{\pm 1, \pm \mathbf{i}\}$

iii) Ist A ein Integritätsring, dann ist $(A[X])^* = A^*$. (Folgt aus der Gradformel.)

1.15 Beispiel und Definition (Hauptideal(-ring))

Sei A ein Ring.

i) Für jedes $x \in A$ ist $(x) := \{xy | y \in A\} \subseteq A$ ein Ideal. Es heißt *das von x erzeugte Hauptideal* (Abkürzung: HI).

ii) Ist A ein Integritätsring, so gilt für alle $x,y \in A$:

$$(x) = (y) \quad \Leftrightarrow \quad \exists_{u \in A^*} : x = uy$$

Insbesondere gilt:

$$(x) = 1 = A \quad \Leftrightarrow \quad x \in A^* \tag{1.1}$$

(Beachte: (1.1) gilt für jeden Ring A.)

iii) A heißt genau dann *Hauptidealring* (Abkürzung: HIR), wenn A ein Integritätsring ist, in dem jedes Ideal $I \subseteq A$ ein Hauptideal ist.

iv) A heißt genau dann *Körper*, wenn $A^* = A \setminus \{0\}$ und $A \neq \{0\}$ ist.

1.16 Beispiel

Die Ringe $\mathbb{Z}, \mathbb{Z}[\mathbf{i}]$ und $k[X]$ für einen Körper k, nicht aber $\mathbb{Z}[X]$ oder $k[X,Y]$ sind Hauptidealringe.
Die Ringe $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ und $\mathbb{F}_p := {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ für eine Primzahl p sind Körper, nicht aber $\mathbb{Z}$.

1.17 Proposition (Ideale eines Körpers)

Für einen Ring $A \neq \{0\}$ sind folgende Aussagen äquivalent:

i) A ist ein Körper.

ii) $(0), (1) \subseteq A$ sind die einzigen Ideale.

iii) Jeder Ringhomomorphismus $f : A \to B \neq \{0\}$ ist injektiv.

Beweis

„i) ⇒ ii)“: Sei $(0) \neq I \subseteq A$ ein Ideal. Also gibt es ein Element $0 \neq x \in I$. Da A ein Körper ist, ist $A^* = A \setminus \{0\} \ni x$. Also folgt $(1) = (x) \subseteq I$. Daher ist $A = I = (1)$.

„ii) ⇒ iii)“: Wegen $f(1) = 1 \neq 0$ in B ist $(1) \neq \ker(f) \subseteq A$. Da der Kern aber ein Ideal ist, bleibt für den Kern nur das einzige andere Ideal $\ker(f) = (0)$, was äquivalent zur Injektivität von f ist.

„iii) ⇒ i)“: Nach Voraussetzung gilt $A \neq \{0\}$, weswegen nach der Definition 1.15 iv) ist nur noch $A \setminus \{0\} \subseteq A^*$ zu zeigen ist. Sei $x \in A \setminus A^*$, dann ist $(x) \subsetneq A$. Wende iii) auf den Quotientenhomomorphismus

$$\pi : A \to B := {}^{A}\!/_{(x)} \neq (0)$$

an und erhalte, dass π injektiv ist. Daher gilt $(0) = \ker(\pi) = (x)$ und somit $x = 0$. $\square_{1.17}$

1.18 Proposition und Definition (Primideal, maximales Ideal)

Sei $I \subsetneq A$ ein Ideal.

i) Äquivalent sind:

   a) $\forall_{a,b \in A} : ab \in I \Rightarrow (a \in I \vee b \in I)$
   b) ${}^{A}\!/_{I}$ ist ein Integritätsring.

   In diesem Fall heißt I *Primideal* (Abkürzung: PI).

ii) Äquivalent sind:

   a) Für alle Ideale $J \subseteq A$ mit $I \subsetneq J$ gilt $J = A$.
   b) ${}^{A}\!/_{I}$ ist ein Körper.

   In diesem Fall heißt I *maximales Ideal*.

Beweis

i) „a) ⇒ b)“: ${}^{A}\!/_{I} \neq \{0\}$, da $I \subsetneq A$ ein echtes Ideal ist. Sind $a,b \in A$ mit $\overline{a} \cdot \overline{b} = \overline{0}$ in ${}^{A}\!/_{I}$, so folgt $ab \in I$. Aus a) ergibt sich $(a \in I \vee b \in I)$ und im Quotientenring bedeutet dies $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$. Daher ist $\overline{0} \in {}^{A}\!/_{I}$ der einzige Nullteiler.

   „b) ⇒ a)“: Folgt analog:
   Sind $a,b \in A$ mit $ab \in I$, so folgt $\overline{a} \cdot \overline{b} = \overline{0}$ in ${}^{A}\!/_{I}$. Da nach b) ${}^{A}\!/_{I}$ ein Integritätsring ist, ist $\overline{0} \in {}^{A}\!/_{I}$ der einzige Nullteiler und somit $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$. Im Ring A bedeutet das $(a \in I \vee b \in I)$, womit a) gezeigt ist. $\square_{\text{i)}}$

ii) Da nach 1.17 i) ⇔ ii) ein Körper genau die Ideale (0) und (1) hat und nach 1.7 die Ideale des Quotientenrings ${}^{A}\!/_{I}$ den Idealen $J \subseteq A$ mit $I \subseteq J$ entsprechen, von denen es aufgrund der Maximalität von I nur die zwei Möglichkeiten $J = I$ und $J = A$ gibt, beziehungsweise andersherum nur diese zwei geben kann, wenn ${}^{A}\!/_{I}$ ein Körper ist, ist die Äquivalenz gezeigt. $\square_{\text{ii)}}$

1.19 Beispiel

i) Jedes maximale Ideal ist ein Primideal, da jeder Körper ein Integritätsring ist.

ii) Das Nullideal $(0) \subseteq \mathbb{Z}$ ist ein Primideal, aber nicht maximal, da ${}^{\mathbb{Z}}\!/_{(0)} = \mathbb{Z}$ ein Integritätsring, aber kein Körper, ist.

iii) Die maximalen Ideal in $\mathbb{Z}$ sind genau die Hauptideale $(p) \subseteq \mathbb{Z}$ mit einer Primzahl p. Das einzige Primideal, welches nicht maximal ist, ist das Nullideal $(0) \subseteq \mathbb{Z}$.

1.20 Proposition (Urbild eines Primideals ist ein Primideal)

Sind $f : A \to B$ ein Ringhomomorphismus und $\mathfrak{p} \subseteq B$ ein Primideal, so ist $f^{-1}(\mathfrak{p}) \subseteq A$ ein Primideal.

Beweis

Wegen $f^{-1}(\mathfrak{p}) = \ker\left(A \xrightarrow{f} B \xrightarrow{\pi} {}^{B}\!/_{\mathfrak{p}} \neq \{0\}\right) \subsetneq A$ ist $f^{-1}(\mathfrak{p})$ ein Ideal und

$$\{0\} \neq {}^{A}\!/_{f^{-1}(\mathfrak{p})} \hookrightarrow {}^{B}\!/_{\mathfrak{p}}$$

ein Unterring des Integritätsrings ${}^{B}\!/_{\mathfrak{p}}$, weshalb ${}^{A}\!/_{f^{-1}(\mathfrak{p})}$ ebenfalls ein Integritätsring ist. Dann ist nach der Definition 1.18 i) auch $f^{-1}(\mathfrak{p})$ ein Primideal. $\square_{1.20}$

1.21 Beispiel

Für den eindeutigen Ringhomomorphismus $f : \mathbb{Z} =: A \hookrightarrow B := \mathbb{Q}$ ist $\mathfrak{p} := (0) \subseteq B$ ein maximales Ideal, da B ein Körper ist, aber $f^{-1}(\mathfrak{p}) = (0) \subseteq A = \mathbb{Z}$ ist kein maximales Ideal.

1.22 Satz (Existenz eines maximalen Ideals)

In jedem Ring $A \neq \{0\}$ existiert mindestens ein maximales Ideal.

Beweis

Dies ist eine bekannte Anwendung des Lemmas von Zorn:

> „Jede halbgeordnete Menge, in der jede Kette (d.h. jede total geordnete Teilmenge) eine obere Schranke hat, enthält mindestens ein maximales Element."

Die Teilmengenrelation auf der Menge M der echten Ideale des Rings A erzeugt eine Halbordnung. Diese Menge ist nicht leer, da sie immer das triviale Ideal (0) enthält.
Außerdem ist für eine Kette K in M die Vereinigung $I := \bigcup_{k \in K} k$ aller Elemente eine obere Schranke für K, denn I ist nicht leer und ein Ideal von A.
Nach dem Lemma von Zorn gibt es also mindestens ein maximales Element von M, also ein maximales Ideal von A. $\square_{1.22}$

1.23 Korollar

Ist A ein Ring und $I \subsetneq A$ ein Ideal, so existiert ein maximales Ideal $\mathfrak{m} \subseteq A$ mit $I \subseteq \mathfrak{m}$.

Beweis

Sei $\mathfrak{n} \subseteq {}^{A}\!/_{I}$ ein maximales Ideal, das nach 1.22 existiert, und $\pi : A \to {}^{A}\!/_{I}$ der kanonische Ringhomomorphismus. Nach 1.7 ist $\mathfrak{m} := \pi^{-1}(\mathfrak{n}) \subseteq A$ ein maximales Ideal mit $I \subseteq \mathfrak{m}$. $\square_{1.23}$

1.24 Korollar

Sei A ein Ring. Für ein beliebiges Element $x \in A$ sind äquivalent:

i) $x \in A^*$

ii) x ist in keinem maximalen Ideal von A enthalten.

Beweis

„i) ⇒ ii)“: Dies ist klar, da $(x) = A$ ist und für jedes Ideal $I \subseteq A$ aus $x \in I$ schon $(x) \subseteq I$ folgt.

„ii) ⇒ i)“: Zeige äquivalent, dass wenn i) nicht gilt, auch ii) nicht gilt:

Sei $x \notin A^*$, so folgt aus 1.15 ii), dass $(x) \subsetneq A$ ein echtes Ideal ist und nach 1.23 gibt es ein maximales Ideal $\mathfrak{m} \subseteq A$ mit $x \in (x) \subseteq \mathfrak{m}$. $\square_{1.24}$

1.25 Ausblick

Seien X ein kompakter Hausdorffraum und $A = C(X,\mathbb{R})$ die $\mathbb{R}$-Algebra der stetigen $\mathbb{R}$-wertigen Funktionen auf X.

Für jedes $f \in A$ gilt:

$$\begin{aligned} f \in A^* &\Leftrightarrow \underset{x\in X}{\forall} : f(x) \neq 0 \\ f \in A^* &\Rightarrow \underset{x\in X}{\forall} : f^{-1}(x) = f(x)^{-1} \end{aligned} \tag{1.2}$$

Ein Vergleich mit 1.24 lässt einen Zusammenhang zwischen den Punkten $x \in X$ und den maximalen Idealen von A vermuten.

Für alle $x \in X$ ist die Auswertungsabbildung

$$\begin{aligned} \mathrm{ev}_x : A &\twoheadrightarrow \mathbb{R} \\ f &\mapsto \mathrm{ev}_x(f) := f(x) \end{aligned}$$

ein surjektiver $\mathbb{R}$-Algebrenhomomorphismus, dessen Kern

$$\mathfrak{m}_x := \ker(\mathrm{ev}_x) = \left\{ f \in C(X,\mathbb{R}) \,\middle|\, f(x) = 0 \right\} \subseteq A \tag{1.3}$$

ein maximales Ideal ist, da ${}^{A}\!/_{\mathfrak{m}_x} \overset{\sim}{=} \mathbb{R}$ ein Körper ist.

Genauer kann man auf der Menge

$$\mathrm{MaxSpec}(A) := \{\mathfrak{m} \subseteq A \text{ maximales Ideal}\}$$

eine Topologie nur mit Hilfe des kommutativen Ringes A definieren, so dass die Abbildung $X \to \mathrm{MaxSpec}(A), x \mapsto \mathfrak{m}_x$ ein Homöomorphismus, also insbesondere bijektiv ist. (vergleiche [Atiyah, Macdonald], chapter 1, exercise 26)

Insbesondere bestimmt der kommutative Ring A den topologischen Raum X.

Nicht jeder kommutative Ring ist von der Form $C(X,\mathbb{R})$. Aber eine Grundidee der topologischen Geometrie ist, dass jeder Ring A der Ring von „stetigen Funktionen“ auf einem „Raum“ sein soll, zum Beispiel:

Betrachte $\mathrm{MaxSpec}(A) := \left\{\mathfrak{m} \subseteq A \middle| \mathfrak{m} \text{ maximales Ideal}\right\}$. Jedes $a \in A$ bestimmt eine Abbildung

$$\begin{aligned} \mathrm{MaxSpec}(A) &\to \dot{\bigcup_{\mathfrak{m}\in\mathrm{MaxSpec}(A)}} \left({}^{A}\!/_{\mathfrak{m}}\right) =: M \\ \mathfrak{m}_0 &\mapsto \underbrace{(a \mod \mathfrak{m}_0)}_{\in {}^{A}\!/_{\mathfrak{m}_0} \subseteq M} =: a(\mathfrak{m}_0) \end{aligned}$$

und es gilt:

i) Für alle $\mathfrak{m} \in \operatorname{MaxSpec}(A)$ gilt nach Definition $\mathfrak{m} = \{a \in A \mid a(\mathfrak{m}) = 0\}$. (vergleiche (1.3))

ii) Für alle $a \in A$ gilt

$$a \in A^* \Leftrightarrow \left(\underset{\mathfrak{m} \in \operatorname{MaxSpec}(A)}{\forall} : a(\mathfrak{m}) \neq 0 \right)$$

da $a(\mathfrak{m}) \neq 0 \Leftrightarrow a \notin \mathfrak{m}$ ist und nach 1.24 eine Einheit in keinem maximalen Ideal enthalten ist. (vergleiche (1.2))

$\square_{1.25}$

Zum Beispiel für $A = \mathbb{Z}$ ist ${}^{A}/_{\mathbb{Z}} = \mathbb{F}_p$ für eine Primzahl p.

1.26 **Definition** (lokaler Ring, Restklassenkörper)

Ein *lokaler Ring* ist ein Ring A mit genau einem maximalem Ideal $\mathfrak{m}$.
(Jeder Körper ist ein lokaler Ring mit $\mathfrak{m} = (0)$.)
Der Körper ${}^{A}/_{\mathfrak{m}}$ heißt der *Restklassenkörper* (*von* A).
Schreibe $(A,\mathfrak{m})$ für einen lokalen Ring mit maximalem Ideal $\mathfrak{m}$, und definiere $\kappa(\mathfrak{m}) := {}^{A}/_{\mathfrak{m}}$.

1.27 **Proposition** (Kriterium für lokalen Ring)

Seien A ein Ring und $\mathfrak{m} \subsetneq A$ ein Ideal.

i) Gilt $A \setminus \mathfrak{m} \subseteq A^*$, so ist $(A,\mathfrak{m})$ ein lokaler Ring.

ii) Ist $\mathfrak{m}$ maximal und gilt $1 + \mathfrak{m} := \{1 + x \mid x \in \mathfrak{m}\} \subseteq A^*$, so ist $(A,\mathfrak{m})$ ein lokaler Ring.

Beweis

i) Ist $I \subseteq A$ ein Ideal mit $\mathfrak{m} \subseteq I$, so existiert ein $u \in I \setminus \mathfrak{m} \subseteq A \setminus \mathfrak{m} \subseteq A^*$, weswegen $I = (1)$ ist. Also ist $\mathfrak{m} \subseteq A$ ein maximales Ideal.

Sei $\mathfrak{n} \subseteq A$ ein (weiteres) maximales Ideal. Zeige $\mathfrak{n} \subseteq \mathfrak{m}$, denn dann folgt, weil beides maximale Ideale sind, schon $\mathfrak{m} = \mathfrak{n}$, das heißt $\mathfrak{m} \subseteq A$ ist das einzige maximale Ideal.

Angenommen es gilt $\mathfrak{n} \subsetneq \mathfrak{m}$, dann existiert ein $x \in \mathfrak{n} \setminus \mathfrak{m} \subseteq A \setminus \mathfrak{m} \subseteq A^*$. Deswegen ist $\mathfrak{n} = (1)$ im Widerspruch zur Maximalität von $\mathfrak{n}$. $\square_{\text{i)}}$

ii) Wegen i) ist nur $A \setminus \mathfrak{m} \subseteq A^*$ zu zeigen.

Sei $x \in A \setminus \mathfrak{m}$, so ist $\mathfrak{m} \subsetneq \mathfrak{m} + (x) = \{y + ax \mid y \in \mathfrak{m}, a \in A\}$ ein Ideal, aber $\mathfrak{m}$ ist ein maximales Ideal, weswegen $\mathfrak{m} + (x) = (1)$ gelten muss. Daher gibt es ein $y \in \mathfrak{m}$ und ein $a \in A$ mit $1 = y + ax$ und somit $ax = 1 + (-y) \in 1 + \mathfrak{m} \subseteq A^*$. Deswegen existiert ein $b \in A$ mit $1 = b(ax) = (ba)x$ und daher ist x invertierbar und somit $x \in A^*$. $\square_{\text{ii)}}$

1.28 Beispiel

Sei $p \in \mathbb{Z}$ eine Primzahl, insbesondere $(p) \neq 0$. Dann ist $\mathbb{Z} \subseteq \mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, p \not| b \in \mathbb{Z} \right\} \subsetneq \mathbb{Q}$ ein Unterring von $\mathbb{Q}$ und $\left(\mathbb{Z}_{(p)}, (p)\right)$ ist ein lokaler Ring mit $\kappa(\mathfrak{p}) \overset{\sim}{=} \mathbb{F}_p$.

Beweis

Nach Beispiel 2.6 aus Algebra ist die Lokalisierung $\mathbb{Z}_{(p)} = (\mathbb{Z} \setminus (p))^{-1}\mathbb{Z}$ von $\mathbb{Z}$ bei (p) ein Unterring von $\mathbb{Z}_{(0)} = \mathbb{Q}$ mit der Einheitengruppe $\mathbb{Z}_{(p)}^* = \mathbb{Z}_{(p)} \setminus (p)$.

Nach 1.27 i) ist also $\big(\mathbb{Z}_{(p)}, (p)\big)$ ein lokaler Ring. $\square_{1.28}$

1.29 **Proposition und Definition** (Nilradikal)

Sei A ein Ring. Dann ist $\mathfrak{N}(A) := \big\{x \in A \big| x \text{ nilpotent}\big\} \subseteq A$ ein Ideal und es gilt:

$$\mathfrak{N}\left(A/\mathfrak{N}(A)\right) = (\overline{0})$$

Das Ideal $\mathfrak{N}(A) \subseteq A$ heißt *das Nilradikal von A.*

Beweis

Überprüfe 1.5 i) a) und b):

$$x,y \in \mathfrak{N}(A) \quad \Rightarrow \quad \underset{N\in\mathbb{N}_{\geq 1}}{\exists} : x^N = y^N = 0 \quad \Rightarrow \quad (x-y)^{2N} = \sum_{i=0}^{2N} \binom{2N}{i} x^i \cdot (-1)^{2N-i} \cdot y^{2N-i}$$

Da für alle $0 \leq i \leq 2N$ gilt $(i \geq N \vee 2N - i \geq N)$ ist in jedem Produkt $x^i \cdot y^{2N-i}$ mindestens einer der Faktoren Null und es folgt $(x-y)^{2N} = (0)$, also $x - y \in \mathfrak{N}(A)$. $\square_{\text{a)}}$

Zu b): Seien $x \in \mathfrak{N}(A)$ und $a \in A$. Dann gibt es ein $N \in \mathbb{N}_{\geq 1}$ mit $x^N = 0$ und somit gilt:

$$(ax)^N = a^N x^N = a^N \cdot 0 = 0$$

Daher ist $ax \in \mathfrak{N}(A)$. $\square_{\text{b)}}$

Sei nun $x \in A$ mit $\overline{x} := (x \mod \mathfrak{N}(A)) \in \mathfrak{N}\left(A/\mathfrak{N}(A)\right)$. Daher gibt es ein $N \in \mathbb{N}_{\geq 1}$ mit $0 = (\overline{x})^N = \overline{(x^N)}$ in $A/\mathfrak{N}(A)$, weswegen $x^N \in \mathfrak{N}(A)$ ist. Also gibt es ein $M \in \mathbb{N}_{\geq 1}$ mit $0 = \big(X^N\big)^M = x^{N\cdot M}$ in A, weshalb $x \in \mathfrak{N}(A)$ ist, also $\overline{x} = 0$ ist. $\square_{1.29}$

1.30 **Satz** (Nilradikal ist Schnitt aller Primideale)

Sei A ein Ring. Dann gilt:

$$\mathfrak{N}(A) = \bigcap_{\mathfrak{p}\subseteq A \text{ Primideal}} \mathfrak{p}$$

(Es folgt nochmal, dass $\mathfrak{N}(A) \subseteq A$ ein Ideal ist.)

Beweis

„$\subseteq$“: Seien $x \in \mathfrak{N}(A)$ und $\mathfrak{p} \subseteq A$ ein Primideal. Dann existiert ein $n \in \mathbb{N}_{\geq 1}$ mit $x^n = 0 \in \mathfrak{p}$.
Aus der Definition eines Primideals 1.18 i) a) folgt $x \in \mathfrak{p}$, da dies der einzige Faktor im Produkt x^n ist.

„$\supseteq$“: Sei $x \in A \setminus \mathfrak{N}(A)$. Zeige, dass ein Primideal $\mathfrak{p} \subseteq A$ mit $x \notin \mathfrak{p}$ existiert.

– 1. Beweis (direkt): Betrachte $\Sigma := \left\{\mathfrak{u} \middle| \mathfrak{u} \subseteq A \text{ Ideal mit } \left(\forall_{n\in\mathbb{N}_{\geq 1}} : x^n \notin \mathfrak{u}\right)\right\}$.
Wegen $x \notin \mathfrak{N}(A)$ gilt $(0) \in \Sigma$, also $\Sigma \neq \emptyset$.
Es ist klar, dass $(\Sigma, \subseteq)$ eine teilweise geordnete Menge ist.
Ist $\Sigma' \subseteq \Sigma$ total geordnet, so gilt:

$$\mathfrak{u}' := \bigcup_{\mathfrak{u}\in\Sigma'} \mathfrak{u} \in \Sigma$$

Denn aus der totalen Ordnung von Σ' folgt, dass $\mathfrak{u}' \subseteq A$ ein Ideal ist und $x^n \notin \mathfrak{u}'$ für alle $n \in \mathbb{N}_{\geq 1}$ ist dann klar, denn sonst müsste es schon in einem $\mathfrak{u}$ sein.
Aus dem Lemma von Zorn folgt daraus die Existenz eines maximalen Elementes $\mathfrak{p} \in \Sigma$.
Wegen $x \notin \mathfrak{p}$ zeige noch, dass $\mathfrak{p}$ ein Primideal ist.
Angenommen dies ist nicht der Fall, dann existieren a,$b \in A$ mit a,$b \notin \mathfrak{p}$ und $ab \in \mathfrak{p}$.
Wegen $\mathfrak{p} \subsetneq \mathfrak{p}+(a)$,$\mathfrak{p}+(b)$ und der Maximalität von $\mathfrak{p}$ existieren n,$m \in \mathbb{N}_{\geq 1}$ mit $x^n \in \mathfrak{p}+(a)$ und $x^m \in \mathfrak{p} + (b)$. Dann folgt:

$$x^{n+m} = x^n \cdot x^m \in \mathfrak{p} + (ab) \overset{ab\in\mathfrak{p}}{=} \mathfrak{p}$$

Dies ist ein Widerspruch zu $\mathfrak{p} \in \Sigma$, also $x^{n+m} \notin \mathfrak{p}$. $\square_{\text{1. Beweis}}$

– 2. Beweis (mit Lokalisierung): $S := \left\{x^n \middle| n \geq 0\right\} \subseteq A$ ist multiplikativ abgeschlossen und wegen $x \notin \mathfrak{N}(A)$ gilt $0 \notin S$. Es folgt $S^{-1}A \neq \{0\}$.
Nach 1.22 existiert ein maximales Ideal $\mathfrak{m} \subseteq S^{-1}A$ und nach 1.19 i) und 1.20 ist

$$\mathfrak{p} := \left(\varphi : A \xrightarrow{\text{kanonisch}} S^{-1}A\right)^{-1}(\mathfrak{m}) \subseteq A$$

ein Primideal. Wegen $\varphi(x) \in \left(S^{-1}A\right)^*$ folgt $\varphi(x) \notin \mathfrak{m}$ nach 1.24 und somit gilt also $x \notin \varphi^{-1}(\mathfrak{m}) = \mathfrak{p}$. $\square_{\text{2. Beweis}}$

1.31 **Korollar und Definition** (Radikal)

Seien A ein Ring und $I \subseteq A$ ein Ideal. Dann heißt $\sqrt{I} := \left\{x \in A \middle| \exists_{n\in\mathbb{N}_{\geq 1}} : x^n \in I\right\}$ *das Radikal von* I. Es gilt:

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p}\subseteq A \text{ PI} \\ \text{mit } I\subseteq\mathfrak{p}}} \mathfrak{p}$$

Beispiel: $\sqrt{(0)} = \mathfrak{N}(A)$

Beweis

Für den kanonischen Ringhomomorphismus $\pi : A \to {}^{A}/_{I}$ gilt $\sqrt{I} = \pi^{-1}\left(\pi\left(\sqrt{I}\right)\right)$, da π surjektiv ist. Zudem ist offenbar $\pi\left(\sqrt{I}\right) = \mathfrak{N}\left({}^{A}/_{I}\right)$. Nach der Definition von $\sqrt{I}$ folgt:

$$\sqrt{I} = \pi^{-1}\left(\pi\left(\sqrt{I}\right)\right) = \pi^{-1}\left(\mathfrak{N}\left({}^{A}/_{I}\right)\right) =$$
$$\overset{1.30}{=} \pi^{-1}\left(\bigcap_{\overline{\mathfrak{p}} \subseteq {}^{A}/_{I} \text{ PI}} \overline{\mathfrak{p}}\right) = \bigcap_{\overline{\mathfrak{p}} \subseteq {}^{A}/_{I} \text{ PI}} \pi^{-1}\left(\overline{\mathfrak{p}}\right) =$$
$$\overset{\substack{1.20\\1.7}}{=} \bigcap_{\substack{\mathfrak{p} \subseteq A \text{ PI}\\ I \subseteq \mathfrak{p}}} \mathfrak{p}$$

$\square_{1.31}$

1.32 **Proposition und Definition** (Summe, Schnitt und Produkt von Idealen)

Seien A ein Ring, K eine Menge und $\forall_{k \in K}$ sei $I_k \subseteq A$ ein Ideal.

i) Das kleinste Ideal, welches alle I_k enthält, ist:

$$\sum_{k \in K} I_k := \left\{ \sum_{k \in K'} x_k \,\middle|\, K' \subseteq K \text{ endlich}, x_k \in I_k \right\} \subseteq A$$

Es heißt *die Summe der* I_k über alle $k \in K$.

ii) $\bigcap_{k \in K} I_k \subseteq A$ ist das größte Ideal, dass in allen I_k enthalten ist.

iii) Sind I und J Ideale, so auch

$$IJ := \left\{ \sum_{i=0}^{n} x_i y_i \,\middle|\, n \in \mathbb{N}, x_i \in I, y_i \in J \right\} \subseteq A$$

das Produkt von X *und* Y.

Beweis

i) Ist $x \in I_k$, so ist nach Definition auch $x \in \sum_{k \in K} I_k$ und somit ist für alle $k \in K$ schon $I_k \subseteq \sum_{k \in K} I_k$.

Andererseits müssen mit alle I_k auch beliebige endliche Summen von Elementen aus den I_k in jedem Ideal liegen, dass die I_k enthält. Daher ist die Summe das kleinste solche Ideal. $\square_{\text{i)}}$

ii) Der Schnitt ist definitionsgemäß in allen I_k enthalten.
Sei J ein Ideal, dass in allen I_k enthalten ist. Dann gilt für jedes $x \in J$ schon $x \in I_k$ für alle $k \in K$ und somit $x \in \bigcap_{k \in K} I_k$. Also ist der Schnitt das größte solche Ideal. $\square_{\text{ii)}}$

iii) Nach Definition ist IJ eine Gruppe bezüglich der Addition. Für $a \in A$ und $x \in IJ$ gilt für ein $n \in \mathbb{N}$ und $1 \leq i \leq n$ mit $x_i \in I$ und $y_i \in J$:

$$x = \sum_{i=0}^{n} x_i y_i$$
$$ax = a\left(\sum_{i=0}^{n} x_i y_i\right) = \sum_{i=0}^{n} \underbrace{(ax_i)}_{\in I} y_i \in IJ$$

Also ist IJ ein Ideal. $\square_{\text{iii)}}$

1.33 Beispiel

i) Sind I und J Ideale, so gilt $IJ \subseteq I \cap J$. Denn ist $a \in IJ$, so gibt es ein $n \in \mathbb{N}$ und für $0 \leq i \leq n$ auch $x_i \in I$ und $y_i \in J$ mit:

$$a = \sum_{i=0}^{n} x_i y_i$$

Da I ein Ideal ist und $x_i \in I$ und $y_i \in A$ ist, folgt $x_i y_i \in I$ und somit auch die Summe aller dieser Faktoren, also $a \in I$. Analog folgt $a \in J$ und somit $a \in I \cap J$.

ii) Für $A = \mathbb{Z}$, $I = (a)$ und $J = (b)$ gilt:

$$(a) + (b) = (\text{ggT}\,(a,b))$$
$$(a) \cap (b) = (\text{kgV}\,(a,b))$$
$$(a)\,(b) = (ab)$$

Insbesondere folgt:

$$(a)\,(b) = (a) \cap (b) \quad \Leftrightarrow \quad \text{kgV}\,(a,b) = \pm ab \quad \Leftrightarrow \quad \text{ggT}\,(a,b) = 1$$

iii) Seien k ein Körper, $n \in \mathbb{N}_{\geq 1}$ und

$$A = k\,[X_1, \ldots, X_n] = \left\{ f = \sum_{i_1,\ldots,i_n \geq 0} a_{(i_1,\ldots,i_n)} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \,\middle|\, a_{(i_1,\ldots,i_n)} \in k \text{ fast alle Null} \right\}$$

der Polynomring über k in den Variablen $X_1, \ldots, X_n$. Dann ist

$$\mathfrak{m} := (X_1, \ldots, X_n) = \left\{ f \in A \,\middle|\, a_{(0,\ldots,0)} = 0 \right\} = \left\{ f \in A \,\middle|\, f\,(0,\ldots,0) = 0 \right\} \subseteq A$$

ein maximales Ideal mit ${}^{A}\!/_{\mathfrak{m}} \overset{\sim}{=} k$ vermöge $\overline{f} \mapsto f\,(0,\ldots,0) \in k$. Für alle $n \in \mathbb{N}_{\geq 1}$ gilt:

$$\mathfrak{m}^n = \left\{ f \in A \,\middle|\, \forall_{(i_1,\ldots,i_n) \in \mathbb{N}^n} : \left(\sum_{j=1}^{n} ij < n \Rightarrow a_{(i_1,\ldots,i_n)} = 0 \right) \right\}$$

Für $n = 2$ gilt zum Beispiel:

$$k[X,Y] \supseteq (X,Y)^n = \left\{ \sum_{\substack{i,j\geq 0 \\ i+j\geq n}} a_{i,j} X^i Y^j \,\middle|\, a_{ij} \in k \text{ fast alle Null} \right\} =$$
$$= \left(X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n\right)$$

$\square_{1.33}$

1.34 **Bemerkung und Definition** (komaximal)

Zwei Ideale I und J heißen genau dann *komaximal*, wenn $I + J = (1)$ ist. Nach 1.31 i) ist dies äquivalent dazu, dass es ein $a \in I$ und ein $b \in J$ mit $a + b = 1$ gibt.
In diesem Fall gilt $IJ = I \cap J$.

Beweis

Wegen 1.32 i) ist nur noch $I \cap J \subseteq IJ$ zu zeigen.
Wähle $a \in I$ und $b \in J$ mit $a + b = 1$ und sei $x \in I \cap J$ beliebig. Dann folgt:

$$x = x \cdot 1 = \underbrace{xa}_{\in JI = IJ} + \underbrace{xb}_{\in IJ} \in IJ$$

$\square_{1.34}$

1.35 **Satz** (Chinesischer Restsatz)

Seien A ein Ring, $n \in \mathbb{N}_{\geq 1}$ und $I_1, \ldots, I_n \subseteq A$ Ideale. Dann ist die Abbildung

$$\varphi : A \to \prod_{i=1}^{n} \left({}^{A}/_{I_i} \right)$$
$$a \mapsto \varphi(a) := (a \mod I_i)_{i_1,\ldots,i_n}$$

ein Ringhomomorphismus und es gilt:

a) φ ist surjektiv $\overset{\text{ii)}}{\Leftrightarrow} \left(\underset{1\leq i,j\leq n, i\neq j}{\forall} I_i + I_j = (1) \right) \overset{\text{i)}}{\Rightarrow} \bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i$

b) $\ker(\varphi) = \bigcap_{i=1}^{n} I_i$

Beweis

Dass φ ein Ringhomomorphismus ist, kann man leicht nachrechnen.

a) i) $n = 1$ ist klar. $n = 2$ wurde in 1.33 gezeigt.
Für $n > 2$ führe eine Induktion über n durch:
Induktionsvoraussetzung:

$$J := \bigcap_{i=1}^{n-1} I_i = \prod_{i=1}^{n-1} I_i$$

Für alle $1 \leq i \leq n-1$ gibt es wegen $I_i + I_n = (1)$ ein $x_i \in I_i$ und ein $y_i \in I_n$ mit:

$$1 = x_i + y_i \tag{1.4}$$

Es folgt:

$$J = \prod_{i=1}^{n-1} I_i \ni \prod_{i=1}^{n-1} x_i \overset{(1.4)}{=} \prod_{i=1}^{n-1} (1 - y_i) \overset{y_i \in I_n}{\equiv} 1 \mod I_n$$

Also gibt es ein $y \in I_n$ mit:

$$1 = \underbrace{\left(\prod_{i=1}^{n-1} x_i \right)}_{\in J} + y$$

$$\Rightarrow \quad J + I_n = (1) \tag{1.5}$$

Es folgt:

$$\prod_{i=1}^{n} I_i = J \cdot I_n \overset{1.5}{\underset{n=2}{=}} J \cap I_n \overset{\text{Induktions-}}{\underset{\text{voraussetzung}}{=}} \bigcap_{i=1}^{n-1} I_i \cap I_n = \bigcap_{i=1}^{n} I_i$$

$\square_{\text{a) i)}}$

ii) „$\Leftarrow$“: Da $\operatorname{im}(\varphi) \subseteq \prod_{i=1}^{n} \left(A/I_i \right)$ ein A-Untermodul ist, genügt es zu zeigen:

$$\underset{1 \leq i \leq n}{\forall} : e_i := (0, \ldots, 0, \underbrace{1}_{i\text{-te Stelle}}, 0, \ldots, 0) \in \operatorname{im}(\varphi)$$

Sei $i = 1$ (sonst analog), so ist zu zeigen, dass es ein $x \in A$ gibt, für das gilt:

$$x \equiv 1 \mod I_1$$
$$x \in \bigcap_{i=2}^{n} I_i$$

Nach Voraussetzung existieren für alle $2 \leq i \leq n$ schon $x_i \in I_1$ und $y_i \in I_i$ mit:

$$1 = x_i + y_i$$
$$\Rightarrow \quad x := \prod_{i=2}^{n} y_i \in \prod_{i=2}^{n} I_i \subseteq \bigcap_{i=2}^{n} I_i$$
$$x = \prod_{i=2}^{n} (1 - x_i) \overset{x_i \in I_1}{\equiv} 1 \mod I_1$$

„⇒“: Seine $1 \leq i,j \leq n$ mit $i \neq j$ gegeben. Da φ surjektiv ist, existiert ein $x \in A$ mit:

$$\varphi(x) = e_i$$

Nach der Definition von φ folgt für alle $1 \leq j \leq n$ mit $j \neq i$:

$$x \equiv 1 \mod I_i \qquad\qquad x \equiv 0 \mod I_j$$

Es folgt $1 = x + y$ mit einem geeigneten $y \in I_i$. Also gilt $I_i + I_j = (1)$. $\square_{\text{a) ii)}}$

b) Dies ist klar, da $\varphi(x) = 0$ bedeutet, dass $x \mod I_i = 0$ für allen $1 \leq i \leq n$ gilt, also x in alle I_i liegt, und somit im Schnitt liegt. $\square_{\text{b)}}$

1.36 **Definition und Bemerkung** (Bild und Urbild eines Ideals)

Sei $f : A \to B$ ein Ringhomomorphismus.

i) Ist $I \subseteq A$ ein Ideal, so ist

$$f_*(I) := \left\{ \sum_{i=1}^{n} b_i \cdot f(x_i) \,\middle|\, n \in \mathbb{N}, b_i \in B, x_i \in I \right\} \subseteq B$$

das kleinste Ideal von B, welches $f(I)$umfasst. Es heißt *das Bild von I unter f*.

ii) Ist $J \subseteq B$ ein Ideal, so ist $f^*(J) := f^{-1}(J) \subseteq A$ ein Ideal, *das Urbild von J unter f*.

iii) Ist $\mathfrak{p} \subseteq B$ ein Primideal, so auch $f^*(\mathfrak{p}) \subseteq A$, wie in 1.20 gezeigt wurde.

iv) Es ist $\mathfrak{p} := (5) \subseteq A := \mathbb{Z}$ ein Primideal, aber für den eindeutigen Ringhomomorphismus $f : \mathbb{Z} \to \mathbb{Q}$ ist $f_*(\mathfrak{p}) = (1) \subseteq \mathbb{Q}$ kein Primideal.

v) Für den eindeutigen Ringhomomorphismus $f : \mathbb{Z} \to \mathbb{Z}[\mathbf{i}]$ und eine Primzahl $p \in \mathbb{Z}$ gelten:

$$f_*((p)) = \begin{cases} \mathfrak{p}^2 & \text{mit } \mathfrak{p} = (1+\mathbf{i}) \subseteq \mathbb{Z}[\mathbf{i}] \text{ für } p = 2 \\ \mathfrak{p}_1 \cdot \mathfrak{p}_2 & \text{für Primideale } \mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_1 \neq \mathfrak{p}_2 \text{ für } p \equiv 1 \mod 4 \\ (p) & p \equiv 3 \mod 4 \end{cases}$$

Durch Betrachten der Norm ist dies äquivalent zu:

$$p \neq 2 \text{ Primzahl } \Rightarrow \left(\underset{x,y \in \mathbb{Z}}{\exists} p = x^2 + y^2 \Leftrightarrow p \equiv 1 \mod 4 \right)$$

(Der Beweis erfolgt später in der algebraischen Zahlentheorie.)

freiwillige Übung: Was aus Kapitel 1 gilt allgemein für nicht notwendig kommutative Ringe?

2 Moduln

2.1 Definition ((Unter-)Modul)

Sei A ein Ring.

i) Ein *A-Modul* ist eine abelsche Gruppe M zusammen mit einer Abbildung

$$\begin{aligned} A \times M &\to M \\ (a,m) &\mapsto am \end{aligned}$$

die *Skalarmultiplikation* heißt, und für die für alle $a,b \in A$ und $x,y \in M$ gilt:

a) $a(x+y) = ax + ay$
b) $(a+b)x = ax + bx$
c) $(ab)x = a(bx)$
d) $1 \cdot x = x$

(Äquivalent dazu ist, dass die Abbildung $A \to \mathrm{End}_{\mathbb{Z}}(M), a \mapsto (m \mapsto am)$ ein Ringhomomorphismus ist.)

ii) Sei M ein A-Modul. Ein *(A-)Untermodul (von M)* (Abkürzung: UM) ist eine abelsche Untergruppe $N \subseteq M$ mit $ax \in N$ für alle $a \in A$ und alle $x \in N$.

2.2 Bemerkung und Beispiel

Sei A ein Ring.

i) Die Ringmultiplikation $A \times A \to A$ definiert auf $(A, +, 0)$ die Struktur eines A-Moduls, und die A-Untermoduln sind genau die Ideale von A.

ii) Ist $A = k$ ein Körper, so ist ein A-Modul dasselbe wie ein k-Vektorraum.

iii) Jede abelsche Gruppe M besitzt genau eine $\mathbb{Z}$-Modulstruktur, nämlich:

$$\begin{aligned} \mathbb{Z} \times M &\to M \\ (n,x) &\mapsto \begin{cases} \sum_{k=1}^{n} x & n \geq 0 \\ -\sum_{k=1}^{-n} x & n < 0 \end{cases} \end{aligned}$$

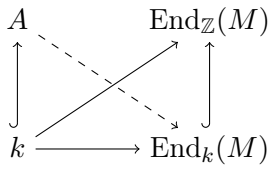
iv) Seien k ein Körper, $A = k[X_1, \ldots, X_n]$ für $n \in \mathbb{N}_{\geq 1}$ und M eine abelsche Gruppe.

Die Angabe eines Ringhomomorphismus $\varphi : A \to \mathrm{End}_{\mathbb{Z}}(M)$ ist äquivalent zur Angabe

a) von einem Ringhomomorphismus $k \to \mathrm{End}_{\mathbb{Z}}(M)$, also ein k-Vektorraumstruktur auf M und

b) von $\varphi_1 = \varphi(X_1), \ldots, \varphi_n = \varphi(X_n) \in \mathrm{End}_k(M)$ mit $\varphi_i \circ \varphi_j = \varphi_j \circ \varphi_i$ für alle $1 \leq i,j \leq n$.

Beachte die universelle Eigenschaft der k-Algebra A:



Die Abbildung $A \to \mathrm{End}_k(M)$ ist dabei durch die φ_i bestimmt.

2.3 **Definition und Bemerkung** (lineare Abbildung)

Seien A ein Ring und M und N zwei A-Moduln.

i) Eine *(A-)lineare Abbildung (von M nach N)* ist ein Homomorphismus abelscher Gruppen $f : M \to N$ mit $f(ax) = af(x)$ für alle $a \in A$ und alle $x \in M$.

ii) Die Menge $\mathrm{Hom}_A(M,N) := \{f : M \to N \mid g \text{ ist } A\text{-linear}\}$ ist ein A-Modul vermöge

$$(f+g)(x) := f(x) + g(x)$$
$$(af)(x) := a(f(x))$$

für alle $f,g \in \mathrm{Hom}_A(M,N)$, alle $x \in A$ und alle $a \in A$.

iii) Sind $\alpha : M' \to M$ und $\beta : N \to N'$ A-linear, so auch

$$\alpha^* : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M',N)$$
$$f \mapsto \alpha^*(f) := f \circ \alpha$$

und:

$$\beta_* : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N')$$
$$f \mapsto \beta^*(f) := \beta \circ f$$

iv) Die Abbildung

$$\varepsilon_M : \mathrm{Hom}_A(A,M) \xrightarrow{\sim} M$$
$$f \mapsto f(1)$$

ist ein A-Modul-Isomorphismus, der *natürlich* in M ist, das heißt, ist $f : M \to N$ A-linear, so ist folgendes Diagramm kommutativ:

$$\begin{array}{ccc} \mathrm{Hom}_A(A,M) & \xrightarrow[\varepsilon_M]{\sim} & M \\ \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f} \\ \mathrm{Hom}_A(A,N) & \xrightarrow[\varepsilon_N]{\sim} & N \end{array}$$

v) Sind wie in 2.2 iv) M_1 und M_2 zwei $A = k[X_1, \ldots, X_n]$-Moduln, bestimmt durch Abbildungen $\varphi_i^{(j)} \in \mathrm{End}_k(M_j)$ für alle $1 \leq i \leq n$, $1 \leq j \leq 2$, so sind die A-linearen Abbildungen $f : M_1 \to M_2$ genau die k-linearen Abbildungen mit $f \circ \varphi_i^{(1)} = \varphi_i^{(2)} \circ f$ für alle $1 \leq i \leq n$.

Beweis

iv): Man sieht leicht, dass ε_M eine A-lineare Abbildung und $\varepsilon_M^{-1}(x)(a) = ax$ ist.
Also ist ε_M ein A-linearer Isomorphismus.
Sei $\varphi \in \mathrm{Hom}_A(A,M)$, so rechne einerseits

$$f(\varepsilon_M(\varphi)) = f(\varphi(1))$$

und andererseits:

$$\varepsilon_N(f_*(\varphi)) = \varepsilon_N(f \circ \varphi) = (f \circ \varphi)(1) = f(\varphi(1))$$

$\square_{\text{iv)}}$

2.4 **Bemerkung und Definition** (Quotientenmodul)

Seien A ein Ring, M ein A-Modul und $N \subseteq M$ ein A-Untermodul.

i) Auf der abelschen Gruppe M/N existiert genau eine A-Modulstruktur so, dass die kanonische Abbildung $\pi : M \to M/N$ A-linear ist, nämlich $a[x] = [ax]$ für alle $a \in A$ und alle $x \in M$.
Der A-Modul M/N heißt *der Quotientenmodul (von M nach N).*

ii) Die Abbildung von Mengen

$$\begin{array}{ccc} \{U \,|\, N \subseteq U \subseteq M \text{ ist } A\text{-Untermodul}\} & \tilde{\to} & \left\{\overline{U} \,|\, \overline{U} \subseteq M/N \text{ ist } A\text{-Untermodul}\right\} \\ U & \mapsto & \pi(U) \end{array}$$

ist bijektiv und inklusionserhaltend. (vergleiche 1.7 für den Spezialfall $M = A$)

iii) Ist L ein weiterer A-Modul, so ist

$$\begin{array}{ccc} \mathrm{Hom}_A\left(M/N, L\right) & \xrightarrow{\sim} & \{f \in \mathrm{Hom}_A(M,L) \,|\, f(N) = 0\} \\ & {\scriptstyle \pi^*} \searrow & \downarrow \\ & & \mathrm{Hom}_A(M,L) \end{array}$$

ein A-linearer Isomorphismus. (vergleiche 1.5 iii))

2.5 Beispiel und Definition (Kokern)

Sei $f : M \to N$ A-linear, so gilt:

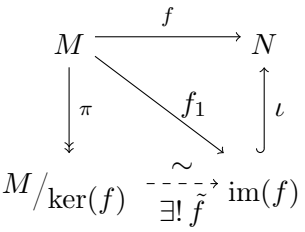
i) $\ker(f) := \{x \in M \mid f(x) = 0\} \subseteq M$ ein A-Untermodul.

ii) Es heißt $\operatorname{koker}(f) := {}^{N}\!/_{\operatorname{im}(f)}$ *der Kokern von* f.

$$\ker(f) \hookrightarrow M \xrightarrow{f} N \twoheadrightarrow \operatorname{koker}(f)$$

2.6 Proposition (Homomorphiesatz)

Sei A ein Ring. Dann faktorisiert jede A-lineare Abbildung $f : M \to N$ wie folgt:



Das heißt es existiert genau eine Abbildung $\tilde{f} : {}^{M}\!/_{\ker(f)} \to \operatorname{im}(f)$ mit $f = \iota \circ \tilde{f} \circ \pi$.
Dieses $\tilde{f}$ ist ein A-linearer Isomorphismus

Beweis

Zunächst faktorisiert f als $f : M \overset{f_1}{\twoheadrightarrow} \operatorname{im}(f) \overset{\iota}{\hookrightarrow} N$, f_1 und ι sind A-linear, es gilt $\ker(f) = \ker(f_1)$ und f_1 ist surjektiv.
Nach 2.4 iii) faktorisiert dann f_1 eindeutig mit einer A-lineare Abbildung $\tilde{f}$

$$f_1 : M \xrightarrow{\pi} {}^{M}\!/_{\ker(f_1)} \xhookrightarrow{\tilde{f}} \operatorname{im}(f)$$

und $\tilde{f}$ ist injektiv und surjektiv, also ein A-linearer Isomorphismus. $\square_{2.6}$

2.7 Definition (Summe, Schnitt, endlich erzeugt)

Seien A ein Ring, M ein A-Modul, I eine Menge und für alle I sei $M_i \subseteq M$ ein A-Untermodul.

i) Der kleinste Untermodul von M, der alle M_i enthält ist:

$$\sum_{i \in I} M_i := \left\{ \sum_{i \in J} x_i \,\middle|\, J \subseteq I \text{ ist endlich, } x_i \in M_i \right\} \subseteq M$$

Er heißt die *Summe der* M_i *(in* M*).*

ii) Der *Schnitt* $\bigcap_{i \in I} M_i \subseteq M$ ist der größte Untermodul von M, der in allen M_i enthalten ist.

iii) Ist für alle $i \in I$ nun $x_i \in M$ ein Element, so ist $Ax_i := \{ax_i | a \in A\} \subseteq M$ der kleinste A-Untermodul, der x_i enthält.

Nach i) ist also $\sum_{i \in I} Ax_i \subseteq M$ der kleinste A-Untermodul von M, der alle x_i enthält.

iv) M heißt genau dann *endlich erzeugt*, wenn es ein $n \in \mathbb{N}_{\geq 1}$ und $x_1, \ldots, x_n \in M$ gibt, mit:

$$M = \sum_{i=1}^{n} Ax_i$$

Beispiel: Für einen Körper k ist der k-Modul $k[X]$ nicht endlich erzeugt.

2.8 **Proposition** (Isomorphiesätze)

Sei A ein Ring.

i) Sind L ein A-Modul und $M \subseteq N \subseteq L$ zwei A-Untermoduln, so existiert genau eine A-lineare Abbildung

$$\varphi : \left(L/M\right) / \left(N/M\right) \xrightarrow{\sim} L/N$$

für die für alle $x \in L$ schon

$$\varphi\left((x + M) + \left(N/M\right)\right) = x + N$$

gilt. Dieses φ ist ein A-linearer Isomorphismus.

ii) Sind M ein A-Modul und M_1,$M_2 \subseteq M$ zwei A-Untermoduln, so existiert genau eine A-lineare Abbildung

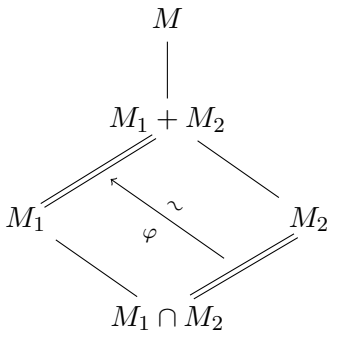
$$\varphi : M_2/(M_1 \cap M_2) \xrightarrow{\sim} M_1 + M_2/M_1$$

für die für alle $x \in M_2$ schon

$$\varphi(x + (M_1 \cap M_2)) = x + M_1$$

gilt. Dieses φ ist ein Isomorphismus.

Merkhilfe:



Beweis

i) Betrachte die Abbildung:

$$\begin{aligned} \psi : {}^{L}\!/_{M} &\to {}^{L}\!/_{N} \\ x + M &\mapsto x + N \end{aligned}$$

Diese ist wegen $M \subseteq N$ wohldefiniert und surjektiv, und offenbar A-linear. Außerdem gilt:

$$\ker \psi = \left\{ x + M \in {}^{L}\!/_{M} \,\middle|\, x + N = N \right\} = \left\{ x + M \in {}^{L}\!/_{M} \,\middle|\, x \in N \right\} = {}^{N}\!/_{M}$$

Damit folgt nach 2.6, dass es eine eindeutige A-lineare Abbildung

$$\varphi : \left({}^{L}\!/_{M} \right) \Big/ \left({}^{N}\!/_{M} \right) \xrightarrow{\sim} {}^{L}\!/_{N}$$

mit

$$\varphi \left((x + M) + \left({}^{N}\!/_{M} \right) \right) = x + N$$

gibt. $\square_{\text{i)}}$

ii) Betrachte die Abbildung:

$$\begin{aligned} \psi : M_2 \hookrightarrow M_1 + M_2 &\twoheadrightarrow {}^{M_1 + M_2}\!/_{M_1} \\ x &\mapsto x + M_1 \end{aligned}$$

Diese Komposition von Inklusions- und Projektionshomomorphismus ist A-linear. Außerdem gilt:

$$\ker \psi = \left\{ x \in M_2 \middle| x + M_1 = M_1 \right\} = \left\{ x \in M_2 \middle| x \in M_1 \right\} = M_1 \cap M_2$$

Damit folgt nach 2.6, dass es eine eindeutige A-lineare Abbildung

$$\varphi : {}^{M_2}\!/_{(M_1 \cap M_2)} \xrightarrow{\sim} {}^{M_1 + M_2}\!/_{M_1}$$

mit

$$\varphi \left(x + (M_1 \cap M_2) \right) = x + M_1$$

gibt. $\square_{\text{ii)}}$

2.9 **Bemerkung und Definition** (Produkt und direkte Summe)

Seien A ein Ring, I eine Menge und für alle $i \in I$ sei M_i ein A-Modul.

i) Das kartesische Produkt $\prod_{i \in I} M_i$ ist ein A-Modul vermöge komponentenweiser Addition und Skalarmultiplikation, *das Produkt der* M_i. Für alle $i_0 \in I$ ist die Abbildung

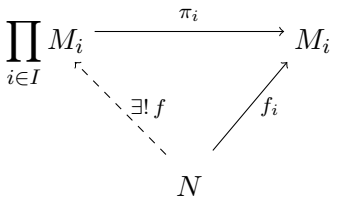
$$\pi_{i_0} : \prod_{i \in I} M_i \to M_{i_0}$$

A-linear und für jeden A-Modul N ist die Abbildung

$$\begin{aligned}\mathrm{Hom}_A\left(N, \prod_{i\in I} M_i\right) &\xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_A\left(N, M_i\right)\\ f &\mapsto \left(\pi_i^* f = \pi_i \circ f\right)_{i\in I}\end{aligned}$$

ein A-linearer Isomorphismus.

Skizze:



Die eindeutige Abbildung ist $f(x) = (f_i(x))_{i\in I}$ für alle $x \in N$.

Dies ist *die universelle Eigenschaft des Produkts.*

ii) Die Teilmenge

$$\bigoplus_{i\in I} M_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} M_i \,\middle|\, \left|\left\{i \in I \middle| x_i \neq 0\right\}\right| < \infty \right\} \subseteq \prod_{i\in I} M_i$$

ist ein A-Untermodul, *die direkte Summe der M_i.*

Die Abbildungen

$$\begin{aligned}\iota_i : M_i &\hookrightarrow \bigoplus_{i\in I} M_i\\ x &\mapsto \left(\iota_i(x)\right)_j := \delta_{ij} \cdot x\end{aligned}$$

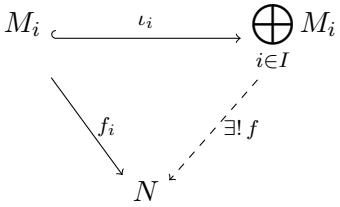
sind A-linear und für jeden A-Modul N ist die Abbildung

$$\begin{aligned}\mathrm{Hom}_A\left(\bigoplus_{i\in I} M_i, N\right) &\xrightarrow{\sim} \prod_{i\in I} \mathrm{Hom}_A\left(M_i, N\right)\\ f &\mapsto \left(f \circ \iota_i = \iota_{i,*}(f)\right)\end{aligned}$$

ein A-linearer Isomorphismus.

Dies ist *die universelle Eigenschaft der direkten Summe.*

Skizze:



Beachte:
$\bigoplus_{i\in I} M_i$ ist nicht dasselbe wie $\sum_{i\in I} M_i$ aus 2.7 i).
Aber falls alle $M_i \subseteq M$ Untermoduln desselben Moduls M sind, gibt es genau eine A-lineare Abbildung

$$f : \bigoplus_{i\in I} M_i \to \sum_{i\in I} M_i$$

für die für alle $i \in I$ und $x_i \in M_i$ schon $f(x_i) = x_i$ gilt.

2.10 Beispiel

Seien A ein Ring und X eine Menge. Dann heißt

$$A^{(X)} := \bigoplus_{x\in X} A$$

der freie A-Modul mit Basis X.
Für jeden A-Modul N erhalte einen A-linearen Isomorphismus:

$$\mathrm{Hom}_A\left(A^{(X)},N\right) \underset{\text{2.9 ii)}}{\overset{\sim}{\to}} \prod_{x\in X} \mathrm{Hom}_A(A,N) \underset{\text{2.3 iv)}}{\overset{\prod \varepsilon_N}{\to}} \prod_{x\in X} N = \mathrm{Abb}(X,N)$$

Dies ist *die universelle Eigenschaft des freien A-Moduls.*

2.11 Satz (Cayley-Hamilton)

Seien A ein Ring, $I \subseteq A$ ein Ideal, M ein durch $n \in \mathbb{N}$ Elemente erzeugbarer A-Modul und

$$f \in \mathrm{End}_A(M) := \mathrm{Hom}_A(M,M)$$

erfülle:

$$f(M) \subseteq IM := \left\{ \sum_{i=1}^{m} \alpha_i x_i \,\middle|\, m \in \mathbb{N}, \alpha_i \in I, x_i \in M \right\} \subseteq M$$

Dann existiert ein

$$P(X) = X^n + a_1 X^{n-1} + \ldots + a_n \in A[X]$$

mit $a_i \in I^i \subseteq A$ für alle $1 \leq i \leq n$ und $P(f) = 0$ in $\mathrm{End}_k(M)$.

Beweis

Wähle Elemente $x_1,\ldots,x_n \in M$ mit $M = \sum_{i=1}^{n} Ax_i$. Schreibe für alle $1 \leq i \leq n$

$$f(x_i) = \sum_{j=1}^{n} a_{ij} \cdot x_j$$

mit geeigneten $a_{ij} \in I$.
Setze $Z := (\delta_{ij} X - a_{ij})_{1 \leq i,j \leq n} \in M_n(A[X])$. Dann gilt:

$$\underbrace{Z(f)}_{\in M_n(\mathrm{End}_A(M))} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

Es folgt durch Linksmultiplikation mit der Adjunkten $Z^{\mathrm{ad}}(f)$ von $Z(f)$:

$$\left(Z^{\mathrm{ad}}(f) \cdot Z(f)\right) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

Wegen $\left(Z^{\mathrm{ad}}(f) \cdot Z(f)\right) = \det(Z)(f) \cdot E_n$ gilt mit $P := \det(Z)$ für alle $1 \leq i \leq n$:

$$P(f)(x_i) = 0$$

Also folgt wegen $M = \sum_{i=1}^{n} Ax_i$, dass $P(f) = 0$ in $\mathrm{End}_A(M)$ gilt.
Bekannte Rechenregeln für die Determinante zeigen, dass P die behauptete Form besitzt. $\square_{2.11}$

2.12 Korollar

Seien A ein Ring, M ein endlich erzeugter A-Modul und $f : M \to M$ ein A-linearer Epimorphismus. Dann ist f ein Isomorphismus.

Beweis

Betrachte M als $A[X]$-Modul vermöge f, das heißt vermöge des Ringhomomorphismus:

$$\begin{aligned} \psi : A[X] &\to \mathrm{End}_{\mathbb{Z}}(M) \\ a(X) &\mapsto a(f) \end{aligned}$$

(vergleiche 2.1 i))

Weil f surjektiv ist, gilt $f(M) = (X)M \overset{f \text{ surjektiv}}{=} M = \mathrm{id}_M(M)$.
Aus dem Satz 2.11 von Cayley-Hamilton mit $A[X]$ als Ring, (X) als Ideal und id_M als Endomorphismus folgt die Existenz eines Polynoms $P(Y) = Y^n + a_1 Y^{n-1} + \ldots + a_n \in A[X][Y]$ mit $a_i \in \left(X^i\right) \subseteq A[X]$ und

$$0 = P(\mathrm{id}_M) = \mathrm{id}_M + a_1 \mathrm{id}_M + \ldots + a_n$$

in $\mathrm{End}_{A[X]}(M)$. Wegen $a_i \in (X)$ folgt durch Ausklammern von X

$$P(Y) = Y^n + g(X,Y) \cdot X$$

für ein geeignetes Polynom $g \in A[X,Y]$ und somit

$$0 = \mathrm{id}_M + g(\mathrm{id}_M, f) \circ f$$

in $\mathrm{End}_A(M)$ für ein geeignetes Polynom g. Damit gilt $\mathrm{id}_M = g(\mathrm{id}_M, f) \circ (-f)$, also ist f injektiv und damit ein Isomorphismus. $\square_{2.12}$

2.13 **Korollar** (Isomorphie erhält Dimension)

Sei $A \neq \{0\}$ ein Ring.
Dann folgt für alle n,$m \in \mathbb{N}_{\geq 1}$ aus der Existenz eines A-linearen Isomorphismus $f : A^n \cong A^m$, dass $n = m$ gilt.

1. Beweis

Sei ohne Einschränkung $n \geq m$, so betrachte die Projektion π auf die ersten m Summanden. Dann ist

$$A^m \underset{f}{\overset{\sim}{\to}} A^n = \underbrace{A \oplus \ldots \oplus A}_{n\text{-mal}} \overset{\pi}{\twoheadrightarrow} A^m$$

ein surjektiver A-linearer Endomorphismus des endlich erzeugten A-Moduls A^m und nach 2.12 also ein Isomorphismus. Damit ist π ein Isomorphismus, also gilt:

$$(0) = \ker(\pi) = A^{n-m}$$

Wegen $A \neq \{0\}$ folgt $n - m = 0$, also $n = m$. $\square_{\text{1. Beweis}}$

2. Beweis

Wegen $A \neq \{0\}$, 1.22 und 1.18 ii) existiert ein maximales Ideal $\mathfrak{m}$ und somit ein Körper $k \cong {}^{A}\!/_{\mathfrak{m}}$ und ein Ringhomomorphismus $A \to k$. Dann ist

$$f \oplus_A 1 : A^n \oplus_A k \overset{\sim}{\to} A^m \oplus_A k$$

ein Isomorphismus von n- und m-dimensionalen k-Vektorräumen. Also gilt $n = m$ nach dem Basisergänzungssatz aus linearer Algebra I. $\square_{\text{2. Beweis}}$

2.14 Bemerkung

i) Offenbar gilt 2.13 nicht für den Nullring.

ii) Es existiert ein notwendigerweise nicht kommutativer Ringe $R \neq \{0\}$ für den $R \cong R^2$ als R-Modul gilt.

2.15 Korollar

Seien A ein Ring, M ein endlich erzeugter A-Modul und $I \subseteq A$ ein Ideal mit $IM = M$.
Dann existiert ein $x \in A$ mit $x \equiv 1 \mod I$ und $xM := \{xm | m \in M\} = (0)$.

Beweis

Wähle in Satz 2.11 von Cayley-Hamilton $f := \mathrm{id}_M$ und dann in dortiger Notation:

$$x := 1 + \underbrace{a_1 + \ldots + a_n}_{\in I} \equiv 1 \mod I$$

$\square_{2.15}$

2.16 **Lemma** (von Nakayama) **und Definition** (Jacobsonradikal)

Seien A ein Ring, M ein endlich erzeugter A-Modul und

$$I \subseteq \mathrm{Jac}\,(A) := \bigcap_{\mathfrak{m} \subseteq A \text{ max. Ideal}} \mathfrak{m}$$

ein Ideal, das im *Jacobsonradikal von* A enthalten ist. Dann folgt aus $IM = M$ schon $M = (0)$.

Beweis

Nach 2.15 existiert ein $x \in A$ mit $xM = (0)$ und $x \equiv 1 \mod I$. Es folgt $x - 1 \in \mathfrak{m}$ für alle maximalen Ideale $\mathfrak{m} \subseteq A$, also $x \notin \mathfrak{m}$, da sonst $1 \in \mathfrak{m}$, und damit $x \in A^*$ nach 1.24 ii) $\Rightarrow$ i). Aus $xM = 0$ und $x \in A^*$ folgt $M = (0)$. $\square_{2.16}$

2.17 Beispiel

Sei $\big(A := \mathbb{Z}_{(p)}, \mathfrak{m} := (p)\big)$ ist nach 1.28 ein lokaler Ring, also gilt $\mathrm{Jac}\,(A) = \mathfrak{m} = (p) \subseteq \mathbb{Z}_{(p)}$.
Für $M := \mathbb{Q}$ aufgefasst als A-Modul – beachte, dass $A \subseteq \mathbb{Q}$ ein Unterring ist – gilt:

$$\mathfrak{m}M = (p) \cdot \mathbb{Q} = \mathbb{Q} = M$$

Wegen $M \neq 0$ folgt aus 2.16, dass M als A-Modul nicht endlich erzeugt ist, beziehungsweise, dass man in 2.16 nicht auf „M endlich erzeugt“ verzichten kann.

2.18 **Proposition** (minimales Erzeugendensystem)

Sei $(A, \mathfrak{m})$ ein lokaler Ring, M ein endlich erzeugter A-Modul und für $x_1, \ldots, x_n \in M$ gelte, dass

$$\{\overline{x}_i\}_{1 \leq i \leq n} \subseteq {}^{M}\!/_{\mathfrak{m}M}$$

eine Basis dieses ${}^{A}\!/_{\mathfrak{m}} = \kappa(\mathfrak{m})$-Vektorraums ist. Dann ist $\{x_1, \ldots, x_n\} \subseteq M$ ein minimales Erzeugendensystem des A-Moduls M.

Beweis

Für

$$N := \sum_{i=1}^{N} Ax_i \subseteq M$$

ist die Komposition $N \hookrightarrow M \overset{\pi}{\twoheadrightarrow} {}^{M}\!/_{\mathfrak{m}M}$ surjektiv, da alle $\overline{x}_i$ im Bild liegen, also gilt:

$$M = \pi(N) = N + \mathfrak{m}M$$

Es folgt ${}^{M}\!/_{N} \subseteq \mathfrak{m} \cdot \left({}^{M}\!/_{N}\right)$ und damit ${}^{M}\!/_{N} = (0)$ nach dem Lemma2.16 von Nakayama, da $\mathrm{Jac}\,(A) = \mathfrak{m}$ ist. Damit gilt:

$$M = N = \sum_{i=1}^{n} Ax_i$$

Also ist $\{x_1, \ldots, x_n\} \subseteq M$ ein Erzeugendensystem, dessen Minimalität sofort aus derjenigen von $\{\overline{x_u}\}_{1 \leq i \leq n}$ folgt. $\square_{2.18}$

2.19 **Definition** (exakte Folge)

Sei A ein Ring. Eine Folge von A-Moduln und A-linearen Abbildungen

$$\ldots \to M_{i-1} \overset{f_{i-1}}{\to} M_i \overset{f_i}{\to} M_{i+1} \to \ldots$$

heißt *exakt an der Stelle* M_i, falls gilt:

$$\operatorname{im}(f_{i-1}) = \ker(f_i)$$

(„$\subseteq$“ bedeutet $f_i \circ f_{i-1} = 0$ und „$\supseteq$“ bedeutet $f_i(x) = 0 \Rightarrow x = f_{i-1}(y)$.)
Sie heißt *exakt*, falls sie an jeder Stelle exakt ist.

2.20 **Beispiel und Definition** (kurze exakte Folge)

In der Situation von 2.19 gilt:

i) $0 \to M \overset{f}{\to} N$ exakt $\Leftrightarrow 0 = \ker(f) \Leftrightarrow f$ ist injektiv.

ii) $M \overset{f}{\to} N \to 0$ exakt $\Leftrightarrow \operatorname{im}(f) = N \Leftrightarrow f$ ist surjektiv.

iii) $0 \to M \overset{f}{\to} N \overset{g}{\to} L \to 0$ exakt $\Leftrightarrow f$ injektiv, g surjektiv und $\operatorname{im}(f) = \ker(g)$.
In diesem Fall heißt die $0 \to M \overset{f}{\to} N \overset{g}{\to} L \to 0$ *eine kurze exakte Folge.*

2.21 **Proposition**

Sei A ein Ring.

i) Eine Folge $\mathscr{E} = \left(M' \overset{f}{\to} M \overset{g}{\to} M'' \to 0\right)$ von A-Moduln ist genau dann exakt, wenn für alle A-Moduln N die Folge

$$\operatorname{Hom}_A(\mathscr{E},N) := \left(0 \to \operatorname{Hom}_A(M'',N) \overset{g^*}{\to} \operatorname{Hom}_A(M,N) \overset{f^*}{\to} \operatorname{Hom}_A(M',N)\right)$$

exakt ist.

ii) Eine Folge $\mathscr{E} = \left(0 \to M' \overset{f}{\to} M \overset{g}{\to} M''\right)$ von A-Moduln ist genau dann exakt, wenn für alle A-Moduln N die Folge

$$\operatorname{Hom}_A(N,\mathscr{E}) := \left(0 \to \operatorname{Hom}_A(N,M') \overset{f_*}{\to} \operatorname{Hom}_A(N,M) \overset{g_*}{\to} \operatorname{Hom}_A(N,M'')\right)$$

exakt ist.

Beweis

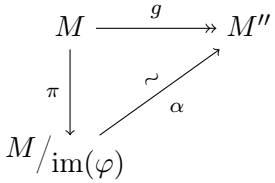
i) Sei $\mathscr{E}$ exakt. Zeige die Exaktheit von $\mathrm{Hom}_A(\mathscr{E},N)$ an der Stelle $\mathrm{Hom}_A(M,N)$:
Für $\varphi \in \mathrm{Hom}_A(M'',N)$ gilt:

$$(f^* \circ g^*)(\varphi) = \varphi \circ \underbrace{g \circ f}_{=0} \overset{\mathrm{im}(f) \subseteq \ker(g)}{=} 0$$

Ist umgekehrt $\varphi \in \ker(f^*) \subseteq \mathrm{Hom}_A(M,N)$, so gilt $0 = f^*(\varphi) = \left(M' \overset{f}{\to} M \overset{\varphi}{\to} N\right)$, das heißt $\varphi(\mathrm{im}(f)) = 0$ und wegen 2.4 iii) (mit $N = \mathrm{im}(\varphi)$ und $L = N$ in dortiger Notation) existiert genau eine A-lineare Abbildung $\psi : {}^{M}\!/_{\mathrm{im}(f)} \to N$ mit:

$$\varphi = \left(M \overset{\pi}{\twoheadrightarrow} {}^{M}\!/_{\mathrm{im}(f)} \overset{\psi}{\to} N\right)$$

Andererseits faktorisiert g über einen Isomorphismus $\alpha : {}^{M}\!/_{\mathrm{im}(f)} \twoheadrightarrow M''$:



Da g surjektiv ist. Es folgt:

$$\varphi = \psi \circ \pi = \psi \circ \alpha^{-1} \circ \alpha \circ \pi = \psi \circ \alpha^{-1} \circ g = g^*\left(\psi \circ \alpha^{-1}\right) \in \mathrm{im}(g^*)$$

Insgesamt gilt also $\ker(f^*) = \mathrm{im}(g^*)$. Der Rest des Beweises bleibt als Übung.

$\square_{2.21}$

2.22 Bemerkung

2.21 überträgt sich nicht auf exakte Folgen $\mathscr{E}$ beliebiger Gestalt.
Zum Beispiel ist

$$\mathscr{E} := \left(0 \to \mathbb{Z} \overset{(\cdot 2)}{\to} \mathbb{Z}\right)$$
$$x \mapsto 2x$$

eine exakte Folge von $\mathbb{Z}$-Moduln, aber die Folge

$$\mathrm{Hom}_{\mathbb{Z}}(\mathscr{E},\mathbb{Z}) = \left(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \overset{(\cdot 2)^*}{\to} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \overset{0^*}{\to} \mathrm{Hom}_{\mathbb{Z}}(0,\mathbb{Z}) = 0\right)$$

ist nicht exakt, da $\mathrm{id}_{\mathbb{Z}} \in \ker(0^*) \setminus \mathrm{im}((\cdot 2)^*)$ liegt, denn sonst wäre $\mathrm{id}_{\mathbb{Z}} = (\cdot 2)^*(f)$ für eine geeignete $\mathbb{Z}$-lineare Abbildung $f : \mathbb{Z} \to \mathbb{Z}$, also

$$1 = \mathrm{id}_{\mathbb{Z}}(1) = ((\cdot 2)^*(f))(1) = f(2 \cdot 1) = 2 \cdot f(1)$$

in $\mathbb{Z}$. Dies ist ein Widerspruch, da $1 \notin 2 \cdot \mathbb{Z}$ ist.

2.23 Projektive Moduln

2.23.1 Definition (spalten, direkter Summand)

i) Eine kurze exakte Folge $0 \to M' \to M \overset{\pi}{\underset{s}{\rightleftarrows}} M'' \to 0$ von A-Moduln *spaltet* genau dann, wenn es eine A-lineare Abbildung $s : M'' \to M$ mit $\pi \circ s = \mathrm{id}_{M''}$ gibt.

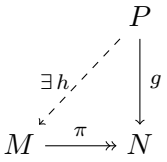
ii) Ein A-Untermodul $N \overset{\iota}{\hookrightarrow} M$ ist genau dann *ein direkter Summand (von M)*, wenn eine A-lineare Abbildung $f : M \to N$ mit $f \circ \iota = \mathrm{id}_N$ existiert.
(In diesem Fall gilt $M = N \oplus \ker(f)$.)
Zum Beispiel ist $2\mathbb{Z} \subseteq \mathbb{Z}$ kein direkter Summand und $0 \to 2\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ spaltet nicht, da die einzige A-lineare Abbildung von $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ die Nullabbildung ist.

2.23.2 Proposition und Definition (Lift, projektiver Modul)

Sei A ein Ring. Für einen A-Modul P sind äquivalent:

i) Jede kurze exakte Folge von A-Moduln der Form $0 \to M' \to M \to P \to 0$ spaltet.

ii) Für jeden A-linearen Epimorphismus $\pi : M \twoheadrightarrow N$ in einen Ring N und jede A-lineare Abbildung $g : P \to N$ existiert *ein Lift von g*, also eine A-lineare Abbildung $h : P \to M$ mit $\pi \circ h = g$.
Skizze:

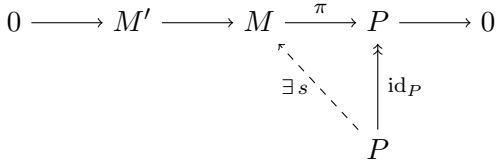


iii) P ist direkter Summand eines freien A-Moduls.

In diesem Fall heißt der A-Modul P *projektiv*.

Beweis

„ii) ⇒ i)“: Betrachte:



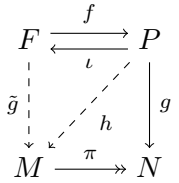
Weil π surjektiv ist und wegen ii) existiert eine A-lineare Abbildung $s : P \to M$ mit $\mathrm{id}_P = \pi \circ s$, das heißt obige Folge spaltet.
„i) ⇒ iii)“: Es existiert ein freier A-Modul F zusammen mit einem A-linearen Epimorphismus $\pi : F \twoheadrightarrow P$, zum Beispiel $F = A^{(P)} \twoheadrightarrow P$ mit der kanonischen Projektion.

Wegen i) spaltet die kurze exakte folge $0 \to \ker(\pi) \to F \xrightarrow{\pi} P \to 0$, das heißt es existiert eine A-lineare Abbildung $\iota : P \to F$ mit $\pi \circ \iota = \mathrm{id}_P$. Damit ist $P' := \iota(P) \subseteq F$ ein zu P isomorpher A-Modul, der durch $f := \iota \circ \pi : F \to P'$ als direkter Summand von F erkannt wird.

„iii) ⇒ ii)“: Nach Voraussetzung gilt $P \xhookrightarrow{\iota} F$ für einen freien A-Modul F und es existiert eine A-lineare Abbildung $f : F \to P$ mit:

$$f \circ \iota = \mathrm{id}_P \tag{2.1}$$

Betrachte:



Sei $X \subseteq F$ eine A-Basis. Weil F frei ist, existiert eine A-lineare Abbildung $\tilde{g} : F \to M$, sodass für alle $x \in X$ gilt:

$$\pi \circ \tilde{g}(x) = g \circ f(x)$$

Man wählt einfach für $\tilde{g}(x)$ ein Element aus $\pi^{-1}(g(f(x))) \neq \emptyset$, was immer geht, da π surjektiv ist. Weil F frei ist und $\tilde{g}$ dadurch auf einer Basis von F bestimmt ist, ist F schon vollständig festgelegt und es folgt:

$$\pi \circ \tilde{g} = g \circ f \tag{2.2}$$

Setze nun $h := \tilde{g} \circ \iota$ und rechne:

$$\pi \circ h = \pi \circ \tilde{g} \circ \iota \overset{2.2}{=} g \circ f \circ \iota \overset{2.1}{=} g \circ \mathrm{id}_P = g$$

Daher ist h ein Lift von g. $\square_{2.23.2}$

2.23.3 Proposition

Äquivalent zu i) bis iii) in 2.23.2 ist ebenfalls:

iv) Für jede kurze exakte Folge von A-Moduln $\mathscr{E} = (0 \to M' \to M \to M'' \to 0)$ ist die Folge $\mathrm{Hom}_A(P, \mathscr{E})$ ebenfalls exakt.

Beweis

Der Beweis bleibt als Übung. $\square_{2.23.3}$

Anhang

Danksagungen

Mein besonderer Dank geht an Professor Naumann, der diese Vorlesung hielt und es mir gestattete, diese Vorlesungsmitschrift zu veröffentlichen.

Außerdem möchte ich mich ganz herzlich bei allen bedanken, die durch aufmerksames Lesen Fehler gefunden und mir diese mitgeteilt haben.

Andreas Völklein

GNU Free Documentation License

0. Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. Applicability and definitions

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "**Document**", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "**you**". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "**Modified Version**" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "**Secondary Section**" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "**Invariant Sections**" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "**Cover Texts**" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "**Transparent**" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "**Opaque**".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "**Title Page**" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "**publisher**" means any person or entity that distributes copies of the Document to the public.

A section "**Entitled XYZ**" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "**Acknowledgements**", "**Dedications**", "**Endorsements**", or "**History**".) To "**Preserve the Title**" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that

these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. Verbatim copying

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. Copying in quantity

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. Modifications

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution

and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. Combining documents

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. Collections of documents

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. Aggregation with independent works

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. Translation

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. Termination

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. Future revisions of this license

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See `https://www.gnu.org/copyleft/`.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. Relicensing

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

Addendum: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright © YEAR YOUR NAME.
> Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation;
>
> with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

> A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with ... Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.