Inhaltsverzeichnis

1 Moduln

1.1 Definitionen und grundlegende Tatsachen

1.1.1 Definition.
Ein *Modul* ist ein Tupel $(R, +_R, \cdot_R, M, +, \cdot)$, wobei $(R, +_R, \cdot_R)$ ein Ring (mit 1, nicht notwendigerweise kommutativ), $(M, +)$ eine abelsche Gruppe und
$\cdot : R \times M \to M$ eine (meist gar nicht oder infix geschriebene) Abbildung mit folgenden Eigenschaften

$(\vec{D})$ $\forall a \in R : \forall x, y \in M : a(x + y) = ax + ay$ „distributiv“

(D') $\forall a, b \in R : \forall x \in M : (a + b)x = ax + bx$ „distributiv“

(N) $\forall x \in M : 1_R \cdot x = x$ „normiert“

(V) $\forall a, b \in R : \forall x \in M : (ab)x = a(bx)$ „verträglich“

1.1.2 Bemerkung.

(a) Schlampiger Sprachgebrauch:
- „Sei M ein R-Modul“ statt „Sei $(R, +_R, \cdot_R, M, +, \cdot)$ ein Modul“
- „Sei M ein Modul“ statt „Es gebe einen Ring R so, dass M ein R-Modul ist“

(b) Statt „R-Modul“ sagt man auch „Modul über R“

(c) Vektorräume sind Moduln über Körper. Viele Sprechweisen (wie „Skalar“, „Linearkombination“, nicht jedoch „Vektor“) übertragen wir stillschweigend von Vektorräumen auf Moduln, ebenso Konventionen (wie „Punkt vor Strich“).

(d) Abelsche Gruppen „sind“ $\mathbb{Z}$-Moduln. Sei G eine abelsche Gruppe. Dann gibt es genau eine Skalarmultiplikation $\cdot : \mathbb{Z} \times G \to G$ vermöge derer G zu einem $\mathbb{Z}$-Modul wird, nämlich die natürliche, die durch

$$n \cdot a := \begin{cases} \underbrace{a + a + \cdots + a}_{n\text{-mal}} & \text{falls } n > 0 \\ 0 & \text{falls } n = 0 \\ \underbrace{-a - a - \cdots - a}_{(-n)\text{-mal}} & \text{falls } n < 0 \end{cases}$$

gegeben ist.

(e) $(\vec{D})$ besagt, dass für alle $a \in R$ die Abbildung $M \to M, x \mapsto ax$ ein Gruppenhomomorphismus ist. Insbesondere gilt $a \cdot 0 = 0$ und $a \cdot (-x) = -ax$ für alle $a \in R, x \in M$.

(D') besagt, dass für alle $x \in M$ die Abbildung $R \to M, a \mapsto ax$ ein Gruppenhomomorphismus ist. Insbesondere gilt $0 \cdot x = 0$ und $(-a) \cdot x = -ax$ für alle $a \in R, x \in M$.

1.1.3 Beispiel.

(a) Nullmoduln $\{0\}$

(b) Sei A ein Unterring des Ringes B. Dann ist B ein A-Modul vermöge der Skalarmultiplikation $\cdot : A \times B \to B, (a, x) \mapsto ax$

Insbesondere ist jeder Ring ein Modul über sich selbst.

(c) Sei R ein kommutativer Ring und $n \in \mathbb{N}_0$. Dann wird die abelsche Gruppe R^n zu einem $R^{n \times n}$-Modul vermöge der Skalarmultiplikation

$$\cdot : R^{n \times n} \times R^n \to R^n, (A, x) \mapsto Ax$$

Dies folgt aus den Rechenregeln für Matrixmultiplikation.

1.1.4 Definitionen, Propositionen, Sätze und Notationen.
Sei R ein Ring. Die folgenden für die Theorie der R-Moduln grundlegenden Begriffe und Resultate sind eine direkte Verallgemeinerung der entsprechenden Tatsachen für Vektorräume (also für den Fall, dass R ein Körper) und für abelsche Gruppen (also $R = \mathbb{Z}$) aus der Linearen Algebra:

(a) Genauso wie bei Vektorräumen führt man *direkte Produkte* von R-Moduln ein.

(b) Sind M und N R-Moduln, so heißt N ein *Untermodul* von M, wenn die N zugrunde liegende abelsche Gruppe eine Untergruppe der M zugrunde liegenden abelschen Gruppe ist und

$$\forall a \in R : \forall x \in M : a \cdot_N x = a \cdot_M x$$

Ein Untermodul eines Moduls ist offenbar durch seine Trägermenge (d.h. seine zugrunde liegende Menge) eindeutig bestimmt.

Ist M ein R-Modul und $N \subseteq M$, so ist N offenbar genau dann (Trägermenge) ein(es) Untermodul(s) von M, wenn

- $0 \in N$
- $\forall x, y \in N : x + y \in N$
- $\forall a \in R : \forall x \in N : ax \in N$

(c) Sei M ein Modul und $(N_i)_{i\in I}$ eine Familie von Untermoduln von M. Dann ist $\bigcap\limits_{i\in I} N_i := \bigcap\{N_i \mid i \in I\}$ (mit $\bigcap\limits_{i\in I} N_i = M$, falls $I = \emptyset$) wieder ein Untermodul von M und zwar der größte Untermodul von M, der in allen N_i enthalten ist.

Weiter ist auch $\sum\limits_{i\in I} N_i := \left\{\sum\limits_{i\in I} x_i \mid (x_i)_{i\in I} \in \prod\limits_{i\in I} N_i, \{i \in I \mid x_i \neq 0\} \text{ endlich}\right\}$ Untermodul von M und zwar der kleinste Untermodul von M, der alle N_i enthält.

(d) Sei M ein R-Modul. Ist $x \in M$, so ist $Rx := \{ax \mid a \in R\}$ ein Untermodul von M und zwar der kleinste Untermodul, der x enthält.

Ist $(x_i)_{i\in I}$ eine Familie von Elementen von M, so ist $\sum_{i\in I} Rx_i$ der kleinste Untermodul von M, der alle x_i enthält.

Man nennt ihn den von den x_i $(i \in I)$ (oder $\{x_i \mid i \in I\}$) erzeugten Untermodul von M (oder lineare Hülle der Span von $\{x_i \mid i \in I\}$).

Man nennt M *zyklisch*, wenn M von einem Element erzeugt wird, d.h. es ein $x \in M$ gibt mit $M = Rx$. Man nennt M endlich erzeugt (e.e.), wenn M von endlich vielen Elementen erzeugt wird, d.h. es ein $n \in \mathbb{N}_0$ und $x_1, \dots, x_n \in M$ gibt mit

$$M = Rx_1 + \cdots + Rx_n := \sum_{i=1}^{n} Rx_i := \sum_{i\in\{1,\dots,n\}} Rx_i$$

(e) Sei M ein R-Modul. Eine Familie $(x_i)_{i\in I}$ in M heißt *linear unabhängig* (l.u.), wenn für alle $n \in \mathbb{N}_0$, alle paarweise verschiedenen $i_1, \dots, i_n \in I$ und alle $a_1, \dots, a_n \in I$ gilt

$$\sum_{j=1}^{n} a_j x_{i_j} = 0 \Rightarrow a_1 = \cdots = a_n = 0$$

Weiter nennt man $x_1, \dots, x_n \in M$ linear unabhängig, wenn $(x_1, \dots, x_n) = (x_i)_{i\in\{1,\dots,n\}}$ linear unabhängig ist, d.h. für alle $a_1, \dots, a_n \in R$ gilt

$$(*) \qquad a_1x_1 + \cdots a_nx_n = 0 \Rightarrow a_1 = \cdots = a_n = 0$$

Schließlich heißt eine Menge $F \subseteq M$ linear unabhängig, wenn $(x)_{x\in F}$ linear unabhängig ist, d.h. für alle $n \in \mathbb{N}_0$, alle paarweise verschiedenen $x_1, \dots, x_n \in F$ und alle $a_1, \dots, a_n \in R$ wieder $(*)$ gilt.

(f) Sei M ein Modul. Eine Familie $(x_i)_{i\in I}$ in M heißt eine *Basis* von M, wenn sie M erzeugt und linear unabhängig ist. Weiter sagt man $x_1, \dots, x_n \in M$ bilden eine Basis von M, wenn $(x_1, \dots, x_n) = (x_i)_{i\in\{1,\dots,n\}}$ eine Basis von M ist. Schließlich heißt $B \subseteq M$ eine Basis, wenn B den Modul M erzeugt und linear unabhängig ist.

(g) Seien M und N R-Moduln. Dann heißt f ein *(R-)(Modul-)Homomorphismus* oder eine ($R-$) lineare Abbildung von M nach N, wenn $f : M \to N$ ein Gruppenhomomorphismus der M und N zugrundeliegenden abelschen Gruppen ist und

$$\forall a \in R : \forall x \in M : f(ax) = af(x)$$

Ein Modulhomomorphismus $f : M \to N$ heißt Einbettung/Monomorphismus (Epimorphismus, Isomorphismus), wenn f injektiv (surjektiv, bijektiv) ist.

Ein Modulhomomorphismus $f : M \to M$ heißt *(Modul-)Endomorphismus* von M. Ein Endomorphismus, der ein Isomorphismus ist, heißt *Automorphismus*. Es heißen M und N *isomorph*, in Zeichen $M \cong N$, wenn es einen Isomorphismus $M \to N$ gibt.

Hintereinanderschaltungen von Modulhomomorphismen sind wieder Modulhomomorphismen. Umkehrabbildungen von Modulisomorphismen sind wieder Modulisomorphismen.

(h) Sei M ein R-Modul. Eine *Kongruenzrelation* auf M ist eine Äquivalenzrelation $\equiv$ der M zugrundeliegenden Menge, für die gilt

$$\forall x, y, x', y' \in M : (x \equiv x' \wedge y \equiv y') \Rightarrow x + y \equiv x' + y'$$

und

$$\forall x, x' \in M : \forall a \in R : x \equiv x' \Rightarrow ax \equiv ax'$$

Diese Definition wurde gerade so gemacht, dass

$$\begin{aligned} + : (M/\equiv) \times (M/\equiv) &\to (M/\equiv) \\ (\overline{x}, \overline{y}) &\mapsto \overline{x+y} \end{aligned}$$

und

$$\begin{aligned} \cdot : R \times (M/\equiv) &\to (M/\equiv) \\ (a, \overline{x}) &\mapsto \overline{ax} \end{aligned}$$

wohldefiniert sind.

Ist M ein R-Modul und $\equiv$ eine Kongruenzrelation auf M, so wird die Quotientenmenge $M/\equiv$ vermöge der Addition $+$ und der Skalarmultiplikation $\cdot$ ein R-Modul, wie man durch direktes Nachrechnen sieht. Die Zuordnungen

$$\equiv \overset{f}{\mapsto} \overline{0}$$

$$\equiv_N \overset{g}{\hookleftarrow} N$$

vermitteln eine Bijektion zwischen der Menge der Kongruenzrelationen auf M und der Menge der Untermoduln von M, wobei $\equiv_N$ gegeben ist durch

$$a \equiv_N b :\Leftrightarrow a - b \in N$$

für $a, b \in M$.

Ist N ein Untermodul von M, so nennt man $M/N := M/\equiv_N$ auch den *Quotientenmodul* von M nach N.

(i) Sind M und N R-Moduln und $f : M \to N$ ein Modulhomomorphismus, so ist der *Kern* $\ker f := \{x \in M \mid f(x) = 0\}$ von f ein Untermodul von M und das *Bild* $\operatorname{im} f := \{f(x) \mid x \in M\}$ von f ist ein Untermodul von N.

(j) Homomorphiesatz: Seien M und N R-Moduln und L ein Untermodul von M und $f : M \to N$ ein Modulhomomorphismus mit $L \subseteq \ker f$. Dann gibt es (genau) einen Modulhomomorphismus $\overline{f} : (M/L) \to N$ mit $\overline{f}(\overline{x}) = f(x)$ für alle $x \in M$.

Ferner gilt, dass

- $\overline{f}$ ist injektiv $\Leftrightarrow L = \ker f$ und
- $\overline{f}$ ist surjektiv $\Leftrightarrow f$ ist surjektiv

(k) Isomorphiesatz: Seien M und N R-Moduln und $f : M \to N$ ein Modulhomomorphismus. Dann ist $\overline{f} : (M/\ker f) \to \operatorname{im} f$ definiert durch $\overline{f}(\overline{x}) = f(x)$ für alle $x \in M$ ein R-Modulisomorphismus. Insbesondere ist $M/\ker f \cong \operatorname{im} f$

1.1.5 Bemerkung.
Sei R ein kommutativer Ring. Dann sind die Untermoduln des R-Modul R [$\to$1.1.3(b)] (oder kurz gesagt die R-Untermoduln von R) genau die Ideale des Ringes R. Insbesondere sind zum Beispiel das von einem $a \in R$ erzeugte Ideal und der davon erzeugte Untermodul als Menge dasselbe $(a)_R = Ra \overset{R \text{ komm.}}{=} \{ab \mid b \in R\} = aR$. Trotzdem macht es vom Sinn her einen Unterschied. ob man (a) oder Ra schreibt. Zum Beispiel meint man mit $R/(a)$ den Ring und mit R/aR den R-Modul (deren zugrundeliegenden abelschen Gruppen dieselben sind)

1.1.6 Warnung.
Für den mit Vektorräumen, aber nicht mit Moduln vertrauten Hörern ist Vorsicht geboten:

(a) In einem R-Modul M kann $ax = 0$ für ein $a \in R$ und ein $x \in M$ gelten, ohne dass $a = 0$ oder $x = 0$ gilt (zum Beispiel $2 \cdot \overline{1} = \overline{2} = 0$ im $\mathbb{Z}$-Modul $\mathbb{Z}/2\mathbb{Z}$)

(b) Nicht jeder Modul hat eine Basis: zum Beispiel ist jedes Element des $\mathbb{Z}$-Moduls $\mathbb{Z}/2\mathbb{Z}$ linear abhängig, denn $1 \cdot \overline{0} = \overline{0} = 0$ und $2 \cdot \overline{1} = \overline{2} = 0$ in $\mathbb{Z}/2\mathbb{Z}$, womit die einzige linear unabhängige Teilmenge von $\mathbb{Z}/2\mathbb{Z}$ die leere Menge is, welche aber $\mathbb{Z}/2\mathbb{Z}$ nicht erzeugt.

1.1.7 Beispiel.

(a) Für jeden Ring R ist R^n ein R-Modul mit der *Standardbasis* $\underline{e} = (e_1, \dots, e_n)$, wobei

$$e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ mit einer 1 an der } i\text{-ten Stelle.}$$

(b) $\mathbb{R}^2$ ist ein zyklischer $\mathbb{R}^{2\times 2}$-Modul [$\rightarrow$1.1.3(c)], welcher von jedem $x \in \mathbb{R}^2 \setminus \{0\}$ erzeugt ist. Da aber jedes $x \in \mathbb{R}^2$ linear abhängig ist, hat dieser Modul keine Basis.

1.2 Direkte Summen von Moduln und freie Moduln

1.2.1 Definition.
Sei R ein Ring und $(M_i)_{i\in I}$ eine Familie von R-Moduln. Dann nennt man den R-Untermodul

$$\bigoplus_{i\in I} M_i := \left\{ x \in \prod_{i\in I} M_i \mid \operatorname{supp}(x) \text{ endlich} \right\}$$

von $\prod\limits_{i\in I} M_i$ die *(äußere) direkte Summe* der M_i $(i \in I)$. Man fasst M_j $(j \in I$ häufig) als Untermodul von $\bigoplus\limits_{i\in I} M_i$ auf vermöge der Einbettung

$$\rho_j : M_j \to \prod_{i\in I} M_i, x \mapsto \left(i \mapsto \begin{cases} x & \text{falls } i = j \\ 0 & \text{sonst} \end{cases} \right)$$

Ist $M_i = M$ für alle $i \in I$, so schreibt man

$$M^{(I)} := \bigoplus_{i\in I} M \subseteq \prod_{i\in I} M = M^I$$

1.2.2 Proposition.
Sei R ein Ring, $(M_i)_{i\in I}$ eine Familie von R-Moduln, N ein R-Modul und $(f_i)_{i\in I}$ eine Familie von Modulhomomorphismen $f_i : M_i \to N$. Dann gibt es genau einen Modulhomomorphismus $f : \bigoplus\limits_{i\in I} M_i \to N$ mit $f\big|_{M_i} = f_i$ für alle $i \in I$ $(f \circ \rho_i = f_i$ für $i \in I)$.

Beweis. Für jedes $x \in \bigoplus\limits_{i\in I} M_i$ gilt $x = \sum\limits_{i\in \operatorname{supp}(x)} \rho_i(x(i))$. Um $f \circ \rho_i = f_i$ für $i \in I$ zu erfüllen, kann man daher nur

$$f : \bigoplus_{i\in I} M_i \to N, x \mapsto \sum_{i\in I} f_i(x(i))$$

definieren. Man überprüft sofort, dass das so definierte f ein Homomorphismus ist. □

1.2.3 Proposition und Definition.
Sei R ein Ring, M ein R-Modul und $(N_i)_{i\in I}$ eine Familie von Untermoduln on M. Dann sind die folgenden Bedingungen äquivalent

(a) Die Abbildung von der äußeren direkten Summe $\bigoplus_{i\in I} N_i$ nach M, die auf N_i die Identität ist, ist ein Isomorphismus

(b) $M = \sum\limits_{i\in I} N_i$ und für alle $n \in \mathbb{N}$, paarweise verschiedenen $i_1, \ldots, i_n \in I$ und alle $x_1 \in N_{i_1}, \ldots, x_n \in N_{i_n}$ gilt

$$(x_1 + \cdots + x_n = 0) \Rightarrow (x_1 = \cdots = x_n = 0)$$

Gelten diese Bedingungen, so nennt man M die *(innere) direkte Summe* der N_i $(i \in I)$ und schreibt (angesichts der Isomorphismus aus (a)) wieder $M = \bigoplus_{i \in I} N_i$

1.2.4 Definition.
Sei R ein Ring, M ein R-Modul und $x \in M$. Der Kern des R-Modulhomomorphismus $R \to M, a \mapsto ax$ nennt man *Annihilator* von x, in Zeichen $\operatorname{ann}(x) = \{a \in R \mid ax = 0\}$. Es heißt x ein *Torsionselement* von M wenn $\operatorname{ann}(x) \neq \{0\}$.

1.2.5 Satz.
Sei R ein Ring, M ein R-Modul und $B \subseteq M$. Dann sind äquivalent

(a) B ist eine Basis von M

(b) $M = \bigoplus_{x \in B} Rx$ und B enthält kein Torsionselement

(c) Für jeden R-Modul N und jede Abbildung $g : B \to N$ gibt e genau einen Homomorphismus $f : M \to N$ mit $f\big|_B = g$.

Beweis.
(a) $\Longrightarrow$ (b) klar

(b) $\Longrightarrow$ (c) Gelte (b). Sei N ein R-Modul und $g : B \to N$ eine Abbildung. Zu zeigen sind Existenz und Eindeutigkeit eines Homomorphismus $f : M \to N$ mit $f\big|_B = g$
Eindeutigkeit: klar aus $M = \sum_{x \in B} Rx$
Existenz: Fixiere zunächst $x \in B$. Dann ist $R \to Rx, a \mapsto ax$ ein Isomorphismus (mit Kern $\operatorname{ann}(x) = \{0\}$), dessen Umkehrfunktion ein Isomorphismus $Rx \to R$ ist, der x auf 1 abbildet. Schaltet man den Homomorphismus $R \to N, a \mapsto ag(x)$ dahinter, so erhält man einen Homomorphismus $Rx \to N$, der x auf $g(x)$ abbildet. Da $x \in B$ beliebig war, erhält man mit 1.2.2 einen Homomorphismus $f : \ M \ = \ \bigoplus_{x \in B} Rx \ \to \ N$, der jedes $x \in B$ auf $g(x)$ abbildet.

(c) $\Longrightarrow$ (a) Gelte (c). Zu zeigen ist, dass B linear unabhängig ist und M erzeugt.
B linear unabhängig: Seien $x_1, \dots, x_n \in B$ paarweise verschieden und $a_1, \dots, a_n \in R$ mit $a_1x_1 + \dots + a_nx_n = 0$. Sei $i \in \{1, \dots, n\}$. Zu zeigen ist $a_i = 0$. Gemäß (c) gibt es einen Homomorphismus $f : M \to R$ mit $f(x_i) = 1$ und $f(x_j) = 0$ für $j \in \{1, \dots, n\} \setminus \{i\}$. Dann

$$0 = f(0) = f\left(\sum_{j=1}^{n} a_j x_j\right) = \sum_{j=1}^{n} a_j f(x_j) = a_i f(x_i) = a_i$$

B erzeugt M: Nach (c) gibt es einen Homomorphismus $M \to M$, der auf B die Identität ist. Einerseits ist id_M ein solcher, andererseits auch $\rho \circ f$, wobei $f : M \to N := \sum_{x \in B} Rx$ der nach (c) existierende Homomorphismus mit $f\big|_B = \mathrm{id}_B$ ist und $\iota : N \hookrightarrow M, x \mapsto x$ die Inklusion. Also $\mathrm{id}_M = \iota \circ f$, insbesondere $M = \operatorname{im}(\mathrm{id}_M) = \operatorname{im}(f) = N$ $\square$

1.2.6 Definition.
Ein Modul heißt *frei*, wenn er eine Basis besitzt.

1.2.7 Bemerkung.
Sei R ein Ring, M ein R-Modul, $n \in \mathbb{N}_0$ und $x_1, \dots, x_n \in M$. Dann bilden $x_1, \dots, x_n$ genau dann eine Basis von M, wenn der Homomorphismus

$$R^n \to M, \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum_{i=1}^{n} a_i x_i$$

ein Isomorphismus ist.

1.2.8 Bemerkung.
Ist M ein $\{0\}$-Modul, so ist $M = \{0\}$, denn ist $x \in M$, so ist $x = 1 \cdot x = 0 \cdot x = 0$

1.2.9 Lemma.
Ein endlich erzeugter Modul hat niemals eine unendliche Basis.

Beweis. Sei M ein endlich erzeugter R-Modul, etwa $M = \sum_{i=1}^{n} Rx_i$ mit $x_1, \dots, x_n \in M$.
Annahme: B ist eine unendliche Basis von M. Dann gibt es für jedes $i \in \{1, \dots, n\}$ ein endliches $B_i \subseteq B$ mit $x_i \in \sum_{y \in B_i} Ry$. Dann ist $B' := B_1 \cup \cdots \cup B_n \subseteq B$ endlich mit $M = \sum_{y \in B'} Ry$. Da B unendlich h ist, gibt es ein $z \in B \setminus B'$

Nun gilt $z \in \sum_{y \in B'} Ry$, was im Widerspruch zur linearen Unabhängigkeit von B steht, außer wenn $1 = 0$ in R, d.h. $R = \{0\}$. Im letzten Fall ist aber nach 1.2.8 nichts zu zeigen. □

1.2.10 Bemerkung.

(a) Jeder Modul über dem Nullring hat genau zwei Basen, nämlich $\emptyset$ und $\{0\}$. In der Tat: Nach 1.2.8 handelt es sich um den Nullmodul und in einem $\{0\}$-Modul ist 0 linear unabhängig.

(b) In den Übungen geben wir einen Ring $R \neq \{0\}$, der als R-Modul zu R^2 isomorph ist. Durch Induktion schließt man, dass $R \cong R^n$ für alle $n \in \mathbb{N}$. Damit besitzt R als R-Modul für jedes $n \in \mathbb{N}$ eine n-elementige Basis, aber nach 1.2.9 keine unendliche Basis.

1.2.11 Satz.
Sei R ein kommutativer Ring mit $1 \neq 0$. Dann sind je zwei Basen eines R-Moduls entweder beide unendlich oder beide endlich mit der selben Anzahl von Elementen

Beweis. Sei M ein R-Modul mit Basen B und C. Im Fall von $|B| = \infty = |C|$ sind wir fertig, sonst ist M endlich erzeugt und daher $m = |B|, n = |C| \in \mathbb{N}_0$ nach Lemma 1.2.9. Nach 1.2.7 gilt $R^n \cong M \cong R^m$, somit reicht es zu zeigen: Sei R ein kommutativer Ring und $m, n \in \mathbb{N}_0, m > n$ mit $R^m \cong R^n$ als R-Modul, dann gilt $1 = 0$ in R.
Um dies zu zeigen, wähle zueinander inverse R-Modulisomorphismen $f : R^n \to R^m$, $g : R^m \to R^n$. Bezeichne mit $\underline{x} = (x_1, \dots, x_n)$ und $\underline{y} = (y_1, \cdots y_m)$ die Standardbasen des R^n und R^m. Wähle $A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \in R^{m \times n}$ mit $f(x_j) = \sum_{i=1}^{m} a_{ij} y_i$ für $j \in \{1, \dots, n\}$ und $B = (b_{ji})_{1 \leq j \leq n, 1 \leq i \leq m} \in R^{n \times m}$ mit $g(y_i) = \sum_{j=1}^{n} b_{ji} x_j$ für $i \in \{1, \dots, m\}$. Dann gilt für $k \in \{1, \dots, m\}$

$$\begin{aligned} y_k &= (f \circ g)(y_k) = f(g(y_k)) \\ &= f\left(\sum_{j=1}^{n} b_{jk} x_j\right) \\ &= \sum_{j=1}^{n} b_{jk} f(x_j) \\ &= \sum_{j=1}^{n} b_{jk} \sum_{i=1}^{m} a_{ij} y_i \\ &= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} b_{jk} a_{ij}\right) y_i \overset{R \text{ komm.}}{=} \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} b_{jk}\right) y_i \end{aligned}$$

und daher

$$\sum_{j=1}^{n} a_{ij} b_{jk} = \begin{cases} 1 & \text{falls } k = i \\ 0 & \text{sonst} \end{cases}$$

für alle $i, k \in \{1, \dots, m\}$, d.h. $AB = I_m$.
Wegen $n < m$ können wir $A' := (A \quad \underbrace{0}_{(m-n)-\text{Spalten}} \quad) \in R^{m \times m}$ und $B' := \begin{pmatrix} B \\ 0 \end{pmatrix} \in R^{m \times m}$ (mit $m - n$ 0-Zeilen) setzen, so dass $A'B' = AB = I_m$.
Mit dem Determinantenproduktsatz folgt

$$0 = 0 \cdot 0 = (\det A')(\det B') = \det(A'B') = 1$$

□

1.2.12 Bemerkung.
Statt Determinantentheorie über kommutativen Ringen zu verwenden, kann man den Beweis des letzten Satzes auch mit der Theorie kommutativer Ringe auf die Dimensionstheorie von Vektorräumen zurückspielen.
Sei R ein kommutativer Ring mit $1 \neq 0$, $m, n \in \mathbb{N}_0$ mit $R^m \cong R^n$. Wir zeigen $m = n$.

Beweis. Wähle ein maximales Ideal $\mathfrak{m}$ von R. Wähle einen R-Modulisomorphismus $f : R^m \to R^n$. Betrachte die R-Untermoduln

$$\mathfrak{m}R^m := \left\{ \sum_{i=1}^{n} a_i x_i \mid n \in \mathbb{N}_0, a_i \in \mathfrak{m}, x_i \in R^m \right\} = \mathfrak{m}^m$$

von R^m und

$$f(\mathfrak{m}R^n) = \left\{ \sum_{i=1}^{n} a_i y_i \mid n \in \mathbb{N}_0, a_i \in \mathfrak{m}, y_i \in R^n \right\} = \mathfrak{m}^n$$

von R^n
Mit dem Isomorphiesatz erhalten wir einen Modulisomorphismus $R^m/\mathfrak{m}^m \to R^n/\mathfrak{m}^n$ und offensichtlich gilt $R^m/\mathfrak{m}^m \cong (R/\mathfrak{m})^m$ (betrachte z.B. $R^m \to (R/\mathfrak{m})^m$).
Da nun $(R/\mathfrak{m})^m$ und $(R/\mathfrak{m})^n$ als R-Moduln isomorph sind, sind sie auch als $(R/\mathfrak{m})$-Moduln isomorph. Für den Körper $K := R/\mathfrak{m}$ gilt also

$$m = \dim_K K^m = \dim_K K^n = n$$

□

1.2.13 Definition.
Sei R ein kommutativer Ring mit $1 \neq 0$ und M ein freier R-Modul mit Basis B. Dann heißt $\operatorname{rk} M := |B| \in \mathbb{N}_0 \cup \{\infty\}$ der *Rang* von M [hängt nach 1.2.11 nicht von der Wahl der Basis B ab]

1.3 Halbeinfache Moduln

1.3.1 Notation.
$0 := \{0\}$ Nullmodul

1.3.2 Definition.
Ein Modul M heißt *einfach* (oder irreduzibel), falls $M \neq 0$ und 0 und M die einzigen Untermoduln von M sind.

1.3.3 Bemerkung.
Sei N ein Untermoduln von M.

(a) Bezeichne $\varphi : M \to M/N$ den kanonischen Epimorphismus. Dann vermitteln die Zuordnungen

$$\begin{aligned} L &\mapsto L/N = \varphi(L) \\ \varphi^{-1}(P) &\leftarrow\!\shortmid P \end{aligned}$$

Eine Bijektion zwischen der Menge der Untermoduln L von M mit $N \subseteq L$ und der Menge der Untermoduln von M/N

(b) Es folgt, dass M/N einfach ist genau dann, wenn N ein maximaler echter Untermodul ist.

1.3.4 Beispiel.

(a) Sei R ein kommutativer Ring und I ein R-Untermodul von R, d.h. ein Ideal von R [$\rightarrow$1.1.5]. Dann ist R/I ein einfacher R-Modul $\Leftrightarrow$ I ist ein maximales Ideal von R $\Leftrightarrow$ R/I ist ein Körper.

(b) Sei R ein Hauptidealring und $p \in R \setminus \{0\}$. Dann ist R/pR ein einfacher Modul genau dann, wenn p irreduzibel in R ist.

Beweis.
„$\Longrightarrow$“: Ist (p) ein maximales Ideal von R, so auch ein Primideal, d.h. p ist prim in R und daher auch irreduzibel in R (wegen $p \neq 0$)

„$\Longleftarrow$“: Ist p irreduzibel in R, so ist $R/(p)$ ein Körper und daher ist (p) ein maximales Ideal in R. $\square$

1.3.5 Lemma.
Sei R ein Ring und M ein R-Modul. Es sind äquivalent:

(i) M ist einfach

(ii) $M \neq 0$ und jedes Element von $M \setminus \{0\}$ erzeugt M

(iii) Es gibt einen maximalen echten R-Untermodul N von R mit $R/N \cong M$

Beweis.
(a)$\Longrightarrow$(c): Gelte (a) Wähle $x \in M \setminus \{0\}$.
Dann ist der Homomorphismus $\varphi : R \to M,\ a \mapsto ax$ surjektiv und daher $R/N \cong M$ mit $N := \ker \varphi$. Mit M ist auch R/N einfach, weswegen nach 1.3.3(b) N ein maximaler echter Untermodul von R ist.

(c)$\Longrightarrow$(b): trivial

(b)$\Longrightarrow$(a): trivial □

1.3.6 Lemma. Lemma von Schur.
Sei R ein Ring, M und N einfache R-Moduln und $f : M \to N$ ein Homomorphismus. Dann ist f entweder die Nullabbildung oder ein Isomorphismus

Beweis. Ist $f \neq 0$, so ist $\ker f \neq M$ und $\operatorname{im} f \neq 0$, also $\ker f = 0$ und $\operatorname{im} f = N$. □

1.3.7 Definition.
Ein Modul heißt *halbeinfach* (oder vollständig reduzibel), wenn er direkte Summe von einfachen Moduln ist.

1.3.8 Lemma.
Jeder endlich erzeugte Modul $\neq 0$ besitzt einen einfachen Quotienten.

Beweis. Sei M ein R-Modul und seinen $x_1, \dots, x_n \in M$ mit $0 \neq M = Rx_1 + \dots + Rx_n$.
Zu zeigen: Es gibt einen Untermodul N von M mit M/N einfach.
Betrachte die durch Inklusion halbgeordnete Menge

$$X := \{P \mid P \text{ Untermodul von } M, P \subsetneq M\} = \{P \mid P \text{ Untermodul von } M, \{x_1, \dots, x_n\} \nsubseteq P\}$$

Jede Kette $K \subseteq X$ besitzt eine obere Schranke in X (0 für $K = \emptyset$, da $M \neq 0$ und $\bigcup K$ für $K \neq \emptyset$, da $\{x_1, \dots, x_n\}$ endlich)
Nach dem Lemma von Zorn gibt es daher ein maximales Element N in X. Gemäß 1.3.3(b) ist M/N einfach. □

1.3.9 Definition.
Sei M ein Modul und N ein Untermodul von M. Dann heißt N ein *direkter Summand* von M, wenn es einen Untermodul P von M gibt mit $M = N \oplus P$.

1.3.10 Satz.
Sei M ein Modul. Dann sind folgende Aussage äquivalent

(a) M ist halbeinfach

(b) M ist die Summe seiner einfachen Untermoduln

(c) Jeder Untermodul von M ist ein direkter Summand von M.

Beweis.
(a)$\Longrightarrow$(b): klar

(b)$\Longrightarrow$(c): Gelte (b) und sei N ein Untermodul von M.

$$X := \{P \mid P \text{ Untermodulvon } M, N \cap P = 0\}$$

Jede Kette $K \subseteq X$ besitzt eine obere Schranke in X (0 für $K = \emptyset$, $\bigcup K$ für $K \neq \emptyset$)
Nach dem Lemma von Zorn gibt es daher ein maximales Element P in X. Um $M = N+P$ zu zeigen, reicht es wegen (b) zu zeigen, dass jeder einfache Untermodul L von M in $N + P$ enthalten ist. Sei also L ein einfacher Untermodul von M. Dann ist entweder $L \cap (N + P) = 0$ oder $L \cap (N + P) = L$. Im letzteren Fall sind wir fertig.
Der erste Fall tritt aber nicht ein:
Ist $L \cap (N + P) = 0$, so $(L + P) \cap N = 0$ (ist $x \in L$ und $y \in P$ mit $x + y \in N$, so $x \in L \cap (N + P) = 0$ und daher $y \in N \cap P = 0$), woraus wegen der Maximalität von P folgt $P = L + P$, also $L \subseteq P$↯

(c)$\Longrightarrow$(a): Gelte (c).
Hilfsbehauptung: Jeder Untermodul eines Untermoduls N von M ist ein direkter Summand von N.

Begründung: Sei N ein Untermodul von M und P ein Untermodul von N. Wähle Q mit $M = P \oplus Q$. Setze $R = Q \cap N$. Wir zeigen $N = P \oplus R$. Es ist klar, dass $P \cap R = 0$ (denn $P \cap Q = 0$) und $P + R \subseteq N$. Zu zeigen ist also noch $N \subseteq P + R$.
Sei hierzu $x \in N$. Schreibe $x = p+q$ mit $p \in P$ und $q \in Q$, dann $q = x-p \in N \cap Q = R$.

Betrachte nun die durch Inklusion halbgeordnete Menge

$$X := \left\{ Y \mid Y \text{ Menge von einfachen Untermoduln von } M \text{ mit } \sum_{N \in Y} N = \bigoplus_{N \in Y} N \right\}$$

Sei K eine Kette in X. Wir behaupten, dass dann $Z := \bigcup K \in X$ gilt und Z eine obere Schranke von K in X ist.
Zu zeigen: $\sum_{N \in Z} N = \bigoplus_{N \in Z} N$
Seien nun $n \in \mathbb{N}$ und $N_1, \dots, N_n \in Z$ paarweise verschieden und $x_1 \in N_1, \dots, x_n \in N_n$ mit $x_1 + \dots + x_n = 0$ [$\rightarrow$1.2.3(b)]. Da K eine Kette ist, gibt es $Y \in K$ mit $\{N_1, \dots, N_n\} \subseteq Y$.
Wegen $\sum_{N \in Y} N = \bigoplus_{N \in Y} N$ folgt mit 1.2.3(b), dass $x_1 = \dots = x_n = 0$.
Da die Kette $K \subseteq X$ beliebig war, gibt es nach dem Lemma von Zorn ein in X maximales Element Z. Setze $P = \sum_{N \in Z} N = \bigoplus_{N \in Z} N$. Wir zeigen $M = P$.
Angenommen $M \setminus P \neq \emptyset$. Wähle gemäß (c) Q mit $M = P \bigoplus Q$. Dann $Q \neq 0$. Wähle einen endlich erzeugten Untermodul $Q' \neq 0$ von Q. Nach Lemma 1.3.8 gibt es einen Untermodul Q'' von Q' mit Q'/Q'' einfach.

Wähle gemäß Hilfsbehauptung R mit $Q' = Q'' \bigoplus R$. Dann ist $R \subseteq Q' \subseteq Q$ und daher $P \cap R = 0$. Weiter ist $R \cong Q'/Q''$ einfach. Es folgt $\sum\limits_{N \in Z \cup \{R\}} N = \bigoplus\limits_{N \in Z \cup \{R\}} N$. Daher ist $Z \cup \{R\} \in X$. Wegen der Maximalität von Z in X gilt $R \in Z$ und daher $R \subseteq P$ ↯. □

1.3.11 Korollar.
Direkte Summen, Untermoduln und Quotienten von halbeinfachen Moduln sind halbeinfach.

Beweis. direkte Summen: klar nach 1.3.7
Untermoduln: Sei N ein Untermodul des halbeinfachen Moduls M. Wir verwenden 1.3.10(c) um zu zeigen, dass N auch halbeinfach ist. Sei also L ein Untermodul von N. Da M halbeinfach ist, gibt es einen Untermodul P von M mit $M = L \oplus P$. Dann gilt $N = L \oplus (P \cap N)$, wie man sofort sieht.
Quotienten: Sei N ein Untermodul des halbeinfachen Moduls M. Zu zeigen: M/N ist halbeinfach.
Wähle einen Untermodul P von M mit $M = N \oplus P$. Dann ist $M/N \cong P$ halbeinfach nach dem gerade Gezeigten (betrachte den Homomorphismus $M = N \oplus P \to P, x+y \mapsto y$ und wende den Homomorphiesatz an). □

1.4 Noethersche und artinsche Moduln

1.4.1 Definition.
Ein Modul M heißt $\begin{Bmatrix} \textit{noethersch} \\ \textit{artinsch} \end{Bmatrix}$, wenn jede $\begin{Bmatrix} \text{aufsteigende} \\ \text{absteigende} \end{Bmatrix}$ Kette von Untermoduln $\begin{Bmatrix} M_1 \subseteq M_2 \subseteq \cdots \\ M_1 \supseteq M_2 \supseteq \cdots \end{Bmatrix}$ von M stationär wird (d.h. $\exists k \in \mathbb{N} : \forall n \geq k : M_n = M_k$).
Ein Ring R heißt $\begin{Bmatrix} \text{noethersch} \\ \text{artinsch} \end{Bmatrix}$, wenn er als R-Modul $\begin{Bmatrix} \text{noethersch} \\ \text{artinsch} \end{Bmatrix}$ ist.

1.4.2 Bemerkung.
Sei R ein kommutativer Ring

(a) R ist genau dann noethersch, wenn jede aufsteigende Kette von Idealen in R stationär wird [$\to$1.1.5]

(b) Ist $S = R[a_1, \dots, a_n]$ ein kommutativer Ring mit $n \in \mathbb{N}_0, a_1, \dots, a_n \in S$, so besagt der *Hilbersche Basissatz*: R noethersch $\Longrightarrow$ S noethersch.

1.4.3 Satz.
Ein Modul ist noethersch genau dann, wenn alle seine Untermoduln endlich erzeugt sind [$\to$1.1.4(d)].

1.4.4 Lemma.
Seien L, L' und N Untermoduln des Moduls M mit $L \subseteq L'$, $L \cap N = L' \cap N$ und $L + N = L' + N$. Dann gilt $L = L'$

Beweis. Sei $x \in L'$. Zu zeigen ist $x \in L$. Schreibe $x = l + n$ mit $l \in L$ und $n \in N$. Dann ist $x - l = n \in L' \cap N = L \cap N$ und daher $x = (x - l) + l \in L$. □

1.4.5 Satz.
Sei N ein Untermodul des Moduls M. Dann ist M $\begin{Bmatrix} \text{noethersch} \\ \text{artinsch} \end{Bmatrix}$ genau dann, wenn sowohl N als auch M/N $\begin{Bmatrix} \text{noethersch} \\ \text{artinsch} \end{Bmatrix}$ ist.

Beweis. klar mit 1.3.3(a) und 1.4.4 □

1.4.6 Korollar.
Endliche Summen $\begin{Bmatrix} \text{noetherscher} \\ \text{artinscher} \end{Bmatrix}$ Moduln sind auch $\begin{Bmatrix} \text{noethersch} \\ \text{artinsch} \end{Bmatrix}$.

Beweis. Sind $N_1, \dots, N_n$ $\begin{Bmatrix} \text{noethersche} \\ \text{artinsche} \end{Bmatrix}$ Untermoduln des Moduls M mit $M = \sum_{i=1}^n N_i$, so gibt es nach 1.2.2 einen Epimorphismus

$$\bigoplus_{i=1}^n N_i \to \sum_{i=1}^n N_i$$

weshalb $M = \sum_{i=1}^n N_i \cong \left(\bigoplus_{i=1}^n N_i\right)/L$ für einen Untermodul L von $\bigoplus_{i=1}^n N_i$ gilt.
Mit 1.4.5 reicht es daher, die Behauptung für direkte Summen zu zeigen.
Durch Induktion nach $n \in \mathbb{N}_0$ zeigen wir daher, dass für alle $\begin{Bmatrix}\text{noetherschen}\\\text{artinschen}\end{Bmatrix}$ R-Moduln $N_1, \dots, N_n$ auch $\bigoplus_{i=1}^n N_i$ $\begin{Bmatrix}\text{noethersch}\\\text{artinsch}\end{Bmatrix}$ ist.
Induktionsanfang für $n = 0$: klar
Induktionsschritt $n-1 \to n, (n \in \mathbb{N})$: Seien $N_1, \dots, N_n$ $\begin{Bmatrix}\text{noethersche}\\\text{artinsche}\end{Bmatrix}$ R-Moduln. Dann ist $\bigoplus_{i=1}^{n-1} N_i$ $\begin{Bmatrix}\text{noethersch}\\\text{artinsch}\end{Bmatrix}$ nach Induktionsvoraussetzung. Wegen

$$\left(\bigoplus_{i=1}^n N_i\right) / \left(\bigoplus_{i=1}^{n-1} N_i\right) \cong N_n$$

folgt mit 1.4.5, dass $\bigoplus_{i=1}^n N_i$ auch $\begin{Bmatrix}\text{noethersch}\\\text{artinsch}\end{Bmatrix}$ ist. □

1.4.7 Korollar.
Jeder endlich erzeugte Modul über einem $\begin{Bmatrix}\text{noetherschen}\\\text{artinschen}\end{Bmatrix}$ Ring ist $\begin{Bmatrix}\text{noethersch}\\\text{artinsch}\end{Bmatrix}$.

Beweis. Sei R ein $\begin{Bmatrix}\text{noetherscher}\\\text{artinscher}\end{Bmatrix}$ Ring und M ein endlich erzeugter R-Modul. Nach 1.4.6 ist ohne Einschränkung M zyklisch. Dann ist $M \cong R/N$ für einen R-Untermodul N von R. Mit R ist nach 1.4.5 auch R/N $\begin{Bmatrix}\text{noethersch}\\\text{artinsch}\end{Bmatrix}$. □

1.4.8 Definition.
Sei M ein Modul. Dann heißt

$$\ell(M) := \sup\{n \in \mathbb{N}_0 \mid \text{es gibt Untermoduln } M_0, \dots, M_n \text{ von } M \text{ mit } M_0 \supsetneq \cdots \supsetneq M_n\} \in \mathbb{N}_0 \cup \{\infty\}$$

die *Länge* von M.
Es heißt M von endlicher Länge, wenn $\ell(M) < \infty$.

1.4.9 Beispiel.
Sei M ein Modul. Dann

(a) $\ell(M) = 0 \Leftrightarrow M = 0$

(b) $\ell(M) = 1 \Leftrightarrow M$ ist einfach

1.4.10 Satz.
Sei N ein Untermodul des Moduls M. Dann gilt

$$\ell(M) < \infty \Leftrightarrow (\ell(M/N) < \infty \wedge \ell(N) < \infty)$$

und falls $\ell(M) < \infty$

$$\ell(M) = \ell(M/N) + \ell(N)$$

Beweis. Man sieht sofort $\ell(M) = \sup \hat{M}, \ell(M/N) \overset{1.3.3(a)}{=} \sup \hat{K}$ und $\ell(N) = \sup \hat{N}$ mit

$$\hat{M} := \{m \in \mathbb{N}_0 \mid \exists \text{Untermoduln } M_0, \dots, M_m \text{ von } M : M = M_0 \supsetneq \cdots \supsetneq M_m = 0\}$$

$$\hat{K} := \{k \in \mathbb{N}_0 \mid \exists \text{Untermoduln } L_0, \dots, L_k \text{ von } M : M = L_0 \supsetneq \cdots \supsetneq L_k = N\}$$

$$\hat{N} := \{n \in \mathbb{N}_0 \mid \exists \text{Untermoduln } N_0, \dots, N_n \text{ von } M : N = N_0 \supsetneq \cdots \supsetneq N_n = 0\}$$

Offensichtlich gilt $\forall k \in \hat{K} : \forall n \in \hat{N} : k + n \in \hat{M}$, was „$\Longrightarrow$" und „$\geq$" beweist. Um „$\Longleftarrow$" und „$\leq$" zu beweisen, reicht es

$$\forall m \in \hat{M} : \exists k \in \hat{K} : \exists n \in \hat{N} : m \leq k + n$$

zu zeigen. Sei hierzu $m \in \hat{M}$.

Wähle Untermoduln $M_0, \dots, M_m$ von M mit $M = M_0 \supsetneq \cdots \supsetneq M_m = 0$. Setze $L_i := M_i + N$ und $N_i := M_i \cap N$ für $i \in \{0, \dots, m\}$. Nach Lemma 1.4.4 ist dann jeweils mindestens eine der beiden Inklusionen $L_i \supseteq L_{i+1}$ und $N_i \supseteq N_{i+1}$ echt (für $i \in \{0, \dots, m-1\}$). Setzt man

$$k := |\{i \in \{0, \dots, m-1\} \, | L_i \supsetneq L_{i+1}\}| \in \hat{K}$$

und

$$n := |\{i \in \{0, \dots, m-1\} \, | N_i \supsetneq N_{i+1}\}| \in \hat{N}$$

so folgt $m \leq k + n$ □

1.4.11 Definition.
Sei M ein Modul. Es heißt $(M_0, \dots, M_n)$ eine *Kompositionsreihe* (der *Länge* n) von M, wenn $M_0, \dots, M_n$ Untermoduln von M sind mit

$$M = M_0 \supsetneq \cdots \supsetneq M_n = 0$$

derart, dass die sogenannten Faktoren M_i/M_{i+1} ($i \in \{0, \dots, n-1\}$) alle einfach sind.

1.4.12 Bemerkung.
Jeder endliche Modul besitzt natürlich eine Kompositionsreihe. Folgender Satz verallgemeinert dies.

1.4.13 Satz.
Sei M ein Modul. Es sind folgende Aussagen äquivalent

(a) $\ell(M) < \infty$

(b) M ist noethersch und artinsch

(c) M besitzt eine Kompositionsreihe.

In diesem Fall ist die Länge einer jeden Kompositionsreihe von M gleich der Länge von M.

Beweis.
(a)$\Longrightarrow$(b): trivial

(b)$\Longrightarrow$(c): Sei M noethersch und artinsch. Da M noethersch ist, gibt es zu jedem Untermodul $N \neq 0$ von M einen Untermodul N' von N mit N/N' einfach (sonst könnte man eine aufsteigende Kette $0 \subsetneq N_1 \cdots \subsetneq \cdots$ von echten Untermoduln von M konstruieren). Setze nun $M_0 = N$ und wähle für $i = 0, 1, \dots$ solange $M_i \neq 0$ einen Untermodul M_{i+1} von M_i mit M_i/M_{i+1} einfach.
Dieses Verfahren bricht ab, da M artinsch ist.

(c)$\Longrightarrow$(a) und Zusatz: Sei $(M_0, \dots, M_n)$ eine Kompositionsreihe von M.
Dann $\ell(M) \overset{1.4.10}{=} \ell(M_0/M_1) + \cdots + \ell(M_{n-1}/M_n) \overset{1.4.9}{=} n$ □

1.4.14 Satz. Satz von Jordan-Hölder
Sei M ein Modul endlicher Länge n und seien $M = M_0 \supsetneq \cdots \supsetneq M_n = 0$ und $M = N_0 \supsetneq \cdots \supsetneq N_n = 0$ zwei Kompositionsreihen von M. Dann gibt es $\sigma \in S_n$ mit $M_{i-1}/M_i \cong N_{\sigma(i)-1}/N_{\sigma(i)}$ für $i \in \{1, \dots, n\}$

Beweis. Induktion nach $n \in \mathbb{N}_0$
$n = 0$: trivial
$n - 1 \to n$ $(n \in \mathbb{N})$: Setze $L := N_1$ und betrachte

$$(*) \qquad M = L + M_0 \supseteq \cdots \supseteq L + M_n = L$$

$$(**) \qquad L = L \cap M_0 \supseteq \cdots \supseteq L \cap M_n = 0$$

Hilfsbehauptung: Für alle $i \in \{1, \dots, n\}$ gilt
entweder $(L + M_{i+1})/(L + M_i) = 0$ und $(L \cap M_{i+1})/(L \cap M_i) \cong M_{i-1}/M_i$
oder $(L + M_{i+1})/(L + M_i) \cong M_{i-1}/M_i$ und $(L \cap M_{i+1})/(L \cap M_i) = 0$

Begründung: Sei $i \in \{1, \dots, n\}$. Ist $(L \cap M_{i-1})/(L \cap M_i) \neq 0$, so ist $(L \cap M_{i-1}) \,/\, (L \cap M_i) \hookrightarrow M_{i-1}/M_i$ ein Isomorphismus, da M_{i-1}/M_i einfach.
Ist $(L + M_{i-1})/(L + M_i) \neq 0$, so ist $M_{i-1}/M_i \twoheadrightarrow (L + M_{i-1})/(L + M_i)$ ein Isomorphismus, da M_{i-1}/M_i einfach. Daher reicht es zu zeigen, dass genau einer der Moduln $(L \cap M_{i-1})/(L \cap M_i)$ und $(L + M_{i-1})/(L + M_i)$ ein Nullmodul ist.
Wegen Lemma 1.4.4 können nicht beide 0 sein. Es reicht daher zu zeigen, dass genau n der $2n$ Inklusionen $(*)$ und $(**)$ echt sind. Dies folgt mit Obigem aus (1.4.13), indem man aus $(*)$ und $(**)$ eine Kompositionsreihe gewinnt.

Da M/L einfach ist, ist genau eine der n Inklusionen in $(*)$ echt, etwa $L + M_{k-1} \supsetneq L + M_k$. Nach der Hilfsbehauptung erhält man aus $(**)$ eine Kompositionsreihe von L der Länge $n - 1$ (beachte $L \cap M_{k-1} = L \cap M_k$). Da $L = N_1 \supsetneq \cdots \supsetneq N_n = 0$ ebenfalls eine solche ist, gibt es nach Induktionsvoraussetzung eine Bijektion $\tau : \{2, \dots, n\} \to \{1, \dots, n\} \setminus \{k\}$ mit $N_{i-1}/N_i \cong (L \cap M_{\tau(i)-1})/(L \cap M_{\tau(i)}) \cong M_{\tau(i)-1}/M_{\tau(i)}$ für $i \in \{2, \dots, n\}$. Zusammen mit $N_0/N_1 \cong M/L = (L + M_{k-1})/(L + M_k) \cong M_{k-1}/M_k$ liefert dies die gewünschte Bijektion. □

1.4.15 Definition. [→1.2.4]
Sei R ein Ring, M ein R-Modul und $E \subseteq M$. Dann nennt man den R-Untermodul $\operatorname{ann}(E) := \{a \in R \mid \forall x \in E : ax = 0\}$ von R den Annihilator von E.

1.4.16 Bemerkung.
Sei R ein kommutativer Ring, M ein R-Modul und $E \subseteq M$. Dann ist $\operatorname{ann}(E) = \operatorname{ann}\left(\sum_{x\in E} Rx\right)$. Insbesondere gilt für $M = R/aR$ mit $a \in R$, dass

$$\operatorname{ann}(R/aR) = \operatorname{ann}(\{\overline{1}\}) = \operatorname{ann}(\overline{1}) = aR$$

1.4.17 Beispiel.

(a) Ist V ein K-Vektorraum, so $\ell(V) = \dim(V)$

(b) Sei R ein Hauptidealring, $n \in \mathbb{N}_0, p_1, \ldots, p_n \in R$ irreduzibel und $m := p_1 \cdot \cdots \cdot p_n$.

Dann gilt $\ell(R/mR) = n$ und

$$R/mR \supsetneq p_1R/mR \supsetneq \cdots \supsetneq p_1 \cdot \cdots \cdot p_nR/mR$$

mit Faktoren $(p_1 \cdots p_{i-1}R/mR)/(p_1 \cdots p_iR/mR) \cong (p_1 \cdots p_{i-1}R)/(p_1 \cdots p_iR) \cong R/p_iR$ für $i \in \{1, \ldots, n\}$.

Nach dem Satz von Jordan-Hölder gibt es für alle Kompositionsreihen $R/mR = M_0 \supsetneq \cdots \supsetneq M_n = 0$ ein $\sigma \in S_n$ mit $M_{i-1}/M_i \cong R/p_{\sigma(i)}R$ und daher $\operatorname{ann}(M_{i-1}/M_i) = \operatorname{ann}(R/p_{\sigma(i)}R) \overset{1.4.16}{=} p_{\sigma(i)}R$

Die Faktoren einer jeden Kompositionsreihe von R/mR liefern also bis auf Reihenfolge und Assoziiertheit genau die Faktoren von $m = p_1 \cdot \cdots \cdot p_n$.

1.5 Unzerlegbare Moduln

1.5.1 Definition.
Ein Modul M heißt *unzerlegbar*, falls $M \neq 0$ und für alle Untermoduln L und N von M gilt

$$M = L \oplus N \Rightarrow (L = 0 \vee N = 0)$$

1.5.2 Bemerkung.
Jeder einfache Modul [$\rightarrow$1.3.2] ist unzerlegbar, aber die Umkehrung stimmt nicht, wie 1.3.4(b) in Verbindung mit Satz 1.5.4 unten zeigt.

1.5.3 Lemma.
Sei M ein zyklischer Modul

(a) Jeder direkte Summand von M [$\rightarrow$1.3.9] ist wieder zyklisch

(b) $M \cong R/N$ für einen R-Untermodul N von R.

Beweis.

(a) Seien L und N Untermoduln von M mit $M = L \oplus N$. Schreibe $M = Rx$ mit $x \in M$ und $x = y + z$ mit $y \in L, z \in N$. Wir zeigen $L = Ry$. Sei hierzu $w \in L$. Zu zeigen ist, dass $w \in Ry$. Schreibe $w = ax$ mit $a \in R$. Dann $ax = ay + az$ und $az = ax - ay = w - ay \in L \cap N = 0$. Also $w = ax = ay \in Ry$.

(b) Schreibe $M = Rx$ mit $x \in M$. Wähle für N den Kern des R-Modulhomomorphismus $R \twoheadrightarrow M, a \mapsto ax$.

$\square$

1.5.4 Satz.
Sei R ein Hauptidealring und $a \in R$. Dann ist R/aR unzerlegbar genau dann, wenn es ein Primelement $p \in R$ und ein $n \in \mathbb{N}$ gibt mit $(a) = (p^n)$

Beweis. Ohne Einschränkung $a \notin R^*$. Gebe es zunächst keine solchen p und n. Dann gibt es $b, c \in R \setminus R^*$ mit $a = bc$ und $(b, c) = (1)$. Nach dem Chinesischen Restsatz ist dann der kanonische R-Modulhomomorphismus $R/aR \to (R/bR) \times (R/cR)$ bijektiv. Daher $R/aR \cong \underbrace{(R/bR)}_{\neq 0} \oplus \underbrace{(R/cR)}_{\neq 0}$

Seien nun $p \in R$ prim und $n \in \mathbb{N}$ mit $(a) = (p^n)$. Gelte $R/p^nR = L \oplus M$. Zu zeigen $L = 0$ oder $M = 0$. Jede Kompositionsreihe von R/p^nR hat Länge n mit allen Faktoren isomorph zu R/pR nach 1.4.17(b). Alle Faktoren von Kompositionsreihen von L und M sind daher isomorph zu R/pR, denn aus je zwei Kompositionsreihen von $(L \oplus M)/M \cong L$ und M kann man eine solche von R/p^nR gewinnen. Nach 1.5.3 gibt es aber Ideale I und J von R mit $L \cong R/I$ und $M \cong R/J$. Da I und J Hauptideale sind, folgt mit 1.4.17(b) also $I = (p^l)$ und $J = (p^m)$ für gewisse $l, m \in \mathbb{N}_0$.

Nun gilt einerseits

$$
\begin{aligned}
n &= \ell(R/p^nR) = \ell(L \oplus M) \\
&= \ell((L \oplus M)/M) + \ell(M) && \text{1.4.10} \\
&= \ell(L) + \ell(M) = \ell(R/p^lR) + \ell(R/p^mR) = l + m
\end{aligned}
$$

und andererseits

$$
\begin{aligned}
(p^n) &= \operatorname{ann}(R/p^nR) && \text{1.4.16} \\
&= \operatorname{ann}(L) \cap \operatorname{ann}(M) && R/p^nR = L + M \\
&= \operatorname{ann}(R/p^lR) \cap \operatorname{ann}(R/p^mR) = (p^l) \cap (p^m)
\end{aligned}
$$

Hieraus folgt $l = 0$ oder $m = 0$. Also $L = 0$ oder $M = 0$. $\square$

1.5.5 Satz.
Jeder noethersche oder artinsche Modul ist die direkte Summe endlich vieler unzerlegbarer Untermoduln.

Beweis. Sei M ein $\begin{Bmatrix}\text{noetherscher}\\ \text{artinscher}\end{Bmatrix}$ Modul. Zu jedem Untermodul $N \neq 0$ von M gibt es einen $\begin{Bmatrix}\text{maximalen}\\ \text{minimalen}\end{Bmatrix}$ direkten Summanden $\begin{Bmatrix}N'' \neq N\\ N' \neq 0\end{Bmatrix}$ von N und daher Untermoduln N' und N'' von N mit $N = N' \oplus N''$ und N' unzerlegbar.

Setze nun $M_0 := M$ und wähle für $i = 0, 1, \ldots$ solange $M_i \neq 0$ Untermoduln N_{i+1} und M_{i+1} von M_i mit $M_i = N_{i+1} \oplus M_{i+1}$ und N_{i+1} unzerlegbar. Dieses Verfahren bricht ab, da $\begin{Bmatrix}N_1 \subsetneq N_1 \oplus N_2 \subsetneq \cdots\\ M_0 \supsetneq M_1 \supsetneq \cdots\end{Bmatrix}$ und M $\begin{Bmatrix}\text{noethersch}\\ \text{artinsch}\end{Bmatrix}$ ist. Ist $M_n = 0$, so $M = \bigoplus_{i=1}^{n} N_i$ $\square$

1.5.6 Definition und Übung.
Sei M ein Modul. Dann bildet

$$\operatorname{End}(M) := \{f \mid f \text{ Endomorphismus von } M\}$$

mit punktweiser Addition und der Hintereinanderschaltung als Multiplikation einen Ring, den sogenannten *Endomorphismenring* von M.

1.5.7 Lemma. „Fitting-Zerlegung“
Sei M ein Modul und $f \in \operatorname{End}(M)$ mit $\ker(f) = \ker(f^2)$ und $\operatorname{im}(f) = \operatorname{im}(f^2)$. Dann $M = \ker f \oplus \operatorname{im} f$

Beweis. Zu zeigen

(a) $\ker f \cap \operatorname{im} f = 0$

(b) $M = \ker f + \operatorname{im} f$

Zu (a): Sei $x \in \ker f \cap \operatorname{im} f$. Wähle $y \in M$ mit $x = f(y)$. Dann $f^2(y) = f(x) = 0$ und daher $y \in \ker(f^2) = \ker(f)$, d.h. $x = f(y) = 0$

Zu (b): Sei $x \in M$. Wegen $f(x) \in \operatorname{im} f = \operatorname{im}(f^2)$ gibt es $y \in M$ mit $f(x) = f^2(y)$. Dann $x = \underbrace{(x - f(y))}_{\in \ker f} + \underbrace{f(y)}_{\in \operatorname{im} f}$ □

1.5.8 Definition.
Sei R ein Ring (z.B. $R = \operatorname{End}(M)$ für einen Modul M)

(a) Ein Element $a \in R$ heißt $\begin{Bmatrix} \textit{idempotent} \\ \textit{nilpotent} \end{Bmatrix}$, wenn $\begin{Bmatrix} a^2 = a \\ a^n = 0 \text{ (für ein } n \in \mathbb{N}) \end{Bmatrix}$

(b) R heißt *lokal*, wenn $0 \neq 1$ in R und $\forall a, b \in R \setminus R^* : a + b \in R \setminus R^*$

1.5.9 Proposition.
Sei M ein Modul. Dann ist M unzerlegbar genau dann, wenn $\operatorname{End}(M)$ genau zwei idempotente Elemente hat (nämlich 0 und $1 = \mathrm{id}_M \neq 0$).

Beweis.
„$\Longrightarrow$“: Sei M unzerlegbar. Wegen $M \neq 0$ gilt $0 \neq 1$ in $\operatorname{End}(M)$.

Sei $f \in \operatorname{End}(M)$ idempotent. Dann $M = \ker f \oplus \operatorname{im} f$ nach 1.5.7. Es folgt $\ker f = 0$ oder $\operatorname{im} f = 0$. Im zweiten Fall ist $f = 0$. Im ersten Fall ist f injektiv, also $f = 1$ (da $f^2 = f$).

„$\Longleftarrow$“: Seien $0 \neq 1$ die einzigen idempotenten Elemente von $\operatorname{End}(M)$. Gelte $M = L \oplus N$. Zu zeigen $L = 0$ oder $N = 0$.

$$\pi_L : M = L \oplus N \to L, x + y \mapsto x$$

($x \in L, y \in N$) ist idempotent, also $\pi_L = 0$ oder $\pi_L = 1$. Dann ist $L = 0$ oder $N = 0$. □

1.5.10 Lemma. Fitting Lemma
Sei M ein Modul endlicher Länge und $f \in \operatorname{End}(M)$. Dann gibt es $N \in \mathbb{N}$ mit $M = \ker(f^n) \oplus \operatorname{im}(f^n)$ für alle $n \geq N$.

Beweis. Die Ketten $\ker f \subseteq \ker f^2 \subseteq \cdots$ und $\operatorname{im} f \supseteq \operatorname{im} f^2 \supseteq \cdots$ werden stationär. Wähle $N \in \mathbb{N}$ mit $\ker f^n = \ker f^N$ und $\operatorname{im} f^n = \operatorname{im} f^N$ für alle $n \geq N$ und nehme die Fitting-Zerlegung nach 1.5.7 für f^n. □

1.5.11 Korollar.
Jeder Endomorphismus eines Unzerlegbaren Moduls endlicher Länge ist entweder nilpotent oder ein Automorphismus.

1.5.12 Satz.
Der Endomorphismenring eines unzerlegbaren Moduls endlicher Länge ist lokal.

Beweis. Sei M ein unzerlegbarer Modul mit $\ell(M) < \infty$. Wegen $M \neq 0$ gilt $0 \neq 1$ in $\mathrm{End}(M)$.

Seien $f, g \in \mathrm{End}(M)$. Statt

$$(f \notin \mathrm{End}(M)^* \wedge g \notin \mathrm{End}(M)^*) \Longrightarrow (f + g \notin \mathrm{End}(M)^*)$$

können wir genauso gut (beachte $\mathrm{End}(M)^* = \mathrm{Aut}(M)$)

$$(f \notin \mathrm{Aut}(M) \wedge f + g \in \mathrm{Aut}(M)) \Longrightarrow g \in \mathrm{Aut}(M)$$

zeigen.

Gelte also $f \notin \mathrm{Aut}(M)$ und $f + g \in \mathrm{Aut}(M)$. Zu zeigen ist $g \in \mathrm{Aut}(M)$.
Mit $h := (f+g)^{-1}$ gilt $hf + hg = h(f+g) = 1$. Wegen $(hf) \notin \mathrm{Aut}(M)$ (f nilpotent nach 1.5.11, also $\ker f \neq 0$) gilt nach 1.5.11 $(hf)^n = 0$ für ein $n \in \mathbb{N}$.
Dann gilt $hg = 1 - hf \in \mathrm{Aut}(M)$ und daher $g \in \mathrm{Aut}(M)$ (sonst g nilpotent nach 1.5.11, also $\ker g \neq 0$), denn $(1 + hf + (hf)^2 + \cdots + (hf)^{n-1})(1 - hf) = 1$ und $(1 - hf)(1 + hf + (hf)^2 + \cdots + (hf)^{n-1}) = 1$. □

1.5.13 Satz. Satz von Krull-Remak-Schmidt
Seien $m, n \in \mathbb{N}_0$ $M_1, \ldots, M_m, N_1, \ldots, N_n$ unzerlegbare Moduln endlicher Länge mit $M_1 \oplus \cdots \oplus M_m \cong N_1 \oplus \cdots \oplus N_n$. Dann gilt $m = n$ und es gibt $\sigma \in S_n$ mit $M_i \cong N_{\sigma(i)}$ für $i \in \{1, \ldots, n\}$

Beweis. Induktion nach $m \in \mathbb{N}_0$. $m = 0$: klar
$m - 1 \to m$ ($m \in \mathbb{N}$)

Wähle einen Isomorphismus $f : \underbrace{\bigoplus_{i=1}^{m} M_i}_{M:=} \to \underbrace{\bigoplus_{j=1}^{n} N_j}_{N:=}$.

$$M_i \underset{\pi_i}{\overset{\iota_i}{\rightleftarrows}} M \xrightarrow[\cong]{f} N \underset{\rho_j}{\overset{\kappa_j}{\leftrightarrows}} N_i$$

$$\begin{aligned}
1 = \mathrm{id}_{M_1} &= \pi_1 \iota_1 \\
&= \pi_1 f^{-1} \, \mathrm{id}_N \, f \iota_1 \\
&= \pi_1 f^{-1} \left(\sum_{j=1}^{m} \kappa_j \rho_j \right) f \iota_1 \\
&= \sum_{j=1}^{m} \underbrace{\pi_1 f^{-1} \kappa_j}_{g_j : N_j \to M_1} \underbrace{\rho_j f \iota_1}_{h_j : M_1 \to N_j}
\end{aligned}$$

Da $\mathrm{End}(M_1)$ nach 1.5.12 lokal ist, gibt es $j \in \{1, \ldots, n\}$ mit $g_j h_j \in \mathrm{Aut}(M_1)$. Insbesondere $n \geq 1$.

Behauptung 1: $M_1 \underset{g_j}{\overset{h_j}{\rightleftarrows}} N_j$ sind Isomorphismen.

Begründung: Wegen $g_j h_j \in \mathrm{Aut}(M)$ ist h_j injektiv und g_j surjektiv. Es genügt zu zeigen, dass $h_j g_j \in \mathrm{Aut}(N_j)$. Dies ist klar, denn sonst gilt nach 1.5.12 $(h_j g_j)^s = 0$ für ein $s \in \mathbb{N}$ und damit

$$0 = g_j (h_j g_j)^s = (g_j h_j)^s g_j$$

was $g_j = 0$ impliziert $\lightning$.

Behauptung 2: $M = f^{-1}(N_j) \oplus M_2 \oplus \cdots \oplus M_m$.

Begründung: Zu zeigen ist

(a) $f^{-1}(N_j) \cap \sum_{i=2}^m M_i = 0$

(b) $M_1 \subseteq f^{-1}(N_j) + \sum_{i=2}^m M_i$

Zu (a) Sei $x \in f^{-1}(N_j) \cap \sum_{i=2}^m M_i$. Zu zeigen ist $x = 0$. Dann gibt es ein $y \in N_j$ mit $x = (f^{-1}\kappa_j)(y)$ und es gilt $\pi_1(x) = 0$. Dann gilt $g_j(y) = (\pi_1 f^{-1} \kappa_j)(y) = \pi_1(x) = 0$ und daher $y = 0$ (denn g_j ist ein Isomorphismus), also $x = 0$.

Zu (b) Sei $x \in M_1$. Wähle ein $y \in N_j$ mit $x = g_j(y)$. Dann $x = f^{-1}(y) + (x - f^{-1}(y))$ und es reicht zu zeigen, dass $\pi_1(x - f^{-1}(y)) = 0$. Es gilt aber

$$\begin{aligned}\pi_1(x - f^{-1}(y)) &= \pi_1(x) - (\pi_1(f^{-1}\kappa_j)(y)) \\ &= \pi_1(g_j(y)) - g_j(y) \\ &= g_j(y) - g_j(y) = 0\end{aligned}$$

Der Kern von $M \xrightarrow[\cong]{f} N \twoheadrightarrow N/N_j$ ist $f^{-1}(N_j)$ und es folgt mit dem Isomorphiesatz $M/f^{-1}(N_j) \cong N/N_j$, also

$$\bigoplus_{i=2}^m M_i \overset{\text{Beh 2}}{\cong} M/f^{-1}(N_j) \cong N/N_j \cong \bigoplus_{k=1, k\neq j}^n N_k$$

Wende die Induktionsvoraussetzung an. $\square$

1.6 Endlich erzeugte Moduln über Hauptidealringen

1.6.1 Definition.
Sei R ein Integritätsring. Dann heißt eine Funktion $\delta : R \to \mathbb{N}_0$ eine *euklidische Funktion* auf R, wenn es für alle $a \in R$ und $b \in R \setminus \{0\}$ Elemente $q \in R$ („Quotienten“) und $r \in R$ („Rest“) gibt mit $a = bq + r$ und $\delta(r) < \delta(b)$ („Division mit Rest“).

Es heißt R *euklidisch*, wenn R eine euklidische Funktion besitzt.

1.6.2 Beispiel.

(a) $\mathbb{Z}$ ist euklidisch mit der euklidischen Funktion

$$\delta : \mathbb{Z} \to \mathbb{N}_0, a \mapsto |a|$$

(b) Ist K ein Körper, so ist $K[X]$ euklidisch mit euklidischer Funktion

$$\delta : K[X] \to \mathbb{N}_0, p \mapsto \begin{cases} \deg p + 1 & \text{falls } p \neq 0 \\ 0 & \text{falls } p = 0 \end{cases}$$

(c) Der Ring der Gaußschen Zahlen $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ ist euklidisch mit euklidischer Funktion

$$\delta : \mathbb{Z}[i] \to \mathbb{N}_0, z \mapsto |z|^2$$

denn zu $q \in \mathbb{Z}[i]$ mit $\left|\frac{a}{b} - q\right| \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$ und für $r := a - bq$ gilt

$$\delta(r) = |r|^2 = \left|\frac{a}{b} - q\right| |b|^2 \leq \frac{1}{2}|b|^2 \leq \frac{1}{2}\delta(b) < \delta(b)$$

1.6.3 Proposition.
Jeder euklidische Ring ist ein Hauptidealring.

Beweis. Sei R ein Integritätsring und $\delta : R \to \mathbb{N}_0$ eine euklidische Funktion. Sei I ein Ideal in R, Ohne Einschränkung $I \neq (0)$. Wähle $a \in I \setminus \{0\}$ mit kleinstmöglichem $\delta(a)$. Wir zeigen $I = (a)$. Sei hierzu $x \in I$. Schreibe $x = aq + r$ mit $q, r \in R$, $\delta(r) < \delta(a)$. Dann ist $r = x - aq \in I$ und folglich $r = 0$ gemäß Wahl von a. Also $x = aq \in (a)$. □

1.6.4 Erinnerung.
Sei R ein Hauptidealring. Wir fixieren eine Menge $\mathbb{P}_R$ von irreduziblen Elementen von R derart, dass jedes irreduzible Element zu genau einem Element von $\mathbb{P}_R$ assoziiert ist, zum Beispiel $\mathbb{P}_\mathbb{Z} := \mathbb{P} := \{2, 3, 5, \ldots\}$ und $\mathbb{P}_{K[X]} := \{p \in K[X] \mid p \text{ normiert und irreduzibel}\}$ (K ein Körper).

Betrachte $N_R := \{0\} \cup \left\{\prod_{i=1}^{n} p_i \mid n \in \mathbb{N}_0, p_1, \ldots, p_n \in \mathbb{P}_R\right\}$. Zum Beispiel $N_\mathbb{Z} = \mathbb{N}_0$ und $N_{K[X]} = \{p \in K[X] \mid p = 0 \text{ oder } p \text{ normiert}\}$ (K Körper).

Seien $m, n \in \mathbb{N}_0$ und setze $l := \min\{m, n\}$. Eine Matrix $S = (s_{ij})_{1 \le i \le m, 1 \le j \le n} \in N_R^{m \times n}$ heißt in *Smithscher Normalform*, wenn $s_{ij} = 0$ für $i \neq j$ und $s_{ii} | s_{(i+1)(i+1)}$ für alle $i \in \{1, \ldots, l-1\}$.

Betrachte die Gruppen $\mathrm{GL}_m(R) = (R^{m \times m})^* = \{P \in R^{m \times m} \mid \det P \in R^*\}$ und $\mathrm{GL}_n(R)$ und betrachte die Äquivalenzrelation $\sim$ auf $R^{m \times n}$ definiert durch $A \sim B \Leftrightarrow \exists P \in \mathrm{GL}_m(R) : \exists Q \in \mathrm{GL}_n(R) : A = PBQ \ (A, B \in R^{m \times n})$

Dann gibt es zu jedem $A \in R^{m \times n}$ genau ein $S \in R^{m \times n}$ in Smithscher Normalform mit $A \sim S$. Für jedes $i \in \{1, \ldots, l\}$ nennt man dann $c_i(A) := s_{ii}$ den i-ten *Elementarteiler* von A und $d_i(A) := \gcd\{i-\text{Minoren von } A\} \in N_R$ den i-ten Determinantenteiler von A.

Es gilt $d_i(A) = \prod_{j=1}^{i} c_j(A)$ für $i \in \{1, \ldots, l\}$.
Mit $c(A) := (c_1(A), \ldots, c_l(A))$ und $d(A) := (d_1(A), \ldots, d_l(A))$ gilt für $A, B \in R^{m \times n}$

$$\begin{aligned} A \sim B &\Leftrightarrow c(A) = c(B) \\ &\Leftrightarrow d(A) = d(B) \\ &\Leftrightarrow A \text{ und } B \text{ haben dieselbe Smithsche Normalform} \\ &\Leftrightarrow A \text{ und } B \text{ gehen aus Zeilen- und Spaltenoperationen vom Typ } (1), (2) \text{ oder } (3) \text{ hervor} \end{aligned}$$

Dabei ist

(1) $Z_i \leftarrow Z_i + aZ_j$ oder $S_i \leftarrow S_i + aS_j$ $\qquad (i \neq j, a \in R)$

(2) $Z_i \leftarrow aZ_i$ oder $S_i \leftarrow aS_i$ $\qquad (a \in R^*)$

(3) $\begin{pmatrix} Z_i \\ Z_j \end{pmatrix} \leftarrow \begin{pmatrix} aZ_i + bZ_j \\ cZ_i + dZ_j \end{pmatrix}$ oder $\begin{pmatrix} S_i \\ S_j \end{pmatrix} \leftarrow \begin{pmatrix} aS_i + bS_j \\ cS_i + dS_j \end{pmatrix}$ $(i \neq j, a, b, c, d \in R, ad - bc = 1)$

All diese Operationen sind umkehrbar. Die Operationen (1) und (3) verändern die Determinante nicht, die Operation (2) verändert sie nur bis auf eine Einheit.

Man überlegt ich leicht, dass man mit den Operationen (1) und (2) die Operation (4)
$\begin{pmatrix} Z_i \\ Z_j \end{pmatrix} \leftarrow \begin{pmatrix} Z_j \\ Z_i \end{pmatrix}$ oder $\begin{pmatrix} S_i \\ S_j \end{pmatrix} \leftarrow \begin{pmatrix} S_j \\ S_i \end{pmatrix}$ $\qquad (i \neq j)$

simulieren kann. Ist R *euklidisch*, so überlegt man sich, dass man damit auch (3) simulieren kann, weshalb in diesem Fall (3) überflüssig ist.

Ist $A \in R^{m \times n}$ gegeben und interessiert man sich nicht nur für ein zu A äquivalentes $B \in R^{m \times n}$ (z.B. die Smithsche Normalform), sondern auch für ein $P \in \mathrm{GL}_m(R)$ und $Q \in \mathrm{GL}_n(R)$ mit $B = PAQ$, so kann man im Schema $\begin{array}{|c|c|} \hline A & I_m \\ \hline I_n & \\ \cline{1-1} \end{array}$ Zeilenoperationen auf $\begin{array}{|c|c|} \hline A & I_m \\ \hline \end{array}$ und Spaltenoperationen auf $\begin{array}{|c|} \hline A \\ \hline I_n \\ \hline \end{array}$ anwenden, um $\begin{array}{|c|c|} \hline B & P \\ \hline Q & \\ \cline{1-1} \end{array}$ mit $P \in \mathrm{GL}_m(R), Q \in \mathrm{GL}_n(R)$ und $B = PAQ$ zu erhalten.

Interessiert man sich nicht nur für P oder nur für Q, so arbeitet man mit dem Schema $\boxed{A \mid I_m}$ oder $\boxed{\begin{array}{c} A \\ \hline I_n \end{array}}$

1.6.5 Notation.
Sei R ein kommutativer Ring. Dann definiert jede Matrix $A \in R^{m\times n}$ einen R-Modulhomomorphismus

$$f_A : R^n \to R^m, x \mapsto Ax$$

Man nennt $\operatorname{im} A := \operatorname{im} f_A$ das *Bild* von A

1.6.6 Bemerkung.

(a) Sei R ein kommutativer Ring und seien $A, B \in R^{m\times n}, P \in \mathrm{GL}_m(R)$ und $Q \in \mathrm{GL}_n(R)$ mit $B = PAQ$. Dann gilt $f_P(\operatorname{im} A) = \operatorname{im} B$, weshalb es (genau) einen R-Modulisomorphismus

$$\begin{aligned} R^m / \operatorname{im} A &\to R^m / \operatorname{im} B \\ \overline{x} &\mapsto \overline{Px} \end{aligned}$$

($x \in R^m$) gibt.

(b) Sei R ein Hauptidealring und sei $A \in R^{m\times n}$. Dann kann man mittels der Operationen (1), (2), (3) (falls R euklidisch ist, reichen (1) und (2)) A auf Smithsche Normalform bringen, wobei man die Zeilenoperationen auf $\boxed{A \mid I_m}$ anwendet, um $\boxed{S \mid P}$ zu erhalten mit $S \in R^{m\times n}$ in Smithscher Normalform und $P \in \mathrm{GL}_m(R)$, derart, dass $Q \in \mathrm{GL}_n(R)$ existiert mit $S = PAQ$.

Da S in Smithscher Normalform ist, kann man sofort $a_1, \ldots, a_k \in N_R \setminus \{1\}$ mit $a_1 | \ldots | a_k$ ablesen mit

$$\operatorname{im} S = R^{m-k} \times a_1 R \times \cdots \times a_k R$$

Gilt $P = \begin{pmatrix} & * & \\ \hline b_{11} & \cdots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{k1} & \cdots & b_{km} \end{pmatrix}$, so ist

$$\begin{aligned} R^m / \operatorname{im} A &\to \prod_{i=1}^{k} R/a_i R \\ \overline{x} &\mapsto (\overline{b_{11}x_1 + \cdots + b_{1m}x_m}, \ldots, \overline{b_{k1}x_1 + \cdots + b_{km}x_m}) \end{aligned}$$

ein R-Modulisomorphismus

1.6.7 Beispiel.

$$\mathbb{Z}^3/\left(\mathbb{Z}\begin{pmatrix}413\\-385\\427\end{pmatrix}+\mathbb{Z}\begin{pmatrix}140\\-126\\147\end{pmatrix}\right)\xrightarrow{\cong}\mathbb{Z}/7\mathbb{Z}\times\mathbb{Z}/133\mathbb{Z}\times\mathbb{Z}$$
$$\overline{(x_1,x_2,x_3)}\mapsto(\overline{-x_1+x_3},\overline{-9x_1-10x_2},\overline{3x_1+x_2-2x_3})$$

denn

413	140	1	0	0
-385	-126	0	1	0
427	147	0	0	1

kann man mit (1) und (2) in

7	0	-1	0	1
0	133	-9	-10	0
0	0	3	1	-2

1.6.8 Proposition und Definition.
Sei R ein Integritätsring und M ein R-Modul. Dann bildet die Menge der Torsionselemente vo M [$\to$1.2.4] einen Untermodul

$$T(M):=\{x\in M|\exists a\in R\setminus\{0\}:ax=0\}$$

von M, den wir den *Torsionsteil* von M nennen.

1.6.9 Satz. Struktursatz für endlich erzeugte Moduln über Hauptidealringen
Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es eindeutig bestimmte

(a) $k\in\mathbb{N}_0$ und $a_1,\dots,a_k\in N_R\setminus\{1\}$ mit $a_1|a_2|\dots|a_k$ und $M\cong\prod_{i=1}^k R/a_iR$

(b) $l,n\in\mathbb{N}_0$ und bis auf Reihenfolge eindeutige $(p_1,k_1),\dots,(p_l,k_l)\in\mathbb{P}_R\times\mathbb{N}$ mit $M\cong\left(\prod_{i=1}^l R/p_i^k R\right)\times R^n$

Beweis. Existenz

(a) Schreibe $M=Rx_1+\dots+Rx_m$ für ein $m\in\mathbb{N}_0$ und $x_1,\dots,x_m\in M$. Als Hauptidealring ist R natürlich noethersch (vgl. 1.4.3 und 1.1.5). Daher ist auch R^m noethersch (nach 1.4.6 oder 1.4.7) und wähle mit 1.2.5 einen Homomorphismus $f:R^m\twoheadrightarrow M$ mit $f(e_i)=x_i$ für alle $i\in\{1,\dots,m\}$. Als Untermodul von R^m ist der Kern von f endlich erzeugt und kann daher als Bild einer Matrix $A\in R^{m\times n}$ (mit m groß genug) geschrieben werden. $\ker f=\operatorname{im}A$. Nun gilt nach dem Isomorphiesatz $M\cong R^m/\ker f=R^m/\operatorname{im}A$ und wir können das Verfahren aus Bemerkung 1.6.6(b) anwenden.

(b)

$$(*)\qquad n:=|\{i\in\{1,\dots,k\}\mid a_i=0\}|$$

Zerlege die a_i mit $a_i\neq0$ in Produkte von Potenzen von paarweise verschiedenen Primfaktoren. Wende den Chinesischen Restsatz an (vgl. Beweis von 1.5.4)

Eindeutigkeit:
Sowohl in (a) als auch in (b) kann man n aus M zurückgewinnen, wobei im Fall (a) n durch $(*)$ definiert sei. In der Tat gilt

$$(**) \qquad T(M) \cong \prod_{i=1, a_i \neq 0}^{k} R/a_i R$$

bzw.

$$T(M) \cong \prod_{i=1}^{l} R/p_i^{k_i} R$$

woraus $M/T(M) \cong R^n$ und daher $n \overset{1.2.13}{=} \operatorname{rk}(M/T(M))$ folgt. Deswegen und wegen $(**)$ kann man nun sowohl in (a) als auch in (b) $n = 0$ voraussetzen.

Da M in (b) dann endllich Länge hat [$\rightarrow$1.4.17(b)] folgt dort Eindeutigkeit sofort aus dem Satz von Krull-Remak-Schmidt 1.5.13 in Verbindung mit 1.5.4 und 1.4.16. Schließlich zu (a).

Seien $k \in \mathbb{N}_0$ und $a_1, \ldots, a_k, b_1, \ldots, b_k \in N_R \setminus \{0\}$ mit $a_1 | \ldots | a_k, b_1 | \ldots | b_k$ und

$$\prod_{i=1}^{k} R/a_i R \cong \prod_{i=1}^{k} R/b_i R$$

Es reicht zu zeigen, dass $(a_1, \ldots, a_k) = (b_1, \ldots, b_k)$. Wir zeigen dazu $(a_j, \ldots, a_k) = (b_j, \ldots, b_k)$ für alle $j \in \{1, \ldots, k+1\}$ durch Induktion nach j.

$j = k$: klar

$j + 1 \rightarrow j$: $(j \in \{1, \ldots, k\})$. Zu zeigen ist $a_j = b_j$.

$$\begin{aligned}
\underbrace{\prod_{i=1}^{j} a_j R/a_i R}_{N} \times \prod_{i=j+1}^{k} a_j(R/b_i R) &\cong a_j \prod_{i=1}^{k} R/b_i R \\
&\cong a_j \prod_{i=1}^{k} R/a_i R \\
&= \prod_{i=1}^{k} a_j(R/a_i R) \\
&\cong \prod_{i=j+1}^{k} a_j(R/a_i R) \\
&= \prod_{i=j+1}^{k} a_j(R/b_i R)
\end{aligned}$$

Da alle beteiligten Moduln endliche Länge haben (wegen $a_i, b_i \neq 0$), erhalten wir $\ell(N) = 0$, also $N = 0$ und insbesondere $a_j(R/b_jR) = 0$, d.h. $a_j \in b_jR$. Analog $b_j \in a_jR$. Daher $(a_j) = (b_j)$ und wegen $a_j, b_j \in N_R$ gilt dann $a_j = b_j$ □

1.6.10 Korollar.
Jede endlich erzeugte abelsche Gruppe ist isomorph zu einem direkten Produkt endlich vieler zyklischer Gruppen.

1.6.11 Korollar.
Jede endliche abelsche Gruppe ist isomorph zu einem direkten Produkt von zyklischen Gruppen von Primzahlpotenzordnung.

1.6.12 Beispiel. Fortsetzung von Beispiel 1.6.7
$133 = 7 \cdot 19$, also nach dem Chinesischen Restsatz

$$\begin{aligned} \mathbb{Z}^3 / \left(\mathbb{Z} \begin{pmatrix} 413 \\ -385 \\ 427 \end{pmatrix} + \mathbb{Z} \begin{pmatrix} 140 \\ -126 \\ 147 \end{pmatrix} \right) &\xrightarrow{\cong} (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/19\mathbb{Z}) \times \mathbb{Z} \\ x &\mapsto (\overline{-x_1 + x_3}, \overline{-9x_1 - 10x_2}, \overline{-9x_1 - 10x_2}, 3x_1 + x_2 - 2x_3) \end{aligned}$$

1.7 Der Satz von Cayley-Hamilton

1.7.1 Definition und Proposition.
Sei R ein Ring und M ein R-Modul. Für $A \in R^{m\times n}$ und $X \in M^{n\times r}$ definieren wir AX durch

$$(AX)_{ik} := \sum_{j=1}^{n} A_{ij}X_{jk}$$

Fr̈ $1 \leq i \leq m, 1 \leq k \leq r$

Da R ein R-Modul ist, verallgemeinern wir damit auch die Matrizenmultiplikation von kommutativen Ringen auf beliebige Ringe. Man rechnet sofort nach, dass für alle $A \in R^{m\times n}, B \in R^{n\times r}, X \in M^{r\times s}$ gilt $(AB)X = A(BX)$. Insbesondere wird $R^{n\times n}$ ein Ring mit $1 = I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ und $M^{n\times r}$ ein $R^{n\times n}$-Modul [$\rightarrow$ 1.1.1].

Im Folgenden benutzen wir, dass $M^n = M^{n\times 1}$ ein $R^{n\times n}$-Modul ist.

1.7.2 Definition und Übung. [vgl. 1.5.6]
Sei R ein *kommutativer* Ring und M und N R-Moduln. Dann bildet

$$\mathrm{Hom}(M, N) := \{f \mid f : M \rightarrow N \text{ Homomorphismus}\}$$

mit punktweiser Addition und Skalarmultiplikation einen R-Modul.

1.7.3 Bemerkung und Notation.
Sei R ein *kommutativer* Ring mit $0 \neq 1$, M ein R-Modul und $f \in \mathrm{End}(M)$. Dann ist

$$R[f] := \left\{ \sum_k a_k f^k \mid a_k \in R \right\}$$

ein *kommutativer* Unterring von $\mathrm{End}(M)$.

Es gibt genau einen Ringhomomorphismus $\varphi : R[X] \rightarrow R[f]$ mit $\varphi\left(\sum_k a_k X^k\right) = \sum_k a_k f^k$ für alle $a_k \in R$. Schreibe $p(f) = \varphi(p)$ für $p \in R[X]$.

1.7.4 Übung.
Sei R ein *kommutativer* Ring mit $0 \neq 1$ und M ein R-Modul. Dann vermitteln die Zuordnungen

$$f \mapsto \begin{pmatrix} R[X] \times M & \rightarrow & M \\ (p, x) & \mapsto & (p(f))(x) \end{pmatrix}$$

$$\begin{pmatrix} M & \rightarrow & M \\ x & \mapsto & X \cdot x \end{pmatrix} \hookleftarrow \cdot$$

Eine Bijektion zwischen $\mathrm{End}(M)$ und der Menge der Skalarmultiplikationen, die M zu einem $R[X]$-Modul machen und die Skalarmultiplikation des R-Moduls M fortsetzen.

1.7.5 Satz. Satz von Cayley-Hamilton
Sei R ein kommutativer Ring, $I \subseteq R$ ein Ideal (z.B. $I = R$), $n \in \mathbb{N}_0$, M ein R-Modul, der von n Elementen erzeugt ist und $f \in \operatorname{End}(M)$ mit $\operatorname{im} f \subseteq IM := \left\{ \sum_i a_i x_i \mid a_i \in I, x_i \in M \right\}$.
Dann gibt es $a_1 \in I, a_2 \in I^2, \dots a_n \in I^n$ mit $f^n + a_1 f^{n-1} + \cdots + a_n \operatorname{id}_M = 0$.

Beweis. Ist $0 = 1$ in R, so $M = 0$ nach 1.2.8. Also sei ohne Einschränkung $0 \neq 1$ in R. Schreibe $M = Rx_1 + \cdots + Rx_n$ mit $x_1, \dots, x_n \in M$. Wähle $A \in I^{n\times n}$ mit $f(x_j) = \sum_{i=1}^{n} A_{ij} x_i$ für alle $j \in \{1, \dots, n\}$. Mache nun M zu einem $R[X]$-Modul vermöge $X \cdot x = f(x)$ für alle $x \in R^n$ [$\to$ 1.7.4].

Dann ist M^n ein $R[X]^{n\times n}$-Modul [$\to$ 1.7.1], in dem gilt

$$\underbrace{\begin{pmatrix} X & 0 & \cdots & 0 \\ 0 & X & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & X \end{pmatrix}}_{\in R[X]^{n\times n}} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} X \cdot x_1 \\ X \cdot x_2 \\ \vdots \\ X \cdot x_n \end{pmatrix} = \begin{pmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_n) \end{pmatrix} = \underbrace{A^T}_{\in R^{n\times n} \subseteq R[X]^{n\times n}} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{\in M^n}$$

also $(A^T - XI_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0$. Multipliziere nun von links mit der transponierten *Komatrix* $\big(\operatorname{com}(A^T - XI_n)\big)^T = \operatorname{com}(A - XI_n)$.

$$\begin{aligned}
0 &= \operatorname{com}(A - XI_n) \left((A^T - XI_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \right) \\
&= \operatorname{com}(A - XI_n)(A^T - XI_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} && 1.7.1 \\
&= \det(A - XI_n) I_n \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \\
&= \underbrace{\det(A - XI_n)}_{=:p \in R[X]} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}
\end{aligned}$$

Schreibe $p = (-1)^n(X^n + a_1 x^{n-1} + \cdots + a_n)$. Aus $(p(f))(x_i) = p \cdot x_i = 0$ für alle $i \in \{1, \ldots, n\}$ und $M = Rx_1 + \cdots + Rx_n$ folgt $p(f) = 0$. $\square$

2 Ganze Ringerweiterungen und Dedekindringe

2.1 Ganzheit

2.1.1 Sprechweise.
Sei A ein Unterring des *kommutativen* Ringes B, so sagen wir „$A \subseteq B$ ist eine *Ringerweiterung*“. Die Sprechweisen „Die Ringerweiterung $A \subseteq B$ hat eine Eigenschaft“ und „B hat eine Eigenschaft über A“ sind synonym.

2.1.2 Definition.
Sei $A \subseteq B$ eine Ringerweiterung. Dann heißt $x \in B$ *ganz* über A, wenn $0 = 1$ in B oder wenn es ein *normiertes* $f \in A[X]$ mit $f(x) = 0$ gibt („Ganzheitsgleichung“). Es heißt $A \subseteq B$ *ganz* (oder B ganz über A vgl. 2.1.1), wenn jedes $x \in B$ ganz über A ist.

2.1.3 Beispiel.

(a) $\sqrt{2}$ ist ganz über $\mathbb{Z}$, da $(\sqrt{2})^2 - 2 = 0$

(b) $\frac{1}{2}$ ist nicht ganz über $\mathbb{Z}$, denn wären $a_1, \ldots, a_n \in \mathbb{Z}$ mit $\left(\frac{1}{2}\right)^n + a_1 \left(\frac{1}{2}\right)^{n-1} + \cdots + a_n = 0$, so $1 + 2a_1 + \cdots + 2^n a_n = 0$ ↯.

(c) i und $i + 1$ sind ganz über $\mathbb{Z}$, denn $i^2 + 1 = 0$ und $(i + 1)^2 - 2(i + 1) + 2 = 0$

(d) Eine Körpererweiterung L/K ist algebraisch genau dann, wenn sie als Ringerweiterung $K \subseteq L$ ganz ist.

2.1.4 Bemerkung.
Ist A ein Unterring von B, so ist B in offensichtlicher Weise ein A-Modul

2.1.5 Satz.
Sei $A \subseteq B$ eine Ringerweiterung und $x \in B$. Es sind äquivalent

(a) x ist ganz über A

(b) $A[x]$ ist endlich erzeugt als A-Modul

(c) $A[x]$ ist in einem Unterring von B enthalten, der ein endlich erzeugter A-Modul ist.

Beweis. **(a)$\Longrightarrow$(b)$\Longrightarrow$(c)**: trivial

(c)$\Longrightarrow$(a): Sei C ein Unterring von B, der $A[X]$ enthält und als A-Modul endlich erzeugt ist. Für den A-Modulendomorphismus $f : C \to C, a \mapsto ax$ gibt es nach Cayley-Hamilton 1.7.5 $n \in \mathbb{N}_0$ und $a_1, \ldots, a_n \in A$ mit $f^n + a_1 f^{n-1} + \cdots + a_n \operatorname{id}_C = 0$. Auswerten in 1 liefert $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ □

2.1.6 Lemma.
Sei A ein Unterring des Ringes B. Sei B als A-Modul endlich erzeugt und sei M ein endlich erzeugter B-Modul. Dann ist M auch als A-Modul endlich erzeugt.

Beweis. Schreibe $B = Ab_1 + \cdots + Ab_m$ mit $b_1, \ldots, b_m \in B$ und $M = Bx_1 + \cdots + Bx_n, x_1, \ldots, x_n \in M$. Dann

$$M = \sum_{i=1}^{m} \sum_{j=1}^{n} A(b_i x_j)$$

□

2.1.7 Korollar.
Sei $A \subseteq B$ eine Ringerweiterung und seien $x_1, \ldots, x_n \in B$ ganz über A. Dann ist $A[x_1, \ldots, x_n]$ ein endlich erzeugter A-Modul.

Beweis. Benutze 2.1.5 $(a) \Longrightarrow (b)$, 2.1.6 und Induktion nach n □

2.1.8 Korollar. „Transitivität der Ganzheit“
Seien $A \subseteq B \subseteq C$ zwei Ringerweiterungen und sei $A \subseteq B$ ganz. Ist $a \in C$ ganz über B, so auch über A.

Beweis. Seien $b_1, \ldots, b_n \in B$ Koeffizienten einer Ganzheitsgleichung von a über B. Dann ist $A[b_1, \ldots, b_n]$ ein endlich erzeugter A-Modul nach 2.1.7 und $A[b_1, \ldots, b_n][a]$ ein endlich erzeugter A-Modul nach 2.1.5. Nach 2.1.6 ist $A[b_1, \ldots, b_n, a]$ dann ein endlich erzeugter A-Modul. Mit 2.1.5 ist dann a ganz über A. □

2.1.9 Korollar.
Seien $A \subseteq B \subseteq C$ Ringerweiterungen. Dann ist $A \subseteq C$ ganz genau dann, wenn $A \subseteq B$ und $B \subseteq C$ ganz sind.

2.1.10 Definition und Satz.
Sei $A \subseteq B$ eine Ringerweiterung. Dann bilden die Elemente von B, die ganz über A sind, einen Unterring von B, der A enthält, den sogenannten *ganzen Abschluss* von A in B.

Beweis. Jedes Element von A ist natürlich ganz über A. Sind $x, y \in B$ ganz über A, so auch $x + y, -x, x \cdot y$, denn $x + y, -x, x \cdot y \in A[x, y]$ und $A[x, y]$ ist nach 2.1.7 ein endlich erzeugter A-Modul (benutze 2.1.5$(c) \Longrightarrow (a)$) □

2.1.11 Definition.
Sei $A \subseteq B$ eine Ringerweiterung. Dann heißt A *ganz abgeschlossen* in B, wenn kein Element von $B \setminus A$ ganz über A ist (d.h. der ganze Abschluss von A in B gleich A ist).

2.1.12 Definition.
Sei A ein kommutativer Ring

(a) Der *ganze Abschluss* von A ist der ganze Abschluss von A in seinem totalen Quotientenring $Q(A)$

(b) A heißt *ganz abgeschlossen*, wenn A ganz abgeschlossen in $Q(A)$ ist.

Erinnerung: $A \subseteq Q(A) = \left\{ \frac{a}{s} \mid a, s \in A, \nexists b \in A \setminus \{0\} : sb = 0 \right\}$.
Ist A ein Integritätsring, so $A \subseteq Q(A) = \mathrm{qf}(A) = \left\{ \frac{a}{s} \mid a, s \in A, s \neq 0 \right\}$

2.1.13 Proposition.
Jeder faktorielle Ring ist ganz abgeschlossen.

Beweis. Sei A ein faktorieller Ring und $x \in \mathrm{qf}(A)$ ganz über A. Schreibe $x = \frac{a}{s}$, $a, s \in A, s \neq 0$ und $\gcd\{a, s\} = 1$. Wähle $a_1, \ldots, a_n \in A$ mit $x^n + a_1 x^{n-1} + \cdots + a_n = 0$. Multiplizieren mit s^n liefert $a^n + a_1 s a^{n-1} + \cdots + a_n s^n = 0$, woraus $s \mid a^n$ folgt. Wegen $\gcd\{a, s\} = 1$, folgt $s \in A^*$, also $\frac{a}{s} \in A$. □

2.1.14 Satz.
Sei A ein ganz abgeschlossener Integritätsring, $K := \mathrm{qf}(A)$ und L/K eine Körpererweiterung. Dann ist ein Element $x \in L$ genau dann ganz über A, wenn es algebraisch über K mit Minimalpolynom $\mathrm{irr}_K(x) \in A[X]$.

Beweis. Sei $x \in L$ ganz über A, etwa $f \in A[X]$ normiert mit $f(x) = 0$. Zu zeigen $\mathrm{irr}_K(x) \in A[X]$. Schreibe $\mathrm{irr}_K(x) = \prod_{i=1}^n (X - a_i) \in \overline{L}[X]$ mit $a_1, \ldots, a_n \in \overline{L}$. Wegen $\mathrm{irr}_K(x) | f$ in $K[X]$ gilt $f(a_i) = 0$ für alle $i \in \{1, \ldots, n\}$. Daher ist jedes a_i ganz über A und damit auch alle Koeffizienten von $\mathrm{irr}_K(x)$, welche damit nicht nur in K, sondern sogar in A liegen. □

2.1.15 Definition.
Ein *Zahlkörper* ist ein Oberkörper K von $\mathbb{Q}$ mit $K/\mathbb{Q}$ endlich. Ist K ein Zahlkörper, so heißt $[K : \mathbb{Q}]$ der *Grad* von K und der ganze Abschluss von $\mathbb{Z}$ in K heißt der *Zahlring* $\mathcal{O}_K$ (oder Ganzheitsring) von K. Zahlkörper von Grad 2 und ihre Zahlringe heißen *quadratisch*

2.1.16 Notation.

- $\boxslash := \{d \in \mathbb{Z} \setminus \{0, 1\} \mid \nexists p \in \mathbb{P} : p^2 | d\}$
- $\boxslash_+ := \{d \in \mathbb{Z} \setminus \{0, 1\} \mid \nexists p \in \mathbb{P} : p^2 | d, d > \}$
- $\boxslash_- := \{d \in \mathbb{Z} \setminus \{0, 1\} \mid \nexists p \in \mathbb{P} : p^2 | d, d < 0\}$

- $\varnothing_{2,3} := \left\{d \in \mathbb{Z} \setminus \{0,1\} \mid \nexists p \in \mathbb{P} : p^2 | d, d \equiv_{(4)} 2 \text{ oder } d \equiv_{(4)} 3\right\}$
- $\varnothing_1 := \left\{d \in \mathbb{Z} \setminus \{0,1\} \mid \nexists p \in \mathbb{P} : p^2 | d, d \equiv_{(4)} 1\right\}$

2.1.17 Proposition.
Für jedes $d \in \varnothing$ ist $\mathbb{Q}(\sqrt{d}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{d}$ ein quadratischer Zahlkörper mit Zahlring

$$\mathcal{O}_d := \mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} & \text{falls } d \in \varnothing_{2,3} \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{falls } d \in \varnothing_1 \end{cases}$$

Zu jedem quadratischen Zahlkörper gibt es genau ein $d \in \varnothing$ mit $K \cong \mathbb{Q}(\sqrt{d})$

Beweis. $\sqrt{d} \notin \mathbb{Q}$ wegen $d \in \varnothing$. Mit $\sqrt{d}^2 = d$ und $\left(\frac{1+\sqrt{d}}{2}\right)^2 = \frac{1+d}{4} + \frac{\sqrt{d}}{2} = \frac{d-1}{4} + \left(\frac{1+\sqrt{d}}{2}\right)$ folgen die drei Zerlegungen in direkte Summen.

Seien $a, b \in \mathbb{Q}$. Wir behaupten

$$(*) \qquad a + b\sqrt{d} \in \mathcal{O}_d \Leftrightarrow a + b\sqrt{d} \in \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{falls } d \in \varnothing_{2,3} \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{falls } d \in \varnothing_1 \end{cases}$$

Ohne Einschränkung $b \neq 0$. Dann

$$\begin{aligned}(X - (a + b\sqrt{d}))(X - (a - b\sqrt{d})) &= ((X - a) + b\sqrt{d})((X - a) - b\sqrt{d}) \\ &= (X - a)^2 - b^2 d \\ &= X^2 - 2aX + (a^2 - b^2 d) \\ &= \operatorname{irr}_{\mathbb{Q}}(a + b\sqrt{d})\end{aligned}$$

daher

$$\begin{aligned} a + b\sqrt{d} \in \mathcal{O}_d &\Leftrightarrow \left\{2a, a^2 - b^2 d\right\} \subseteq \mathbb{Z} && 2.1.14 \\ &\Leftrightarrow \left\{2a, a^2 - b^2 d, 4b^2 d\right\} \subseteq \mathbb{Z} \\ &\Leftrightarrow \left\{2a, a^2 - b^2 d, 2b\right\} \subseteq \mathbb{Z} && d \in \varnothing \end{aligned}$$

Setzt man $x := 2a, y := 2b$, so folgt aus beiden Seiten $\{x, y\} \subseteq \mathbb{Z}$, weshalb wir dies ab jetzt annehmen. Also

$$(**) \qquad a + b\sqrt{d} \in \mathcal{O}_d \Leftrightarrow \overline{x}^2 = \overline{y}^2\overline{d} \text{ in } \mathbb{Z}/(4)$$

Wegen $\overline{x}^2, \overline{y}^2 \in \left\{\overline{0}, \overline{1}\right\} \subseteq \mathbb{Z}/(4)$ gilt

- Im Fall $d \in \varnothing_{2,3}$

$$\begin{aligned}(**) &\Leftrightarrow \overline{y}^2 = 0 \wedge \overline{x}^2 = 0 \\ &\Leftrightarrow \{\overline{x}, \overline{y}\} \subseteq \left\{\overline{0}, \overline{2}\right\} \subseteq \mathbb{Z}/(4) \\ &\Leftrightarrow \{x, y\} \subseteq 2\mathbb{Z} \\ &\Leftrightarrow \{a, b\} \subseteq \mathbb{Z} \\ &\Leftrightarrow a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]\end{aligned}$$

- Im Fall $d \in \boxslash_1$

$$\begin{aligned}
(**) &\Leftrightarrow \overline{x}^2 = \overline{y}^2 \\
&\Leftrightarrow x \equiv_{(2)} y \\
&\Leftrightarrow \frac{x-y}{2} \in \mathbb{Z} \\
&\Leftrightarrow a - b \in \mathbb{Z} \\
&\Leftrightarrow (a-b) + 2b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]
\end{aligned}$$

Dass jeder quadratische Zahlkörper K zu einem $\mathbb{Q}(\sqrt{d})$ mit $d \in \boxslash$ isomorph ist, ist klar. Sind schließlich $d, e \in \boxslash$ mit $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}(\sqrt{e})$, so gibt es $a, b \in \mathbb{Q}$ mit $(a+b\sqrt{d})^2 = e$. Es folgt $2ab = 0$. Es gilt $b \neq 0$, da $e \in \boxslash$. Also $a = 0$ und $b^2 d = e$. Da $e \in \boxslash$, folgt $b^2 = 1$, also $d = e$ $\square$

2.2 Dedekindringe

2.2.1 Erinnerung.
Sei R ein kommutativer Ring

(a) Ein Ideal $\mathfrak{p}$ in R heißt prim (oder Primideal), wenn $1 \notin \mathfrak{p}$ und

$$\forall a, b \in R : (ab \in \mathfrak{p} \Rightarrow (a \in \mathfrak{p} \vee b \in \mathfrak{p}))$$

(b) Ein Element $p \in R$ heißt prim (oder Primelement), wenn (p) ein Primideal ist, d.h. $p \notin R^*$ und

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

(c) Sind $I_1, \ldots, I_n$ Ideale von R, so nennt man

$$\begin{aligned}\prod_{k=1}^{n} I_k := I_1 \cdot \cdots \cdot I_n &:= (\{a_1 \cdot \cdots \cdot a_n \mid a_1 \in I_1, \ldots, a_n \in I_n\}) \\ &= \begin{cases} R & \text{falls } n = 0 \\ \{\sum_i a_{i_1} \ldots a_{i_n} \mid a_{i_1} \in I_1, \ldots a_{i_n} \in I_n\} & \text{falls } n \geq 1 \end{cases}\end{aligned}$$

deren *Produkt*

(d) In Integritätsringen sind Primfaktorzerlegungen (im Wesentlichen) eindeutig, d.h. ist R ein Integritätsring, $m, n \in \mathbb{N}_0$ und $p_1, \ldots, p_m, q_1, \ldots, q_n \in R \setminus \{0\}$ prim mit $p_1 \cdot \cdots \cdot p_m = q_1 \cdot \cdots \cdot q_m$, so gilt $m = n$ und es gibt ein $\sigma \in S_n$ mit $(p_i) = (q_{\sigma(i)})$ für $i \in \{1, \ldots, n\}$ (vergleiche auch 1.4.17(b)).

(e) R heißt faktoriell, wenn R ein Integritätsring ist und jedes $a \in R$ eine Primfaktorzerlegung besitzt, d.h. es gibt $c \in R^*, n \in \mathbb{N}_0$ und Primelemente $p_1, \ldots, p_n \in R$ mit $a = cp_1 \cdot \cdots \cdot p_n$.

(f) R euklidisch $\overset{1.6.3}{\Longrightarrow}$ R Hauptidealring $\Longrightarrow$ R faktoriell $\Longrightarrow$ R Integritätsring

2.2.2 Beispiel.
Wegen $-5 \equiv_{(4)} -1 \equiv_{(4)} 3$ sind $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[\sqrt{5}i]$ quadratische Zahlringe [$\rightarrow$2.1.17].

Der Beweis von 1.6.2(c) dafür, dass $\mathbb{Z}[\sqrt{-1}]$ euklidisch ist, funktioniert für $\mathbb{Z}[\sqrt{-5}]$ nicht mehr, da man nur noch

$$\left|\frac{a}{b} - q\right| \leq \left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{5}}{2}\right)^2 = \frac{1}{4} + \frac{5}{4} = \frac{6}{4}$$

erhält, aber $\frac{6}{4} \geq 1$.

Tatsächlich ist $\mathbb{Z}[\sqrt{-5}]$ nicht einmal faktoriell, denn 2 besitzt darin keine Primfaktorzerlegung, weil sonst 2 prim in $\mathbb{Z}[\sqrt{-5}]$ sein müsste, was aber nicht der Fall ist, denn $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, aber $2 \nmid (1 + \sqrt{-5})$ und $2 \nmid (1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$.

Andererseits besitzt (2) eine *Primidealzerlegung*, d.h. es ist Produkt von Primidealen, denn $(2, 1+\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$ ist ein Primideal mit

$$\begin{aligned}(2, 1+\sqrt{-5})^2 &= (2, 1+\sqrt{-5})(2, 1+\sqrt{-5}) \\ &= (4, 2+2\sqrt{-5}, -4+2\sqrt{-5}) \\ &= (4, 2+2\sqrt{-5}, 2\sqrt{-5}) \\ &= (4, 2, 2\sqrt{-5}) = (2)\end{aligned}$$

Dass $(2, 1+\sqrt{-5})$ prim (und sogar maximal) ist, folgt, daraus, dass es der Kern des Ringhomomorphismus

$$\varphi : \mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_2, a + b\sqrt{-5} \mapsto \overline{a+b}$$

ist, wie man unter Beachtung von $\varphi(\sqrt{-5})^2 = 1 = -5$ in $\mathbb{F}_2$ sofort nachrechnet.

2.2.3 Motivation.
Zahlringe spielen eine wichtige Rolle bei der Untersuchung arithmetischer Eigenschaften von $\mathbb{Z}$. Leider sind sie nicht immer faktoriell. Der Ausweg wird sein, statt Elemente Ideale und statt Primelemente Primideale zu betrachten

2.2.4 Definition. [vgl. 2.2.1(e)]
Ein Integritätsring heißt *Dedekindring*, wenn darin jedes Ideal ein Produkt von Primidealen ist.

2.2.5 Beispiel.
Jeder Hauptidealring ist ein Dedekindring

2.2.6 Definition.
ei A ein Integritätsring. Ein *gebrochenes Ideal* von A ist ein A-Untermodul von $\operatorname{qf}(A)$ mit $sI \subseteq A$ für ein $s \in A \setminus \{0\}$.

Zyklische [$\to$1.1.4(d)] gebrochene Ideale nennt man *gebrochene Hauptideale*.

2.2.7 Bemerkung.
Sei A ein Integritätsring.

(a) Jedes gebrochene Ideal von A ist als A-Modul isomorph zu einem Ideal von A (ist nämlich $s \in A \setminus \{0\}$ mit $sI \subseteq A$, so $I \xrightarrow{\cong} sI, a \mapsto sa$).

(b) Die gebrochenen Ideale von A sind genau die $s^{-1}I$ ($s \in A \setminus \{0\}$, I ein Ideal von A).

(c) A ist ein Hauptidealring genau dann, wenn jedes gebrochene Ideal von A ein gebrochenes Hauptideal von A ist.

(d) Jeder endlich erzeugte A-Untermodul von $\operatorname{qf}(A)$ ist ein gebrochenes Ideal

(e) Ist A noethersch, so sind die gebrochenen Ideale von A genau die endlich erzeugten A-Untermoduln von $\operatorname{qf}(A)$

2.2.8 Proposition und Definition.
Seien A ein Integritätsring und I, J gebrochene Ideale von A. Dann sind auch $I + J$, $I \cap J, I \cdot J = \left\{ \sum_i a_i b_i \mid a_i \in I, b_i \in J \right\}$ und für $J \neq 0$ auch $I : J := \{a \in \mathrm{qf}(A) \mid aJ \subseteq I\}$ gebrochene Ideale von A.

Beweis. Mit I und J sind auch $I + J, I \cap J$ (trivial), IJ und $I : J$ A-Untermoduln von $\mathrm{qf}(A)$. Sind $s, t \in A \setminus \{0\}$ mit $sI \subseteq A$ und $tJ \subseteq A$, so ist auch $st(I+J) \subseteq A$, $s(I \cap J) \subseteq A$ und $(st)(IJ) \subseteq A$. Ist ferner $J \neq 0$, so gibt es $b \in J \cap (A \setminus \{0\})$ und es gilt für $a \in I : J$, dass $(sb)a = s(ab) \in s(aJ) \subseteq sI \subseteq A$, also $sb(I : J) \subseteq A$. □

2.2.9 Definition und Proposition.
Sei A ein Integritätsring und I ein gebrochenes Ideal von A. Dann heißt I *invertierbar*, wenn es ein gebrochenes Ideal J von A gibt mit $IJ = A$. In diesem Fall gilt $J = I^{-1} := A : I$ und I und J sind endlich erzeugt.

Beweis. Gelte $IJ = A$. Dann $J \subseteq A : I = (A : I)IJ \subseteq AJ = J$, also $J = A : I$.
Schreibe $1 = \sum_i a_i b_i$ mit $a_i \in I, b_i \in J$. Dann gilt

$$I = (\sum_i a_i b_i)I = \sum_i \underbrace{(b_i I)}_{\subseteq A} a_i \subseteq \sum_i A a_i \subseteq I$$

Womit $I = \sum_i A a_i$ endlich erzeugt ist. Analog für J. □

2.2.10 Beispiel.
Jedes gebrochene Hauptideal $\neq 0$ eines Integritätsring ist invertierbar.

2.2.11 Satz. (Eindeutigkeit der Primidealzerlegung invertierbarer Ideale, unter Beachtung von 2.2.10 und 2.2.1(b) Verallgemeinerung von 2.2.1(d))

Sei A ein Integritätsring und I ein Ideal von A, was als gebrochenes Ideal invertierbar ist. Seien $m, n \in \mathbb{N}_0$ und $\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q}_1, \dots, \mathfrak{q}_n$ Primideale in A mit $\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_m = \mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_n = I$. Dann gilt $m = n$ und es gibt $\sigma \in S_n$ mit $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ für alle $i \in \{1, \dots, n\}$.

Beweis. Induktion nach m. $m = 0$: trivial.
$m - 1 \to m (m \in \mathbb{N})$. Mit I sind alle $\mathfrak{p}_i$ und $\mathfrak{q}_j$ invertierbar. Aus $\mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_n \subseteq \mathfrak{p}_1$ folgt, dass es ein j mit $\mathfrak{q}_j \subseteq \mathfrak{p}_1$ gibt (insbesondere $n \geq 1$). denn andernfalls gäbe es $b_1 \in \mathfrak{q}_1 \setminus \mathfrak{p}_1, \dots b_n \in \mathfrak{q}_n \setminus \mathfrak{p}_1$ und $b_1 \cdot \dots \cdot b_n \in \mathfrak{q}_1 \cdot \dots \cdot \mathfrak{q}_n \setminus \mathfrak{p}_1$.
Ohne Einschränkung $j = 1$. Nun ist $\mathfrak{p}^{-1}\mathfrak{q}_1$ ein Ideal, weil $\mathfrak{p}_1^{-1}\mathfrak{q}_1 \subseteq \mathfrak{p}_1^{-1}\mathfrak{p}_1 = A$, weshalb $\mathfrak{p}_1(\mathfrak{p}_1^{-1}\mathfrak{q}_1) = \mathfrak{q}_1$ impliziert, dass $\mathfrak{p}_1 \subseteq \mathfrak{q}_1$ oder $\mathfrak{p}_1^{-1}\mathfrak{q}_1 \subseteq \mathfrak{q}_1$, aber letzteres ist unmöglich, da sonst $A = \mathfrak{p}_1\mathfrak{p}_1^{-1}\mathfrak{q}_1\mathfrak{q}_1^{-1} \subseteq \mathfrak{p}_1\mathfrak{q}_1\mathfrak{q}_1^{-1} = \mathfrak{p}_1$. Also $\mathfrak{q}_1 \subseteq \mathfrak{p}_1 \subseteq \mathfrak{q}_1$ und daher $\mathfrak{p}_1 = \mathfrak{q}_1$. Somit $\mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_n = I\mathfrak{p}_1^{-1} = \mathfrak{q}_2 \cdot \dots \cdot \mathfrak{q}_m$. Wende nun die Induktionsvoraussetzung an. □

2.2.12 Satz.
Sei A ein Dedekindring. Dann gilt

(a) Jedes Ideal $\neq (0)$ von A ist invertierbar [$\to$2.2.9].

(b) A ist ganz abgeschlossen

(c) A ist noethersch

(d) In A ist jedes Primideal $\neq (0)$ maximal.

Beweis.
Behauptung 1: Jedes invertierbare Primideal von A ist ein maximales Ideal [In (d) wird dies sogar für alle Primideale $\neq (0)$ behauptet].

Begründung: Sei $\mathfrak{p}$ ein invertierbares Primideal von A. Wir zeigen, dass $A/\mathfrak{p}$ ein Körper ist. Sei hierzu $a \in A$ mit $\overline{a} \neq 0$ in $A/\mathfrak{p}$, das heißt $a \notin \mathfrak{p}$. Zu zeigen ist $\overline{a} \in (A/\mathfrak{p})^*$. Es reicht zu zeigen, dass $I := aA + \mathfrak{p} = A$. Da $\mathfrak{p}$ invertierbar ist, reich es $a\mathfrak{p} + \mathfrak{p}^2 = \mathfrak{p}$ zu zeigen. Wir zeigen zunächst $I^2 = J := a^2A + \mathfrak{p}$, was wegen $I^2 = a^2A + a\mathfrak{p} + \mathfrak{p}^2$ eine Abschwächung der Behauptung ist. Wir wissen $(I/\mathfrak{p})^2 = J/\mathfrak{p}$.

Da A ein Dedekindring ist, gibt es $m, n \in \mathbb{N}_0$ und Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ und $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ von A mit $I = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ und $J = \mathfrak{q}_1 \cdots \mathfrak{q}_n$. Es gilt $\mathfrak{p} \subseteq I \subseteq \mathfrak{p}_i$ für alle $i \in \{1, \dots, m\}$ und $\mathfrak{p} \subseteq J \subseteq \mathfrak{q}_j$ für alle $j \in \{1, \dots, n\}$.

Da die Primideale in $A/\mathfrak{p}$ den Primidealen von A entsprechen, die $\mathfrak{p}$ enthalten, erhalten wir im Integritätsring $A/\mathfrak{p}$ die Primidealzerlegungen

$$I/\mathfrak{p} = (\mathfrak{p}_1/\mathfrak{p}) \cdots (\mathfrak{p}_m/\mathfrak{p})$$

und

$$J/\mathfrak{p} = (\mathfrak{q}_1/\mathfrak{p}) \cdots (\mathfrak{q}_n/\mathfrak{p})$$

Es folgt $(\mathfrak{p}_1/\mathfrak{p})^2 \cdots (\mathfrak{p}_m/\mathfrak{p})^2 = (I/\mathfrak{p})^2 = J/\mathfrak{p} = (\mathfrak{q}_1/\mathfrak{p}) \cdots (\mathfrak{q}_n/\mathfrak{p})$

Da $J/\mathfrak{p} = (\overline{a}^2) \neq 0$ als Hauptideal nach 2.2.10 invertierbar ist, folgt mit 2.2.11 ohne Einschränkung $(\mathfrak{p}_1/\mathfrak{p}, \mathfrak{p}_1/\mathfrak{p}, \dots, \mathfrak{p}_m/\mathfrak{p}, \mathfrak{p}_m/\mathfrak{p}) = (\mathfrak{q}_1/\mathfrak{p}, \dots, \mathfrak{q}_n/\mathfrak{p})$ und daher $(\mathfrak{p}_1, \mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{p}_m) = (\mathfrak{q}_1, \dots, \mathfrak{q}_n)$, also $I^2 = J$.

Um schließlich $a\mathfrak{p} + \mathfrak{p}^2 = \mathfrak{p}$, sei $b \in \mathfrak{p}$. Zu zeigen ist $b \in a\mathfrak{p} + \mathfrak{p}^2$. Wegen $b \in J$ gilt $b \in I^2 = a^2A + a\mathfrak{p} + \mathfrak{p}^2$. Schreibe $b = a^2c + b'$ mit $c \in A, b' \in a\mathfrak{p} + \mathfrak{p}^2$. Dann $a^2c = b - b' \in \mathfrak{p}$ und daher $c \in \mathfrak{p}$. Somit auch $b \in a\mathfrak{p} + \mathfrak{p}^2$

Behauptung 2: Jedes Primideal $\neq (0)$ von A ist invertierbar [In (a) wird dies sogar für alle Ideale $\neq 0$ behauptet]

Begründung: Sei $\mathfrak{p} \neq (0)$ ein Primideal von A. Wähle ein $a \in \mathfrak{p} \setminus \{0\}$. Schreibe $aA = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ mit Primidealen $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ von A. Da aA invertierbar ist [$\to$2.2.10] ist es auch jedes $\mathfrak{p}_i$. Wegen $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}$ ist aber auch $\mathfrak{p}$ eines dieser $\mathfrak{p}_i$, denn es gibt ein i mit $\mathfrak{p}_i \subseteq \mathfrak{p}$ und $\mathfrak{p}_i$ ist maximal nach Behauptung 1.

Wegen der Existenz der Primfaktorzerlegung in A, folgt aus Behauptung 2 sofort (a). Damit ist Behauptung 1 gleichbedeutend mit (d).

Aus (a) folgt (c) mit 2.2.9. Um schließlich (b) zu zeigen, sei $a \in \mathrm{qf}(A)$ ganz über A. Dann ist $A[a]$ ein endlich erzeugter A-Modul [$\to$2.1.5] und damit ein gebrochenes Ideal von A [$\to$ 2.2.7(d)], das nach (a) invertierbar ist.

Aus $A[a]^2 \subseteq A[a]$ folgt daher $A[a] \subseteq A$ und daher $a \in A$ wie gewünscht. $\square$

2.3 Charakterisierung von Dedekindringen

2.3.1 Lemma. In einem noetherschen Integritätsring enthält jedes Ideal $\neq (0)$ ein Produkt von Primidealen $\neq (0)$.

Beweis. Sei A ein Integritätsring und $I \neq (0)$ ein Ideal von A, welches kein Produkt von Primdiealen $\neq (0)$ enthält. Es reicht ein Ideal $J \supsetneq I$ von A zu finden, welches auch kein Produkt von Primidealen $\neq 0$ enthält. Da I weder ein Primideal von ganz A ist, gibt es $a, b \in A \setminus I$ mit $ab \in I$. Dann sind $J := I + (a)$ und $K := I + (b)$ Ideale von A mit $J \supsetneq I$ und $K \supsetneq I$ und $JK \subseteq I$. Es können nicht sowohl J als auch K ein Produkt von Primidealen $\neq 0$ enthalten. □

2.3.2 Satz. Sei A ein Ring. Dann ist A ein Dedekindring genau dann, wenn A ein noetherscher, ganz abgeschlossener Integritätsring ist, indem alle Primideale $\neq (0)$ maximal sind.

Beweis. Ist A ein Dedekindring, so besitzt A die gewünschten Eigenschaften nach 2.2.12. Sei umgekehrt A ein noetherscher, ganz abgeschlossener Integritätsring, in dem alle Primideale $\neq (0)$ maximal sind.
Behauptung 1: Seien I und J gebrochene Ideale von A mit $J \neq (0)$ und $IJ \subseteq J$. Dann $I \subseteq A$.
Begründung: Sei $x \in I$. Zu zeigen ist $x \in A$. Es reicht zu zeigen, dass x ganz über A ist. Nach 2.1.5 reicht es zu zeigen, dass $A[x]$ ein endlich erzeugter A-Modul ist.

Durch Induktion zeigt man $\forall n \in \mathbb{N}_0 : x^n J \subseteq J$ (In der Tat $x^{n-1}J \subseteq J$ für ein $n \in \mathbb{N}$, so $x^n J = x(x^{n-1}J) \subseteq xJ \subseteq IJ \subseteq J$)

Es folgt $A[x]J \subseteq J$. Wählt man $y \in J \setminus \{0\}$, so folgt also $A[x]y \subseteq J$. Da A noethersch ist, ist J ein endlich erzeugter A-Modul [$\rightarrow$2.2.7(e)] und daher selber noethersch [$\rightarrow$1.4.7], womit $A[x]y \cong A[x]$ ein endlich erzeugter A-Modul ist.

Behauptung 2: Sei $\mathfrak{p} \neq (0)$ ein Primideal von A. Dann ist $\mathfrak{p}$ invertierbar.
Begründung: Wegen $\mathfrak{p} = 1 \cdot \mathfrak{p} \subseteq (A : \mathfrak{p})\mathfrak{p} \subseteq A$ und da $\mathfrak{p}$ maximal ist, reicht es $\mathfrak{p} \neq (A : \mathfrak{p})\mathfrak{p}$, d.h. $(A : \mathfrak{p})\mathfrak{p} \not\subseteq \mathfrak{p}$ zu zeigen, was nach Behauptung 1 mit $A : \mathfrak{p} \not\subseteq A$ gleichbedeutend ist.
Wähle $b \in \mathfrak{p} \setminus \{0\}$. Nach Lemma 2.3.1 gibt es ein $n \in \mathbb{N}_0$ und Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_n \neq (0)$ mit $\mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_n \subseteq (b) \subseteq \mathfrak{p}$, wobei wir n so klein wie möglich wählen.
Dann gibt es i mit $\mathfrak{p}_i \subseteq \mathfrak{p}$, ohne Einschränkung $i = 1$. Da $\mathfrak{p}_1$ maximal ist, folgt $\mathfrak{p}_1 = \mathfrak{p}$.
Nach Wahl von n gilt $\mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_n \not\subseteq (b)$ und wir können $a \in (\mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_n) \setminus (b)$ wählen.
Dann $a\mathfrak{p} \subseteq (b)$, also $\frac{a}{b}\mathfrak{p} \subseteq A$, das heißt, $\frac{a}{b} \in A : \mathfrak{p}$. Aber $\frac{a}{b} \notin A$, da $a \notin (b)$.

Angenommen A wäre kein Dedekindring. Da A noethersch gäbe es dann ein Ideal $I \subseteq A$, welches bezüglich der Eigenschaft, kein Produkt von Primidealen zu sein, maximal ist. Wähle ein maximales Ideal $\mathfrak{p}$ von A mit $I \subseteq \mathfrak{p}$. Es gälte $I \subsetneq I\mathfrak{p}^{-1}$ [$\rightarrow$Beh. 2] (, denn $A \subseteq A : \mathfrak{p} = \mathfrak{p}^{-1}$ und daher $I \subseteq I\mathfrak{p}^{-1}$ und wäre $I = I\mathfrak{p}^{-1}$, so $\mathfrak{p}^{-1} \subseteq A$ nach Beh. 1 und daher $A \subseteq \mathfrak{p}$ ↯)
Wegen der Maximalität von I wäre $I\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A$ und daher auch $I = \mathfrak{p}(I\mathfrak{p}^{-1})$ ein Produkt von Primidealen ↯ □

2.4 Norm, Spur und Diskriminante

2.4.1 Definition.
Sei $L|K$ eine endlich Körpererweiterung und $a \in L$. Dann ist $\varphi_a : L \to L, x \mapsto ax$ ein Endomorphismus des K-Vektorraumes L.
Ist $\underline{v} = (v_1, \ldots, v_n)$ eine beliebige Basis des K-Vektorraumes L (insbesondere $n = [L : K]$) und $A = (a_{ij})_{1 \leq i,j \leq n} = M(\varphi_a, \underline{v})$ die Darstellungsmatrix von φ_a bezüglich $\underline{v}$ (also $av_j = \sum_{i=1}^{n} a_{ij} v_i$ für alle $j \in \{1, \ldots, n\}$), so heißt

$$\chi_{L|K}(a) := \chi_{\varphi(a)} = \det(A - XI_n) \in K[X]$$

das *charakteristische Polynom*,

$$N_{L|K}(a) := \det(A) = \chi_{L|K}(0)$$

die *Norm* und

$$\mathrm{tr}_{L|K}(a) := \mathrm{tr}\, A = \sum_{i=1}^{n} a_{ii} = (-1)^{n-1} \text{„Koeffizient von } X^{n-1} \text{ in } \chi_{L|K}(a)\text{“}$$

die *Spur* von A bezüglich $L|K$ [diese Begriffe hängen nicht von der Wahl der Basis $\underline{v}$ ab].

2.4.2 Beispiel.
Sei $d \in \varnothing$ [$\to$ 2.1.16]. Seien $a, b \in \mathbb{Q}$ und $x = a + b\sqrt{d} \in \mathbb{Q}(d)$.
Betrachte Basis $\underline{v} = (1, \sqrt{d})$ von $\mathbb{Q}(\sqrt{d})$ [$\to$2.1.17]. Dann $x \cdot 1 = a + b\sqrt{d}$ und $x\sqrt{d} = bd + a\sqrt{d}$.
Setzt man also $A = \begin{pmatrix} a & bd \\ b & a \end{pmatrix} \in \mathbb{Q}^{2\times 2}$, so

$$\chi_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}(x) = \det \begin{pmatrix} a - X & bd \\ b & a - X \end{pmatrix} = (a - X)^2 - b^2 d = X^2 - 2aX + (a^2 - b^2 d)$$

und daher $N_{Q(\sqrt{d})|\mathbb{Q}}(x) = a^2 - b^2 d$ und $\mathrm{tr}_{Q(\sqrt{d})|\mathbb{Q}}(x) = 2a$

2.4.3 Proposition.
Sei $L|K$ eine endliche Körpererweiterung. Dann ist $\mathrm{tr}_{L|K} : L \to K$ K-linear und es gilt $N_{L|K}(ab) = N_{L|K}(a) N_{L|K}(b)$ für alle $a, b \in L$.
Es ist $N_{K|L}\big|_{L^*} L^* \to K^*$ ein Gruppenhomomorphismus.

Beweis. Wähle eine Basis $\underline{v} = (v_1, \ldots, v_n)$ des K-Vektorraumes L. Sind $a, b \in L$ und $c \in K$, so gilt

$$\begin{aligned}
\mathrm{tr}_{L|K}(a + b) &= \mathrm{tr}\, M(\varphi_{a+b}, \underline{v}) \\
&= \mathrm{tr}\, M(\varphi_a + \varphi_b, \underline{v}) \\
&= \mathrm{tr}(M(\varphi_a, \underline{v}) + M(\varphi_b, \underline{v})) \\
&= \mathrm{tr}\, M(\varphi_a, \underline{v}) + \mathrm{tr}\, M(\varphi_b, \underline{v}) \\
&= \mathrm{tr}_{L|K}(a) + \mathrm{tr}_{L|K}(b)
\end{aligned}$$

und

$$\begin{aligned}\operatorname{tr}_{L|K}(ca) &= \operatorname{tr} M(\varphi_{ca}, \underline{v}) \\ &= \operatorname{tr} M(c\varphi_a, \underline{v}) \\ &= \operatorname{tr}(cM(\varphi_a, \underline{v})) \\ &= c \operatorname{tr} M(\varphi_a, \underline{v}) \\ &= c \operatorname{tr}_{L|K}(a)\end{aligned}$$

$$\begin{aligned}N_{L|K}(ab) &= \det M(\varphi_{ab}, \underline{v}) \\ &= \det M(\varphi_a \circ \varphi_b, \underline{v}) \\ &= \det(M(\varphi_a, \underline{v}) M(\varphi_b, \underline{v})) \\ &= \det M(\varphi_a, \underline{v}) \det M(\varphi_b, \underline{v}) \\ &= N_{L|K}(a) N_{L|K}(b)\end{aligned}$$

$$\begin{aligned}N_{L|K}(a) = 0 &\Leftrightarrow \det M(\varphi_a, \underline{v}) = 0 \\ &\Leftrightarrow \varphi_a \text{ nicht bijektiv} \\ &\Leftrightarrow a = 0\end{aligned}$$

(denn $a \neq 0 \Rightarrow \varphi_a \circ \varphi_{a^{-1}} = \mathrm{id}_L = \varphi_{a^{-1}} \circ \varphi_a$). □

2.4.4 Proposition.
Sei F ein Zwischenkörper der endlichen Körpererweiterung $L|K$. Dann gilt für alle $a \in F$

$$\chi_{L|K}(a) = (\chi_{F|K}(a))^{[L:F]}$$

$$N_{L|K}(a) = (N_{F|K}(a))^{[L:F]}$$

$$\operatorname{tr}_{L|K}(a) = [L:F] \operatorname{tr}_{F|K}(a)$$

Beweis. Wähle eine Basis $\underline{u} = (u_1, \ldots, u_m)$ des K-Vektorraumes F und eine Basis $\underline{v} = (v_1, \ldots, v_n)$ des F-Vektorraumes L.

Dann ist $\underline{w} := (u_1 v_1, \ldots, u_m v_1, \ldots, u_m v_n)$ eine Basis des K-Vektorraumes L.

Für alle $a \in F$ gilt nun

$$M(\varphi_a, \underline{w}) = \begin{pmatrix} M(\psi_a, \underline{u}) & & & \\ & M(\psi_a, \underline{u}) & & \\ & & \ddots & \\ & & & M(\psi_a, \underline{u}) \end{pmatrix}$$

wobei $\varphi_a : L \to L, x \mapsto ax$ und $\psi_a : F \to F, x \mapsto ax$ □

2.4.5 Proposition.
Sei $L|K$ eine endliche Körpererweiterung und $a \in L$. Dann $\chi_{L|K}(a) = (-a)^{[L:K]}(\mathrm{irr}_K(a))^{[L:K(a)]}$

Beweis. Nach 2.4.4 genügt es $\chi_{K(a)|K}(a) = (-1)^{K(a)|K}\,\mathrm{irr}_K(a)$ zu zeigen.
Wegen $\deg \chi_{K(a)|K}(a) = [K(a) : K] = \deg \mathrm{irr}_K(a)$ reicht es $\mathrm{irr}_K(a)|\chi_{K(a)|K}(a)$ zu zeigen, was aber aus Cayley-Hamilton folgt. □

2.4.6 Satz.
Sei $L|K$ eine endliche separable Körpererweiterung und seien $\varphi_1, \dots, \varphi_n$ die verschiedenen K-Einbettungen (K-Homomorphismen) von L in einen festen algebraischen Abschluss $\overline{K}$ von K (insbesondere $[L : K] = [L : K]_s = n$).
Dann gilt für alle $a \in L$

$$\chi_{L|K}(a) = \prod_{i=1}^{n}(\varphi_i(a) - X)$$

und daher $N_{L|K}(a) = \prod_{i=1}^n \varphi_i(a)$ sowie $\mathrm{tr}_{L|K}(a) = \sum_{i=1}^n \varphi_i(a)$.

Beweis. Sei $a \in L$. Jeder Körperhomomorphismus $K(a) \to \overline{K}$ lässt sich zu genau $[L : K(a)]_s = [L : K(a)]$ Körperhomomorphismen $L \to \overline{K}$ fortsetzen. Daher kann man die φ_i so neu indizieren, dass φ_{ij} $(1 \leq i \leq l, 1 \leq j \leq m)$ die verschiedenen K-Homomorphismen $L \to \overline{K}$ sind mit

$$\varphi_{ij}\big|_{K(a)} = \varphi_{st}\big|_{K(a)} \Leftrightarrow i = s \ (1 \leq i, s \leq l, 1 \leq j, t \leq m)$$

Hierbei gilt $l = [K(a) : K]_s = [K(a) : K]$ und $m = [L : K(a)]_s = [L : K(a)]$.
Zu zeigen ist

$$\chi_{L|K}(a) = \prod_{i=1}^{l}\prod_{j=1}^{m}(\varphi_{ij}(a) - X)$$

Das heißt

$$\chi_{L|K}(a) = \left(\prod_{i=1}^{l}(\varphi_{i1}(a) - X)\right)^m$$

Nach 2.4.5 reich es $\mathrm{irr}_K(a) = \prod_{i=1}^l (X - \varphi_{i1}(a))$ zu zeigen.
Dies folgt daraus, dass mit den $\varphi_{i1}\big|_{K(a)}$ auch die φ_{i1} $(1 \leq i \leq l)$ verschieden sind und die letzteren alle Nullstellen des Polynoms $\mathrm{irr}_K(a)$ sind, welches Grad l hat. □

2.4.7 Erinnerung.

(a) Sei K ein Körper der Charakteristik $p \in \{0\} \cup \mathbb{P}$ und $f \in K[X]$ irreduzibel. Dann gibt es genau ein Paar (n, g) mit $n \in \mathbb{N}_0, g \in K[X]$ irreduzibel und separabel und $f = g(X^{p^n})$

(b) Sei F ein Zwischenkörper der algebraischen Körpererweiterung $L|K$. Dann gilt $[L : K] = [L : F][F : K]$ und $[L : K]_s = [L : F]_s[F : K]_s$, wobei man $n \cdot \infty := \infty \cdot n := \infty \cdot \infty := \infty$ setzt für $n \in \mathbb{N}$

(c) Ist K ein Körper der Charakteristik 0, so ist K vollkommen, das heißt, jede algebraische Körpererweiterung $L|K$ ist separabel.

(d) Sei $L|K$ eine algebraische Körpererweiterung. Dann ist der separable Abschluss von K in L $\overline{k^{s_L}} = \{a \in L | a \text{ separabel über } K\}$ ein Zwischenkörper von $L|K$ mit $[L : K]_s = [\overline{K^{s_L}} : K]$

(e) Ist R ein kommutativer Ring mit $p := \operatorname{char} R \in \mathbb{P}$, so ist

$$\Phi_R : R \to R, a \mapsto a^p$$

ein Endomorphismus („Frobeniushomomorphismus“)

2.4.8 Definition.
Eine algebraische Körpererweiterung $L|K$ heißt *rein inseparabel*, wenn kein $a \in L \setminus K$ separabel über K ist.

2.4.9 Proposition.
Sei $L|K$ eine algebraische Körpererweiterung mit $p := \operatorname{char} K > 0$. Dann sind äquivalent

(a) $L|K$ ist rein inseparabel

(b) $\forall x \in L : \exists n \in \mathbb{N}_0 : x^{p^n} \in K$

(c) $\forall x \in L : \exists n \in \mathbb{N}_0 : \exists a \in K : \operatorname{irr}_K(x) = X^{p^n} - a$

Beweis. Übung □

2.4.10 Beispiel.

(a) Ist $L|K$ eine algebraische Körpererweiterung, so ist wegen der Transitivität der Separabilität $L|\overline{K^{s_L}}$ rein inseparabel.

(b) Jede Teilerweiterung einer rein inseparablen Körpererweiterung ist wegen 2.4.9(b) wieder rein inseparabel

(c) Ist K ein Körper mit $p := \operatorname{char} K > 0$ und ist $n \in \mathbb{N}_0$, so ist $K(X)|K(X^{p^n})$ rein inseparabel, wie man mit 2.4.9(b) und 2.4.7(e) leicht sieht.

2.4.11 Definition.
Sei $L|K$ eine endliche Körpererweiterung. Dann heißt

$$[L : K]_i := \frac{[L : K]}{[L : K]_s} \overset{2.4.7(d)}{=} \frac{[L : K]}{[\overline{K^{s_L}} : K]} \overset{2.4.7(b)}{=} [L : \overline{K^{s_L}}]$$

der *Inseparabilitätsgrad* von $L|K$.

2.4.12 Proposition.
Sei F ein Zwischenkörper der endlichen Körpererweiterung $L|K$.
Dann $[L : K]_i = [L : F]_i[F : K]_i$.

Beweis.

$$\begin{aligned}[L:K]_i &= \frac{[L:K]}{[L:K]_s} \\ &= \frac{[L:F][F:K]}{[L:F]_s[F:K]_s} && 2.4.7(d) \\ &= [L:F]_i[F:K]_i\end{aligned}$$

□

2.4.13 Korollar.
Sei $L|K$ eine endliche Körpererweiterung und $p := \operatorname{char} K$. Dann gibt es $n \in \mathbb{N}_0$ mit $[L:K]_i = p^n$.

Beweis. Benutze 2.4.12 und 2.4.9(c) □

2.4.14 Satz. (vergleiche 2.4.6)
Sei $L|K$ eine endliche Körpererweiterung und seien $\varphi_1, \dots, \varphi_n$ die verschiedenen K-Einbettungen von L in einen festen algebraischen Abschluss $\overline{K}$ von K.

Dann

$$N_{L|K}(a) = \left(\prod_{i=1}^{n} \varphi_i(a)\right)^{[L:K]_i}$$

und

$$\operatorname{tr}_{L|K}(a) = [L:K]_i \sum_{i=1}^{n} \varphi_i(a)$$

für alle $a \in L$.

Beweis. Wegen $[L : \overline{K^{s_L}}] \overset{2.4.7(b)}{=} \frac{[L:K]_s}{[\overline{K^{s_L}}:K]_s} \overset{2.4.7(a)}{=} \frac{[L:K]_s}{[L:K]_s} = 1$ sind $\varphi_1\big|_{\overline{K^{s_L}}}, \dots, \varphi_n\big|_{\overline{K^{s_L}}}$ verschiedene K-Einbettungen von $\overline{K^{s_L}}$ in $\overline{K}$.

Weil $[L:K]_i = [L:\overline{K^{s_L}}]$ gilt und $\overline{K^{s_L}} : K$ separabel ist, folgen die behaupteten Gleichungen für alle $a \in \overline{K^{s_L}}$ mit 2.4.4 und 2.4.6.

Sei also nun $a \in L \setminus \overline{K^{s_L}}$. Dann gibt es nach 2.4.7(a) ein $m \in \mathbb{N}$ und $g \in K[X]$ irreduzibel und separabel mit $\operatorname{irr}_K(a) = g(X^{p^m})$, wobei $p := \operatorname{char} K \overset{2.4.7(c)}{\in} \mathbb{P}$. Mit 2.4.5folgt

$$\chi_{L|K}(a) = (-1)^{[L:K]} \left(g(X^{p^m})\right)^{[L:K(a)]}$$

woraus sicher $\operatorname{tr}_{L|K}(a) = 0$ folgt (beachte $m \geq 1$), was wegen $[L:K]_i \overset{2.4.13}{\equiv}_{(p)} 0$ die Gleichung mit der Spur zeigt.

Wegen 2.4.7(e) reicht es für die Gleichung mit der Norm zu zeigen, dass

$$\Phi_p^m(N_{L|K}(a)) = \Phi_p^m\left(\left(\prod_{i=1}^{m} \varphi_i(a)\right)^{[L:K]_i}\right)$$

, das heißt

$$N_{L|K}(a^{p^m}) = \Phi_p^m\left(\left(\prod_{i=1}^{m}\varphi_i(a)\right)^{[L:K]_i}\right)$$

, was aber aus $a^{p^m} \in \overline{K^{s_L}}$ folgt (siehe oben). $\square$

2.4.15 Satz. („Schachtelungsformel für Norm und Spur")
Sei F ein Zwischenkörper der endlichen Körpererweiterung $L|K$. Dann

$$N_{L|K} = N_{F|K} \circ N_{L|F}$$
$$\mathrm{tr}_{L|K} = \mathrm{tr}_{F|K} \circ \mathrm{tr}_{L|F}$$

Beweis. Übung. $\square$

2.4.16 Erinnerung.
Sei V ein K-Vektorraum mit Basis $\underline{v} := (v_1, \dots, v_n)$

(a) $\underline{v}^* := (v_1^*, \dots, v_n^*)$ definiert durch $v_i^*(v_j) := \delta_{ij} = \begin{cases} 0 & \text{falls } i \neq j \\ 1 & \text{falls } i = j \end{cases}$ $(i, j \in \{1, \dot{,} n\})$ ist eine Basis des Dualraums $V^* = \mathrm{Hom}(V, K)$ [$\to$ 1.6.8] genannt die zu $\underline{v}$ duale Basis.

(b) $b : V \times V \to K$ heißt eine Bilinearform auf V, wenn für alle $v \in V$ sowohl $b(\cdot, v) : V \to K, w \mapsto b(w, v)$ als auch $b(v, \cdot) : V \to K, w \mapsto b(v, w)$ linear sind. Es heißt b symmetrisch, wenn $b(v, w) = b(w, v)$ für alle $v, w \in V$.

(c) Sei b eine Bilinearform auf V. Dann sind $\overleftarrow{b} : V \to V^*, v \mapsto b(\cdot, v)$ und $\overrightarrow{b} : V \to V^*, v \mapsto b(v, \cdot)$ linear und es gilt

$$M(b, \underline{v}) := (b(v_i, v_j))_{1 \leq i,j \leq n} = M(\overleftarrow{b}, \underline{v}, \underline{v}^*) = M(\overrightarrow{b}, \underline{v}, \underline{v}^*)^T$$

denn $\overleftarrow{b}(v_j) = \sum_{i=1}^n b(v_i, v_j) v_i^*$ und $\overrightarrow{b}(v_j) = \sum_{i=1}^n b(v_j, v_i) v_i^*$ für $j \in \{1, \dots, n\}$, was man durch Auswerten in v_k $(k \in \{1, \dots, n\})$ sofort sieht. Es gilt daher:

$$\begin{aligned} b \text{ nicht ausgeartet} &:\Leftrightarrow \overleftarrow{b} \text{ injektiv} \\ &\Leftrightarrow \overleftarrow{b} \text{ surjektiv} \\ &\Leftrightarrow \overleftarrow{b} \text{ Isomorphismus} \\ &\Leftrightarrow \overrightarrow{b} \text{ injektiv} \\ &\Leftrightarrow \overrightarrow{b} \text{ surjektiv} \\ &\Leftrightarrow \overrightarrow{b} \text{ Isomorphismus} \\ &\Leftrightarrow \det(M(b, \underline{v})) \neq 0 \end{aligned}$$

(d) Sei b eine Bilinearform auf V und $\underline{w} := (w_1, \dots, w_n)$ eine weitere Basis von V. Dann gilt

$$M(\underline{w}^*, \underline{v}^*) = M(\underline{v}, \underline{w})^T$$

denn ist $M(\underline{v}, \underline{w}) = (a_{ij})_{1 \le i,j \le n}$, so $v_j = \sum_{i=1}^n a_{ij} w_i$ und daher $w_j^* = \sum_{i=1}^n a_{ji} v_i^*$ für $j \in \{1, \dots, n\}$, was man durch Auswerten in v_k ($k \in \{1, \dots, n\}$) sieht.

Daher gilt

$$\begin{aligned} M(b, \underline{v}) &= M(\overleftarrow{b}, \underline{v}, \underline{v}^*) && (c) \\ &= M(\underline{w}^*, \underline{v}^*) M(\overleftarrow{b}, \underline{w}, \underline{w}^*) M(\underline{v}, \underline{w}) \\ &= M(\underline{v}, \underline{w})^T M(\overleftarrow{b}, \underline{w}, \underline{w}^*) M(\underline{v}, \underline{w}) && (c) \end{aligned}$$

und $\det(M(b, \underline{v})) = (\det(M(\underline{v}, \underline{w})))^2 \det(M(b, \underline{w}))$

2.4.17 Proposition und Definition.
Sei V ein K-Vektorraum mit Basis $\underline{v} := (v_1, \dots, v_n)$ und $b : V \times V \to K$ eine nicht ausgeartete Bilinearform.

Dann gibt es genau ein Tupel $\underline{w} = (w_1, \dots, w_n) \in V^n$ mit $b(v_i, w_j) = \delta_{ij}$ für alle $i, j \in \{1, \dots, n\}$.

Es ist $\underline{w}$ eine Basis von V, genannt die zu $\underline{v}$ bezüglich b duale Basis.

Beweis. Für alle $w_1, \dots, w_n \in V$ gilt

$$\begin{aligned} \forall i, j : b(v_i, w_j) = \delta_{ij} &\Leftrightarrow \forall i, j : b(v_i, w_j) = v_j^*(v_i) \\ &\Leftrightarrow \forall j : \overleftarrow{b}(w_j) = v_j^* \\ &\Leftrightarrow \forall j : w_j = \left(\overleftarrow{b}\right)^{-1} (v_j^*) \end{aligned}$$

und $\overleftarrow{b}$ ist ein Isomorphismus. □

2.4.18 Sprechweise.
Sei $L|K$ eine endliche Körpererweiterung. Dann ist $L \times L \to K, (x, y) \mapsto \mathrm{tr}_{L|K}(xy)$ eine symmetrische Bilinearform auf dem K-Vektorraum L, genannt die *Spurform* von $L|K$

2.4.19 Definition.
Sei $L|K$ eine Körpererweiterung mit $n := [L : K] < \infty$. Für alle $x_1, \dots, x_n \in L$ heißt

$$d_{L|K}(x_1, \dots, x_n) := \det((\mathrm{tr}_{L|K}(x_i x_j))_{1 \le i,j \le n})$$

die *Diskriminante* von $(x_1, \dots, x_n)$ bezüglich $L|K$.

2.4.20 Bemerkung.
Sei $L|K$ eine Körpererweiterung mit $n := [L : K] < \infty$.

Dann $d_{L|K}(x_1, \dots, x_n) = d_{L|K}(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ für alle $x_1, \dots, x_n \in L$ und $\sigma \in S_n$, da jede Permutation ein Produkt von Transpositionen ist und eine simultane Zeilen- und Spaltenvertauschung die Determinante nicht ändert.

2.4.21 Proposition.
Sei $L|K$ endlich und separabel. Seien $\varphi_1, \ldots, \varphi_n$ die verschiedenen K-Einbettungen von L in $\overline{K}$.

Dann gilt für alle $x_1, \ldots, x_n \in L$

$$d_{L|K}(x_1, \ldots, x_n) = \left(\det \begin{pmatrix} \varphi_1(x_1) & \cdots & \varphi_1(x_n) \\ \vdots & \ddots & \vdots \\ \varphi_n(x_1) & \cdots & \varphi_n(x_n) \end{pmatrix}\right)^2$$

Beweis. Für $x_1, \ldots, x_n \in L$ gilt

$$\begin{aligned} d_{L|K}(x_1, \ldots, x_n) &= \det((\mathrm{tr}_{L|K}(x_i x_j)_{1 \le i,j \le n}) \\ &= \det\left(\left(\sum_{k=1}^{n} \varphi_k(x_i x_j)\right)_{1 \le i,j \le n}\right) && 2.4.6 \\ &= \det\left((\varphi_k(x_i))_{1 \le i,k \le n} \cdot (\varphi_k(x_j))_{1 \le k,j \le n}\right) \\ &= \det((\varphi_k(x_i))_{1 \le k,i \le n})^2 \end{aligned}$$

□

2.4.22 Satz.
Sei $L|K$ endlich und separabel und $a \in L$ mit $L = K(a)$. Seien $\varphi_1, \ldots, \varphi_n$ die verschiedenen K-Einbettungen von L in $\overline{K}$. Bezeichne f das Minimalpolynom von a über K und f' seine formale Ableitung.

Dann gilt

$$N_{L|K}(f'(a)) = \prod_{i,j=1; i \neq j}^{n} (\varphi_i(a) - \varphi_j(a)) = (-1)^{\frac{n(n-1)}{2}} d_{L|K}(1, a, \ldots, a^{n-1})$$

Beweis. Übung □

2.4.23 Korollar.
Sei $L|K$ eine endliche Körpererweiterung und $\underline{v} = (v_1, \ldots, v_n)$ eine Basis des K-Vektorraumes L. Dann sind äquivalent:

(a) $L|K$ ist separabel

(b) Die Spurform [$\to$ 2.4.18] von $L|K$ ist nicht ausgeartet

(c) $d_{L|K}(v_1, \ldots, v_n) \neq 0$

(d) $\mathrm{tr}_{L|K} \neq 0$

Beweis.
(a)⟹(b): Gelte (a). Wähle mit dem Satz vom primitiven Element ein $a \in L$ mit $L = K(a)$. Sind $\varphi_1, \dots, \varphi_n$ die verschiedenen K-Homomorphismen $K \to \overline{K}$ so

$$d_{L|K}(1, \dots, a^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i,j=1;i\neq j}^{n} (\varphi_i(a) - \varphi_j(a)) \neq 0 \qquad 2.4.22$$

Es ist $\underline{w} := (1, a, \dots, a^{n-1})$ eine Basis des K-Vektorraumes L und daher $d_{L|K}(1, a, \dots, a^{n-1})$ die Determinante der Darstellungsmatrix der Spurform bezüglich $\underline{w}$. Nach 2.4.16 folgt (b)

(b)⟹(c): wieder mit 2.4.16

(c)⟹(d): trivial

(d)⟹(a): mit 2.4.14 □

2.4.24 Proposition.
Sei $L|K$ separabel mit $n := [L : K] < \infty$ und seien $x_1, \dots, x_n \in L$. Dann gilt

(a)
$$d_{L|K}(x_1, \dots, x_n) = 0 \Leftrightarrow x_1, \dots, x_n \text{ linear abhängig über } K$$

(b) Für jede K-lineare Abbildung $f : L \to L$ gilt

$$d_{L|K}(f(x_1), \dots, f(x_n)) = (\det f)^2 d_{L|K}(x_1, \dots, x_n)$$

Beweis. (a) „⟹“ aus 2.4.23 und „⟸“ aus Definition 2.4.19

(b) Setze $\underline{v} := (x_1, \dots, x_n)$ und $\underline{w} := (f(x_1), \dots, f(x_n))$.

Ist $\underline{v}$ keine Basis von L, so auch $\underline{w}$ nicht und beide Diskriminanten sind null.

Ist $\underline{v}$ eine Basis von L, aber $\underline{w}$ nicht, so $d_{L|K}(\underline{w}) = \det f = 0$.

Sind $\underline{v}$ und $\underline{w}$ K-Basen von L und bezeichnet b die Spurform von $L|K$, so

$$\begin{aligned} d_{L|K}(\underline{w}) &= \det M(b, \underline{w}) \\ &= \det(M(\underline{w}, \underline{v}))^T M(b, \underline{v}) M(\underline{w}, \underline{v}) && 2.4.16(d) \\ &= (\underbrace{\det M(\underline{w}, \underline{v})}_{M(f(\underline{v}))})^2 d_{L|K}(\underline{v}) \end{aligned}$$

□

2.4.25 Proposition.
Sei A ein ganz abgeschlossener Integritätsring, $K := \mathrm{qf}(A)$, $L|K$ eine endliche Körpererweiterung und B der ganze Abschluss von A in L. (z.B. $A\mathbb{Z}, K = \mathbb{Q}, L$ ein Zahlkörper und B ein Zahlring [$\to$ 2.1.15]).

Dann gilt $N_{L|K}(B) \subseteq A, \mathrm{tr}_{L|K}(B) \subseteq A$ und $B^* = \left\{b \in B | N_{L|K}(b) \in A^*\right\}$.

Beweis. Sei $b \in B$. Nach 2.4.15 gilt $\chi_{L|K}(b) = (-1)^{[L:K]}(\operatorname{irr}_K(b))^{[L:K]}$ und nach 2.1.14 gilt $\operatorname{irr}_K(b) \in A[X]$, also $\chi_{L|K}(b) \in A[X]$ und damit $N_{L|K}(b) \in A$ und $\operatorname{tr}_{L|K}(b) \in A$ [$\rightarrow$ 2.4.1].

Wegen $N_{L|K}(B) \subseteq A$ und der Multiplikativität von $N_{L|K}$ folgt $B^* \subseteq \{b \in B | N_{L|K}(b) \in A^*\}$

Sei umgekehrt $b \in B$ mit $N_{L|K}(b) \in A^*$. Dann gibt es $a_1, \ldots, a_n \in A$ mit $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ und $a_n \in A^*$ (wegen $(\chi_{L|K}(b))(b) = 0$ und $(\chi_{L|K}(b)(0) \in A^*)$).

Teilt man durch $a_n b^n \neq 0$, so ist

$$\left(\frac{1}{b}\right)^n + \frac{a_{n-1}}{a_n}\left(\frac{1}{b}\right)^{n-1} + \cdots + \frac{a_1}{a_n}\left(\frac{1}{b}\right) + \frac{1}{a_n} = 0$$

eine Ganzheitsgleichung von $\frac{1}{b}$ über A, also ist $\frac{1}{b} \in B$ und somit $b \in B^*$. □

2.5 Dedekindringe und Körpererweiterungen

2.5.1 Lemma.
Sei A ein Integritätsring, $K := \mathrm{qf}(A), L|K$ eine endliche Körpererweiterung und B der ganze Abschluss von A in L.

Dann ist $L = (A \setminus \{0\})^{-1} B = \{a^{-1}b \mid a \in A \setminus \{0\}, b \in B\}$ und es gibt Elemente von B, die eine Basis des K-Vektorraumes L bilden.

Beweis. Sei $x \in L$. Dann gibt es $n \in \mathbb{N}$ und $a_0, \ldots, a_n \in A$ mit $a_n x^n + \cdots + a_0 = 0$ und $a_n \neq 0$. Multiplizieren mit a_n^{n-1} liefert

$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_0 a_n^{n-1} = 0$$

woraus $a_n x \in B$ folgt und damit $x = a_n^{-1}(a_n x) \in (A \setminus \{0\})^{-1} B$ folgt. □

2.5.2 Satz.
Sei A ein ganz abgeschlossener noetherscher Integritätsring, $K := \mathrm{qf}(A), L|K$ eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L.

Dann ist B als A-Modul und daher als Ring noethersch.

Beweis. Nach Lemma 2.5.1 gibt es $n \in \mathbb{N}_0$ und $v_1, \ldots, v_n \in B$ derart, dass $\underline{v} := (v_1, \ldots, v_n)$ eine Basis des K-Vektorraumes L ist.

Bezeichne $\underline{w} := (w_1, \ldots, w_n)$ die dazu bezüglich der nach 2.4.23 nicht ausgearteten Spurform von $L|K$ duale Basis [$\rightarrow$ 2.4.17]

Behauptung: $\forall x \in L : x = \sum_{i=1}^{n} \mathrm{tr}_{L|K}(v_i x) w_i$.

Begründung: Wähle $a_1, \ldots, a_n \in K$ mit $x = \sum_{i=1}^{n} a_i w_i$. Dann

$$\begin{aligned} \mathrm{tr}_{L|K}(v_j x) &= \mathrm{tr}_{L|K}\left(v_j \sum_{i=1}^{n} a_i w_i\right) \\ &= \sum_{i=1}^{n} a_i \, \mathrm{tr}_{L|K}(v_j w_i) \\ &= a_j \end{aligned}$$

für alle $j \in \{1, \ldots, n\}$.

Wegen $v_1, \ldots, v_n \in B$ und $\mathrm{tr}_{L|K}(B) \overset{2.4.25}{\subseteq} A$, folgt, dass $B \subseteq \sum_{i=1}^{n} A w_i =: M$. Da A noethersch ist, ist M als endlich erzeugter A-Modul nach 1.4.7 auch noethersch. Damit ist auch B ein noetherscher A-Modul.

Natürlich ist B auch als B-Modul noethersch (d.h. als Ring), denn jeder B-Untermodul (d.h. jedes Ideal) von B ist auch ein A-Untermodul von B und daher als A-Modul und dann erst recht als B-Modul endlich erzeugt. □

2.5.3 Lemma.
Sei $A \subseteq B$ ein ganze Erweiterung von Integritätsringe. Sei $\mathfrak{p}$ ein Primideal und I ein Ideal von B mit $\mathfrak{p} \subseteq I$. Dann

$$(A \cap \mathfrak{p} = A \cap I) \Longrightarrow \mathfrak{p} = I$$

Beweis. Gelte $A \cap \mathfrak{p} = A \cap I$ und sei $x \in I$. Zu zeigen ist $x \in \mathfrak{p}$.

Wähle $n \in \mathbb{N}_0$ und $a_0, \dots, a_n \in A$ mit $a_0 x^n + \dots + a_n = 0$ und $a_0 = 1$. Wähle $m \in \{0, \dots, n\}$ mit $a_m \notin \mathfrak{p}$ und $a_{m+1}, \dots, a_n \in \mathfrak{p}$. Nun

$$x^{n-m}(a_0 x^m + a_1 x^{m-1} + \dots + a_m) = -a_{m+1} x^{n-m-1} \dots - a_n \in \mathfrak{p}$$

also $x \in \mathfrak{p}$ oder $a_0 x^m + \dots a_m \in \mathfrak{p} \subseteq I$. Gälte letzteres, so $a_m \in I$ wegen $x \in I$ und daher $a_m \in A \cap I = A \cap \mathfrak{p} \subseteq \mathfrak{p}\lightning$. □

2.5.4 Satz.
Sei A ein Dedekindring, $K := \mathrm{qf}(A), L|K$ eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L.

Dann ist B ein Dedekindring.

Beweis. Wir benutzen die Charakterisierung 2.3.2 von Dedekindringen.

Wegen 2.5.2 ist B noethersch. Wegen Lemma 2.5.1 ist $L = \mathrm{qf}(B)$ und daher B ganz abgeschlossen.

Sei schließlich $\mathfrak{p} \neq (0)$ ein Primideal von B. Zu zeigen: $\mathfrak{p}$ ist maximal. Sei I ein Ideal von B mit $1 \notin I$ und $\mathfrak{p} \subseteq I$. Zu zeigen $\mathfrak{p} = I$.

Nach Lemma 2.5.3 reicht es $A \cap \mathfrak{p} = A \cap I$ zu zeigen. Dies folgt daraus, dass A ein Dedekindring ist, denn $A \cap \mathfrak{p}$ ist ein Primideal und $A \cap I$ ist ein Ideal von A mit $A \cap \mathfrak{p} \subseteq A \cap I, 1 \notin A \cap I$ und $A \cap \mathfrak{p} \neq (0)$ (wäre $A \cap \mathfrak{p} = (0)$, so wende man Lemma 2.5.3 nochmal an mit (0) als Primideal und $\mathfrak{p}$ als Ideal). □

2.5.5 Satz.
Sei A ein Hauptidealring, $K := \mathrm{qf}(A), L|K$ eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L.

Dann ist B ein freier A-Modul vom Rang $[L : K]$. Jede Basis des A-Moduls B ist auch eine Basis des K-Vektorraumes L.

Beweis. Nach 2.5.2 ist B ein endlich erzeugter (sogar noetherscher) A-Modul. Da B ein Integritätsring ist, besitzt dieser Modul offensichtlich keine Torsionselemente $\neq 0$. Aber nach 1.6.9 ist offensichtlich jeder endlich erzeugte Modul über einem Hauptidealring, der keine Torsionselemente $\neq 0$ besitzt, frei. Insbesondere ist B ein freier A-Modul.

Insbesondere ist B ein freier A-Modul. Wegen $K := \mathrm{qf}(A)$, ist jede seiner Basen auch K-linear unabhängig und wegen Lemma 2.5.1 auch ein Erzeugenden System des K-Vektorraumes L. □

2.5.6 Korollar.
Jeder Zahlring vom Grad n [$\rightarrow$ 2.1.15] ist ein Dedekindring, dessen additive Gruppe ein freier $\mathbb{Z}$-Modul vom Rang n ist.

2.6 Die Idealklassengruppe

2.6.1 Proposition.
Sei A ein kommutativer Ring. Es sind äquivalent:

(a) A ist lokal [$\to$ 1.5.8(b)]

(b) $A \setminus A^*$ ist ein Ideal von A

(c) A besitzt genau ein maximales Ideal

(d) $0 \neq 1$ und $\forall x \in A : (x \in A^* \vee 1 - x \in A^*)$

Beweis.
(a)$\Longrightarrow$(b): Gelte (a) und setzte $I := A \setminus A^*$. Dann $0 \in I$ (denn $0 \neq 1$ in A), $I + I \subseteq I$ und $AI \subseteq I$ (denn sind $a \in A$ und $x \in I$, so $ax \in I$, denn wäre $ax \in A^*$, so auch $x \in A^*$, da A kommutativ ist)

(b)$\Longrightarrow$(c): Ist $I := A \setminus A^*$ ein Ideal von A, so ist jedes Ideal J von A mit $1 \notin J$ in I enthalten. Es ist also I das größte Ideal $\neq A$ von A. Insbesondere ist I ein maximales Ideal und jedes maximale Ideal von A gleich I.

(c)$\Longrightarrow$(d): Beweis durch Kontraposition. Gelte $0 = 1$ oder $\exists x \in A : (x \notin A^* \wedge 1 - x \notin A^*)$.

Falls $0 = 1$ in A, so besitzt A kein maximales Ideal.

Sei nun $x \in A$ mit $x \notin A^*$ und $1 - x \notin A^*$. Wegen $1 \notin (x)$ und $1 \notin (1 - x)$ gibt es maximale Ideale $(x) \subseteq \mathfrak{m}, (1-x) \subseteq \mathfrak{n}$. Es gilt $\mathfrak{m} \neq \mathfrak{n}$, denn sonst $1 = x + (1-x) \in \mathfrak{m} = \mathfrak{n}$.

(d)$\Longrightarrow$(a): Gelte (d) und seien $a, b \in A$ mit $a + b \in A^*$. Zu zeigen $a \in A^*$ oder $b \in A^*$.

Wähle $c \in A$ mit $ac + bc = (a + b)c = 1$. Wegen (d) gilt $ac \in A^*$ oder $bc \in A^*$, also $a \in A^*$ oder $b \in A^*$. $\square$

2.6.2 Erinnerung.

(a) Sei K ein Körper. Dann heißt $v : K \to \mathbb{Z} \cup \{\infty\}$ ein *diskrete Bewertung* auf K, wenn $v(0) = \infty$, $v\big|_{K^*}$ ein Gruppenhomomorphismus von $(K^*, \cdot)$ nach $(\mathbb{Z}, +)$ ist und $v(a + b) \geq \min \{v(a), v(b)\}$ für alle $a, b \in K$.

(b) Sei K ein Körper und v eine diskrete Bewertung auf K. Dann ist $\mathcal{O}_v := \{a \in K \mid v(a) \geq 0\}$ ein Unterring von K, der sogenannte Bewertungsring von v. Es gilt $\mathcal{O}_v^* = \{a \in K \mid v(a) = 0\}$ und $\mathcal{O}_v$ ist ein lokaler Ring mit maximalem Ideal $\mathfrak{m}_v = \{a \in K \mid v(a) > 0\}$ und Restklassenkörper $\mathcal{O}_v / \mathfrak{m}_v$.

(c) Sei A ein faktorieller Ring, $K := \mathrm{qf}(A)$. Für jedes $x \in K^*$ gibt es genau ein $(c, \alpha_x) \in A^* \times \mathbb{Z}^{(\mathbb{P}_A)}$ mit $x = c \prod_{p \in \mathrm{supp}(\alpha_x)} p^{\alpha_x(p)}$. Dann ist für jedes $p \in \mathbb{P}_A$ die p-Bewertung $v_p : K \to \mathbb{Z}, x \mapsto \begin{cases} \infty & \text{falls } x = 0 \\ \alpha_x(p) & \text{sonst} \end{cases}$ eine diskrete Bewertung auf K.

2.6.3 Notation.
Sei A ein Dedekindring.

$$M_A := \{\mathfrak{p} \mid \mathfrak{p} \text{ Primideal von } A, \mathfrak{p} \neq (0)\} \overset{2.2.12(d)}{=} \{\mathfrak{m} \mid \mathfrak{m} \text{ maximales von } A, \mathfrak{m} \neq (0)\}$$

$$\begin{aligned} I_A &:= \{I \mid I \text{ gebrochenes Ideal von } A, I \neq (0)\} \\ &\overset{2.2.7(e),2.2.12(c)}{=} \{I \mid I \text{ e.e. A-Untermodul von } \operatorname{qf}(A), I \neq 0\} \end{aligned}$$

$$\begin{aligned} P_A &:= \{I \mid I \text{ gebrochenes Hauptideal von } A, I \neq (0)\} \\ &\overset{2.2.6}{=} \{I \mid I \text{ zyklischer A-Untermodul von} \operatorname{qf}(A), I \neq 0\} \end{aligned}$$

2.6.4 Satz und Notation.
Sei A ein Dedekindring, $K := \operatorname{qf}(A)$. Für jedes $I \in I_A$ gibt es genau ein $\alpha_I \in \mathbb{Z}^{(M_A)}$ mit $I = \prod\limits_{\mathfrak{p} \in \operatorname{supp}(\alpha_I)} \mathfrak{p}^{\alpha_I(\mathfrak{p})}$

Definiere für $\mathfrak{p} \in M_A$

$$\begin{aligned} \tilde{v}_\mathfrak{p} : I_A \cup \{0\} &\to \mathbb{Z} \cup \{\infty\} \\ I &\mapsto \begin{cases} \infty & \text{falls } I = 0 \\ \alpha_I(\mathfrak{p}) & \text{sonst} \end{cases} \end{aligned}$$

und die $\mathfrak{p}$-*Bewertung* $v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}, x \mapsto \tilde{v}_\mathfrak{p}(xA)$.
Dann gilt

(a) $I_A \to \mathbb{Z}^{(M_A)}, I \mapsto \alpha_I = (\tilde{v}_\mathfrak{p}(I))_{\mathfrak{p} \in M_A}$ ist ein Isomorphismus zwischen der Menge der durch Inklusion halbgeordneten Menge I_A und der durch

$$(*) \qquad \alpha \preceq \beta :\Longleftrightarrow \forall \mathfrak{p} \in M_A : \alpha(\mathfrak{p}) \geq \beta(\mathfrak{p})$$

$(\alpha, \beta \in \mathbb{Z}^{(M_A)})$ halbgeordneten Menge $\mathbb{Z}^{M_A}$

(b) Für alle $\mathfrak{p} \in M_A$ und $I, J \in I_A$ gilt $\tilde{v}_\mathfrak{p}(IJ) = \tilde{v}_\mathfrak{p}(I) + \tilde{v}_\mathfrak{p}(J)$, $\tilde{v}_\mathfrak{p}(I \cap J) = \max\{\tilde{v}_\mathfrak{p}(I), \tilde{v}_\mathfrak{p}(J)\}$ und $\tilde{v}_\mathfrak{p}(I + J) = \min\{\tilde{v}_\mathfrak{p}(I), \tilde{v}_\mathfrak{p}(J)\}$

(c) Für alle $\mathfrak{p} \in M_A$ ist $v_\mathfrak{p}$ ein diskrete Bewertung auf K.

Beweis. Die Existenz von $\alpha_I \in \mathbb{N}_0^{(M_A)}$ mit $I = \prod_{\mathfrak{p} \in \operatorname{supp}(\alpha_I)} \mathfrak{p}^{\alpha_I(\mathfrak{p})}$ folgt für Ideale $I \in I_A$ aus der Definition eines Dedekindringes 2.2.4.

Da jedes $I \in I_A$ von der Form JK^{-1} für Ideale $J, K \in I_A$ ist (sogar mit K Hauptideal, siehe 2.2.7(b)) folgt die Existenz von $\alpha_I \in \mathbb{Z}^{(M_A)}$ mit $I = \prod_{\mathfrak{p} \in \operatorname{supp}(\alpha_I)} \mathfrak{p}^{\alpha_I(\mathfrak{p})}$.

Die Eindeutigkeit dieses α_I folgert man leicht aus 2.2.11 mit 2.2.12(a).

(a) Betrachte $\Phi : I_A \to \mathbb{Z}^{(M_A)}, I \mapsto \alpha_I$ und $\Psi : \mathbb{Z}^{(M_A)} \to I_A, \alpha \mapsto \prod_{\mathfrak{p} \in \operatorname{supp}(\alpha)} \mathfrak{p}^{\alpha(\mathfrak{p})}$.

Es reicht zu zeigen

(1) $\Phi \circ \Psi = \mathrm{id}_{\mathbb{Z}^{(M_A)}}$

(2) $\Psi \circ \Phi = \mathrm{id}_{I_A}$

(3) $\forall I, J \in I_A : (I \subseteq J \Longrightarrow \Phi(I) \preceq \Phi(J))$

(4) $\forall \alpha, \beta \in \mathbb{Z}^{(M_A)} : (\alpha \preceq \beta \Longrightarrow \Psi(\alpha) \subseteq \Psi(\beta))$

(1) und (2) sind klar. Zu (3). Seien $I, J \in I_A$ mit $I \subseteq J$. Dann ist $J^{-1}I \subseteq J^{-1}J = A$ ein Produkt von Primidealen, also $\Phi(J^{-1}I) \preceq 0$.

Somit $\Phi(I) = \Phi((JJ^{-1})I) = \Phi(J(J^{-1}I)) = \Phi(J) + \Phi(J^{-1}I) \preceq \Phi(J)$.

Zu (4). Seien $\alpha, \beta \in \mathbb{Z}^{(M_A)}$ mit $\alpha \preceq \beta$. Dann $\alpha - \beta \preceq 0$ und daher $\Psi(\alpha - \beta) \subseteq A$.

Somit $\Psi(\alpha) = \Psi(\alpha - \beta + \beta) = \Psi(\alpha - \beta)\Psi(\beta) \subseteq A\Psi(\beta) \subseteq \Psi(\beta)$

(b) Die erste Gleichung ist trivial. Die beiden anderen Gleichungen folgen aus (a) durch die folgenden Beobachtungen:

In der halbgeordneten Menge I_A ist $\inf\{I, J\} = I \cap J$ und $\sup\{I, J\} = I + J$ für alle $I, J \in I_A$ und in der durch $(*)$ halbgeordneten Menge $\mathbb{Z}^{(M_A)}$ ist

$$\inf\{\alpha, \beta\} = \begin{pmatrix} M_A & \to & \mathbb{Z} \\ \mathfrak{p} & \mapsto & \max\{\alpha(\mathfrak{p}), \beta(\mathfrak{p})\} \end{pmatrix}$$

und

$$\sup\{\alpha, \beta\} = \begin{pmatrix} M_A & \to & \mathbb{Z} \\ \mathfrak{p} & \mapsto & \min\{\alpha(\mathfrak{p}), \beta(\mathfrak{p})\} \end{pmatrix}$$

für alle $\alpha, \beta \in \mathbb{Z}^{(M_A)}$

(c) Sei $\mathfrak{p} \in M_A$. Dann gilt $v_\mathfrak{p}(0) = \tilde{v}_\mathfrak{p}(0) = \infty$,

$$v_\mathfrak{p}(xy) = \tilde{v}_\mathfrak{p}((xy)A) = \tilde{v}_\mathfrak{p}((xA)(yA)) \overset{(b)}{=} \tilde{v}_\mathfrak{p}(xA) + \tilde{v}_\mathfrak{p}(yA)$$

für alle $x, y \in K^*$ und

$$v_\mathfrak{p}(x+y) = \tilde{v}_\mathfrak{p}((x+y)A) \geq \tilde{v}_\mathfrak{p}(xA) + \tilde{v}_\mathfrak{p}(yA) \overset{(b)}{=} \min\{\tilde{v}_\mathfrak{p}(xA), \tilde{v}_\mathfrak{p}(yA)\} = \min\{v_\mathfrak{p}(x), v_\mathfrak{p}(y)\}$$

für alle $x, y \in K^*$ mit $x + y \neq 0$ □

2.6.5 Korollar.
Sei A ein Dedekindring. I_A ist eine multiplikativ geschriebene abelsche Gruppe und als solche ein freier $\mathbb{Z}$-Modul mit Basis M_A.

Beweis. Dass I_A eine abelsche Gruppe ist , ist klar. Aus 2.6.4 folgt, dass $I_A \to \mathbb{Z}^{(M_A)}, I \mapsto (\tilde{v}_\mathfrak{p}(I))_{\mathfrak{p} \in M_A}$ auch ein Isomorphismus zwischen der multiplikativ geschriebenen Gruppe I_A und der additiv geschriebenen Gruppe $\mathbb{Z}^{(M_A)}$ ist. Unter diesem Isomorphismus wird M_A auf die kanonische Basis des $\mathbb{Z}$-Moduls $\mathbb{Z}^{(M_A)}$ abgebildet wird. □

2.6.6 Bemerkung und Notation.
Sei A ein Dedekindring. Dann ist P_A eine Untergruppe von I_A. Man nennt $C_A := I_A/P_A$ die *(Ideal-)Klassengruppe* von A und deren Ordnung $\#C_A \in \mathbb{N} \cup \{\infty\}$ die *Klassenzahl* von A.

2.6.7 Proposition.
Sei A ein Dedekindring. Es sind äquivalent

(a) A ist ein Hauptidealring

(b) $\#C_A = 1$

(c) A ist faktoriell

Beweis.
(a) $\Longleftrightarrow I_A = P_A \Leftrightarrow I_A/P_A = \{1\} \Longleftrightarrow C_A = \{1\} \Longleftrightarrow \#C_A = 1 \Longleftrightarrow (b)$.

(a)$\Longrightarrow$(c) klar

(c)$\Longrightarrow$(a). Gelte (c). Da die Gruppe I_A von M_A erzeugt wird, reicht es $M_A \subseteq P_A$ zu zeigen. Sei hierzu $\mathfrak{p} \in M_A$. Wähle $x \in \mathfrak{p}$ mit $x \neq 0$. Wähle $n \in \mathbb{N}$ und Primelemente $p_1, \ldots, p_n \in A$ mit $x = p_1 \cdot \cdots \cdot p_n$. Wegen $p_1 \cdot \cdots \cdot p_n \in \mathfrak{p}$ gibt es $i \in \{1, \ldots, n\}$ mit $p_i \in \mathfrak{p}$. Weil $(p_i) \in M_A$ gilt muss $(p_i) = \mathfrak{p}$ sein. □

2.6.8 Korollar.
Ein Ring genau dann ein Hauptidealring, wenn er ein faktorieller Dedekindring ist.

2.6.9 Bemerkung.
Sei A ein Hauptidealring. Dann gilt für alle $p \in \mathbb{P}_A, v_p = v_{\mathfrak{p}}$, wobei $\mathfrak{p} = (p) \in M_A$.

2.7 Zerlegungsgesetze

2.7.1 Satz. (Nakayama-Lemma)
Sei R ein kommutativer Ring, I ein Ideal von R und M ein endlich erzeugter R-Modul mit $IM := \{\sum_i a_i x_i \mid a_i \in R, x_i \in M\} = M$.

Dann gibt es $a \in R$ mit $1 - a \in I$ und $aM = 0$.

Beweis. Wendet man Cayley-Hamilton 1.7.5 auf $f := \mathrm{id}_M$ an, so erhält man $n \in \mathbb{N}_0$ und $a_1, \ldots, a_n \in I$ mit $f^n + af^{n-1} + \cdots + a_n \mathrm{id}_M = 0$. Dann $1 - a = -(a_1 + \cdots + a_n) \in I$ und $a\,\mathrm{id}_M = 0$. □

2.7.2 Bemerkung.
In der Situation 2.7.1 ist $1 - a \in I$ ein „Zeuge" für $IM = M$, denn $M = 1 \cdot M = (1 - a + a)M \subseteq (1 - a)M + aM = (1 - a)M$, also $(\underbrace{1 - a}_{\in I})M = M$.

2.7.3 Lemma.
Sei A ein Dedekindring, $I \in I_A$ und $\mathfrak{p} \in M_A$.

Dann $A/\mathfrak{p} \cong I/I\mathfrak{p}$ als A-Modul [schon in 1.4.17(b) gezeigt, falls A Hauptidealring]

Beweis. Es gibt $x \in I \setminus I\mathfrak{p}$ (sonst $I = I\mathfrak{p}$ und daher $A = \mathfrak{p}$). Der Kern des A-Modulhomomorphismus $A \to I/I\mathfrak{p}, a \mapsto \overline{ax}$ umfasst $\mathfrak{p}$, aber enthält nicht 1, und somit $\mathfrak{p}$. Z.z. ist dieser Homomorphismus ist surjektiv, da $I = Ax + I\mathfrak{p}$. Dies folgt mit $I\mathfrak{p} \subsetneq Ax + I\mathfrak{p} \subseteq I$ aus 2.6.4(a) □

2.7.4 Bemerkung und Notation.
Ist $A \subseteq B$ eine Ringerweiterung und I ein Ideal von A, so bezeichne BI das von I in B erzeugte Ideal. Es gilt $BI = \left\{ \sum_i b_i a_i \mid b_i \in B, a_i \in I \right\}$

2.7.5 Definition und Satz.
Sei A ein Dedekindring, $K := \mathrm{qf}(A)$, $L|K$ eine endliche separable Körpererweiterung und B der ganze Abschluss von A in L (damit B ein Dedekindring nach 2.5.4)

(a) Sei $\mathfrak{q} \in M_B$. Dann gibt es genau ein $\mathfrak{p} \in M_A$ mit $\mathfrak{p} \subseteq \mathfrak{q}$, nämlich $\mathfrak{p} := A \cap \mathfrak{q}$.

Man nennt $e_A(\mathfrak{q}) = \tilde{v}_\mathfrak{q}(B\mathfrak{p})$ den *Verzweigungsindex* und $f_A(\mathfrak{q}) = [(B/\mathfrak{q}) : (A/\mathfrak{p})]$ den *Trägheitsindex* von $\mathfrak{q}$ über A, wobei man $A/\mathfrak{p}$ vermöge $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}, \overline{a}^\mathfrak{p} \mapsto \overline{a}^\mathfrak{q} (a \in A)$ als Unterkörper von $B/\mathfrak{q}$ auffasst. Es gilt $e_A(\mathfrak{q}) \in \mathbb{N}$ und $f_A(\mathfrak{q}) \in \mathbb{N}$.

(b) Sei $\mathfrak{p} \in M_A$. Dann ist $Q := \{\mathfrak{q} \in M_B | \mathfrak{p} \subseteq \mathfrak{q}\}$ endlich. Es gilt $B\mathfrak{p} = \prod_{\mathfrak{q} \in Q} \mathfrak{q}^{e_A(\mathfrak{q})}$ und $\sum_{\mathfrak{q} \in Q} e_A(\mathfrak{q}) f_A(\mathfrak{q}) = \dim_{A/\mathfrak{p}}(B/B\mathfrak{p}) = [L : K]$, wobei man $B/B\mathfrak{p}$ vermöge $\overline{a}^\mathfrak{p}\overline{b}^{B\mathfrak{p}} := \overline{ab}^{B\mathfrak{p}}$ $(a \in A, b \in B)$ als $A/\mathfrak{p}$ Vektorraum auffasst. Insbesondere $Q \neq \emptyset$

Beweis.

(a) Nach Lemma 2.5.3 gilt $A \cap \mathfrak{q} \neq (0)$ also $A \cap \mathfrak{q} \in M_A$. Ist $\mathfrak{p} \in M_A$ mit $\mathfrak{p} \subseteq \mathfrak{q}$, so ist $\mathfrak{p} \subseteq A \cap \mathfrak{q}$ und daher $\mathfrak{p} = A \cap \mathfrak{q}$.

Wegen $(0) \neq B\mathfrak{p} \subseteq B$ ist $e_A(\mathfrak{q}) = \tilde{v}_\mathfrak{q}(B\mathfrak{p}) \in \mathbb{N}$ klar.

Nach Satz 2.5.2 (und 2.2.12) ist B als A-Modul endlich erzeugt und daher $B/\mathfrak{q}$ ein endlich erzeugter $A/\mathfrak{p}$ Vektorraum, also $f_A(\mathfrak{q}) = [(B/\mathfrak{q}) : (A/\mathfrak{p})] = \dim_{A/\mathfrak{p}}(B/\mathfrak{q}) \in \mathbb{N}$.

(b) Es ist $Q = \{\mathfrak{q} \in M_B \mid B\mathfrak{p} \subseteq \mathfrak{q}\} \overset{2.4.6(a)}{\subseteq} \{\mathfrak{q} \in M_B \mid \tilde{v}_\mathfrak{q}(B\mathfrak{p}) \geq 1\}$ endlich und $B\mathfrak{p} = \prod_{\mathfrak{q} \in Q} \mathfrak{q}^{e_A(\mathfrak{q})}$ nach 2.6.4.

Wie in 1.4.17(b) kann man eine Kompositionsreihe des B-Moduls $B/B\mathfrak{p}$ der Länge $\sum_{\mathfrak{q} \in Q} e_A(\mathfrak{q})$ hinschreiben, deren Faktoren nach Lemma 2.7.3 gerade die $B/\mathfrak{q}$ ($\mathfrak{q} \in Q$, $B/\mathfrak{q}$ $e_A(\mathfrak{q})$-mal) sind.

Die in dieser Kompositionsreihe vorkommenden abelschen Gruppen bilden auch Untervektorräume des $A/\mathfrak{p}$-Vektorraum $B/B\mathfrak{p}$ und es folgt (vgl. 1.4.10)

$$\dim_{A/\mathfrak{p}}(B/B\mathfrak{p}) = \sum_{\mathfrak{q} \in Q} e_A(\mathfrak{q}) \dim_{A/\mathfrak{p}}(B/\mathfrak{q}) = \sum_{\mathfrak{q} \in Q} e_A(\mathfrak{q}) f_A(\mathfrak{q})$$

Es bleibt noch $\dim_{A/\mathfrak{p}}(B/B\mathfrak{p}) = \dim_K L$ zu zeigen. Wähle hierzu $n \in \mathbb{N}_0$ und $x_1, \ldots, x_n \in B$ derart, dass $\overline{x_1}^{B\mathfrak{p}}, \ldots, \overline{x_n}^{B\mathfrak{p}}$ eine Basis des $A/\mathfrak{p}$-Vektorraumes $B/B\mathfrak{p}$ ist (beachte, dass B ein endlich erzeugter A-Modul ist, wie schon erwähnt).

Wir zeigen, dass $x_1, \ldots, x_n$ eine Basis des K-Vektorraumes L bilden.

Um die lineare Unabhängigkeit zu zeigen: Seien $a_1, \ldots, a_n \in K$ mit $a_1x_1 + \cdots + a_nx_n = 0$. Annahme $I := a_1A + \cdots a_nA \neq 0$. Dann $I \in I_A$. Für jedes $s \in I^{-1}$ gilt dann $\overline{sa_1}^B \overline{x_1}^{B\mathfrak{p}} + \cdots + \overline{sa_n}^B \overline{x_n}^{B\mathfrak{p}} = 0$, also $\overline{sa_1}^B = \cdots = \overline{sa_n}^B = 0$ und somit $sI \subseteq \mathfrak{p}$. Da $s \in I^{-1}$ beliebig war, folgt $A = I^{-1}I \subseteq \mathfrak{p}$ $\lightning$.

Schließlich zeigen wir $L = Kx_1 + \cdots + Kx_n$. Wegen $L = (A \setminus \{0\})^{-1}B$ [$\rightarrow$ 2.5.1] reicht es $B \subseteq Kx_1 + \cdots + Kx_n$ zu zeigen.

Tatsächlich zeigen wir $B \subseteq \frac{1}{a}(Ax_1 + \cdots + Ax_n)$ für ein $a \in A \setminus \{0\}$.

Dies ist äquivalent zu $aB \subseteq Ax_1 + \cdots Ax_n$ für ein $a \in A \setminus \{0\}$, was wiederum zu $a(B/(Ax_1 + \cdots Ax_n)) = 0$ für ein $a \in A \setminus \{0\}$ äquivalent ist.

Wegen des Nakayama Lemma 2.7.1 reicht es zu zeigen

$$B/(Ax_1 + \cdots + Ax_n) = \mathfrak{p}(B/(Ax_1 + \cdots + Ax_n))$$

Dies folgt aber aus $B \subseteq Ax_1 + \cdots Ax_n + B\mathfrak{p}$

□

2.7.6 Satz und Definition.
Sei A ein Dedekindring, $K := \mathrm{qf}(A)$, $L|K$ eine endliche Galoiserweiterung, B der ganze Abschluss von A in L und $\mathfrak{p} \in M_A$.

Dann wirkt die Galoisgruppe $G := \mathrm{Aut}(L|K)$ in natürlicher Weise auf L, auf B, auf M_B und auf $Q := \{\mathfrak{q} \in M_B | \mathfrak{p} \subseteq \mathfrak{q}\} \overset{2.7.5(b)}{\neq} \emptyset$.

Die Wirkung von G auf Q ist transitiv. Insbesondere ist für $\mathfrak{p} \in M_A$ der *Verzweigungsgrad über* $\mathfrak{p}$ in B $e_\mathfrak{p}(B) := e_A(\mathfrak{q})$ und der Trägheitsindex über $\mathfrak{p}$ in B $f_\mathfrak{p}(B) := f_A(\mathfrak{q})$ unabhängig von $\mathfrak{q} \in Q$ und es gilt $e_\mathfrak{p}(B) f_\mathfrak{p}(B) \#Q = [L : K]$

Beweis. Angenommen $G := \mathrm{Aut}(L|K)$ wirkt auf Q nicht transitiv. Dann gibt es $\mathfrak{m}, \mathfrak{q} \in Q$ mit $\mathfrak{m} \neq \varphi\mathfrak{q}$ für alle $\varphi \in G$. Nach 2.6.4(b) gilt dann $\mathfrak{m} + \prod_{\varphi \in G} \varphi\mathfrak{q} = B$. Wähle $x \in \mathfrak{m}, y \in \prod_{\varphi \in G} \varphi\mathfrak{q}$ mit $x + y = 1$.

Es gilt $x \notin \varphi\mathfrak{q}$ für alle $\varphi \in G$, denn sonst $1 = x + y \in \varphi\mathfrak{q}$ für ein $\varphi \in G$.

Also $\varphi^{-1}(x) \notin \mathfrak{q}$ für alle $\varphi \in G$.

Da $\mathfrak{q}$ ein Primideal ist, folgt $\prod_{\varphi \in G} \varphi^{-1}(x) \notin \mathfrak{q}$, also

$$N_{L|K}(x) \overset{2.4.6}{=} \prod_{p \in G} \varphi(x) = \prod_{\varphi \in G} \varphi^{-1}(x) \notin \mathfrak{q}$$

Andererseits $N_{L|K}(x) = x \prod_{\varphi \in G \setminus \{1\}} \varphi(x) \in \mathfrak{m} \cap A = \mathfrak{p} \subseteq \mathfrak{q}$, da $x \in \mathfrak{m}$ und $N_{L|K}(x) \in A$ (2.4.5). $\square$

3 Zahlringe

3.1 Gitter in Zahlkörpern

3.1.1 Proposition und Definition. Sei K ein Zahlkörper vom Grad n.

Jede endlich erzeugte Untergruppe M von K ist als $\mathbb{Z}$-Modul frei vom Rang $\leq n$ und es sind äquivalent:

(a) $\operatorname{rk} M = n$

(b) M hat eine $\mathbb{Z}$-Basis, welche eine $\mathbb{Q}$-Basis von K ist

(c) Jede $\mathbb{Z}$-Basis von M ist eine $\mathbb{Q}$-Basis von K

(d) $\forall a \in K : \exists s \in \mathbb{N} : sa \in M$

Sind (a)-(d) erfüllt, so heißt M ein *Gitter* in K.

Beweis. Übung $\square$

3.1.2 Definition. Ein Gitter M heißt *multiplikativ*, wenn es eine multiplikative Menge ist, das heißt $1 \in M$ und $\forall x, y \in M : xy \in M$.

3.1.3 Beispiel. Nach 2.5.6 ist jeder Zahlring ein multiplikatives Gitter im zugehörigen Zahlkörper.

3.1.4 Lemma. Seien M und N Gitter im Zahlkörper K.

Dann gibt es ein $s \in \mathbb{N}$ mit $sM \subseteq N$ und $sN \subseteq M$. Gilt zusätzlich $N \subseteq M$, so ist M/N endlich.

Beweis. Nach 3.1.1(d) gilt $\forall a \in K : \exists s \in \mathbb{N} : sa \in N$, insbesondere $\forall a \in M : \exists s \in \mathbb{N} : sa \in N$. Da M endlich erzeugt ist, haben wir sogar $\exists s \in \mathbb{N} : \forall a \in M : sa \in N$. Also gibt es $s_1 \in \mathbb{N}$ mit $s_1 M \subseteq N$ und analog $s_2 \in \mathbb{N}$ mit $s_2 N \subseteq M$. Dann $sM \subseteq N$ und $sN \subseteq M$ für $s := s_1 s_2 \in \mathbb{N}$.

Gelte nun $N \subseteq M$. Dann $s(M/N) = 0$ und da M/N ein endlich erzeugter $\mathbb{Z}$-Modul ist, folgt $\#(M/N) < \infty$. $\square$

3.1.5 Satz. Sei K ein Zahlkörper und $M \subseteq K$.

Dann ist M ein multiplikatives Gitter in K genau dann, wenn M ein Unterring von $\mathcal{O}_K$ mit $K = \operatorname{qf}(M)$ ist.

Beweis. Übung □

3.1.6 Definition und Proposition. Sei M ein Gitter im Zahlkörper K und $x_1, \dots, x_n$ ein $\mathbb{Z}$-Basis von M.

Dann heißt $d(M) := d_{K|\mathbb{Q}}(x_1, \dots, x_n) \overset{2.4.24(a)}{\in} \mathbb{Q}^*$ die *Diskriminante* des Gitters M. Sie hängt nicht von der Wahl der Basis ab. Gilt $M \subseteq \mathcal{O}_K$, so $d(M) \in \mathbb{Z}$.

Beweis. Seien $\underline{x} = (x_1, \dots, x_n)$ und $\underline{y} = (y_1, \dots, y_n)$ $\mathbb{Z}$-Basen von M.

Dann sind nach 3.1.1(c) $\underline{x}$ und $\underline{y}$ auch $\mathbb{Q}$-Basen von K. Bezeichne $f : K \to K$ die $\mathbb{Q}$-lineare Abbildung von K mit $f(x_i) = y_i$ für $i \in \{1, \dots, n\}$. Wegen $y_i \in \mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$ für $i \in \{1, \dots, n\}$ gilt $M(f, \underline{x}) \in \mathbb{Z}^{n \times n}$. Also $\det f = \det M(f, \underline{x}) \in \mathbb{Z}$. Analog $\det f^{-1} \in \mathbb{Z}$. Wegen $(\det f)(\det f^{-1}) = \det \mathrm{id}_K = 1$, also $\det f \in \mathbb{Z}^* = \{-1, 1\}$, also $(\det f)^2 = 1$. Nach 2.4.24(b) gilt $d_{K|\mathbb{Q}}(f(x_1), \dots, f(x_n)) = d_{K|\mathbb{Q}}(x_1, \dots, x_n)$.

Ist schließlich $M \subseteq \mathcal{O}_K$, so $d(M) \in \mathbb{Z}$ wegen 2.4.19 und 2.4.25. □

3.1.7 Satz. Seien M und N Gitter des Zahlkörpers K mit $N \subseteq M$. Dann $d(N) = [M : N]^2 d(M)$.

Beweis. Wähle $\mathbb{Z}$-Basen $\underline{x} = (x_1, \dots, x_n)$ von M und $\underline{y} = (y_1, \dots, y_n)$ von N.

Bezeichne wieder $f : K \to K$ die $\mathbb{Q}$-lineare Abbildung mit $f(x_i) = y_i$ für $i \in \{1, \dots, n\}$.

Nach 2.4.24(b) ist $\det f = [M : N]$ zu zeigen. Betrachte den $\mathbb{Z}$-Modulisomorphismus
$\iota : \mathbb{Z}^n \to M, \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum_{i=1}^n a_i x_i$ [→ 1.2.7].

Setzt man $N' := \iota^{-1}(N)$, so gilt natürlich $[M : N] = [\mathbb{Z}^n : N'] = \#(\mathbb{Z}^n / N')$. Weiter ist $\iota^{-1}(y_i)$ die i-te Spalte von $M(f, \underline{x})$, also $N' = \mathbb{Z}\iota^{-1}(y_1) + \dots + \mathbb{Z}\iota^{-1}(y_n) = \operatorname{im} M(f, \underline{x})$.

Wendet man nun das Verfahren aus 1.6.6(b) auf $M(f, \underline{x}) \in \mathbb{Z}^{n \times n}$ an, so erhält man $S \in \mathbb{N}^{n \times n}$ in Diagonalform (sogar Smithscher Normalform) und $P, Q \in \mathrm{GL}_n(\mathbb{Z})$ mit $S = PM(f, \underline{x})Q$.

Ist $S = \begin{pmatrix} a_1, 0 \cdots & 0 & & \\ 0 & a_2 & \cdots 0 & \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$, so gilt nach 1.6.6(a) $\mathbb{Z}^n/N' \cong \mathbb{Z}^n/(a_1\mathbb{Z} \times \dots \times a_n\mathbb{Z}) \cong (\mathbb{Z}/a_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/a_n\mathbb{Z})$ und somit $[M : N] = [\mathbb{Z}^n : N'] = a_1 \cdots a_n = \det S = \underbrace{(\det P)}_{\in \mathbb{Z}^*}(\det M(f, \underline{x}))\underbrace{(\det Q)}_{\in \mathbb{Z}^*}$.

Also wegen $\mathbb{Z}^* = \{-1, 1\}$

$$|\det f| = |\det M(f, \underline{x})| = [M : N]$$

□

3.1.8 Korollar. Sei K ein Zahlkörper und M ein multiplikatives Gitter in K mit $\forall p \in \mathbb{P} : p^2 \nmid d(M)$.

Dann gilt $M = \mathcal{O}_K$

Beweis. Nach 3.1.5 gilt $M \subseteq \mathcal{O}_K$ und daher nach 3.1.7 $d(M) = [\mathcal{O}_K : M]^2 d(\mathcal{O}_K)$, also $[\mathcal{O}_K : M] = 1$ □

3.1.9 Beispiel. Sei $d \in \boxslash$ [$\rightarrow$ 2.1.16]. Dann sind die Identität und $x + y\sqrt{d} \mapsto (x + y\sqrt{d})^* := x - y\sqrt{d}$ $(x, y \in \mathbb{Q})$ die beiden verschiedenen Einbettungen des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$ in seinen algebraischen Abschluss.

Dann ist $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ ein multiplikatives Gitter in $\mathbb{Q}(\sqrt{d})$ mit Diskriminante [$\rightarrow$ 2.4.21]

$$\left(\det\begin{pmatrix} 1 & \sqrt{d} \\ 1^* & \sqrt{d}^* \end{pmatrix}\right)^2 = (-2\sqrt{d})^2 = 4d$$

Ist $d \in \boxslash_1$ (d.h. $d \equiv_{(4)} 1$), so ist

$$\left(\frac{1+\sqrt{d}}{2}\right)^2 = \frac{1 + 2\sqrt{d} + d}{4} = \frac{1+\sqrt{d}}{2} + \frac{d-1}{4}$$

eine Ganzheitsgleichung für $\frac{1+\sqrt{d}}{2}$ und daher $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2}$ ein multiplikatives Gitter in $\mathbb{Q}(\sqrt{d})$, dessen Diskriminante

$$\left(\det\begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1^* & \left(\frac{1+\sqrt{d}}{2}\right)^2 \end{pmatrix}\right)^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2}\right)^2 = d$$

ist.

Für $d \in \boxslash$ ergibt sich also mit 3.1.8 ein neuer Beweis für die in 2.1.17 schon bewiesene Tatsache $\mathcal{O}_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Für $d \in \boxslash_{2,3}$ liefert 3.1.7 die (auch sonst leicht zu sehende) Tatsache

$$[(\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}) : \mathbb{Z}[\sqrt{d}]] = \sqrt{\frac{d(\mathbb{Z}[\sqrt{d}])}{d(\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2})}} = \sqrt{\frac{4d}{d}} = 2$$

3.2 Zerlegung von Primzahlen in Zahlringen

3.2.1 Bemerkung. Ein wesentlicher Grund für die Betrachtung von Gittern und vor allem von multiplikativen Gittern ist, dass sie oftmals „ einfacher“ sind als der Zahlring (zum Beispiel ist für $d \in \varnothing_1$ das multiplikative Gitter $\mathbb{Z}[\sqrt{d}]$ „ einfacher“ als $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathcal{O}_d$) und für gewisse Zwecke doch den Zahlring ersetzen können. Siehe Zeile (b) und (c) dieser Bemerkung und Satz **??** unten.

Seien K ein Zahlkörper und $x_1, \ldots, x_n$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$.

(a) Sei $I \neq (0)$ ein Ideal von $\mathcal{O}_K$. Nach Lemma 2.5.3 gilt $I \cap \mathbb{Z} \neq (0)$, das heißt es gibt ein eindeutig bestimmtes $m \in \mathbb{N}$ mit $I \cap \mathbb{Z} = (m)$.

Insbesondere gilt $m\mathcal{O}_K \subseteq I$ und man kann I sehen als m zusammen mit dem Bild von I unter $\mathcal{O}_K \to \mathcal{O}_K/m\mathcal{O}_K$.

ein Ideal $\neq (0)$ des Zahlringes $\mathcal{O}_K$ ist also gegeben durch eine natürliche Zahl m und ein Ideal des endlichen Ringes $\mathcal{O}_K/m\mathcal{O}_K = (\mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n)/(m\mathbb{Z}x_1 + \cdots + m\mathbb{Z}x_n)$, dessen additive Gruppe in natürlicher Weise ein freier $\mathbb{Z}/m\mathbb{Z}$-Modul mit Basis $\overline{x_1}, \ldots, \overline{x_n}$ ist.

Insbesondere ist $\mathcal{O}_K/I$ endlich mit $\#(\mathcal{O}_K/I) | m^n$

Index