<u>*Dedekindringe und ihre Moduln*</u>

Definition. *Ein Ring $\mathfrak{o}$ heißt Dedekindring, falls $\mathfrak{o}$*

1. *nullteilerfrei,*
2. *noethersch,*
3. *ganz abgeschlossen (in $K = \mathrm{Quot}(\mathfrak{o})$)*
4. *und falls jedes Primideal $\neq 0$ in $\mathfrak{o}$ maximal ist.*

Hauptbeispiele von Dedekindringen sind (neben Hauptidealringen) die ganzen Abschlüsse von $\mathbb{Z}$ in Zahlkörpern K, also in endlichen Körpererweiterungen $K/\mathbb{Q}$.

Satz. *In einem Dedekindring $\mathfrak{o}$ ist jedes Ideal $\neq 0$ eindeutig als Produkt von endlich vielen Primidealen $\neq 0$ darstellbar.*

Das verallgemeinert die ZPE-Eigenschsft von Hauptidealringen. – Für den Beweis (und für spätere Ausführungen) ist der Begriff eines *gebrochenen* Ideals $\mathfrak{g}$ des Dedekindringes $\mathfrak{o}$ nützlich: dies ist ein endlich erzeugter $\mathfrak{o}$-Untermodul in $K = \mathrm{Quot}(\mathfrak{o})$. Gleichbedeutend ist $\mathfrak{g} = r^{-1} \cdot \mathfrak{a}$ mit einem $0 \neq r \in \mathfrak{o}$ und einem Ideal $0 \neq \mathfrak{a}$ von $\mathfrak{o}$. Wir vereinbaren: (gebrochene) Ideale eines Dedekindringes seien ab jetzt stets $\neq 0$; wir zählen also das Nullideal extra.
Obiger Satz folgt nun im wesentlichen aus *für Primideale $\mathfrak{p}$ gilt $\mathfrak{o} \subsetneqq \mathfrak{p}^{-1}$* .

Folgerung. 1. *Zu jedem Ideal $\mathfrak{a} \subset \mathfrak{o}$ gibt es ein gebrochenes Ideal $\mathfrak{a}^{-1}$ mit $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathfrak{o}$.*

2. *Die gebrochenen Ideale eines Dedekindringes $\mathfrak{o}$ bilden eine freie abelsche Gruppe $\mathfrak{I}_{\mathfrak{o}}$ mit den Primidealen als Erzeugenden.*
3. *Hat der Dedekindring $\mathfrak{o}$ nur endlich viele Primideale, so ist er schon ein Hauptidealring.*
4. *Jedes Ideal $\mathfrak{a}$ von $\mathfrak{o}$ ist von zwei Elementen erzeugt, wobei eines beliebig $\neq 0$ in $\mathfrak{a}$ vorgegeben werden darf.*

Lemma. *Ist $\mathfrak{o}$ ein Dedekindring und $1 \in M \subset \mathfrak{o}$ eine multiplikativ abgeschlossene Menge, so ist die zugehörige Lokalisierung $\mathfrak{o}_M$ auch ein Dedekindring. Die Abbildung $\mathfrak{g} \mapsto \mathfrak{g}_M$ ist ein Gruppenepimorphismus $\mathfrak{I}_{\mathfrak{o}} \twoheadrightarrow \mathfrak{I}_{\mathfrak{o}_M}$ mit Kern $\{\mathfrak{g} : \mathfrak{g} \cap M \neq \emptyset\}$.*

Definition. *$L \supset K$ seien endliche Körpererweiterungen von $\mathbb{Q}$. Die ganzen Abschlüsse von $\mathbb{Z}$ in L und K werden mit $\mathfrak{o}_L$ bzw. $\mathfrak{o}_K$ bezeichnet. Dies sind Dedekindringe und zugleich freie $\mathbb{Z}$-Moduln vom Rang $[L : \mathbb{Q}]$ bzw. $[K : \mathbb{Q}]$.*

Es gilt $\mathfrak{o}_{\mathbb{Q}} = \mathbb{Z}$; der ganze Abschluß von $\mathfrak{o}_K$ in L ist $\mathfrak{o}_L$; $\mathfrak{o}_L$ ist ein endlich erzeugter (torsionsfreier) $\mathfrak{o}_K$-Modul. Über jedem Primideal $\mathfrak{p}$ von $\mathfrak{o}_K$ liegen nur endlich viele $\mathfrak{p}$ enthaltende Primideale $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ von $\mathfrak{o}_L$, nämlich die in der Produktzerlegung

$$\mathfrak{p}\mathfrak{o}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}$$

auftretenden; natürlich ist deren Anzahl $g \geq 1$ abhängig von $\mathfrak{p}$. Die Zahl e_i heißt Verzeigungsindex von $\mathfrak{P}_i$ bezüglich K; die Zahl g die Zerlegungszahl von $\mathfrak{p}$ bezüglich L.

Ist $\mathfrak{P}$ Primideal in $\mathfrak{o}_L$ und $\mathfrak{p}$ eines in $\mathfrak{o}_K$, so sagen wir $\mathfrak{P}|\mathfrak{p}$, falls $\mathfrak{P} \supset \mathfrak{p}$ (oder gleichbedeutend, falls $\mathfrak{P} \cap \mathfrak{o}_K = \mathfrak{p}$).

LEMMA. *1. $\mathfrak{o}_K/\mathfrak{p}$ ist ein endlicher Körper. Seine Charakteristik ist die Primzahl p, die in $\mathfrak{p}$ liegt, also $\mathfrak{p}|p$.*

2. $\mathfrak{P}|\mathfrak{p} \implies \mathfrak{o}_L/\mathfrak{P}$ ist eine endliche Körpererweiterung von $\mathfrak{o}_K/\mathfrak{p}$ (vom Grad $f_{\mathfrak{P}}$, dem Restklassengrad von $\mathfrak{P}$ bezüglich K).

3. Ist L/K galoissch mit Gruppe $G = G_{L/K}$ und gilt $\mathfrak{P}|\mathfrak{p}$, so sind die (nicht notwendig verschiedenen) $\sigma(\mathfrak{P}) = \{\sigma(a) : a \in \mathfrak{P}\}$, für $\sigma \in G$, genau alle über $\mathfrak{p}$ liegenden Primideale. Diese haben alle den gleichen Verzweigungsindex und alle den gleichen Restklassengrad bezüglich K.

Bemerkung: In der Zahlentheorie beweist man $\sum_{i=1}^{g} e_i f_i = [L : K]$ für jedes $\mathfrak{p}$.

DEFINITION. *1. $\mathfrak{H}_{\mathfrak{o}_K}$ ist die von allen gebrochenen Hauptidealen erzeugte Untergruppe von $\mathfrak{I}_{\mathfrak{o}_K}$, also $\mathfrak{H}_{\mathfrak{o}_K} = \{a \cdot \mathfrak{o}_k : 0 \neq a \in K\}$.*

2. Der Quotient $\mathrm{cl}_K = \mathfrak{I}_{\mathfrak{o}_K}/\mathfrak{H}_{\mathfrak{o}_K}$ heißt die (Ideal-) Klassengruppe von K.

Bemerkung: In der Zahlentheorie beweist man, daß cl_K eine endliche (abelsche) Gruppe ist; ihre Ordnung k_K heißt die Klassenzahl von K. Beispiel: $h_{\mathbb{Q}} = 1$. Berechnen kann man h_K mit Hilfe des Residuums der Zetafunktion von K.

Endlich erzeugte Moduln über Dedekindringen $\mathfrak{o}$:

Wegen der etwas stiefmütterlichen Behandlung dieser Theorie in der Literatur fügen wir den meisten der folgenden Aussagen Beweisskizzen an. Wir beginnen mit dem

LEMMA. *Zu gegebenen ganzen*[1] *Idealen $\mathfrak{a}, \mathfrak{b}$ existiert ein ganzes Ideal $\mathfrak{c}$ mit $\mathfrak{a} + \mathfrak{c} = \mathfrak{o}$, $\mathfrak{b}\mathfrak{c} = \gamma\mathfrak{o}$ (mit einem $0 \neq \gamma \in \mathfrak{o}$).*

Es seien nämlich $\mathfrak{a} = \prod_{i=1}^{t} \mathfrak{p}_i^{a_i}$, $\mathfrak{b} = \prod_{i=1}^{t} \mathfrak{p}_i^{b_i}$ die Primidealzerlegungen von $\mathfrak{a}$ und $\mathfrak{b}$, also $0 \leq a_i, b_i \in \mathbb{Z}$. Wähle $\gamma_i \in \mathfrak{p}_i^{b_i} \setminus \mathfrak{p}_i^{b_i+1}$ und $\gamma \equiv \gamma_i \mod \mathfrak{p}_i^{b_i+1}$. Es folgt $\gamma \in \bigcap_{i=1}^{t} \mathfrak{p}_i^{b_i} = \prod_{i=1}^{t} \mathfrak{p}_i^{b_i} = \mathfrak{b}$ und $\gamma\mathfrak{o} + \mathfrak{a}\mathfrak{b} = \mathfrak{b}$, weil der Exponent von $\mathfrak{p}_i$ in der linken Seite das Minimum aus b_i und $a_i + b_i$, also $= b_i$ ist. Definiere nun $\mathfrak{c}$ durch $\gamma\mathfrak{o} = \mathfrak{c}\mathfrak{b}$. Dann gilt $\mathfrak{c}\mathfrak{b} + \mathfrak{a}\mathfrak{b} = \mathfrak{b}$, also $\mathfrak{c} + \mathfrak{a} = \mathfrak{o}$.

Bemerkung: Ist $\mathfrak{b}$ nicht ganz, so gilt die Aussage des Lemmas mit einem $0 \neq \gamma \in K$.

Anwendungen:

1. $\mathfrak{a} \oplus \mathfrak{b} \simeq \mathfrak{o} \oplus \mathfrak{a}\mathfrak{b}$ für gebrochene Ideale $\mathfrak{a}, \mathfrak{b}$.

2. Gebrochene Ideale $\mathfrak{a}$ sind projektive $\mathfrak{o}$-Moduln.

3. $\mathfrak{b}/\mathfrak{a}\mathfrak{b} \simeq \mathfrak{o}/\mathfrak{a}$ für gebrochene Ideale $\mathfrak{b}$ und ganze Ideale $\mathfrak{a}$.

[1] Ein gebrochenes Ideal heißt ganz, wenn es in $\mathfrak{o}$ liegt.

Hier folgt 2. aus 1., indem man $\mathfrak{b} = \mathfrak{a}^{-1}$ wählt. Und 1. folgt so: Sind $\mathfrak{a}$ und $\mathfrak{b}$ ganz und noch prim zueinander, so liefert $\mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{o}$, $(a,b) \mapsto a+b$ den Isomorphismus (weil $\mathfrak{o}$ frei und damit projektiv ist). Im allgemeinen Fall finde zunächst $0 \neq \alpha, \beta \in K$ so, daß $\alpha\mathfrak{a}$ und $\beta\mathfrak{b}^{-1}$ ganz sind, dann wähle ein ganzes Ideal $\mathfrak{c}$ mit $\alpha\mathfrak{a} + \mathfrak{c} = \mathfrak{o}$, $\mathfrak{c}\beta\mathfrak{b}^{-1} = \gamma\mathfrak{o}$. Nun ist $\alpha\mathfrak{a} \simeq \mathfrak{a}$, $\mathfrak{c} = \beta^{-1}\gamma\mathfrak{b} \simeq \mathfrak{b}$ und $\alpha\mathfrak{a}\mathfrak{c} = \alpha\beta^{-1}\gamma\mathfrak{a}\mathfrak{b} \simeq \mathfrak{a}\mathfrak{b}$.

Schließlich zu 3. Wähle $\mathfrak{c}$ wie im Lemma und definiere $\mathfrak{o} \to \mathfrak{b}/\mathfrak{a}\mathfrak{b}$ durch $1 \mapsto \gamma \mod \mathfrak{b}\mathfrak{a}$. Weil $\gamma \in \mathfrak{b}$ (denn $\mathfrak{c} \subset \mathfrak{o}$), liegt $\mathfrak{a}$ im Kern. Umgekehrt: wird $\alpha \in \mathfrak{o}$ auf 0 abgebildet, also $\alpha\gamma \in \mathfrak{b}\mathfrak{a}$, so folgt $\alpha\gamma\mathfrak{c} \subset \mathfrak{b}\mathfrak{c}\mathfrak{a} = \gamma\mathfrak{a}$, mithin $\alpha\mathfrak{c} \subset \mathfrak{a}$. Mit $\nu + \mu = 1$, $\nu \in \mathfrak{a}$, $\mu \in \mathfrak{c}$, erhält man $\alpha = \alpha\nu + \alpha\mu \in \mathfrak{a}$. Die Surjektivität der Abbildung resultiert aus $\mathfrak{b} = \mathfrak{b}\mathfrak{o} = \mathfrak{b}(\mathfrak{a} + \mathfrak{c}) = \mathfrak{b}\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{b}\mathfrak{a} + \gamma\mathfrak{o}$.

Definition. *Ist M ein endlich erzeugter $\mathfrak{o}$-Modul, so heißt $m = \dim_K M_{\mathfrak{o}\setminus 0}$* [2] *der Rang von M.*

Beobachtung: $m = 0 \iff M = \mathrm{tor}(M)$.

Ab jetzt sei M ein endlich erzeugter torsionsfreier $\mathfrak{o}$-Modul vom Rang m.

Fall $m = 1$: Wähle $0 \neq x \in M$ und definiere $\mathfrak{a} = \{\alpha \in K : \alpha x \in M\}$. Dann liefert $\mathfrak{a} \to M$, $\alpha \mapsto \alpha x$, einen Isomorphismus $\mathfrak{a} \simeq M$. Insbesondere ist $\mathfrak{a}$ ein gebrochenes Ideal und $M = \mathfrak{a}x$. Die Rang-1-Moduln sind also (bis auf Isomorphie) genau die gebrochenen Ideale. Zwei solche, $M_1 \simeq \mathfrak{a}_1$, $M_2 \simeq \mathfrak{a}_2$, sind isomorph genau wenn $\mathfrak{a}_1 = \gamma\mathfrak{a}_2$ für ein $0 \neq \gamma \in K$ gilt, wenn also $\mathfrak{a}_1$ und $\mathfrak{a}_2$ dasselbe Element in cl_K bestimmen. Denn $M_1 \simeq M_2$ erzwingt $(M_1)_{\mathfrak{o}\setminus 0} \simeq (M_2)_{\mathfrak{o}\setminus 0}$, also einen Isomorphismus von K-Vektorräumen der Dimension 1, und der wird durch eine 1×1-Matrix $\gamma \neq 0$ geliefert.

Satz. *1. Jeder endlich erzeugte torsionsfreie $\mathfrak{o}$-Modul M ist isomorph zu einer direkten Summe*

$$\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$$

von gebrochenen Idealen $\mathfrak{a}_i$. Dabei ist deren Anzahl m der Rang von M. Insbesondere sind die endlich erzeugten torsionsfreien $\mathfrak{o}$-Moduln alle projektiv.

2. Sind M und N zwei endlich erzeugte torsionsfreie $\mathfrak{o}$-Moduln mit

$$M \simeq \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m \, , \; N \simeq \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_n$$

für gebrochene $\mathfrak{o}$-Ideale $\mathfrak{a}_i, \mathfrak{b}_j$, so gilt:

$$M \simeq N \iff m = n \;\&\; \prod_{i=1}^{m} \mathfrak{a}_i \, , \; \prod_{j=1}^{n} \mathfrak{b}_j \text{ liegen in der gleichen Idealklasse.}$$

Aussage 1. wird mit Induktion nach m, dem Rang von M, bewiesen. Den Anfang erledigt unsere Diskussion zu $m = 1$. Der Schluß besteht in der Wahl eines $0 \neq y \in M$, der Bildung des Rang-1-Untermoduls $M_1 = Ky \cap M \subset M_{\mathfrak{o}\setminus 0}$ von M und der Feststellung, daß M/M_1 torsionsfrei vom Rang $m-1$ und damit $\simeq \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_{m-1}$ ist. Da nun gebrochene Ideale projektiv sind, ist es auch M/M_1, und $M = M_1 \oplus M/M_1$ resultiert.

2. folgt so: Wie schon früher verändern wir die $\mathfrak{a}_i$ und $\mathfrak{b}_j$ durch Multiplikation mit Elementen aus $K^\times$ so, daß sie alle die 1 enthalten. Der Isomorphismus $\bigoplus \mathfrak{a}_i \simeq \bigoplus \mathfrak{b}_j$ sende nun $1 \in \mathfrak{a}_k$ auf $(\beta_{k1}, \ldots, \beta_{km})$ und $1 \in \mathfrak{b}_j$ auf $(\alpha_{j1}, \ldots, \alpha_{jm})$. Die zugehörigen Matrizen seien $B = (\beta_{kj})$

[2] gemeint ist die Lokalisierung von M nach der multiplikativ abgeschlossenen Teilmenge $\mathfrak{o} \setminus 0$ von $\mathfrak{o}$; also z.B. $K = \mathfrak{o}_{\mathfrak{o}\setminus 0}$

und $A = (\alpha_{ji})$. Offenbar gilt $BA = 1$. Wir zeigen weiter unten: $\mathfrak{b}_j \supset \beta_{kj}\mathfrak{a}_k$ für alle j und k (und entsprechend $\mathfrak{a}_i \supset \alpha_{ij}\mathfrak{a}_j$). Daraus fogt $\prod_j \mathfrak{b}_j \supset \beta_{1\pi(1)} \cdot \ldots \cdot \beta_{m\pi(m)} \prod_i \mathfrak{a}_i$ für alle Permutationen $\pi \in S_m$, also

$$\prod_j \mathfrak{b}_j \supset \det(B) \prod_j \mathfrak{a}_i \supset \det(B)\det(A) \prod_j \mathfrak{b}_j = \prod_j \mathfrak{b}_j \,,$$

woraus $\prod_j \mathfrak{b}_j = \gamma \prod_i \mathfrak{a}_i$ mit $\gamma = \det(B)$ folgt.
Nachweis von $\mathfrak{b}_j \supset \beta_{kj}\mathfrak{a}_k$: Es sei $\alpha_k \in \mathfrak{a}_k$ und $\rho\alpha_k \in \mathfrak{o}$ für ein $0 \neq \rho \in \mathfrak{o}$. Also $(\rho\alpha_k)1 \mapsto (\rho\alpha_k)(\beta_{k1}, \ldots, \beta_{km}) = (\ldots, \rho\alpha_k\beta_{kj}, \ldots)$; α_k selbst werde auf $(x_1, \ldots, x_m) \in \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_m$ abgebildet. Es folgt $\rho\alpha_k\beta_{kj} = \rho x_j$, also $\alpha_k\beta_{kj} = x_j \in \mathfrak{b}_j$.

Nun sei M weiter ein endlich erzeugter torsionsfreier $\mathfrak{o}$-Modul vom Rang m und N ein $\mathfrak{o}$-Untermodul in M_S. Wir interessieren uns nur für den Isomorphietypus von N und nehmen daher sogar an, daß $N \subset M$ gilt (indem wir nämlich N durch rN mit einem geeigneten $0 \neq r \in \mathfrak{o}$ ersezen). Definiere

$$N' = \{x \in M : \exists\, 0 \neq r \in \mathfrak{o} \text{ mit } rx \in N\} \,.$$

Dies ist ein zwischen N und M gelegener $\mathfrak{o}$-Modul mit

$T = N'/N$ ist ein $\mathfrak{o}$-Torsionsmodul

M/N' ist torsionsfrei, also $M \simeq N' \oplus M/N'$.

Wir studieren die Situation $N \subset N'$, nennen aber N' wieder M.

Satz. *$M \supset N$ seien torsionsfrei vom gleichen Rang m. Dann gibt es Elemente $x_1, \cdots, x_m \in M$, gebrochene Ideale $\mathfrak{a}_1, \cdots, \mathfrak{a}_m$ und ganze Ideale $\mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_m$ mit*

$$M = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_m x_m \quad , \quad N = \mathfrak{a}_1\mathfrak{b}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_m\mathfrak{b}_m x_m \,.$$

Insbesondere gilt $M/N \simeq \bigoplus_{i=1}^m \mathfrak{o}/\mathfrak{b}_i$ sowie für einen Torsionsmodul T eine Isomorphie

$$T \simeq \mathfrak{o}/\mathfrak{c}_1 \oplus \cdots \oplus \mathfrak{o}/\mathfrak{c}_t$$

mit ganzen Idealen $\mathfrak{c}_1 \supset \cdots \supset \mathfrak{c}_t$. Die $\mathfrak{b}_i$ $(1 \leq i \leq m)$ und $\mathfrak{c}_j$ $(1 \leq j \leq t)$ sind durch M, N bzw. T eindeutig bestimmt und heißen Elementarteiler.

Wähle zum Beweis zuerst ein $0 \neq \gamma \in \mathfrak{o}$ mit $\gamma M \subset N$ (die Elemente von M können wir in Termini einer Basis aus Elementen in N von $M_{\mathfrak{o}\setminus 0} = N_{\mathfrak{o}\setminus 0}$ schreiben; das γ ist also ein Nenner). Definiere dann $\mathfrak{g}^{-1} = \{\alpha \in K : \alpha N \subset M\}$; wegen $\gamma\mathfrak{g}^{-1}N \subset N$ ist $\gamma\mathfrak{g}^{-1}$ ein Ideal in $\mathfrak{o}$, damit $\mathfrak{g}^{-1}$ ein gebrochenes Ideal und $\mathfrak{g}$ selbst ein ganzes Ideal (wegen $N \subset M$), und zwar das kleinste Ideal mit $N \subset \mathfrak{g}M$. Insbesondere gilt $N \not\subset \mathfrak{p}\mathfrak{g}M$ für jedes Primideal $\mathfrak{p}$ von $\mathfrak{o}$; wir beschränken uns auf die, die γ enthalten. Zu jedem solchen wähle ein $y_{\mathfrak{p}} \in N \not\subset \mathfrak{p}\mathfrak{g}M$. Durch Wahl von Elementen $\rho_{\mathfrak{p}} \notin \mathfrak{p}$, aber enthalten in allen anderen oberhalb γ gelegenen Primidealen, erreichen wir $x_1 \stackrel{\text{def}}{=} \sum_{\mathfrak{p}|\gamma} \rho_{\mathfrak{p}} y_{\mathfrak{p}} \in N$ mit $x_1 \notin \mathfrak{p}\mathfrak{g}M$ $(\forall\, \mathfrak{p}|\gamma)$.
Definiere $N_1 = Kx_1 \cap N$, $M_1 = Kx_1 \cap M$. Dann gilt $N_1 = \mathfrak{h}x_1$, $M_1 = \mathfrak{a}_1 x_1$ mit gebrochenen Idealen $\mathfrak{h}, \mathfrak{a}_1$, sowie: N/N_1 und M/M_1 sind torsionsfrei vom Rang $m-1$. Also $M = M_1 \oplus M_1'$, $N = N_1 \oplus N_1'$ mit $N_1' = N \cap M_1'$.

$N_1' \subset M_1'$ erledigen wir durch Induktion: $M_1' = \mathfrak{a}_2 x_2 \oplus \cdots \oplus \mathfrak{a}_m x_m$, $N_1' = \mathfrak{a}_2\mathfrak{b}_2 x_2 \oplus \cdots \oplus \mathfrak{a}_m \mathfrak{b}_m x_m$ mit gebrochenen Idealen $\mathfrak{a}_i$ und ganzen Idealen $\mathfrak{b}_2 \supset \mathfrak{b}_3 \supset \cdots \supset \mathfrak{b}_m$.
Wir zeigen: $\mathfrak{h} = \mathfrak{g}\mathfrak{a}_1$. Denn $\mathfrak{g}^{-1}\mathfrak{h}x_1 \subset \mathfrak{g}^{-1}N \subset M \implies \mathfrak{g}^{-1}\mathfrak{h} \subset \mathfrak{a}_1$ und $\gamma\mathfrak{a}_1 x_1 \subset \gamma M \subset N \implies \gamma\mathfrak{a}_1 \subset \mathfrak{h} \implies \gamma \in \mathfrak{h}\mathfrak{a}_1^{-1}$. Definiere $\mathfrak{c} \subset \mathfrak{o}$ durch $\mathfrak{a}_1\mathfrak{c} = \mathfrak{g}^{-1}\mathfrak{h}$. Es resultiert $\gamma \in \mathfrak{g}\mathfrak{c} \subset \mathfrak{c}$, weshalb $\mathfrak{c}$ nur in den Primidealen $\mathfrak{p} \ni \gamma$ enthalten sein kann. Die Annahme $\mathfrak{c} \subset \mathfrak{p} \ni \gamma$ erzwänge allerdings, daß $x_1 \in \mathfrak{h}x_1 = \mathfrak{g}\mathfrak{a}_1\mathfrak{c}x_1 \subset \mathfrak{g}\mathfrak{c}M \subset \mathfrak{p}\mathfrak{g}M$. Also ist $\mathfrak{c} = \mathfrak{o}$.

Setze nun $\mathfrak{b}_1 = \mathfrak{g}$; $\mathfrak{b}_1 \supset \mathfrak{b}_2$ folgt dann aus $\mathfrak{g}M_1' \supset N_1'$ und der Beobachtung, daß $\mathfrak{b}_2$ minimal mit der Eigenschaft $\mathfrak{b}_2 M_1' \supset N_1'$ ist.

Die Eindeutigkeitsaussage wird analog zu der Eindeutigkeit der Elementarteiler bei Hauptidealringen bewiesen.

Für die Aussage bezüglich T wähle Erzeugende $y_1, \cdots, y_t$ von T und bilde $M = \mathfrak{o}^t$ auf T mit einem Kern N ab.