Lorenzen's Reshaping of Krull's Fundamentalsatz for Integral Domains (1938–1953)

Stefan Neuwirth

Abstract Krull's Fundamentalsatz, the generalisation of the main theorem of elementary number theory to integral domains, is the starting point of Lorenzen's career in mathematics. This article traces a conceptual history of Lorenzen's successive reformulations of the Fundamentalsatz on the basis of excerpts of his articles. An edition of the extant correspondence of Lorenzen with Hasse, Krull, and Aubert provides a better understanding of the context of these investigations.

1 Introduction

In the period considered, Paul Lorenzen is a professional mathematician whose research in abstract algebra leads to new insights on the way algebraic objects are given to us. His genuine interest in mathematical logic certainly triggers these insights; conversely, they also influence his conception of a consistency proof for elementary number theory as the construction of an embedding of a preordered set into a σ -complete pseudocomplemented semilattice (see [Coquand and Neuwirth 2020](#)).

The broader framework in which this happens is that of lattice theory getting to the core of mathematical research, after the work of the precursors Dedekind, Schröder, and Skolem. The introduction of lattice theory into ideal theory is credited to Wolfgang Krull ([1926](#)), whose assistant Lorenzen is from 1939 until his habilitation in 1946.

Herbert Mehrrens ([1979](#), 146), in considering Steinitz' work, describes the development of modern algebra in the following terms: 1. the algebraic structure of concrete objects is unveiled; 2. it is given an abstract axiomatic

Stefan Neuwirth

Laboratoire de mathématiques de Besançon, Université Bourgogne Franche-Comté, France,
e-mail: stefan.neuwirth@univ-fcomte.fr

formulation; 3. the abstract concepts are subjected to a detailed investigation of their structure. It is at this third stage that lattice theory becomes instrumental:

After the first step, where the algebraic fundamental structures had emerged in the investigation of numbers, equations, and functions, and the second phase, where the abstract-axiomatic formulation had been achieved, now the abstract concepts became the base of a careful structural investigation.

Seen in this way, the third phase in the development of abstract algebra, the “modern age”, starts with Steinitz. Dedekind’s work belongs to the first, concrete phase; it is part of this developmental stage by virtue of containing the germ of the further development. This is also attested by the fact that, in one detail, he himself carried out all three phases – in the investigation of the dual group [the lattice]. For abstract algebra, the third phase is marked by E. Noether, E. Artin, H. Hasse, W. Krull, and others, whose most productive time were the 20s and 30s.

This article proposes to follow Lorenzen’s work in algebra by focusing on a specific theorem, Krull’s Fundamentalsatz for integral domains. The theorem is introduced on the basis of excerpts of articles by Krull (1930; 1932; 1936) with a short comment. Thus the starting point of Lorenzen’s research is described. Then, excerpts of each of his four articles on the subject (1939; 1950; 1952; 1953) are given and commented on, in chronological order, so as to follow his enterprise of deepening the understanding of the Fundamentalsatz. In his letter to Krull dated 6 June 1944 (page 234), Lorenzen describes his goal as follows:

And yet the simplification and clarification of the proof methods is precisely the proper main goal of my work. I have not tried to generalise the theorems of multiplicative ideal theory at any price, even at the price of complicating – on the contrary, I rather care only to discern the basic ideas of the proof methods in their ultimate simplicity. If e.g. I replace the concept of valuation by “homomorphism of a semilattice into a linearly preordered set”, then I see therein a conceptual simplification instead of a complication. For the introduction of the concept of valuation (e.g. the *prima facie* arbitrary triangle inequality) is justified only by the subsequent success, whereas the concept of homomorphism bears its justification in itself. I would say that the homomorphism into a linear preorder is the “pure concept” that underlies the concept of valuation. And the underlying, pure concept seems to me to be undeniably the simpler one.

If I am mistaken in this point, then I urge you to tell it to me, because it has to date always been my endeavour in my whole mathematical work to bring to light these underlying, pure concepts themselves in their simple and transparent clarity.

In this tendency toward conceptual clarification, the paper [Lorenzen 1950] also differs from my dissertation [Lorenzen 1939]. That this clarification, this understanding of the inner significance, as you call it once, is the most urgent duty has really become evident to me only in the last years.

This article allows for several different readings, according to the objectives of the readers and to their German language skills. Krull's formulation and analysis of his Fundamentalsatz and Lorenzen's reshaping of it are presented as a process that takes place in seven articles, of which the arguments relevant for our history are presented in a comprehensive way, sometimes accompanied by translations of selected paragraphs; then, excerpts of the original article, chosen so as to allow for a direct and coherent reading and comparison with my presentation, are reproduced. The correspondence of Lorenzen with Hasse, Krull, and Aubert, together with a few documents, provides an insight into their respective conceptions as well as into the human and administrative component of this history.

2 Krull 1930: a first attempt at introducing valuations for an integral domain

Krull 1930 describes the goal of a Fundamentalsatz for integral domains: it should generalise the “main theorem of elementary number theory” to the case of an integral domain $\mathfrak{O}$ with field of fractions $\mathfrak{K}$. The theorem to be generalised answers the question of when a nonzero element α of $\mathfrak{K} = \mathbb{Q}$ is divisible by another nonzero element β , i.e. of when the quotient $\alpha \cdot \beta^{-1}$ lies in $\mathfrak{O} = \mathbb{Z}$. It does so in terms of the difference between the exponents with which each prime number p appears in the numerator and the denominator of α (the *value of α at p*) and of β : the value of α must be greater than or equal to the value of β at each p .

Krull proposes an abstract version of these differences of exponents by defining valuations as functions $\mathfrak{K} \rightarrow \mathbb{R} \cup \{+\infty\}$ satisfying three properties 1, 2 and 3, and investigates when valuations decide divisibility.

Excerpt

Our excerpt is from pages 531–532 of “Idealtheorie in unendlichen algebraischen Zahlkörpern Π ”, *Mathematische Zeitschrift* 31.

§ 1.

Bewertung; Begriff der Zahlentheorie.

Das Grundproblem und der Hauptsatz der elementaren Zahlentheorie kann folgendermaßen formuliert werden:

Frage: Wann ist das Element α aus dem Körper $\mathbb{K}_r$ der rationalen Zahlen hinsichtlich der Ordnung $\mathfrak{O}_r$ der ganzen rationalen Zahlen durch das gleichfalls zu $\mathbb{K}_r$ gehörige Element β teilbar, d.h. wann liegt der Quotient $\alpha \cdot \beta^{-1}$ in $\mathfrak{O}_r$?

Antwort: Man ordne jeder Primzahl p aus $\mathfrak{O}_r$ eine „Stelle“ P zu und verstehe für beliebiges $\alpha \neq 0$ aus $\mathbb{K}_r$ unter dem Wert von α in P die Differenz der Exponenten, mit denen die zu P gehörige Primzahl p bei einer Quotientendarstellung von α durch ganze Zahlen in Zähler und Nenner aufgeht. Dann gilt der Satz: α ist dann und nur dann durch β teilbar, wenn der Wert von α in bezug auf eine beliebige Stelle niemals kleiner ist als der Wert von β in bezug auf die gleiche Stelle.

Es bedeute von jetzt ab $\mathbb{K}$ einen beliebigen Körper, unter einer *Ordnung* $\mathfrak{O}$ möge ein Unterring von $\mathbb{K}$ verstanden werden, der das Einheits-element enthält, von $\mathbb{K}$ selbst verschieden ist und die Eigenschaft besitzt, daß jedes Element aus $\mathbb{K}$ als Quotient von Elementen aus $\mathfrak{O}$ geschrieben werden kann, daß also $\mathbb{K}$ den Quotientenkörper von $\mathfrak{O}$ darstellt. Wir nennen das Körperelement α durch das Körperelement β *hinsichtlich* $\mathfrak{O}$ *teilbar*, wenn $\alpha \cdot \beta^{-1}$ zu $\mathfrak{O}$ gehört und fragen:

Welche Eigenschaften muß $\mathfrak{O}$ besitzen, damit über die Teilbarkeitsverhältnisse der Elemente von $\mathbb{K}$ hinsichtlich $\mathfrak{O}$ nach dem Vorbild der elementaren Zahlentheorie durch Einführung von „Stellen“ und zugehörigen „Bewertungen“ entschieden werden kann?

Um die aufgeworfene Frage zu präzisieren, haben wir vor allem genau festzulegen, was unter einer Stelle mit zugehöriger Bewertung verstanden werden soll. Von einer *Bewertung* von $\mathbb{K}$ sprechen wir, wenn jedem Körperelement $\alpha \neq 0$ eindeutig eine reelle Zahl r , der Null das Symbol $+\infty$ als Wert zugeordnet ist, und wenn dabei die folgenden Bedingungen erfüllt sind: 1. Der Wert von $\alpha \cdot \beta$ ist gleich der Summe der Werte von α und β . 2. Der Wert von $\alpha + \beta$ ist nie kleiner als der kleinere der Werte von α und β . 3. Nicht alle Elemente haben den Wert 0.

3 Krull 1932: the Fundamentalsatz for integral domains

Krull (1932) discovers that the concept of valuation in Krull 1930 is too narrow for deciding divisibility. He starts by redefining a valuation as a surjective function $w: \mathbb{K}^* \rightarrow \Gamma$, with Γ an abelian linearly preordered group, not necessarily Archimedean, such that

$$w(a \cdot b) = w(a) + w(b), \quad (1)$$

$$w(a + b) \geq \min(w(a), w(b)). \quad (2)$$

The former concept corresponds to subgroups Γ of the additive group $\mathbb{R}$ and is from now on called "special valuation". A valuation defines the *valuation ring* $\mathfrak{B}$ formed by 0 together with the elements where it is nonnegative.

For example, if $\mathfrak{K} = \mathbb{Q}$ and p is a prime number, then the value of $a \in \mathbb{Q}^*$ at p may be defined by writing $a = p^n a'$ with $n \in \mathbb{Z}$ and p dividing neither the numerator nor the denominator of a' , and by letting $\Gamma = \mathbb{Z}$ and $w(a) = n$. Then $\mathfrak{B}$ is the ring of those fractions that can be written with a denominator not divisible by p .

Krull starts by proving two characterisations of a valuation ring $\mathfrak{B}$:

1. It is a subring of the field of fractions $\mathfrak{K}$ that preorders $\mathfrak{K}$ linearly by divisibility: if $a \in \mathfrak{K}$, then $a \in \mathfrak{B}$ or $a^{-1} \in \mathfrak{B}$. It is here that he needs the freedom of constructing an arbitrary abelian linearly preordered group Γ .

2. It is a local ring (i.e. its nonunits form an ideal) such that every ring $\mathfrak{B}'$ with $\mathfrak{B} \subset \mathfrak{B}' \subseteq \mathfrak{K}$ contains the inverse of a nonunit of $\mathfrak{B}$. Note that this property gives rise to nonconstructive instantiations of such an inverse of a nonunit in arguments by contradiction.

Then he focuses on the connection with integral closedness:

As usual, the element p is to be called *integrally dependent on the ring* $\mathfrak{R}$ if it satisfies an equation $p^n + a_1 p^{n-1} + \dots + a_n = 0$ with coefficients a_i in $\mathfrak{R}$; $\mathfrak{R}$ will be termed *integrally closed* if every element in the field of fractions $\mathfrak{K}$ that is integrally dependent on $\mathfrak{R}$ already belongs to $\mathfrak{R}$.

He observes on the way that valuation rings are integrally closed. This proves one direction of the Fundamentalsatz for integral domains, viz.:

Theorem 7. *A proper subring $\mathfrak{R}$ of $\mathfrak{K}$ may be represented as the intersection of (finitely or infinitely many) valuation rings if and only if it is integrally closed.*

The other direction follows from the fact that if $a \in \mathfrak{K} \setminus \mathfrak{R}$ with $\mathfrak{R}$ integrally closed, then a^{-1} is a nonunit of $\mathfrak{R}[a^{-1}]$: if a does not belong to $\mathfrak{R}$, then it is not integrally dependent on $\mathfrak{R}$ either, and this may be expressed as the absence of a relation of the form $a^{-1}(a_1 + a_2 a^{-1} + \dots + a_n (a^{-1})^{n-1}) = 1$. Then Zorn's lemma provides a maximal subring $\mathfrak{B}$ of $\mathfrak{K}$ containing $\mathfrak{R}[a^{-1}]$ but not a ; $\mathfrak{B}$ turns out to be a valuation ring by the second characterisation of a valuation ring.

Excerpt

Our excerpt is from pages 163–165 and 168–169 of "Allgemeine Bewertungstheorie", *Journal für die reine und angewandte Mathematik* 167.

§ 1. Definition und Grundeigenschaften der allgemeinen Bewertungen.

$\mathfrak{K}$ bedeutet stets einen Körper, Γ eine Abelsche Gruppe mit der Addition als Verknüpfungsrelation und der 0 als Einheitsselement. ... Γ bzw. $\mathfrak{K}$ soll *linear geordnet* heißen, wenn zwischen den Elementen von Γ bzw. $\mathfrak{K}$ eine Ordnungsbeziehung definiert ist mit den üblichen charakteristischen Eigenschaften:

Von einer *Bewertung* B von $\mathfrak{K}$ mit der Wertgruppe Γ soll gesprochen werden, wenn jedem Element $a \neq 0$ aus $\mathfrak{K}$ eindeutig ein Element $\alpha = w(a)$ aus Γ als *Wert* zugeordnet ist, und wenn dabei folgende Bedingungen erfüllt sind: 1. $w(a \cdot b) = w(a) + w(b)$. – 2. $w(a + b) \geq \min(w(a), w(b))$. – 3. Zu jedem α aus Γ gibt es ein a aus $\mathfrak{K}$, so daß $\alpha = w(a)$.

Die Gesamtheit der Elemente a , die in einer festen Bewertung B von $\mathfrak{K}$ nichtnegative Werte haben, bildet zusammen mit dem Nullelement einen echten Unterring $\mathfrak{B}$ von $\mathfrak{K}$, den „zu B gehörigen Bewertungsring“.

Satz 1. Ein echter Unterring $\mathfrak{B}$ von $\mathfrak{K}$ ist dann und nur dann Bewertungsring, wenn $\mathfrak{B}$ den Körper $\mathfrak{K}$ zum Quotientenkörper hat und wenn in $\mathfrak{B}$ von zwei Elementen a_1 und a_2 stets (mindestens) eines durch das andre teilbar ist.

§ 3. Kennzeichnung der ganz abgeschlossenen Ringe.

Das Element p soll wie üblich vom Ringe $\mathfrak{K}$ *ganz abhängig* heißen, wenn es einer Gleichung $p^n + a_1 p^{n-1} + \dots + a_n = 0$ mit Koeffizienten a_i aus $\mathfrak{K}$ genügt; $\mathfrak{K}$ wird *ganz abgeschlossen* genannt, wenn jedes von $\mathfrak{K}$ ganz abhängige Element aus dem Quotientenkörper $\mathfrak{K}$ bereits zu $\mathfrak{K}$ selbst gehört. Bezeichnen wir für beliebiges a mit $\mathfrak{K}[a]$ stets den Ring aller Polynome in a mit Koeffizienten aus $\mathfrak{K}$, so können wir die von $\mathfrak{K}$ ganz abhängigen Elemente auch folgendermaßen charakterisieren:

Das Element p hängt von $\mathfrak{K}$ dann und nur dann ganz ab, wenn p^{-1} in $\mathfrak{K}[p^{-1}]$ Einheit ist.

In der Tat, $p^n - a_1 p^{n-1} - \dots - a_n = 0$ ist vollkommen gleichwertig mit $1 = p^{-1} \cdot (a_1 + a_2 p^{-1} + \dots + a_n (p^{-1})^{n-1})$ und das Bestehen einer Gleichung der letzteren Form mit Koeffizienten a_i aus $\mathfrak{K}$ ist notwendig und hinreichend dafür, daß p^{-1} in $\mathfrak{K}[p^{-1}]$ Einheit ist. – Aus unserm Kriterium für ganz abhängige Elemente folgt sofort:

Ist a Nichteinheit in $\mathfrak{K}$, so kann a^{-1} niemals von $\mathfrak{K}$ ganz abhängen.

Wäre nämlich a^{-1} von $\mathfrak{K}$ ganz abhängig, so müßte $a = (a^{-1})^{-1}$ in $\mathfrak{K}[a] = \mathfrak{K}$ gegen Voraussetzung Einheit sein.

Satz 5. Ein echter Unterring $\mathfrak{B}$ von $\mathfrak{K}$ ist dann und nur dann Bewertungsring, wenn in $\mathfrak{B}$ die Gesamtheit der Nichteinheiten ein Ideal bildet, und wenn

in $\mathfrak{K}$ jeder echte Oberring von $\mathfrak{B}$ mindestens ein Reziprokes einer Nichteinheit von $\mathfrak{B}$ enthält.

Daß jeder Bewertungsring die in Satz 5 angegebenen Eigenschaften besitzt, ist klar nach § 1. – Ist umgekehrt $\mathfrak{B}$ irgendein Ring mit diesen Eigenschaften, so muß zunächst $\mathfrak{B}$ ganz abgeschlossen sein. Denn der Ring $\mathfrak{B}^*$ aller von $\mathfrak{B}$ ganz abhängigen Elemente aus $\mathfrak{K}$ muß mit $\mathfrak{B}$ zusammenfallen, weil er sicher kein einziges Reziprokes einer Nichteinheit von $\mathfrak{B}$ enthält. Es seien ferner a_1 und a_2 zwei beliebige Elemente aus $\mathfrak{B}$, und es sei etwa a_2 nicht in $\mathfrak{B}$ durch a_1 teilbar, also $a_2 \cdot a_1^{-1} = p$ nicht Element von $\mathfrak{B}$. Bilden wir dann $\mathfrak{B}[p]$, so muß in $\mathfrak{B}[p]$ das Reziproke a^{-1} einer gewissen Nichteinheit a aus $\mathfrak{B}$ auftreten, es muß also eine Gleichung $a^{-1} = a_0 + a_1 p + \dots + a_n p^n$ mit Koeffizienten a_i aus $\mathfrak{B}$ gelten. Diese Gleichung kann aber in die Form $(a_0 \cdot a - 1) \cdot (p^{-1})^n + a_1 \cdot a \cdot (p^{-1})^{n-1} + \dots + a_n \cdot a = 0$ gebracht werden, und hier muß wegen der besonderen Eigenschaften von $\mathfrak{B}$ der Koeffizient $a_0 \cdot a - 1$ als Differenz einer Nichteinheit und einer Einheit selbst Einheit sein. Es ist also p^{-1} von $\mathfrak{B}$ ganz abhängig und somit nach dem bereits Bewiesenen Element von $\mathfrak{B}$. – Wir haben jetzt gezeigt: Sind a_1 und a_2 zwei beliebige Elemente aus $\mathfrak{B}$, so ist in $\mathfrak{B}$ entweder a_1 durch a_2 oder a_2 durch a_1 teilbar. Nach Satz 1 muß $\mathfrak{B}$ daher Bewertungsring sein. – Mit Hilfe von Satz 5 beweisen wir weiter:

Satz 6. Zu jedem echten Unterring $\mathfrak{A}$ von $\mathfrak{K}$ gibt es (mindestens) einen Bewertungsring $\mathfrak{B}$, der $\mathfrak{A}$ enthält.

Es sei a eine beliebige Nichteinheit aus $\mathfrak{A}$. Dann existiert, wie aus trivialen Wohlordnungsschlüssen zu ersehen, in $\mathfrak{K}$ mindestens ein Ring $\mathfrak{B}$, der $\mathfrak{A}$, aber nicht a^{-1} enthält, und der außerdem die Eigenschaft hat, daß a^{-1} in jedem echten Oberring von $\mathfrak{B}$ vorkommt. $\mathfrak{B}$ wird nach Satz 5 Bewertungsring sein, wenn die Gesamtheit der Nichteinheiten in $\mathfrak{B}$ ein Ideal bildet. Es sei nun $\mathfrak{p}$ irgendein Primidealteiler von a in $\mathfrak{B}$, $\mathfrak{B}_{\mathfrak{p}}$ bedeute den Ring aller der Elemente, die sich als Quotienten von Elementen aus $\mathfrak{B}$ mit durch $\mathfrak{p}$ unteilbarem Nenner schreiben lassen. Dann enthält $\mathfrak{B}_{\mathfrak{p}}$ das Element a^{-1} nicht, und es muß daher $\mathfrak{B}_{\mathfrak{p}} = \mathfrak{B}$ sein. Das ist aber nur möglich, wenn $\mathfrak{p}$ gerade aus allen Nichteinheiten von $\mathfrak{B}$ besteht.

Satz 7. Ein echter Unterring $\mathfrak{A}$ von $\mathfrak{K}$ läßt sich dann und nur dann als Durchschnitt von (endlich oder unendlich vielen) Bewertungsringen darstellen, wenn er ganz abgeschlossen ist.

Daß alle Bewertungsringe und damit auch alle Durchschnitte von Bewertungsringen ganz abgeschlossen sind, wurde beim Beweise von Satz 5 mitbewiesen. Es sei jetzt umgekehrt $\mathfrak{A}$ irgendein ganz abgeschlossener Ring, a ein nicht in $\mathfrak{A}$ vorkommendes Element aus $\mathfrak{K}$. Dann haben wir nur zu zeigen, daß mindestens ein Bewertungsring $\mathfrak{B}$ existiert, der zwar $\mathfrak{A}$, aber nicht a enthält. Wir bilden $\mathfrak{A}[a^{-1}]$; in diesem Ringe kann a nicht vorkommen, denn andernfalls wäre a^{-1} in $\mathfrak{A}[a^{-1}]$ Einheit, und es müßte daher a von $\mathfrak{A}$ ganz abhängen und damit gegen Voraussetzung in $\mathfrak{A}$

enthalten sein. Da also a^{-1} in $\mathfrak{R}[a^{-1}]$ Nichteinheit ist, gibt es nach dem Beweise von Satz 6 einen Bewertungsring $\mathfrak{B}$, der Obermenge von $\mathfrak{R}[a^{-1}]$ also erst recht auch von $\mathfrak{R}$ ist, in dem aber a nicht vorkommt. Damit ist schon alles bewiesen. – Um die Bedeutung von Satz 7 noch klarer hervortreten zu lassen, führen wir den Begriff der *Hauptordnung* ein. Der Ring $\mathfrak{R}$ soll Hauptordnung heißen, wenn in $\mathfrak{R}$ über die Teilbarkeitsverhältnisse der Elemente durch Einführung von Bewertungen entschieden werden kann, d.h. wenn sich (endlich oder unendlich viele) Bewertungen $\mathfrak{B}_\tau$ des Quotientenkörpers $\mathfrak{K}$ so definieren lassen, daß der folgende Satz gilt: In $\mathfrak{R}$ ist das Element a dann und nur dann durch das Element b teilbar, wenn a in keiner der Bewertungen $\mathfrak{B}_\tau$ einen kleineren Wert besitzt als b .

Man sieht ohne Schwierigkeit, daß der Ring $\mathfrak{R}$ dann und nur dann Hauptordnung ist, wenn er als Durchschnitt von (endlich oder unendlich vielen) Bewertungsringen $\mathfrak{B}_\tau$ dargestellt werden kann. Aus Satz 7 ergibt sich daher:

Satz 7*. *Ein echter Unterring $\mathfrak{R}$ von $\mathfrak{K}$ ist dann und nur dann Hauptordnung, wenn er ganz abgeschlossen ist.*

Wie man in plausibler und naheliegender Weise zu dem Begriff der Hauptordnung gelangt, habe ich bereits früher ausführlich auseinandergesetzt. Doch konnte ich dort die Hauptordnungen nicht so einfach und befriedigend charakterisieren, wie es hier durch Satz 7* geschehen ist. Der Grund für diesen Mangel meiner früheren Arbeit lag einfach darin, daß ich damals nur Bewertungen mit archimedischer Wertgruppe in den Kreis der Betrachtung zog. Satz 7* zeigt also, daß die Einführung der allgemeinen Bewertungen nicht nur naheliegend, sondern auch für die naturgemäße Behandlung mancher arithmetischer Probleme schlechtweg notwendig ist.

4 Krull 1936a: the computational content of the Fundamentalsatz

In the introduction to his 1936, Krull explains that the Fundamentalsatz is the basis for a proof method: if a theorem is to be proved for an integrally closed integral domain, then it mostly suffices to prove it in a valuation ring, in which the property of linearity grants very simple computational arguments.

He also explains the defect of the Fundamentalsatz: its proof does not construct the valuation rings, and the example of polynomial rings shows that this goal is out of reach.

A. The valuation rings are characterised by the fact that in them, of two arbitrary elements, one is always divisible by the other. –

B. Every integrally closed integral domain $\mathfrak{I}$ may be represented as an intersection of valuation rings.

A. and B. form the basis of an important proof method: if a theorem on $\mathfrak{I}$ is to be derived which one knows to hold for the intersection of arbitrarily many rings provided that it holds for each individual component ring, then, according to B., the theorem concerned needs to be proved only for valuation rings, and in this latter case, on account of A., usually a quite elementary computation leads to the goal.

On the other hand, B. serves as a connecting link for novel questions, whose fruitfulness is to be substantiated in this contribution. B. is a pure existence theorem. For the "proof method", this does not constitute a drawback; nevertheless it seems theoretically desirable to go beyond the bare standpoint of existence. This goal would be reached if one were in a position to represent in some constructive manner, for an arbitrary given $\mathfrak{I}$, the set of all those valuation rings out of the field of fractions $\mathfrak{K}$ that contain the integral domain $\mathfrak{I}$. Yet even the consideration of quite elementary special cases, e.g. of polynomial rings, indicates that one is there confronted with an, at least so far, unsolvable task. – On the other hand, it becomes apparent that, surprisingly, already the attempt to turn the given task into the ideal-theoretic leads to very curious connexions with certain penetrating investigations by H. Prüfer that refer chiefly to Kronecker.

Excerpt

Here is the source of our translation, from page 546 of "Beiträge zur Arithmetik kommutativer Integritätsbereiche I: Multiplikationsringe, ausgezeichnete Idealsysteme und Kroneckersche Funktionalringe", *Mathematische Zeitschrift* 41.

A. Die Bewertungsringe sind dadurch gekennzeichnet, daß in ihnen von zwei beliebigen Elementen stets eines durch das andere teilbar ist. – B. Jeder ganz abgeschlossene Integritätsbereich $\mathfrak{I}$ läßt sich als Durchschnitt von Bewertungsringen darstellen.

A. und B. bilden die Grundlage für eine wichtige Beweismethode: Soll ein Satz über $\mathfrak{I}$ abgeleitet werden, von dem man weiß, daß er für den Durchschnitt beliebig vieler Ringe richtig ist, sobald er nur für jeden einzelnen Komponentenring gilt, so braucht der betreffende Satz nach B. nur für Bewertungsringe bewiesen zu werden, und in diesem letzteren Fall führt wegen A. meistens eine ganz einfache Rechnung zum Ziel.

Andererseits dient B. als Anknüpfungspunkt für neuartige Fragestellungen, deren Fruchtbarkeit in diesem Beitrag nachgewiesen werden soll.

B. ist ein reines Existenztheorem. Für die „Beweismethode“ bedeutet das keinen Nachteil; trotzdem scheint es theoretisch wünschenswert, über den bloßen Existenzstandpunkt hinauszukommen. Dieses Ziel wäre erreicht, wenn man imstande wäre, bei beliebig gegebenem $\mathfrak{I}$ die Menge aller der Bewertungsringe aus dem Quotientenkörper $\mathfrak{K}$, die den Integritätsbereich $\mathfrak{I}$ umfassen, irgendwie konstruktiv darzustellen. Doch lehrt schon die Betrachtung ganz einfacher Spezialfälle, z. B. der Polynomringe, daß man da vor einer wenigstens vorläufig unlösbaren Aufgabe steht. – Dagegen zeigt es sich überraschenderweise, daß bereits der Versuch, die gestellte Aufgabe ins Idealtheoretische zu wenden, zu sehr merkwürdigen Zusammenhängen mit gewissen tiefeindringenden, vorwiegend an Kronecker anknüpfenden Untersuchungen von H. Prüfer führt.

5 Lorenzen 1939: the Fundamentalsatz for preordered cancellative monoids

Lorenzen 1939 is an “abstract foundation of multiplicative ideal theory” on the theory of preordered cancellative monoids. Lorenzen’s letter to Krull dated 22 March 1938 (page 191) provides a dictionary that translates the concepts of ring theory into a framework that takes into account only the multiplicative structure of an integral domain $\mathfrak{I}$: its nonzero elements form a cancellative monoid $\mathfrak{g}$, and the nonzero elements of its field of fractions form what is today called the Grothendieck group $\mathfrak{G}$ of $\mathfrak{g}$. Divisibility is the equivariant preorder $\preceq$ on $\mathfrak{G}$ whose positive cone is $\mathfrak{g}$: $a \preceq b \Leftrightarrow \mathfrak{g} \ni b \cdot a^{-1}$.

Lorenzen’s analysis of Krull’s valuation theory proceeds in three steps: elaborating a theory of ideals that fits preordered monoids (Subsection 5.1), making a valuation-theoretic analysis of lattice-preordered groups (Subsection 5.2), and establishing a transfer of valuations between a preordered monoid and the positive cone of the Grothendieck lattice-preordered group of its system of ideals (Subsection 5.3).

5.1 Systems of ideals

Prüfer (1932) proposes to define a system of r -ideals as an operation $\{a_1, \dots, a_n\} \mapsto \{a_1, \dots, a_n\}_r$ on finite subsets of the field of fractions of an integral domain. Lorenzen adapts this definition into an operation on finite or infinite bounded-from-below subsets $\mathfrak{a}$ of the group $\mathfrak{G}$ (i.e. subsets such that there is a $c \in \mathfrak{G}$ with $\mathfrak{g} \supseteq c\mathfrak{a}$; Lorenzen’s notation for this is $\mathfrak{a}^{-1} \neq 0$), taking values in subsets of $\mathfrak{G}$, and satisfying four conditions: 1. $\mathfrak{a}_r \supseteq \mathfrak{a}$; 2. $\mathfrak{b}_r \supseteq \mathfrak{a} \Rightarrow \mathfrak{b}_r \supseteq \mathfrak{a}_r$; 3. $\{\mathfrak{a}\}_r = \mathfrak{a} \cdot \mathfrak{g}$; 4. $\mathfrak{a} \cdot \mathfrak{a}_r = (\mathfrak{a} \cdot \mathfrak{a})_r$.

For example, the system of t -ideals, used in Subsection 5.2, is defined by

$$\mathfrak{a}_t = \left\{ b \in \mathfrak{G} \mid \exists a_1, \dots, a_n \in \mathfrak{a} \quad \forall a \in \mathfrak{G} \quad a \preccurlyeq a_1, \dots, a \preccurlyeq a_n \Rightarrow a \preccurlyeq b \right\}$$

for finite or infinite bounded-from-below sets $\mathfrak{a}$ as the set of those elements b that are greater than or equal to every lower bound a of some finite subset $\{a_1, \dots, a_n\}$ of $\mathfrak{a}$.

A system of ideals has the structure of a meet-semilattice-preordered monoid (a *meet-monoid* for short) for the multiplication $\mathfrak{a}_r \cdot \mathfrak{b}_r = (\mathfrak{a} \cdot \mathfrak{b})_r$ and the meet operation $\mathfrak{a}_r \wedge \mathfrak{b}_r = (\mathfrak{a} \cup \mathfrak{b})_r$. Item 3 above means that the group $\mathfrak{G}$ may be embedded into this meet-monoid by identifying a with $a \cdot \mathfrak{g}$.

The system of Dedekind ideals corresponds to the operation that associates to $\mathfrak{a}$ the set $\mathfrak{a}_d$ of nonzero elements of the module generated by $\mathfrak{a}$ in the integral domain $\mathcal{I}$ hidden behind $\mathfrak{g}$. The definition of this operation therefore takes into account the additive structure of $\mathcal{I}$, but once the definition is done, it will be forgotten. Let us show how this works for the three following concepts: 1. valuation ring, 2. integral closedness, 3. integral dependence.

1. Lorenzen separately analyses Equality (1) and Inequality (2) of the definition of a valuation given on page 145.

- He says that a supermonoid $\mathfrak{B}$ of $\mathfrak{g}$ ($\mathfrak{G} \supseteq \mathfrak{B} \supseteq \mathfrak{g}$) is *linear* if for $a \in \mathfrak{G}$ either $a \in \mathfrak{B}$ or $a^{-1} \in \mathfrak{B}$, i.e. if the preorder on $\mathfrak{G}$ having $\mathfrak{B}$ as its positive cone is linear.

- Inequality (2) expresses that a valuation ring is closed under addition. He observes that this is equivalent to $\mathfrak{B} \supseteq \{a_1, \dots, a_n\} \Rightarrow \mathfrak{B} \supseteq \{a_1, \dots, a_n\}_d$.

2. Prüfer (1932) shows that an integral domain is integrally closed if

$$\{a_1, \dots, a_n\}_d \supseteq a \cdot \{a_1, \dots, a_n\}_d \quad \text{implies} \quad \mathfrak{g} \supseteq a \cdot \mathfrak{g},$$

i.e. $1 \preccurlyeq a$. This means that $\{a_1, \dots, a_n\}_d$ can be cancelled in the containment $\{a_1, \dots, a_n\}_d \supseteq a \cdot \{a_1, \dots, a_n\}_d$.

3. He further shows that an element a is integrally dependent on $\{a_1, \dots, a_n\}_d$ if and only if there is $\{c_1, \dots, c_p\}$ such that $\{a_1, \dots, a_n\}_d \cdot \{c_1, \dots, c_p\}_d \supseteq a \cdot \{c_1, \dots, c_p\}_d$.

On the basis of these observations, Lorenzen proposes the following definitions in the multiplicative setting of a system of r -ideals for the cancellative monoid $\mathfrak{g}$:

1. The multiplicative counterpart of a valuation ring is a linear r -supermonoid of $\mathfrak{g}$, i.e. a linear supermonoid $\mathfrak{B}$ of $\mathfrak{g}$ such that $\mathfrak{B} \supseteq \{a_1, \dots, a_n\} \Rightarrow \mathfrak{B} \supseteq \{a_1, \dots, a_n\}_r$.

2. The monoid $\mathfrak{g}$ is r -closed if $\{a_1, \dots, a_n\}_r \supseteq a \cdot \{a_1, \dots, a_n\}_r \Rightarrow 1 \preccurlyeq a$.

3. The r_a -operation is given by setting $\{a_1, \dots, a_n\}_{r_a}$ equal to

$$\left\{ a \in \mathfrak{G} \mid \exists \{c_1, \dots, c_p\} \quad \{a_1, \dots, a_n\}_r \cdot \{c_1, \dots, c_p\}_r \supseteq a \cdot \{c_1, \dots, c_p\}_r \right\},$$

i.e. to the set of elements that are r -dependent on $\{a_1, \dots, a_n\}$. Note that the r_a -operation satisfies Item 3 of the definition of a system of ideals if and only if $\mathfrak{g}$ is r -closed.

Lorenzen observes that the arguments of Prüfer (1932, 18) show that the cancellativity of the meet-monoid of r -ideals may be forced by passing to the meet-monoid of r_a -ideals. One may then construct the Grothendieck lattice-preordered group $\mathfrak{h}^*$ of this system of r_a -ideals (see, for this construction, Coquand, Lombardi, and Neuwirth 2019, § 3A). Its positive cone $\mathfrak{h}$ is formed by the fractions $\frac{\{a_1, \dots, a_n\}_{r_a}}{\{b_1, \dots, b_m\}_{r_a}}$ such that $\{b_1, \dots, b_m\}_{r_a} \supseteq \{a_1, \dots, a_n\}_{r_a}$. The group $\mathfrak{G}$ may be embedded into $\mathfrak{h}^*$ by identifying a with $\frac{a \cdot \mathfrak{g}}{\mathfrak{g}}$.

5.2 Ideals in a lattice-preordered group

For developing a “valuation theory” of $\mathfrak{g}$ when $\mathfrak{G}$ is a lattice-preordered group (an ℓ -group for short), Lorenzen uses the t -ideals, whose definition, thanks to the existence of finite meets, simplifies to

$$\mathfrak{a}_t = \left\{ b \in \mathfrak{G} \mid a_1 \wedge \dots \wedge a_n \preceq b \text{ for some } a_1, \dots, a_n \in \mathfrak{a} \right\}.$$

Clifford (1940, 470) emphasises their similarity with the semilattice-theoretic ideals. A finite t -ideal $\{a_1, \dots, a_n\}_t$ is the set $(a_1 \wedge \dots \wedge a_n)\mathfrak{g}$ and may thus be thought of as $a_1 \wedge \dots \wedge a_n$, and the set-theoretic clothing is needed only for an infinite t -ideal, which is a colimit of finite ones, in particular for a *prime* t -ideal, i.e. a t -ideal $\mathfrak{p}$ such that $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Lorenzen shows that the linear t -supermonoids of $\mathfrak{g}$ are the localisations $\mathfrak{g}_{\mathfrak{p}}$, i.e. the monoids of fractions $\frac{a}{b}$ with $a \in \mathfrak{g}$ and $b \in \mathfrak{g} \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime t -ideal. In fact, the nonunits of $\mathfrak{g}_{\mathfrak{p}}$ have the form $\frac{p}{s}$ with $p \in \mathfrak{p}$ and $s \in \mathfrak{g} \setminus \mathfrak{p}$; if $\frac{p'}{s'}$ is another nonunit, then the meet $\frac{p}{s} \wedge \frac{p'}{s'} = \frac{s'p \wedge sp'}{ss'}$ is again a nonunit because $ss' \in \mathfrak{g} \setminus \mathfrak{p}$ by primeness, $s'p, sp' \in \mathfrak{p}$ by Items 2 and 3 of the definition of a system of ideals, and $s'p \wedge sp' \in \mathfrak{p}$ by t -idealness. But this shows that $\mathfrak{g}_{\mathfrak{p}}$ is linear, as every $a \in \mathfrak{G}$ satisfies $a = \frac{a_+}{a_-}$ with $a_-, a_+ \in \mathfrak{g}$ and $a_- \wedge a_+ = 1$, so that either a_- or a_+ is a unit of $\mathfrak{g}_{\mathfrak{p}}$ and either a or $a^{-1} = \frac{a_-}{a_+}$ is in $\mathfrak{g}_{\mathfrak{p}}$.

The Fundamentalsatz follows easily in this case, in the following two shapes.

Theorem 11. *Let N be a set of prime t -ideals of $\mathfrak{g}$ such that every nonunit of $\mathfrak{g}$ lies in at least one $\mathfrak{p} \in N$, then $\mathfrak{g}$ is the intersection of the linear supermonoids $\mathfrak{g}_{\mathfrak{p}}$ ($\mathfrak{p} \in N$)*

$$\mathfrak{g} = \bigcap_N \mathfrak{g}_{\mathfrak{p}}.$$

For if $a \in \mathfrak{G} \setminus \mathfrak{g}$, then a_- is a nonunit of $\mathfrak{g}$, so that it lies in some $\mathfrak{p} \in N$ and is a nonunit of $\mathfrak{g}_{\mathfrak{p}}$; therefore $a = \frac{a_+}{a_-} \notin \mathfrak{g}_{\mathfrak{p}}$.

Theorem 12. *If N contains all maximal prime t -ideals, then, for all t -ideals $\mathfrak{a}$ of $\mathfrak{g}$, the intersection representation $\mathfrak{a} = \bigcap_N \mathfrak{a}\mathfrak{p}$ holds.*

For if $a \notin \mathfrak{a}$, then $\mathfrak{g}$ contains properly the t -ideal $a^{-1}\mathfrak{a} \cap \mathfrak{g}$. Zorn's lemma provides a maximal prime t -ideal $\mathfrak{p}$ that contains it, so that its elements are nonunits of $\mathfrak{g}_{\mathfrak{p}}$. Therefore $a^{-1}\mathfrak{a}\mathfrak{p} \not\supseteq 1$ and $\mathfrak{a}\mathfrak{p} \not\supseteq \mathfrak{a}$.

Krull's well-ordering argument is confined to the proof of this last theorem.

5.3 Transfer to the system of t -ideals

To consider a linear r -supermonoid $\mathfrak{B}$ of $\mathfrak{g}$ ($\mathfrak{G} \supseteq \mathfrak{B} \supseteq \mathfrak{g}$) is to consider a linear t -supermonoid $\mathfrak{L}$ of the positive cone $\mathfrak{h}$ of the Grothendieck lattice-preordered group $\mathfrak{h}^*$ ($\mathfrak{h}^* \supseteq \mathfrak{L} \supseteq \mathfrak{h}$).

1. If $\mathfrak{L}$ is given, then $\mathfrak{B} = \mathfrak{L} \cap \mathfrak{G}$ (using the identification of a with $\frac{a \cdot \mathfrak{g}}{\mathfrak{g}}$) is a linear supermonoid of $\mathfrak{g}$. Furthermore, if $\mathfrak{B} \supseteq \{a_1, \dots, a_n\}$, then $\mathfrak{L} \supseteq \{\frac{a_1 \cdot \mathfrak{g}}{\mathfrak{g}}, \dots, \frac{a_n \cdot \mathfrak{g}}{\mathfrak{g}}\}$, so that, by hypothesis, $\mathfrak{L} \supseteq (\frac{a_1 \cdot \mathfrak{g}}{\mathfrak{g}} \wedge \dots \wedge \frac{a_n \cdot \mathfrak{g}}{\mathfrak{g}})\mathfrak{h} = \frac{\{a_1, \dots, a_n\}_{r_a}}{\mathfrak{g}}\mathfrak{h}$ and $\mathfrak{B} \supseteq \{a_1, \dots, a_n\}_{r_a} \supseteq \{a_1, \dots, a_n\}_r$. At this point of his argument, Lorenzen compares it to Krull 1936, Satz 15.

2. Conversely, if $\mathfrak{B}$ is given, then $\mathfrak{B}$ is even an r_a -supermonoid: if $\mathfrak{B} \supseteq \{a_1, \dots, a_n\}$ and $\{a_1, \dots, a_n\}_{r_a} \ni a$, consider $\{c_1, \dots, c_p\}$ such that $\{a_1, \dots, a_n\}_r \cdot \{c_1, \dots, c_p\}_r \supseteq a \cdot \{c_1, \dots, c_p\}_r$; one may suppose that c_1 is minimal w.r.t. the linear monoid $\mathfrak{B}$ among $c_1, \dots, c_p$, i.e. $\mathfrak{B} \supseteq \{1, \dots, c_1^{-1}c_p\}$, so that $\mathfrak{B} \supseteq \{a_1, \dots, a_n\} \cdot \{1, \dots, c_1^{-1}c_p\}$; by hypothesis, $\mathfrak{B} \supseteq \{a_1, \dots, a_n\}_r \cdot \{1, \dots, c_1^{-1}c_p\}_r \ni a$, and we conclude that $\mathfrak{B} \supseteq \{a_1, \dots, a_n\}_{r_a}$. For every finite subset $\{a_1, \dots, a_n\}$ of $\mathfrak{G}$, one may suppose that a_1 is minimal w.r.t. $\mathfrak{B}$ among $a_1, \dots, a_n$, i.e. $\mathfrak{B} \supseteq \{1, \dots, a_1^{-1}a_n\}$, and then $\mathfrak{B} \supseteq \{1, \dots, a_1^{-1}a_n\}_{r_a}$ and $a_1\mathfrak{B} = \{a_1, \dots, a_n\}_{r_a}\mathfrak{B}$. Consider

$$\mathfrak{L} = \left\{ \frac{\{a_1, \dots, a_n\}_{r_a}}{\{b_1, \dots, b_m\}_{r_a}} \mid \{b_1, \dots, b_m\}_{r_a}\mathfrak{B} \supseteq \{a_1, \dots, a_n\}_{r_a}\mathfrak{B} \right\}:$$

as for all $a, b \in \mathfrak{G}$ either $b\mathfrak{B} \supseteq a\mathfrak{B}$ or vice versa, $\mathfrak{L}$ is a linear supermonoid of $\mathfrak{h}$; it is a linear t -supermonoid of $\mathfrak{h}$ because the meet of two elements of $\mathfrak{L}$ is in $\mathfrak{L}$: if $\{b_1, \dots, b_m\}_{r_a}\mathfrak{B} \supseteq \{a_1, \dots, a_n\}_{r_a}\mathfrak{B}$ and $\{d_1, \dots, d_q\}_{r_a}\mathfrak{B} \supseteq \{c_1, \dots, c_p\}_{r_a}\mathfrak{B}$, then $\{b_1d_1, \dots, b_md_q\}_{r_a}\mathfrak{B} \supseteq \{a_1d_1, \dots, a_nd_q, b_1c_1, \dots, b_mc_p\}_{r_a}\mathfrak{B}$. Finally, note that $\mathfrak{L} \cap \mathfrak{G} = \mathfrak{B}$.

This transfer proves at once

Theorem 14. *Every r -closed monoid is an intersection of linear r -supermonoids.*

Excerpt

Our excerpt is from pages 535–537, 540, and 544–546 of “Abstrakte Begründung der multiplikativen Idealtheorie”, *Mathematische Zeitschrift* 45.

Note that in this article and in his 1938 letters to Krull, Lorenzen consistently makes a choice opposite to the now standard one: he considers $\mathfrak{g}$ as the cone of nonpositive elements of $\mathfrak{G}$, so that his preorder $\preceq$ satisfies $a \preceq b \Leftrightarrow a \cdot b^{-1} \in \mathfrak{g}$. Consistently, he writes $a \vee b$ and $\mathfrak{a}_r + \mathfrak{b}_r$ where we write $a \wedge b$ and $\mathfrak{a}_r \wedge \mathfrak{b}_r$, respectively. He probably does so to match the preorder relation $\subseteq$ between subsets of $\mathfrak{G}$.

§ 1.

Idealsysteme.

Wir wollen eine Menge $\mathfrak{g}$, für deren Elemente $a, b, c, \dots$ eine kommutative und assoziative Multiplikation definiert ist, eine *Halbgruppe* nennen, wenn

1. aus $ac = bc$ stets $a = b$ folgt,
2. $\mathfrak{g}$ ein Einselement 1 enthält.

Zu jeder Halbgruppe $\mathfrak{g}$ gibt es eindeutig die Gruppe $\mathfrak{G}$, die aus den Quotienten $\frac{a}{b}$ besteht. $\mathfrak{G}$ heißt die Quotientengruppe von $\mathfrak{g}$. So ist z. B. die Menge der von Null verschiedenen Elemente eines Integritätsbereiches eine Halbgruppe, und die von Null verschiedenen Elemente des Quotientenkörpers bilden die Quotientengruppe.

Viele Definitionen der Teilbarkeitstheorie in Integritätsbereichen lassen sich unmittelbar auf Halbgruppen übertragen. Von den Elementen von $\mathfrak{G}$ nennen wir die Elemente von $\mathfrak{g}$ die ganzen Elemente, b heißt ein Teiler von a , und a heißt Vielfaches von b , wenn $\frac{a}{b}$ ganz ist. Das Hauptideal (a) besteht aus allen Vielfachen von a . Ist eine Verwechslung ausgeschlossen, dann wird das Hauptideal (a) einfach mit a bezeichnet. Ein ganzes Element a heißt Einheit, wenn a^{-1} ganz ist.

Die Dedekindsche Definition der Ideale in Integritätsbereichen läßt sich natürlich nicht übertragen, da in Halbgruppen ja keine Addition erklärt zu sein braucht. Dagegen ist der Begriff der Idealsysteme, wie er von Prüfer und Krull aufgestellt worden ist, fast unmittelbar auch in Halbgruppen anzuwenden. Zur Formulierung der Definition wollen wir, wenn $\mathfrak{a}, \mathfrak{b}$ beliebige Untermengen von $\mathfrak{G}$ sind, unter $\mathfrak{a}\mathfrak{b}$ die Menge der Elemente ab mit $a \in \mathfrak{a}, b \in \mathfrak{b}$ und unter $\mathfrak{a}:\mathfrak{b}$ die Menge der Elemente c mit $c\mathfrak{b} \subseteq \mathfrak{a}$ verstehen. Statt $(1):\mathfrak{a}$ schreiben wir $\mathfrak{a}^{-1}$.

Definition 1. Es seien zu jeder endlichen oder zu jeder beliebigen Untermenge $\mathfrak{a}$ von $\mathfrak{G}$, für die $\mathfrak{a}^{-1} \neq 0$ ist, eine Untermenge $\mathfrak{a}_r$ von $\mathfrak{G}$ so definiert, daß die folgenden Bedingungen erfüllt sind:

1. $\mathfrak{a} \subseteq \mathfrak{a}_r$,
2. aus $\mathfrak{a} \subseteq \mathfrak{b}_r$ folgt $\mathfrak{a}_r \subseteq \mathfrak{b}_r$,
3. für ein Element a ist $\mathfrak{a}_r = (a)$,

4. $aa_r = (aa)_r$.

a_r heit dann das *aus a erzeugte r-Ideal*. Ist a endlich, so heit a_r ein endliches *r-Ideal*. Die Menge aller *r-Ideale* nennen wir das *r-Idealsystem*. Ist sogar fr jede Untermenge a mit $a^{-1} \neq 0$ ein *r-Ideal* definiert, so nennen wir die Menge aller *r-Ideale* das *totale r-Idealsystem*.

Die Summe zweier Ideale wird durch $a_r + b_r = (a \cup b)_r$, das Produkt durch $a_r b_r = (ab)_r$ definiert. Diese Definitionen sind unabhngig von der Erzeugung der Ideale. Wegen 4. gilt das Distributivgesetz:

$$(a_r + b_r)c_r = a_r c_r + b_r c_r.$$

Fr beliebige Halbgruppen konstruieren wir jetzt zwei wichtige Idealsysteme. Wir setzen:

$$a_s = \bigcup_{a \in a} (a), \quad a_v = \bigcap_{a \subseteq (a)} (a).$$

Definition 2. Eine Halbgruppe heit *r-abgeschlossen*, wenn $c_r : c_r = 1$ fr jedes endliche *r-Ideal* c_r gilt.

Die Bedeutung der *r-Abgeschlossenheit* liegt darin, da in jeder *r-abgeschlossenen* Halbgruppe die folgende Konstruktion eines neuen Idealsystems mglich ist ...:

Definition 3. Ist a eine endliche Untermenge von $\mathfrak{G}$, und ist $\mathfrak{g}$ *r-abgeschlossen*, so soll a_{r_a} aus den Elementen a bestehen, fr die es ein endliches *r-Ideal* c_r gibt mit $ac_r \subseteq a_r c_r$.

Die Mengen a_{r_a} bilden dann ein Idealsystem, das System der a_r -Ideale. Die a_r -Ideale haben nun die Eigenschaft, eine *Halbgruppe* zu bilden, d.h. fr beliebige endliche a_r -Ideale a, b, c folgt aus $ac = bc$ stets $a = b$

§ 2.

Totale Idealsysteme, Endlichartigkeit.

... Wir bezeichnen dazu mit $\mathfrak{e}$ stets Mengen aus endlich vielen Elementen von $\mathfrak{G}$. Ist dann a eine beliebige Untermenge von $\mathfrak{G}$ mit $a^{-1} \neq 0$, so setzen wir

$$a_{r_s} = \bigcup_{\mathfrak{e} \subseteq a} \mathfrak{e}_r, \quad a_{r_v} = \bigcap_{a \subseteq \mathfrak{e}_r} \mathfrak{e}_r.$$

Wir nennen das v_s -System krzer das *t-System*.

§ 3.

Vollständige Halbgruppen.

Im § 4 werden wir zeigen, wie der Idealbegriff dazu dienen kann, viele Fragen über Halbgruppen auf die Untersuchung der folgenden sehr speziellen Klasse von Halbgruppen zurückzuführen:

Definition 5. Eine Halbgruppe heißt *vollständig*, wenn je zwei Elemente a, b einen größten gemeinsamen Teiler $a \vee b$ besitzen.

Außerdem müssen wir noch den Begriff der Quotientenringe eines Integritätsbereiches auf Halbgruppen übertragen. Sei dazu g eine beliebige Halbgruppe, S eine Unterhalbgruppe von g , dann soll g_S die Halbgruppe aller Quotienten $\frac{a}{b}$ ($a \in g, b \in S$) sein. g_S heißt eine *Quotientenhalbgruppe* von g (vgl. Grell [1]).

Die Nichteinheiten von g_S , die gleichzeitig in g liegen, bilden ein s -Primideal p von g . Bezeichnen wir dann mit g_p die Quotientenhalbgruppe der Elemente $\frac{a}{b}$ ($a \in g, b \in g, b \notin p$) so wird $g_p = g_S$. Die Quotientenhalbgruppen von g entsprechen also umkehrbar eindeutig den s -Primidealen von g .

Ist nun g vollständig, so auch jede Quotientenhalbgruppe g_S , denn sind s, s' Elemente von S , so liegt mit $\frac{a}{s}, \frac{a'}{s'}$ auch

$$\frac{a}{s} \vee \frac{a'}{s'} = \frac{s'a \vee sa'}{ss'}$$

in g_S und liefert gleichzeitig den größten gemeinsamen Teiler von $\frac{a}{s}, \frac{a'}{s'}$ bezüglich der Teilbarkeit in g_S .

Umgekehrt ist aber auch jede Oberhalbgruppe $\bar{g}$ von g (natürlich $g \subseteq \bar{g} \subseteq \mathfrak{G}$), die mit zwei Elementen a, b auch $a \vee b$ enthält, eine Quotientenhalbgruppe von g , denn für jedes Element a von $\mathfrak{G}$ gilt $a = \frac{a(1 \vee a)^{-1}}{(1 \vee a)^{-1}}$, wobei $a(1 \vee a)^{-1}$ und $(1 \vee a)^{-1}$ Elemente von g sind. Ist $a \in \bar{g}$, so folgt $1 \vee a \in \bar{g}$ und damit $\bar{g} = g_S$, wenn S aus den Einheiten von $\bar{g}$ besteht, die in g liegen.

Die wichtigsten Quotientenhalbgruppen sind die Quotientenhalbgruppen g_p , bei denen p ein t -Primideal von g ist, denn es gilt:

Satz 10. Jede Quotientenhalbgruppe g_p nach einem t -Primideal p ist linear.

Jede Nichteinheit von g_p läßt sich nämlich als Quotient $\frac{p}{s}$ ($p \in p, s \notin p$) darstellen, und sind $\frac{p}{s}, \frac{p'}{s'}$ zwei Nichteinheiten, so ist auch

$$\frac{p}{s} \vee \frac{p'}{s'} = \frac{s'p \vee sp'}{ss'}$$

Nichteinheit, da $s'p \vee sp' \in p$. Für jedes $a \in \mathfrak{G}$ folgt also aus

$$\frac{1}{1 \vee a} \vee \frac{1}{1 \vee a^{-1}} = 1,$$

daß $\frac{1}{1 \vee a}$ oder $\frac{1}{1 \vee a^{-1}}$ Einheit von $\mathfrak{g}_p$ ist, d.h. $a \in \mathfrak{g}_p$ oder $a^{-1} \in \mathfrak{g}_p$.

Satz 11. *Es sei N eine Menge von t -Primidealen von $\mathfrak{g}$ derart, daß jede Nichteinheit von $\mathfrak{g}$ in mindestens einem $\mathfrak{p} \in N$ liegt, dann ist $\mathfrak{g}$ Durchschnitt der linearen Oberhalbgruppen $\mathfrak{g}_p$ ($p \in N$)*

$$\mathfrak{g} = \bigcap_N \mathfrak{g}_p.$$

Denn ist $a \notin \mathfrak{g}$, so ist $(1 \vee a)^{-1}$ Nichteinheit von $\mathfrak{g}$. Also gibt es ein $p \in N$ mit $(1 \vee a)^{-1} \in \mathfrak{p}$, und hieraus folgt $a \notin \mathfrak{g}_p$.

Satz 12. *Enthält N alle maximalen t -Primideale, so gilt für alle t -Ideale $\mathfrak{a}$ von $\mathfrak{g}$ die Durchschnittsdarstellung $\mathfrak{a} = \bigcap_N \mathfrak{a}\mathfrak{g}_p$.*

Denn ist $a \notin \mathfrak{a}$, so ist $a^{-1}\mathfrak{a} \cap \mathfrak{g} \subset \mathfrak{g}$. Es gibt also ein $p \in N$ mit $a^{-1}\mathfrak{a} \cap \mathfrak{g} \subseteq \mathfrak{p}$, woraus wieder $a \notin \mathfrak{a}\mathfrak{g}_p$ folgt.

Diese Sätze gestatten zunächst für vollständige Halbgruppen Fragen über die linearen Oberhalbgruppen von $\mathfrak{g}$ in rein idealtheoretische Fragen zu verwandeln. Diese Reduktion auch für allgemeinere Halbgruppen durchzuführen, ist das Ziel von § 4.

§ 4.

Idealbrüche.

Die Konstruktion der vollständigen Halbgruppe, auf die die Strukturuntersuchung allgemeinerer Halbgruppen zurückgeführt werden soll, ist z. B. für total abgeschlossene Halbgruppen $\mathfrak{g}$ leicht geschehen, denn dann bilden ja die sämtlichen ganzen v -Ideale von $\mathfrak{g}$ ihrerseits eine vollständige Halbgruppe. Ebenso, wenn $\mathfrak{g}$ eine Multiplikationshalbgruppe bezüglich irgendeines Idealsystems ist, d.h. also wenn jedes endliche Ideal umkehrbar ist, so bilden die ganzen Ideale der Form $\mathfrak{a}\mathfrak{b}^{-1}$, wobei $\mathfrak{a}, \mathfrak{b}$ endliche Ideale sind, eine vollständige Halbgruppe. Gehört nämlich noch $\mathfrak{c}\mathfrak{d}^{-1}$ dazu, so auch der größte gemeinsame Teiler von $\mathfrak{a}\mathfrak{b}^{-1}$ und $\mathfrak{c}\mathfrak{d}^{-1}$; denn dieser ist:

$$\mathfrak{a}\mathfrak{b}^{-1} + \mathfrak{c}\mathfrak{d}^{-1} = (\mathfrak{a}\mathfrak{d} + \mathfrak{b}\mathfrak{c})(\mathfrak{b}\mathfrak{d})^{-1}.$$

Aber wir brauchen von unserer Halbgruppe, in der etwa das System der r -Ideale gegeben sei, nur vorauszusetzen, daß sie r -abgeschlossen ist, um auf eine vollständige Halbgruppe zu kommen. Denn ist $\mathfrak{g}$ r -abgeschlossen, so bilden die endlichen r_a -Ideale eine Halbgruppe; wir können also deren Quotientengruppe bilden. Diese besteht aus den „Idealbrüchen“ $\frac{\mathfrak{a}}{\mathfrak{b}}$, wobei $\mathfrak{a}, \mathfrak{b}$ endliche r_a -Ideale sind. Wir definieren dann für zwei Idealbrüche $\frac{\mathfrak{a}}{\mathfrak{b}} \subseteq \frac{\mathfrak{c}}{\mathfrak{d}}$, wenn $\mathfrak{a}\mathfrak{d} \subseteq \mathfrak{b}\mathfrak{c}$. Es wird dadurch die Relation $\subseteq$ fortgesetzt in die Quotientengruppe.

Betrachten wir nun alle Idealbrüche $\frac{a}{b} \subseteq 1$. Diese bilden eine Halbgruppe $\mathfrak{h}$, und zwar eine vollständige Halbgruppe. Der größte gemeinsame Teiler von $\frac{a}{b}$ und $\frac{c}{d}$ ist natürlich durch $\frac{ad+bc}{bd}$ gegeben. Ist $\frac{a}{b} \subseteq 1$, so nennen wir $\frac{a}{b}$ einen „ganzen Idealbruch“. Die vollständige Halbgruppe der ganzen Idealbrüche ersetzt uns den Kroneckerschen Funktionalring, wie er in Prüfer [1] konstruiert worden ist. Das wichtige Ergebnis, das Krull [5] über den Funktionalring beweist, läßt sich auf $\mathfrak{h}$ übertragen. Es handelt sich dabei um die linearen Oberhalbgruppen von $\mathfrak{g}$ einerseits, $\mathfrak{h}$ andererseits. Ist $\mathfrak{L}$ eine lineare Oberhalbgruppe von $\mathfrak{h}$, so bilden die Elemente a von $\mathfrak{G}$, deren Hauptideal (a) in $\mathfrak{L}$ liegt, ersichtlich eine ebenfalls lineare Oberhalbgruppe $\mathfrak{B}$ von $\mathfrak{g}$. Enthält $\mathfrak{L}$ mit endlich vielen Elementen auch deren größten gemeinsamen Teiler, so hat $\mathfrak{B}$ noch folgende Eigenschaft:

$\mathfrak{B}$ enthält mit endlich vielen Elementen $a_1, \dots, a_n$ auch das r -Ideal $(a_1, \dots, a_n)_r$.

Nennen wir Halbgruppen mit dieser Eigenschaft r -Halbgruppen, so können wir unser Ergebnis kurz so fassen:

Jede lineare t -Oberhalbgruppe von $\mathfrak{h}$ liefert eine lineare r -Oberhalbgruppe von $\mathfrak{g}$.

Dieser Satz läßt sich nun umkehren. Ist nämlich eine lineare r -Oberhalbgruppe $\mathfrak{B}$ von $\mathfrak{g}$ gegeben, so zeigen wir zunächst, daß $\mathfrak{B}$ auch r_a -Oberhalbgruppe ist. Dazu sei $d \in (a_1, \dots, a_n)_{r_a}$, $a_v \in \mathfrak{B}$ ($v = 1, \dots, n$), d.h. es gibt ein endliches r -Ideal $\mathfrak{c} = (c_1, \dots, c_m)_r$, so daß $d\mathfrak{c} \subseteq (a_1, \dots, a_n)_r\mathfrak{c}$. Da $\mathfrak{B}$ linear ist, gibt es unter den Elementen $c_1, \dots, c_m$ eines – etwa c_1 –, so daß $c_1^{-1}c_v \in \mathfrak{B}$ ($v = 1, \dots, m$). Dann folgt wegen

$$d(1, c_1^{-1}c_2, \dots, c_1^{-1}c_m)_r \subseteq (a_1, \dots, a_n)_r(1, c_1^{-1}c_2, \dots, c_1^{-1}c_m)_r,$$

daß d in einem endlichen r -Ideal liegt, das aus lauter Elementen von $\mathfrak{B}$ erzeugt wird, also muß d in $\mathfrak{B}$ liegen. $\mathfrak{B}$ ist somit lineare r_a -Oberhalbgruppe, woraus weiter folgt, daß für jedes endliche r_a -Ideal $\mathfrak{a} = (a_1, \dots, a_n)_{r_a}$ stets $\mathfrak{a}$ in dem aus $a_1, \dots, a_n$ erzeugten s -Ideal von $\mathfrak{B}$ enthalten ist. $\mathfrak{a}\mathfrak{B}$ ist also Hauptideal in $\mathfrak{B}$. Wir definieren jetzt eine lineare Oberhalbgruppe $\mathfrak{L}$ von $\mathfrak{h}$ durch $\frac{a}{b} \in \mathfrak{L}$, wenn

$$\mathfrak{a}\mathfrak{B} \subseteq \mathfrak{b}\mathfrak{B}.$$

$\mathfrak{L}$ ist dann eine lineare t -Oberhalbgruppe von $\mathfrak{h}$ und enthält ein Hauptideal (a) genau dann, wenn a in $\mathfrak{B}$ liegt. Insgesamt erhalten wir unter Berücksichtigung von § 3:

Satz 13. *Die linearen r -Oberhalbgruppen einer r -abgeschlossenen Halbgruppe entsprechen umkehrbar eindeutig den linearen t -Oberhalbgruppen der Halbgruppe $\mathfrak{h}$ der ganzen Idealbrüche und damit den t -Primidealen von $\mathfrak{h}$.*

Als Folgerung dieses Satzes ergibt sich sofort:

Satz 14. *Jede r -abgeschlossene Halbgruppe ist Durchschnitt von linearen r -Oberhalbgruppen.*

Literaturverzeichnis.

H. Grell.

[1] Beziehungen zwischen den Idealen verschiedener Ringe, Math. Annalen **97** (1927).

W. Krull.

[5] Beiträge zur Arithmetik kommutativer Integritätsbereiche, Beitrag I, Math. Zeitschr. **41** (1936).

H. Prüfer.

[1] Untersuchungen über die Teilbarkeitseigenschaften von Körpern, J. reine angew. Math. **168** (1932).

6 Lorenzen 1950: the Fundamentalsatz without valuations

Lorenzen 1950 takes place in the framework of preordered noncommutative monoids. It proposes an analysis of a system of ideals as an embedding into a semilattice:

In the commutative setting, the systems of ideals are always introduced as systems of certain subsets. But if one removes this set-theoretic clothing, then the concept of an ideal may be defined quite simply: a system of ideals of a preordered set is nothing but an embedding into a semilattice.

This enables Lorenzen to analyse the concept of r -supermonoid of Lorenzen 1939 as r -allowable monoid corresponding to an r -allowable preorder, i.e. a preorder that is the restriction of a homomorphic image of the system of r -ideals. The reader is invited to return to the part of the letter to Krull dated 6 June 1944 that is translated in the introduction (page 142), and to reflect upon the simplification and clarification w.r.t. Inequality (2) of the definition of a valuation.

In the letter to Krull dated 13 March 1944 (page 226), Lorenzen stresses the importance of these discoveries in his research:

E.g. the insight that a system of ideals is intrinsically nothing but a supersemilattice, and a valuation nothing but a linear preorder, strikes me as the most essential result of my effort.

In the noncommutative framework, integral dependence cannot be captured anymore by passing from the r - to the r_a -system. Therefore Lorenzen devises a new construction that may be considered as the birth of dynamical

algebra. In the introduction, he describes it for the system of Dedekind ideals:

Let I be an arbitrary integral domain, $\mathfrak{a}$ a (finite or infinite) ideal of I , a an element of the field of fractions K . We ask ourselves under what circumstances $a \in \mathfrak{a}B$ holds for every valuation superring B of I . For arbitrary $z \in K^*$ and any valuation superring B of I , it always holds that

$$z \in B \quad \text{or} \quad z^{-1} \in B.$$

Therefore, whenever $a \in \mathfrak{a}I[z]$ and $a \in \mathfrak{a}I[z^{-1}]$ holds, so does $a \in \mathfrak{a}B$. Likewise follows: if there are elements $z_1, \dots, z_n \in K^*$ for which

$$3) \quad a \in \mathfrak{a}I[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$$

holds for each of the 2^n combinations of signs, then, for every valuation superring B of I , it holds that

$$a \in \mathfrak{a}B.$$

This condition 3) is also necessary. Namely, if 3) is not fulfilled for any $z_1, \dots, z_n$, then a simple well-ordering argument shows that there is a maximal superring $\bar{I}$ of I with the property that, for all $z_1, \dots, z_n \in K^*$,

$$a \notin \mathfrak{a}\bar{I}[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$$

holds for at least one combination of signs. Therefore in particular $a \notin \mathfrak{a}\bar{I}$ holds. If this $\bar{I}$ were not a valuation ring, then there would be a $z \in K^*$ with $z \notin \bar{I}$ and $z^{-1} \notin \bar{I}$, therefore there would be elements $x_1, \dots, x_m$ and $y_1, \dots, y_n$ with

$$a \in \mathfrak{a}\bar{I}[z][x_1^{\pm 1}, \dots, x_m^{\pm 1}]$$

$$a \in \mathfrak{a}\bar{I}[z^{-1}][y_1^{\pm 1}, \dots, y_n^{\pm 1}]$$

for each combination of signs. But from this,

$$a \in \mathfrak{a}\bar{I}[z^{\pm 1}, x_1^{\pm 1}, \dots, x_m^{\pm 1}, y_1^{\pm 1}, \dots, y_n^{\pm 1}]$$

would follow, i.e. a contradiction. Therefore $\bar{I}$ is a valuation ring.

With that, the following new result is gained:

$a \in \mathfrak{a}B$ holds for every valuation superring B of I exactly when there are elements $z_1, \dots, z_n \in K^*$ for which

$$a \in \mathfrak{a}I[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$$

holds for each combination of signs.

.....

a is integrally dependent on I if there are elements $z_1, \dots, z_n$ of the

field of fractions that fulfil $a \in I[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$ for each combination of signs.

The gist of Lorenzen's new construction is that in a computation in an integral domain I , one may at any time open two branches concerning an element z : in one branch, one supposes that I contains z ; in the other, that I contains z^{-1} . If a result may be obtained in each branch by a computation, then there is a computation that yields this result without opening the branches. This construction embodies the computational content of the proof method described by Krull (1936): see [page 148](#).

This leads to a reshaping of Krull's Fundamentalsatz for integral domains into Theorem 26. We postpone our discussion of this reshaping until the next section, on [Lorenzen 1952](#), instead of dwelling on the 1950 version.

But let us stress another discovery reported in this article: the property of regularity (see Satz 8 on [page 165](#)). It consists in requiring of an ℓ -group that if $a \wedge xax^{-1} = 1$, then $a = 1$. This property may be seen as specifying the amount of commutativity that must be granted in an ℓ -group in order to be allowed to open branches in computations as described above. For more on this, see [Coquand, Lombardi, and Neuwirth 2020](#).

Excerpt

Our excerpt is from pages 483–490, 492–494, 496–500, 502–503, 506, 509–512, and 515–518 of “Über halbgeordnete Gruppen”, *Mathematische Zeitschrift* 52.

Ein Integritätsbereich I definiert in der multiplikativen Gruppe K^* seines Quotientenkörpers K eine Teilbarkeitsrelation. . . .

Wie man der Theorie der kommutativen Halbgruppen entnehmen kann, sind die Ordnungen, die einen Bewertungsring B bestimmen, der I umfaßt, dadurch gekennzeichnet, daß sie zugleich eine Ordnung der Ideale $a, b, \dots$ von I ermöglichen, so daß stets gilt:

$$5) \quad c \leq a, c \leq b \Rightarrow c \leq a + b.$$

Genauer gesagt: die Teilbarkeitsrelationen der Bewertungsoberringe von I sind die Ordnungen von K^* , die durch die Ordnungen des Idealsystems von I induziert werden, die 5) erfüllen. Die hier auftretenden Ordnungen des Idealsystems nennen wir die zulässigen Ordnungen.

Wir definieren in § 4 Idealsysteme für beliebige halbgeordnete Mengen und insbesondere für halbgeordnete Gruppen. Wir definieren auch für diesen allgemeinen Fall die zulässigen Ordnungen eines Idealsystems und dann weiter:

Eine Ordnung einer halbgeordneten Gruppe G , zu der ein Idealsystem H gegeben ist, heißt zulässig (bezgl. H), wenn sie durch eine zulässige Ordnung von H in G induziert wird. Die Teilbarkeitsrelationen der Bewertungsoberringe von I sind dann also genau die (bezgl. des DEDEKINDSchen Idealsystems) zulässigen Ordnungen von K^* .

Gegeben sei eine beliebige halbgeordnete Gruppe G und ein beliebiges Idealsystem H von G . Wann und wie ist die Halbordnung von G als Konjunktion zulässiger Ordnungen von G darstellbar? ...

Wie läßt sich eine halbgeordnete Gruppe in eine Verbandsgruppe einbetten – vorausgesetzt, daß eine solche Einbettung möglich ist?

Wir erhalten die Antwort auf unsere Frage durch eine genaue halbordnungstheoretische Analyse des Idealbegriffs. Im Kommutativen werden die Idealsysteme stets als Systeme von gewissen Untermengen eingeführt. Beseitigt man aber diese mengentheoretische Einkleidung, so läßt sich der Idealbegriff ganz einfach definieren: ein Idealsystem einer halbgeordneten Menge ist nichts anderes als eine Einbettung in einen Halbverband. (Ich bemerke ausdrücklich, daß man hier statt „Halbverband“ nicht „Verband“ setzen darf.)

Ist die Halbordnung von G als Konjunktion zulässiger Ordnungen von G darstellbar, so gibt es ein Idealsystem H' von G , dessen v -Ideale eine reguläre Verbandsgruppe bilden. ...

Die hier auftretenden Idealsysteme H' , die in der Arithmetik „arithmetisch brauchbar“ heißen, nennen wir auch im allgemeinen Fall „brauchbar“.

Wie in der Arithmetik ergibt sich dann weiter, daß unter den brauchbaren Idealsystemen eines ausgezeichnet ist, zu dem alle anderen homomorph sind ...

Zur Beantwortung unserer Ausgangsfragestellung für halbgeordnete Gruppen bleibt uns jetzt vor allem folgende Frage:

Wie läßt sich das ausgezeichnete brauchbare Idealsystem einer halbgeordneten Gruppe G konstruieren – vorausgesetzt, daß es überhaupt existiert.

Wir setzen also voraus, daß die Halbordnung von G als Konjunktion zulässiger Ordnungen von G darstellbar ist. Bei der Konstruktion des ausgezeichneten brauchbaren Idealsystems wollen wir aber die Kenntnis

dieser Ordnungen nicht voraussetzen, weil wir gerade mit Hilfe des Idealsystems die zulässigen Ordnungen bestimmen wollen.

Diese Konstruktion wird in der Arithmetik geliefert durch den PRÜFERSchen Begriff der Ganzabhängigkeit von einem Ideal $\mathfrak{a}$ des gegebenen Integritätsbereiches I .

Ein Element a des Quotientenkörpers K heißt ganz abhängig von $\mathfrak{a}$, wenn a einer Gleichung

$$1) \quad a^n + a_1 a^{n-1} + \dots + a_n = 0$$

mit $a_\nu \in \mathfrak{a}^\nu$ genügt.

In der Theorie der kommutativen Halbgruppen tritt an die Stelle von 1) die Bedingung, daß es ein endliches Ideal $\mathfrak{c}$ geben soll, so daß

$$2) \quad a\mathfrak{c} \subseteq \mathfrak{c}$$

gilt. Auch diese Bedingung 2) läßt sich jedoch nicht auf den nichtkommutativen Fall ausdehnen.

Um den Grundgedanken unserer neuen Konstruktion, die wir statt 1) oder 2) verwenden, deutlich zu machen, führe ich sie hier für den arithmetischen Spezialfall durch. § 6 des Textes bringt die Durchführung für beliebige halbgeordnete Gruppen.

I sei ein beliebiger Integritätsbereich, $\mathfrak{a}$ ein (endliches oder unendliches) Ideal von I , a ein Element des Quotientenkörpers K . Wir fragen uns, wann für jeden Bewertungsoberring B von I gilt: $a \in \mathfrak{a}B$. Für beliebiges $z \in K^*$ und jeden Bewertungsoberring B von I gilt stets

$$z \in B \quad \text{oder} \quad z^{-1} \in B.$$

Gilt also $a \in \mathfrak{a}I[z]$ und $a \in \mathfrak{a}I[z^{-1}]$, so gilt stets $a \in \mathfrak{a}B$. Ebenso folgt: Gibt es Elemente $z_1, \dots, z_n \in K^*$, für die

$$3) \quad a \in \mathfrak{a}I[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$$

für jede der 2^n Vorzeichenkombinationen gilt, so gilt für jeden Bewertungsoberring B von I :

$$a \in \mathfrak{a}B.$$

Diese Bedingung 3) ist auch notwendig. Ist nämlich 3) für kein $z_1, \dots, z_n$ erfüllt, so zeigt ein einfacher Wohlordnungsschluß, daß es einen maximalen Oberring $\bar{I}$ von I gibt, mit der Eigenschaft, daß für jedes $z_1, \dots, z_n \in K^*$

$$a \notin \mathfrak{a}\bar{I}[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$$

für mindestens eine Vorzeichenkombination gilt. Insbesondere gilt also $a \notin \mathfrak{a}\bar{I}$. Wäre dieses $\bar{I}$ kein Bewertungsring, so gäbe es ein $z \in K^*$ mit $z \notin \bar{I}$

und $z^{-1} \notin \bar{I}$, also gäbe es Elemente $x_1, \dots, x_m$ und $y_1, \dots, y_n$ mit

$$\begin{aligned} a &\in \mathfrak{a}\bar{I}[z][x_1^{\pm 1}, \dots, x_m^{\pm 1}] \\ a &\in \mathfrak{a}\bar{I}[z^{-1}][y_1^{\pm 1}, \dots, y_n^{\pm 1}] \end{aligned}$$

für jede Vorzeichenkombination. Hieraus würde aber

$$a \in \mathfrak{a}\bar{I}[z^{\pm 1}, x_1^{\pm 1}, \dots, x_m^{\pm 1}, y_1^{\pm 1}, \dots, y_n^{\pm 1}]$$

folgen, d.h. ein Widerspruch. Also ist $\bar{I}$ Bewertungsring.

Damit ist das folgende neue Ergebnis gewonnen:

Es gilt genau dann $a \in \mathfrak{a}B$ für jeden Bewertungsoberring B von I , wenn es Elemente $z_1, \dots, z_n \in K^*$ gibt, für die

$$a \in \mathfrak{a}I[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$$

für jede Vorzeichenkombination gilt.

Der Beweis ist so einfach, daß er sich ohne weiteres in beliebigen halbgeordneten Gruppen durchführen läßt und hier sowohl eine Konstruktion des ausgezeichneten brauchbaren Idealsystems liefert (vorausgesetzt, daß es existiert), als auch die folgende Frage beantwortet:

Wann ist die Halbordnung einer halbgeordneten Gruppe G als Konjunktion zulässiger Ordnungen von G darstellbar?

Zum Schluß zeigen wir, daß sich diese Ergebnisse mit den bekannten Ergebnissen im Kommutativen in Übereinstimmung befinden. ... Ferner erhält man für den grundlegenden Begriff der Ganzabhängigkeit eines Elementes a von einem Integritätsbereich I einen neuen gleichwertigen Ausdruck:

a ist genau dann ganz abhängig von I , wenn es Elemente $z_1, \dots, z_n$ des Quotientenkörpers gibt, die $a \in I[z_1^{\pm 1}, \dots, z_n^{\pm 1}]$ für jede Vorzeichenkombination erfüllen.

§ 1.

Halbordnungen.

.....

Für jede Halbordnung benutzen wir außerdem zur Abkürzung:

$$\begin{aligned} a &\geq b, \text{ wenn } b \leq a \text{ gilt,} \\ a &\equiv b, \text{ wenn } a \leq b \text{ und } a \geq b \text{ gilt,} \end{aligned}$$

.....

Die ganzen Elemente einer halbgeordneten Gruppe G bilden eine invariante Unterhalbgruppe $\mathfrak{g}$ von G . Es gilt nämlich

für jedes $a, b \in G$:

$$1 \geq 1,$$

$$a \geq 1, b \geq 1 \Rightarrow ab \geq 1,$$

für jedes $a, x \in G$:

$$a \geq 1 \Rightarrow xax^{-1} \geq 1.$$

Dies bedeutet für die Menge $\mathfrak{g}$ der ganzen Elemente

$$1 \in \mathfrak{g},$$

für jedes $a, b \in G$:

$$a \in \mathfrak{g}, b \in \mathfrak{g} \Rightarrow ab \in \mathfrak{g},$$

für jedes $a, x \in G$:

$$a \in \mathfrak{g} \Rightarrow xax^{-1} \in \mathfrak{g}.$$

Wir nennen die invariante Unterhalbgruppe der ganzen Elemente kurz die (zu $\leq$) zugehörige Halbgruppe.

Satz 1. Die Halbordnungen einer Gruppe G entsprechen eineindeutig den invarianten Unterhalbgruppen von G .

.....

§ 2.

Verbandsgruppen.

.....

Wir nennen zwei Elemente a und b einer Verbandsgruppe teilerfremd, wenn $a \wedge b \equiv 1$ gilt, und schreiben hierfür $a \parallel b$

.....

§ 3.

Hauptgruppen.

.....

Wir nennen diese direkten Produkte von geordneten Gruppen Vektorgruppen. ...

Satz 8. In einer Vektorgruppe G gilt für jedes $a, x \in G$

$$a \parallel xax^{-1} \Rightarrow a \equiv 1.$$

Beweis. Wir haben nur nachzuweisen, daß diese Bedingung für geordnete Gruppen gilt. Aus $a > 1 \Rightarrow xax^{-1} > 1$ folgt aber sofort $a > 1 \Rightarrow \min(a, xax^{-1}) > 1$.

Wir nennen jede Verbandsgruppe, die die Bedingung des Satzes 8 erfüllt, regulär. Also ist jede Vektorgruppe eine reguläre Verbandsgruppe.

Dieser Satz läßt sich nicht umkehren, wohl aber gilt, daß jede reguläre Verbandsgruppe Untergruppe einer Vektorgruppe ist. Dieses wollen wir im Folgenden beweisen.

Wir definieren zunächst: Jede Untergruppe einer Vektorgruppe heißt eine Hauptgruppe.

.....
Es seien H und H' Halbverbandshalbgruppen und $\rightarrow$ eine Abbildung von H in H' , die für jedes $a, b \in H, a', b' \in H'$ mit $a \rightarrow a'$ und $b \rightarrow b'$ erfüllt:

- 1) $a \leq b \Rightarrow a' \leq b'$
- 2) $a \wedge b \rightarrow a' \wedge b'$
- 3) $ab \rightarrow a'b'$.

Eine solche Abbildung nennen wir einen Homomorphismus von H .

Jeder Homomorphismus definiert eine Relation $\leq$ in H auf folgende Weise. Wir setzen fest, daß $a \leq b$ in H genau dann gelten soll, wenn $a' \leq b'$ in H' gilt. H ist bzgl. dieser Relation wieder eine Halbverbandshalbgruppe und die Relation $\leq$ erfüllt:

- i) $a \leq b \Rightarrow a \leq b$
- ii) $x \leq a, x \leq b \Rightarrow x \leq a \wedge b$.

Es gilt auch die Umkehrung: Ist $\leq$ eine Halbordnung von H , die i) und ii) erfüllt, so ist H bzgl. $\leq$ eine Halbverbandshalbgruppe (wir wollen diese mit H' bezeichnen) und die Abbildung $a \rightarrow a$ von H auf H' ist ein Homomorphismus.

.....
Aufgrund dieser Gleichwertigkeit betrachten wir statt der Homomorphismen von H nur die Halbordnungen von H , die i) und ii) erfüllen. Wir nennen diese Halbordnungen kurz die zulässigen Halbordnungen von H .

Zwei Homomorphismen von H , die dieselbe zulässige Halbordnung definieren, nennen wir äquivalent. Es entsprechen dann also die Homomorphismen von H bis auf Äquivalenz eineindeutig den zulässigen Halbordnungen von H .

Für eine Verbandsgruppe G entsprechen die zulässigen Halbordnungen von G aber auch eineindeutig gewissen Unterhalbgruppen von G . Aus Satz 1 folgt nämlich sofort:

Ist $\mathfrak{g}$ die zugehörige Halbgruppe einer Verbandsgruppe G , so entsprechen die zulässigen Halbordnungen von G eineindeutig den invarianten Unterhalbgruppen $\mathfrak{g}$ von G , die für jedes $a, b \in G$

- i) $\mathfrak{g} \subseteq \mathfrak{g}$
- ii) $a \in \mathfrak{g}, b \in \mathfrak{g} \Rightarrow a \wedge b \in \mathfrak{g}$

erfüllen.

Diese Halbgruppen $\mathfrak{g}$ nennen wir die zulässigen Halbgruppen von G . Die Homomorphismen einer Verbandsgruppe G entsprechen also bis auf Äquivalenz eineindeutig den zulässigen Halbgruppen von G .

Die zulässigen Halbgruppen einer Verbandsgruppe lassen sich nun durch „Quotientenbildung“ aus der zugehörigen Halbgruppe $\mathfrak{g}$ gewinnen. Dazu haben wir invariante Unterhalbgruppen S von $\mathfrak{g}$ zu betrachten. Gilt für jedes $a, b \in \mathfrak{g}$

$$a \leq b, b \in S \Rightarrow a \in S,$$

so nennen wir S vollständig.

Satz 9. Die Homomorphismen einer Verbandsgruppe G entsprechen bis auf Äquivalenz eineindeutig den vollständigen, invarianten Unterhalbgruppen der zugehörigen Halbgruppe $\mathfrak{g}$.

.....
Satz 13. Jede reguläre Verbandsgruppe ist Hauptgruppe.
.....

Zusammengefaßt erhalten wir also eine Kennzeichnung der Hauptgruppen, die unabhängig ist vom Ordnungsbegriff. Die Bedeutung dieser Kennzeichnung liegt darin, daß sich die Ordnungen einer Gruppe im allgemeinen nur mit Wohlordnungsschlüssen konstruieren lassen – die Oberverbandsgruppen dagegen lassen sich auch ohne Wohlordnung konstruieren mit Hilfe des Idealbegriffs.

§ 4.

Idealsysteme.

Wir definieren den Idealbegriff zunächst für beliebige halbgeordnete Mengen.

Unter einem Idealsystem $\mathfrak{S}$ einer halbgeordneten Menge M verstehen wir einen minimalen Oberhalbverband von M . Ein Oberhalbverband von M enthält zu endlich vielen Elementen a_μ von M ($\mu = 1, \dots, m$) stets den g.g.T. $a_1 \wedge \dots \wedge a_m$. Er heißt minimal, wenn er nur aus Elementen dieser Form besteht. Es gibt dann nämlich keinen echten Unterhalbverband, der auch noch M umfaßt.

.....
Der Idealbegriff ist für halbgeordnete Gruppen in dieser Form noch zu unbestimmt. Als Idealsystem einer halbgeordneten Halbgruppe H wollen wir nur diejenigen Idealsysteme der halbgeordneten Menge H bezeichnen, in denen durch die Festsetzung

$$(a_1 \wedge \dots \wedge a_m)(b_1 \wedge \dots \wedge b_n) \equiv a_1 b_1 \wedge \dots \wedge a_m b_n$$

eine Multiplikation definiert werden kann.

.....

Die Einführung der Idealsysteme geschieht, um mit ihrer Hilfe die Einbettung einer Hauptgruppe G in eine reguläre Verbandsgruppe konstruktiv ohne Benutzung der Ordnungen von G zu ermöglichen.

.....

§ 5. r -Gruppen.

.....

Damit unsere Untersuchung der halbgeordneten Gruppen auch die speziellen Fragen der Arithmetik der kommutativen Integritätsbereiche umfaßt, legen wir daher von jetzt ab eine halbgeordnete Gruppe zugrunde, zu der von vornherein ein festes Idealsystem gegeben ist. Ist dies das System der r -Ideale, so nennen wir die halbgeordnete Gruppe kurz eine r -Gruppe.

In einer r -Gruppe erklären wir nur diejenigen Halbordnungen als r -zulässig, die durch eine zulässige Halbordnung des r -Idealsystems induziert werden.

Die r -zulässigen Halbordnungen lassen sich unabhängig von dem Begriff der zulässigen Halbordnung eines Halbverbandes kennzeichnen. Ist nämlich eine beliebige halbgeordnete Gruppe G gegeben, und ist H ein Idealsystem von G , so gilt

Satz 17. Eine Halbordnung $\leq$ von G wird genau dann durch eine zulässige Halbordnung von H induziert, wenn

$$1) \ a \leq b \Rightarrow a \dot{\leq} b$$

erfüllt ist und wenn aus $a_1 \wedge \dots \wedge a_m \leq a$ in H für jedes $x \in G$ folgt

$$2) \ x \dot{\leq} a_1, \dots, x \dot{\leq} a_m \Rightarrow x \dot{\leq} a.$$

.....

Für die Ordnungen von G gilt darüber hinaus

Satz 18. Die zulässigen Ordnungen von H entsprechen eineindeutig den Ordnungen von G , die 1) und 2) erfüllen.

.....

Ist G eine r -Gruppe und $\mathfrak{g}$ die zugehörige Halbgruppe, so entsprechen die r -zulässigen Halbordnungen bzw. Ordnungen von G den invarianten Unterhalbgruppen bzw. den linearen, invarianten Unterhalbgruppen $\dot{\mathfrak{g}}$ die

$$1) \ \mathfrak{g} \subseteq \dot{\mathfrak{g}}$$

erfüllen, und für die aus $a_1 \wedge \dots \wedge a_m \leq_r a$ folgt:

$$2) a_1 \in \mathfrak{g}, \dots, a_m \in \mathfrak{g} \Rightarrow a \in \mathfrak{g}.$$

Statt 2) läßt sich auch schreiben:

$$a_1 \in \mathfrak{g}, \dots, a_m \in \mathfrak{g} \Rightarrow (a_1, \dots, a_m)_r \subseteq \mathfrak{g}.$$

Wir nennen die invarianten Unterhalbgruppen von G , die 1) und 2) erfüllen, die r -zulässigen Halbgruppen von G .

Eine r -Gruppe G heißt r -Hauptgruppe, wenn die Halbordnung von G nicht nur Konjunktion von Ordnungen von G ist, sondern sogar Konjunktion von r -zulässigen Ordnungen ist. Das ist also genau dann der Fall, wenn die zugehörige Halbgruppe Durchschnitt von linearen r -zulässigen Halbgruppen ist.

.....

§ 6.

Die r -Abschließung.

Wir wollen in diesem § nachweisen, daß sich das ausgezeichnete r -brauchbare Idealsystem, das r_a -System, einer r -Hauptgruppe unabhängig von den Begriffen der vorhergehenden §§ kennzeichnen läßt.

Es sei G eine beliebige r -Gruppe, $\mathfrak{g}$ die zugehörige Halbgruppe, $\mathfrak{a}$ eine r -zulässige Halbgruppe, $\mathfrak{a} = \{a_1, \dots, a_m\}$ eine endliche Untermenge von G und $a \in G$.

Wir bezeichnen das r -Ideal $(a_1, \dots, a_m)_r$ mit $\mathfrak{a}_r$.

Wir definieren das Produkt $\mathfrak{a}_r \cdot \mathfrak{g}$ als die kleinste Untermenge von G , die sämtliche Elemente $a\mathfrak{g}$ mit $a \in \mathfrak{a}_r$ und $\mathfrak{g} \in \mathfrak{g}$ enthält und außerdem für jedes $x_1, \dots, x_n \in G$ die Bedingung

$$x_1 \in \mathfrak{a}_r \cdot \mathfrak{g}, \dots, x_n \in \mathfrak{a}_r \cdot \mathfrak{g} \Rightarrow (x_1, \dots, x_n)_r \subseteq \mathfrak{a}_r \cdot \mathfrak{g}$$

erfüllt.

.....

... bezeichnen wir für jedes $x \in G$ mit $\mathfrak{g}(x)_r$ den Durchschnitt aller r -zulässigen Halbgruppen, die $\mathfrak{g}$ umfassen und außerdem x enthalten. $\mathfrak{g}(x)_r$ ist wieder eine r -zulässige Halbgruppe, die „ r -Erweiterung“ von $\mathfrak{g}$ mit x .

.....

Wir definieren dazu eine Relation α_r zwischen den Elementen a und den Produkten $\mathfrak{a}_r \cdot \mathfrak{g}$.

Wir setzen $a \alpha_r \mathfrak{a}_r \cdot \mathfrak{g}$, wenn es Elemente $x_1, \dots, x_n$ von G gibt mit $a \in \mathfrak{a}_r \cdot \mathfrak{g}(x_1^{\pm 1}, \dots, x_n^{\pm 1})_r$ für jede der 2^n möglichen Vorzeichenkombinationen.

Satz 24. a ist genau dann r -abhängig von $\mathfrak{a}_r$ in $\mathfrak{g}$, wenn $a \alpha_r \mathfrak{a}_r \cdot \mathfrak{g}$ gilt.

.....

Die Bedeutung dieses Satzes liegt darin, daß es jetzt möglich ist, für jede r -Hauptgruppe eine direkte Konstruktion des r_a -Idealsystems anzugeben.

.....

... Gilt $a \alpha_r (1) \cdot \dot{g}$, so nennen wir a r -abhängig von $\dot{g}$, da $(1) \cdot \dot{g} = \dot{g}$ ist.

Liegt jedes von $\dot{g}$ r -abhängige Element in $\dot{g}$, so nennen wir $\dot{g}$ r -abgeschlossen.

.....

Satz 26. Eine r -Gruppe ist genau dann r -Hauptgruppe, wenn die zugehörige Halbgruppe r -abgeschlossen ist.

7 Lorenzen 1952: the Fundamentalsatz for semilattice domains

The first three sections of [Lorenzen 1952](#) propose a streamlined version of [Lorenzen 1950](#) in the more general framework of a *domain* $(B, \preceq_B, G)$, i.e. of a preordered set $(B, \preceq_B)$ with a monoid G of preorder-preserving operators on B . $(H, \preceq_H, G)$ is a *semilattice domain* if $(H, \preceq_H)$ is a semilattice and if the action of G preserves meets. A preorder $\preceq$ on a semilattice domain H is $\preceq_H$ -allowable if it is coarser than $\preceq_H$ and if meets (w.r.t. $\preceq_H$) are also meets w.r.t. $\preceq$. One can similarly define lattice domains and the corresponding allowability.

A *domain of ideals* H_r for a domain B is a minimal supersemilattice domain. A preorder $\preceq$ on B is r -allowable if it is induced by an allowable preorder of H_r . B is an r -principal domain if its preorder is a conjunction of r -allowable linear preorders.

Krull's Fundamentalsatz for integral domains becomes a characterisation of an r -principal domain as a domain B in which behaving as if it were linearly preordered, i.e. assuming that certain pairs of elements $\alpha_1, \dots, \alpha_e \in B \times B$ are linearly preordered, does not add new preordered pairs to the preorder. His formulation of this "as if" goes as follows: it is the simultaneous consideration of 2^e different preorders corresponding to preordering each pair one way or the other (a way described by a combination of signs $\varepsilon_1, \dots, \varepsilon_e = \pm 1$), and each of these preorders is the conjunction $R[\alpha_1^{\varepsilon_1}, \dots, \alpha_e^{\varepsilon_e}]_r$ of all the r -allowable preorders coarser than $\preceq_B$ in which the pairs are preordered in the described way (here below, R is Lorenzen's notation for the preorder $\preceq_B$).

Theorem 1. *An r -domain B (w.r.t. R and G) is an r -principal domain if, and only if, for all pairs $\alpha_1, \dots, \alpha_e$ from B ,*

$$\bigcap_{\varepsilon=\pm 1} R[\alpha_1^{\varepsilon_1}, \dots, \alpha_e^{\varepsilon_e}]_r \subset R$$

I holds.

This final shape of the Fundamentalsatz corresponds to Satz 26 of [Lorenzen 1950](#) (see above) and is obtained by the arguments developed there. The characterisation given in Theorem 1 is but a formulation of *r-closedness*: compare the formulation of integral dependence at the end of the introduction of [Lorenzen 1950](#) (page 164, translated on page 160).

Note that the article [Lorenzen 1951](#) shows that Lorenzen had the means of a considerably simpler formulation of this “as if” by starting from the logic-free and set-theory-free formal system given by H_r and by adding the e axioms corresponding to preordering the pairs (see, in this respect, [Coquand, Lombardi, and Neuwirth 2019; 2020](#)). He may have refrained from doing so in order to stick to a purely algebraic framework that would suit his potential readers.

In the last section, the property of regularity introduced in [Lorenzen 1950](#) is given the following symmetrical form for a distributive lattice domain $(V, \preceq_V, G)$: if $a, b \in V$ and $x, y \in G$, then $xa \wedge yb \preceq_V xb \vee ya$.

Excerpt

Our excerpt is from pages 269–274 of “Teilbarkeitstheorie in Bereichen”, *Mathematische Zeitschrift* 55.

§ 1.

Bereiche.

B sei eine Menge (Elemente $a, b, \dots$), R eine zweistellige Relation in B und G eine Menge von Operatoren $x, y, \dots$ von B .

Definition 1. B heißt ein *Bereich* (bezügl. R und G), wenn für alle a, b, c und x gilt

$$(1.1) \quad a R a$$

$$(1.2) \quad a R b, b R c \rightarrow a R c$$

$$(1.3) \quad a R b \rightarrow xa R xb.$$

Da (1.3) für den Operator 1 (definiert durch $1 \cdot a = a$) und für xy (definiert durch $(xy)a = x(ya)$) gilt, falls für x und y , sei im Folgenden stets angenommen, daß G eine Halbgruppe mit Einselement ist.

R heißt die Halbordnung von B . Statt $a R b$ werde $a < b$ oder $b > a$ geschrieben. $a = b$ bedeute $a < b$ und $b < a$ (= braucht nicht die Identität zu sein).

Gilt $a < b$ oder $a > b$ für alle a und b , dann heißt R eine *Ordnung*.

Definition 2. Ein Bereich B heißt ein *Halbverbandsbereich*, wenn für alle a, b ein größter gemeinsamer Teiler $a \wedge b$ existiert, so daß für alle c und x gilt

$$(1.4) \quad c < a \wedge b \iff c < a, c < b$$

$$(1.5) \quad x(a \wedge b) = xa \wedge xb.$$

.....

Definition 3. Eine Halbordnung S eines Halbverbandsbereiches B (bezügl. R und G) heißt *zulässig*, wenn für alle a, b, c und x gilt

$$(1.6) \quad R \subset S$$

$$(1.7) \quad a S b \rightarrow xa S xb$$

$$(1.8) \quad c S a, c S b \rightarrow c S a \wedge b.$$

.....

Die Halbordnung R eines Bereichs B induziert in jeder Untermenge B_0 von B eine Halbordnung R_0 von B_0 . R heißt eine *Fortsetzung* von R_0 auf B . Ist B_0 zulässig bezügl. G (d.h. $xB_0 \subset B_0$ für alle x), dann induziert G eine Operatorenhalbgruppe G_0 von B_0 . B heißt dann ein *Oberbereich* von B_0 (bezügl. R_0 und G_0).

§ 2.

Ideale.

B sei ein Bereich (bezügl. R und G).

Definition 4. Ein minimaler Halbverbandsoberbereich H von B heißt ein *Idealbereich* von B .

.....

Die Idealbereiche H werden durch einen Kennbuchstaben unterschieden. r sei eine Variable für diese Kennbuchstaben.

Ein Bereich B mit einem Idealbereich H_r heiße ein *r -Bereich*.

Definition 5. Eine Halbordnung S eines r -Bereiches B heiße *r -zulässig*, wenn S durch eine zulässige Halbordnung von H_r induziert wird.

.....

Definition 6. Ein r -Bereich B heißt *r -Hauptbereich*, wenn die Halbordnung R von B Konjunktion r -zulässiger Ordnungen von B ist.

.....

werde für jede r -zulässige Halbordnung S und jedes Paar $\alpha = a_1, a_2$ aus B die r -Erweiterung $S[\alpha]_r$ als Konjunktion aller r -zulässigen Halbordnungen $\bar{S}$ von B mit

$$(2.1) \quad S \subset \bar{S}$$

$$(2.2) \quad a_1 \bar{S} a_2$$

definiert. Zur bequemerem Formulierung sei ferner gesetzt

.....
$$\alpha^{+1} = a_1, a_2, \qquad \alpha^{-1} = a_2, a_1.$$

.....

Satz 1. Ein r -Bereich B (bezügl. R und G) ist genau dann ein r -Hauptbereich, wenn für alle Paare $\alpha_1, \dots, \alpha_e$ aus B gilt:

.....
$$\bigcap_{\varepsilon=\pm 1, \dots, \varepsilon_e} R[\alpha_1^{\varepsilon_1}, \dots, \alpha_e^{\varepsilon_e}]_r \subset R.$$

.....

§ 4.
Reguläre Verbandsbereiche.

Definition 9. Ein Verbandsbereich V heißt *regulär*, wenn V distributiv ist und für a, b und x, y gilt: $xa \wedge yb < xb \vee ya$.

Satz 3. Die Halbordnung eines Verbandsbereiches V ist genau dann Konjunktion zulässiger Ordnungen von V , wenn V regulär ist.

8 Lorenzen 1953: the Fundamentalsatz for integral domains as an embedding into a super- ℓ -group

The introduction of [Lorenzen 1953](#) describes his state of the art on Krull’s Fundamentalsatz for integral domains:

- [Lorenzen 1950](#) shows that the problem of representing an integral domain I as an intersection of valuation rings may be reduced to the problem of constructing a super- ℓ -group of the divisibility group G of I such that the meets of elements of G form a homomorphic image of the system of Dedekind ideals.
- In fact, Satz 3 of [Lorenzen 1952](#) (see above) establishes that the preorder of a regular lattice domain may be represented as a conjunction of allowable linear preorders, and this corresponds to an intersection of valuation rings in the case of an integral domain.

According to the Fundamentalsatz, the integral domains I that are representable as intersections of valuation rings are characterised by being integrally closed. On the other hand, the representability of I as an intersection of valuation rings is equivalent to the existence of a lattice-preordered supergroup V of the multiplicative group G of the field of fractions K of I – where V must satisfy the condition that the domain of

ideals H (which consists of all g.c.d.s $a_1 \wedge \cdots \wedge a_n$ with $a_v \in G$) contained in V is a homomorphic image of the domain of Dedekind ideals H_d of I .

This last equivalence results from the more general domain-theoretic theorem that the preorder of every regular lattice-preordered domain is a conjunction of allowable total orders – if one adds that every commutative lattice-preordered group is trivially regular. Therefore two routes to the proof of Krull's Fundamentalsatz are available: one has to construct, for an integrally closed integral domain, either an intersection representation through valuations or a lattice-preordered supergroup. Both proof possibilities are carried out for commutative groups – for noncommutative groups, however, and more generally for domains, only the first route has been hitherto practicable.

The present work describes the second proof course also in the general case. If afterwards one specialises the general method to divisibility in commutative fields K , then the following results. For the construction of a lattice-preordered supergroup it is only required to define when, for arbitrary elements a_μ, b_ν of the multiplicative group G of K ,

$$a_1 \wedge \cdots \wedge a_m \prec b_1 \vee \cdots \vee b_n$$

is to hold ($\prec$ stands for “divides”, $\wedge$ denotes the g.c.d., $\vee$ the l.c.m.).

For every integrally closed integral domain I , one obtains a lattice-preordered supergroup of G if one defines

$$(1) \quad a_1 \wedge \cdots \wedge a_m \prec b_1 \vee \cdots \vee b_n \iff 1 \in \sum_1^{\times} (a_1 b_1^{-1}, \dots, a_\mu b_\mu^{-1}, \dots, a_m b_n^{-1})^{\times}.$$

For $n = 1, b_1 = b$, this definition changes into the Prüferian definition of integral dependence of b on $(a_1, \dots, a_m)$

$$(2) \quad a_1 \wedge \cdots \wedge a_m \prec b \iff b^k + c_1 b^{k-1} + \cdots + c_k = 0 \quad [c_\times \in (a_1, \dots, a_m)^{\times}].$$

Therefore (1) describes a suitable expansion of the concept of integral dependence.

In this last article on the subject, Lorenzen proposes the construction of an ℓ -group from a preordered group G and a semilattice of ideals H_r ; G embeds into this ℓ -group if and only if it is r -closed. He does so by first constructing the distributive lattice generated by an “entailment relation” associated with H_r (see [Coquand, Lombardi, and Neuwirth 2020](#)) and then proving that it is a lattice-preordered group.

Excerpt

Our excerpt is from page 15 of "Die Erweiterung halbgeordneter Gruppen zu Verbandsgruppen", *Mathematische Zeitschrift* 58.

Nach dem KRULLschen Fundamentalsatz [1] sind die Integritätsbereiche I , die als Durchschnitt von Bewertungsringen darstellbar sind, dadurch charakterisiert, daß sie ganz abgeschlossen sind. Die Darstellbarkeit von I als Durchschnitt von Bewertungsringen ist andererseits äquivalent [3] mit der Existenz einer Verbandsobergruppe V der multiplikativen Gruppe G des Quotientenkörpers K von I – wobei V der Bedingung genügen muß, daß der in V enthaltene Idealbereich H (der aus allen g.g.T. $a_1 \wedge \dots \wedge a_n$ mit $a_v \in G$ besteht) ein homomorphes Bild des DEDEKINDschen Idealbereichs H_d von I ist.

Diese letztere Äquivalenz ergibt sich aus dem allgemeineren bereichstheoretischen [4] Satz, daß die Halbordnung jedes regulären Verbandsbereiches Konjunktion von zulässigen Ordnungen ist – wenn man hinzufügt, daß jede kommutative Verbandsgruppe trivialerweise regulär ist. Daher stehen zum Beweis des KRULLschen Fundamentalsatzes zwei Wege zur Verfügung: Man hat für einen ganz abgeschlossenen Integritätsbereich entweder eine Durchschnittsdarstellung durch Bewertungen oder eine Verbandsobergruppe zu konstruieren. Beide Beweismöglichkeiten sind für kommutative Gruppen durchgeführt – für nichtkommutative Gruppen und allgemeiner für Bereiche ist bisher jedoch nur der erste Weg gangbar.

Die vorliegende Arbeit stellt den zweiten Beweisgang auch im allgemeinen Falle dar. Spezialisiert man anschließend die allgemeine Methode auf die Teilbarkeit in kommutativen Körpern K , so ergibt sich folgendes. Zur Konstruktion einer Verbandsobergruppe braucht nur definiert zu werden, wann für beliebige Elemente a_μ, b_ν aus der multiplikativen Gruppe G von K gelten soll [5]

$$a_1 \wedge \dots \wedge a_m \prec b_1 \vee \dots \vee b_n$$

($\prec$ steht für „teilt“, $\wedge$ bezeichnet den g.g.T., $\vee$ das k.g.V.).

Für jeden ganz abgeschlossenen Integritätsbereich I erhält man eine Verbandsobergruppe von G , wenn man definiert

$$(1) \quad a_1 \wedge \dots \wedge a_m \prec b_1 \vee \dots \vee b_n \iff 1 \in \sum_{\mathcal{Z}} (a_1 b_1^{-1}, \dots, a_\mu b_\nu^{-1}, \dots, a_m b_n^{-1})^{\mathcal{Z}}.$$

Für $n = 1, b_1 = b$ geht diese Definition über in die PRÜFERSche Definition der Ganzabhängigkeit von b von $(a_1, \dots, a_m)$

$$(2) \quad a_1 \wedge \dots \wedge a_m \prec b \iff b^k + c_1 b^{k-1} + \dots + c_k = 0 \quad [c_{\mathcal{Z}} \in (a_1, \dots, a_m)^{\mathcal{Z}}].$$

Daher stellt (1) eine zweckmäßige Ausdehnung des Begriffes der Ganzabhängigkeit dar.

.....

Literatur.

[1] KRULL, W.: Allgemeine Bewertungstheorie. J. reine angew. Math. **167**, 160–196 (1931). – ... [3] LORENZEN, P.: Über halbgeordnete Gruppen. Math. Z. **52**, 483–526 (1949). – [4] LORENZEN, P.: Teilbarkeitstheorie in Bereichen. Math. Z. **55**, 269–275 (1952). – [5] LORENZEN, P.: Algebraische und logistische Untersuchungen über freie Verbände. J. Symb. Log. **16**, 81–106 (1951).

9 A letter from Krull to Scholz from 1953: the well-ordering theorem

Extract

We translate an extract from the letter that Krull sent to Scholz on 18 April 1953 (Heinrich Scholz Archive at University and State Library of Münster), edited on [page 244](#).

In working with the uncountable, in particular with the well-ordering theorem, I always had the feeling that one uses fictions there that need to be replaced some day by more reasonable concepts. But I was not getting upset over it, because I was convinced that in a careful application of the common “fictions”, nothing false comes out, and because I was firmly counting on the man who would some day put all in order. Lorenzen has now found according to my conviction the right way

Well-ordering arguments and constructions

In his articles, Lorenzen uses well-ordering arguments in several places:

- in [Lorenzen 1939](#) for the proof of Satz 4 (spelled out in our comment on the proof of Theorem 12 on [page 153](#));
- in [Lorenzen 1950](#) for the proof of Satz 24 (stated in the introduction for the case of integral domains, see [page 163](#) and the translation on [page 160](#)); for the proof of Satz 13 and of Satz 1 in Teil II;
- in [Lorenzen 1952](#) for the proof of his lemma for Theorem 1, a version of [Lorenzen 1950](#), Satz 24; for the proof of Satz 3, a version of [Lorenzen 1950](#), Satz 13.
- However, no well-ordering argument appears in [Lorenzen 1953](#). Three kinds of uses may be distinguished:

- [Lorenzen 1939](#), Satz 4: Zorn's lemma is used in order to obtain a maximal prime ideal.

- [Lorenzen 1950](#), Satz 24; [Lorenzen 1952](#), lemma to Theorem 1: a "more reasonable concept", which amounts to behaving as if the domain were linearly preordered, is introduced to replace the "fiction" of valuations.

- [Lorenzen 1950](#), Satz 13; [Lorenzen 1952](#), Satz 3: Zorn's lemma is used to obtain linear preorders. These are "fictions", which are replaced by the "more reasonable concept" of an ℓ -group, in which one may compute as if it were linearly preordered.

We can retrace Lorenzen's position w.r.t. well-ordering arguments through his use of the word *construction* and related words. Let us gather the relevant passages.

1. In Lorenzen's correspondence edited in the next chapter, these words appear only in his letter to Krull, dated 25 April 1944 ([page 230](#)), in which he provides a detailed description of his habilitation, and in his last two letters to Hasse, dated July and September 1963.

2. In the introduction to [Lorenzen 1950](#), he writes the following (see [page 162](#)):

How can a preordered group be embedded into a lattice-preordered group – assuming that such an embedding is possible?

.....

How can the distinguished brauchbar¹ system of ideals of a preordered group G be constructed – assuming that it actually exists?

We thus assume that the preorder of G is representable as a conjunction of allowable linear preorders of G . But we do not want to use the knowledge of these linear preorders, because the allowable linear preorders are just what we want to determine by dint of the system of ideals.

In arithmetic, this construction is provided by the Prüferian concept of integral dependence on an ideal $\mathfrak{a}$ of the given integral domain I .

3. After presenting his "new construction", he adds the following (see [page 164](#)):

The proof is so easy that it may be carried out in arbitrary preordered groups and here provides a construction of the distinguished brauchbar system of ideals (assuming that it exists), and also answers the following question:

When is the preorder of a preordered group G representable as a conjunction of allowable preorders of G ?

4. After having proved Satz 13, he makes the following comment (see [page 167](#)):

¹ In Lorenzen's approach, the distinguished brauchbar system of ideals is the system of $r_{\mathfrak{a}}$ -ideals.

The significance of this characterisation lies in the fact that, in general, the linear preorders of a group can be constructed only with well-ordering arguments – whereas the superlattice-preordered groups can also be constructed without a well-ordering, by means of the concept of ideal.

5. He repeats this a few pages later (see [page 168](#)):

Systems of ideals are introduced in order to make possible by their aid the embedding of a principal group G into a regular lattice-preordered group constructively, without use of the linear preorders of G .

6. Satz 24 is accompanied by the following comment (see [page 170](#)):

The significance of this theorem lies in the fact that it is now possible to state, for every r -principal group, a direct construction of the system of r_a -ideals.

7. [Lorenzen 1952](#), 273, uses the following wording, which is the most explicit in the articles studied here:

For ϱ -principal domains B , Theorem 2 provides a “constructive” definition of the domain of ϱ_a -superideals V_{ϱ_a} of B , i.e. a definition without use of the ϱ -allowable linear preorders of B .

8. Finally, [Lorenzen 1953](#) uses the following formulation (see [page 174](#)):

... one has to construct, for an integrally closed integral domain, either an intersection representation through valuations or a lattice-preordered supergroup.

As these passages show, Lorenzen holds that a well-ordering argument provides a construction, but he makes distinctions: such an argument avers *that* something is possible, but not *how*; other strategies have to be developed in order to gain knowledge of the thing over and above its bare existence. He also specifies for each construction whether it relies on a well-ordering argument or not, in which latter case it is “direct”, or “constructive”. This adjective and the adverb “constructively” have a more restricted use than the word “construction” and mean that the well-ordering argument or the “fiction” of a linear preorder have been avoided.

The distinctions he makes show that, like [Krull \(1936\)](#), he thinks that well-ordering arguments provide only the “mere existence” of the thing constructed. He therefore devises new constructions that bypass them: systems of ideals, super-lattice-preordered groups, the right to compute as if everything were linearly preordered. However, we have not found any passage in which he explains the problem as clearly and simply as Krull does, or in which he motivates his work along the lines of Krull’s letter to Scholz.

* * *

Lorenzen’s reshaping of Krull’s Fundamentalsatz for integral domains can be presented as a process in three steps:

1. [Lorenzen 1939](#) generalises Krull's well-ordering argument from integral domains to preordered cancellative monoids; valuation rings become linear r -supermonoids.

2. [Lorenzen 1950](#) and [1952](#) successively generalise the well-ordering argument to preordered noncommutative monoids and to domains, so that valuations correspond to r -allowable linear preorders; the right to compute as if the monoid were linearly preordered is embodied in the relation α_r , which is shown to yield finite approximations of them on the proviso that they exist; Lorenzen describes a direct construction of an embedding into a lattice-preordered group on the proviso that it exists.

3. [Lorenzen 1953](#) provides the construction of the free lattice-preordered group generated by a regular noncommutative monoid *without* this proviso by applying Satz 7 of [Lorenzen 1951](#), nowadays called the *fundamental theorem of entailment relations* (see [Coquand, Lombardi, and Neuwirth 2019](#), § 2B).

Let us state a further step forward, which Lorenzen does not make:

4. The condition of integral closedness for an integral domain consists in the admissibility of the axiom that divisibility is linear for the formal system generated by the integral domain. The condition of r -closedness for a regular noncommutative monoid consists in the admissibility of the axiom that the preorder is linear.

In the articles discussed here, Lorenzen does not question the existence of a thing provided by a well-ordering argument, but the nonconstructive nature of its existence fails to provide the mathematical clarity needed for extending his work to a noncommutative setting.

The three steps made by Lorenzen are thus genuinely motivated by his endeavour to clarify mathematics, as he writes in his letter to Krull dated 6 June 1944 ([page 234](#), partly translated on [page 142](#)), rather than philosophically: viz.,

1. to unveil the order-theoretic nature of the Fundamentalsatz;
2. to devise a counterpart of valuations that works in a noncommutative setting;
3. to bypass valuations by the direct construction of the free lattice-preordered group.

With Step 4 above, dynamical algebra is taking up this process of clarification: see [Lombardi in progress](#).

References

- Clifford, A. H. 1940. "Partially ordered abelian groups." *Annals of Mathematics* (2) 41:465–473. doi:10.2307/1968728
- Coquand, Thierry, Henri Lombardi, and Stefan Neuwirth. 2019. "Lattice-ordered groups generated by an ordered group and regular systems

- of ideals." *Rocky Mountain Journal of Mathematics* 49:1449–1489. doi: 10.1216/rmj-2019-49-5-1449
- . 2020. "Regular entailment relations." In this volume, pages 101–112.
- Coquand, Thierry, and Stefan Neuwirth. 2020. "Lorenzen's proof of consistency for elementary number theory." *History and Philosophy of Logic*. doi:10.1080/01445340.2020.1752034
- Krull, Wolfgang. 1926. "Axiomatische Begründung der allgemeinen Idealtheorie." *Sitzungsberichte der Physikalisch-Medicinischen Societät zu Erlangen* 56–57 (1924–1925), 47–63.
- . 1930. "Idealtheorie in unendlichen algebraischen Zahlkörpern II." *Mathematische Zeitschrift* 31:527–557. <http://eudml.org/doc/168193>
- . 1932. "Allgemeine Bewertungstheorie." *Journal für die reine und angewandte Mathematik* 167:160–196. <http://eudml.org/doc/149803>
- . 1936. "Beiträge zur Arithmetik kommutativer Integritätsbereiche I: Multiplikationsringe, ausgezeichnete Idealsysteme und Kroneckersche Funktionalringe." *Mathematische Zeitschrift* 41:545–577. <http://eudml.org/doc/168685>
- Lombardi, Henri. In progress. "Théories géométriques pour l'algèbre constructive." <http://hlombardi.free.fr/Theories-geometriques.pdf>
- Lorenzen, Paul. 1939. "Abstrakte Begründung der multiplikativen Idealtheorie." *Mathematische Zeitschrift* 45:533–553. <http://eudml.org/doc/168865>
- . 1950. "Über halbgeordnete Gruppen." *Mathematische Zeitschrift* 52:483–526. <http://eudml.org/doc/169131>
- . 1951. "Algebraische und logistische Untersuchungen über freie Verbände." *Journal of Symbolic Logic* 16:81–106. <http://www.jstor.org/stable/2266681>. Translation by Stefan Neuwirth: "Algebraic and logistic investigations on free lattices," <http://arxiv.org/abs/1710.08138>
- . 1952. "Teilbarkeitstheorie in Bereichen." *Mathematische Zeitschrift* 55:269–275. <http://eudml.org/doc/169251>
- . 1953. "Die Erweiterung halbgeordneter Gruppen zu Verbandsguppen." *Mathematische Zeitschrift* 58:15–24. <http://eudml.org/doc/169331>
- Mehrtens, Herbert. 1979. *Die Entstehung der Verbandstheorie*. arbor scientiarum: Beiträge zur Wissenschaftsgeschichte, volume VI in Reihe A: Abhandlungen. Hildesheim: Gerstenberg.
- Prüfer, Heinz. 1932. "Untersuchungen über Teilbarkeitseigenschaften in Körpern." *Journal für die reine und angewandte Mathematik* 168:1–36. <http://eudml.org/doc/149823>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.