

Jarník's Notes of the Lecture Course Allgemeine Idealtheorie by B. L. van der Waerden (Göttingen 1927/1928)

[Illustrations]

In: Jindřich Bečvář (author); Martina Bečvářová (author): Jarník's Notes of the Lecture Course Allgemeine Idealtheorie by B. L. van der Waerden (Göttingen 1927/1928). (English). Praha: Matfyzpress, 2020. pp. I–XXII.

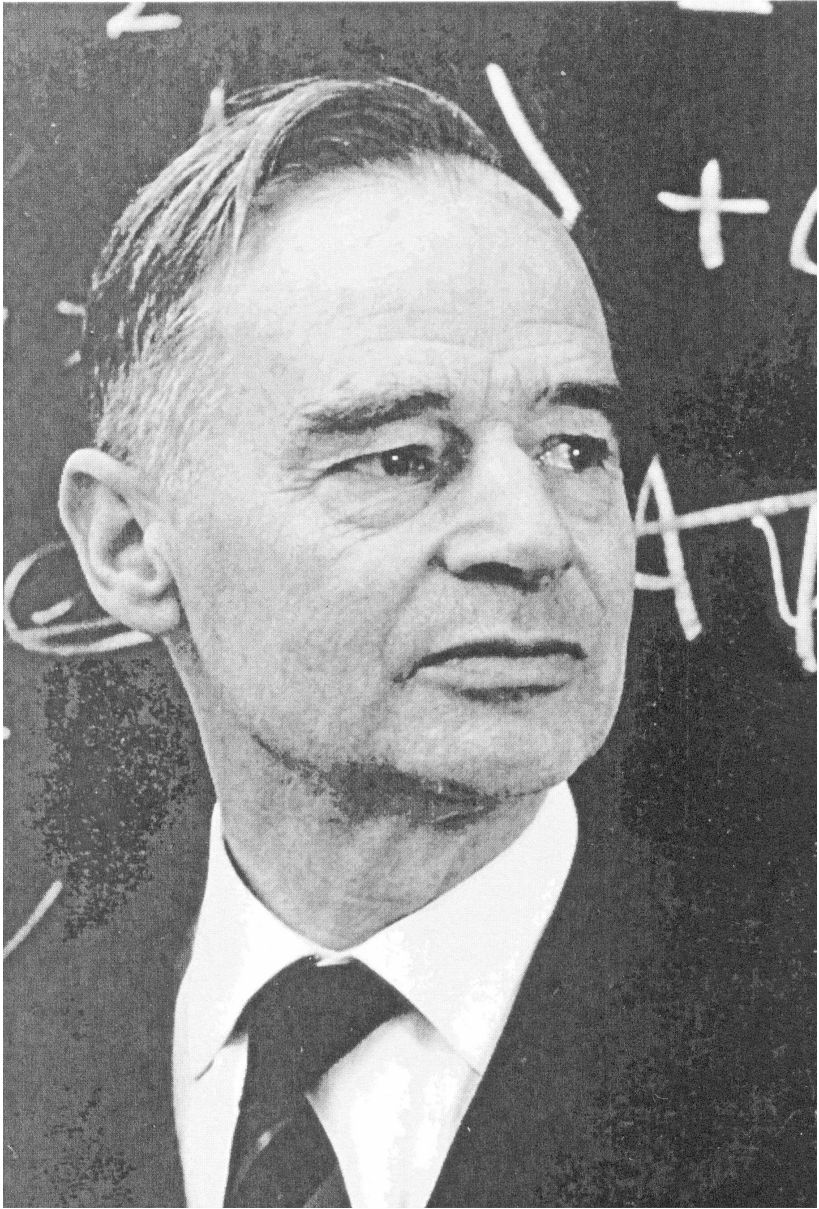
Persistent URL: <http://dml.cz/dmlcz/404386>

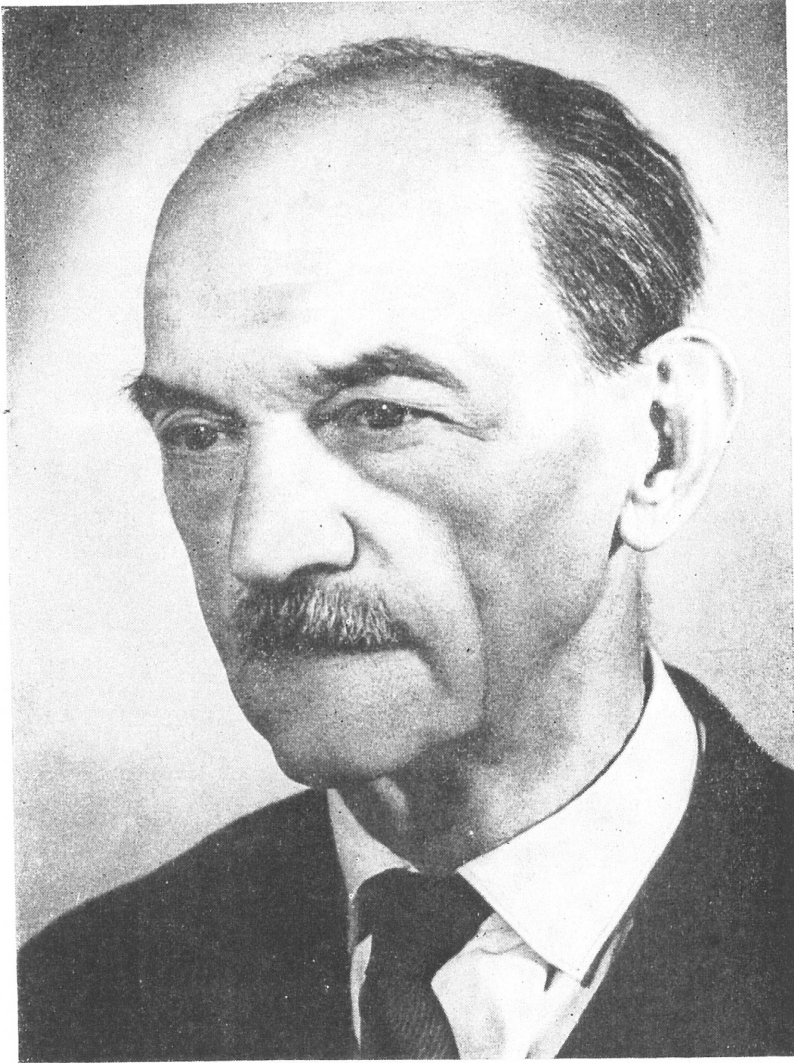
Terms of use:

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>





V. Jarník





MATHEMATISCHE ANNALEN

BEGRÜNDET 1868 DURCH
ALFRED CLEBSCH UND CARL NEUMANN

FORTGEFÜHRT DURCH
FELIX KLEIN

GEGENWÄRTIG HERAUSGEGEBEN
VON

DAVID HILBERT
IN GÖTTINGEN

UNTER MITWIRKUNG VON

OTTO BLUMENTHAL
IN AACHEN

ERICH HECKE
IN HAMBURG

BARTEL L. VAN DER WAERDEN
IN LEIPZIG

109. BAND



BERLIN
VERLAG VON JULIUS SPRINGER
1934

Über die fundamentalen Identitäten der Invariantentheorie.

Von

B. L. van der Waerden in Amsterdam.

Einleitung.

Die Invarianten eines endlichen oder unendlichen Systems von Linearformen in kogredienten und kontragredienten Variablen x und u' kann man nach dem „ersten Fundamentalsatz der symbolischen Methode“ vollständig angeben: sie bauen sich auf aus „Klammerfaktoren“ (Determinanten) und „Linearfaktoren“ $(a' b) = \sum_1^n a'^{(i)} b^{(i)}$. Zwischen diesen bestehen algebraische Identitäten, und es handelt sich im folgenden um die Angabe eines Fundamentalsystems von Identitäten, aus denen sich alle übrigen durch Addition und Multiplikation mit beliebigen Invarianten ableiten lassen.

Um das Problem schärfer zu fassen, bilden wir einen Polynombereich Ω von endlich oder unendlich vielen Unbestimmten, denen später die oben charakterisierten einfachsten Invarianten zugeordnet werden. Diejenigen Polynome aus Ω , die identisch (in den Formenkoeffizienten als Unbestimmte) verschwinden, wenn man für die erstgenannten Unbestimmten diese Invarianten einsetzt, bilden ein Ideal in Ω , und es handelt sich um eine Basis für dieses Ideal¹⁾. Beschränkt man sich auf endlichviele Unbestimmte, so hat das Ideal nach dem Hilbertschen Basissatz eine endliche Basis; die Anzahl der Elemente dieser Basis ist bei wachsender Anzahl der Unbestimmten zwar nicht beschränkt, aber E. Pascal hat bewiesen²⁾,

¹⁾ Diese Auffassung hat E. Noether vertreten (Die Endlichkeit des Systems der ganzzahligen Invarianten binärer Formen, Gött. Nachr. 1919). Sie gestattet eine präzise und einfache Ausdrucksweise.

²⁾ E. Pascal, *Memorie d. R. A. d. Lincei* (4) 5 (1888). Für das binäre Gebiet siehe Gordan-Kerschensteiner, *Vorlesungen über Invariantentheorie II*, S. 132; für das ternäre E. Study, *Methoden zur Theorie der ternären Formen*, Leipzig 1889, S. 75.

MODERNE ALGEBRA

VON

DR. B. L. VAN DER WAERDEN

O. PROFESSOR AN DER UNIVERSITÄT
GRONINGEN

UNTER BENUTZUNG VON VORLESUNGEN

VON

E. ARTIN UND E. NOETHER

ERSTER TEIL



BERLIN
VERLAG VON JULIUS SPRINGER
1930

VII

Moderne Algebra

von

Dr. B. L. van der Waerden

o. Professor der Mathematik an der Universität Leipzig

Unter Benutzung von Vorlesungen von E. Artin und E. Noether

Zweiter Teil

Zweite, verbesserte Auflage

(Die Grundlehren der mathematischen Wissenschaften
in Einzeldarstellungen, Band XXXIV)

VIII, 224 Seiten. 1940. RM 16.50

Inhaltsübersicht:

Eliminationstheorie. Das Resultantensystem für mehrere Polynome in einer Veränderlichen. Allgemeine Eliminationstheorie. Der Hilbertsche Nullstellensatz. Kriterium für die Lösbarkeit eines homogenen Gleichungssystems. Über Tragheitsformen. Die Resultante von n -Formen in n -Variablen. Die u -Resultante und der Satz von Bezout. — **Allgemeine Idealtheorie der kommutativen Ringe.** Basissatz und Teilerketensatz. Produkte und Quotienten von Idealen. Primideale und Primär Ideale. Der allgemeine Zerlegungssatz. Die Eindeutigkeitsätze. Theorie der teilerfremden Ideale. Einarige Ideale. — **Theorie der Polynomideale.** Algebraische Mannigfaltigkeiten. Algebraische Funktionen. Die Nullstellen eines Primideales. Die Dimensionzahl. Die Primär Ideale. Der Noethersche Satz. Zurückführung der mehrdimensionalen Ideale auf nulldimensionale. Ungemischte Ideale. — **Ganze algebraische Größen.** Endliche \mathfrak{K} -Moduln. Ganze Größen in bezug auf einen Ring. Die ganzen Größen eines Körpers. Axiomatische Begründung der klassischen Idealtheorie. Umkehrung und Ergänzung der Ergebnisse. Gebrochene Ideale. Idealtheorie beliebiger ganz-abgeschlossener Integritätsbereiche. Zusammenfassung der Idealtheorie. — **Lineare Algebra.** Moduln. Linearformen. Vektoren. Matrizen. Moduln in bezug auf einen Schiefkörper. Lineare Gleichungen. Moduln in endlichen Ringen. Elementarteiler. Der Hauptsatz über abelsche Gruppen. Darstellungen und Darstellungsmoduln. Normalformen für eine Matrix in einem kommutativen Körper. Elementarteiler und charakteristische Funktionen. Quadratische und Hermitesche Formen. — **Theorie der hyperkomplexen Größen.** Systeme hyperkomplexer Größen. Hyperkomplexe Systeme als Gruppen mit Operatoren. Verallgemeinerung. Nilpotente Ideale. Die volle Reduzibilität der Ringe ohne Radikal. Zweiseitige Zerlegungen und Zentrumserlegung. Der Endomorphismenring eines vollständig reduziblen Moduls. Struktur der vollständig reduziblen Ringe mit Einselement. Das Verhalten der halbeinfachen hyperkomplexen Systeme bei Erweiterung des Grundkörpers. — **Darstellungstheorie der Gruppen und hyperkomplexen Systeme.** Problemstellung. Darstellung hyperkomplexer Systeme. Die Darstellungen des Zentrums. Spuren und Charaktere. Darstellung abelscher Gruppen. Darstellungen endlicher Gruppen. Gruppencharaktere. Die Darstellungen der symmetrischen Gruppen. Halbgruppen von linearen Transformationen und ihr Verhalten bei Erweiterung des Grundkörpers. Anwendungen der Darstellungstheorie auf die Theorie der Schiefkörper. Die Brauerschen Algebrenklassen. Charakterisierung der Zerfallungskörper. Verschränkte Produkte; Faktorensysteme. Sachverzeichnis.

S P R I N G E R - V E R L A G · B E R L I N

Springer-Verlag in Berlin W9. — Verantwortlich für den Anzeigenteil: Albert Meyer, Berlin-Steglitz, Kuhlbornweg 5. — Druck von Friedr. Vieweg & Sohn in Braunschweig
Printed in Germany

Pl. 3.

8. V. Jannik, Göttingen, Prüfl. Nr. 28.

Von der Waerden
Allgemeine Idealtheorie

Göttingen, Wintersem. 1917-18.
§ 1. Einleitung.

4.
XI.

Man ist auf verschiedenen Wegen zu dem
Idealbegriff gekommen. Erstens hat es sich
ergeigt, dass in algebraischen Zahlkörpern
die Zerlegung in unzerlegbare Faktoren
nicht eindeutig ist. z. B. im Körper $\mathbb{Q}(\sqrt{5})$;
immer) hier sind die ganzen Zahlen die
Zahlen $a + b\sqrt{5}$, a, b ganz rational. Es ist

$9 = 3 \cdot 3 = (2 - \sqrt{5})(2 + \sqrt{5})$, und doch
sind $3, 2 - \sqrt{5}, 2 + \sqrt{5}$ unzerlegbar. Denn
eine ganze Zahl α dieses Körpers $\alpha = a + b\sqrt{5}$
hat ihre Norm $N\alpha = |a|^2 = a^2 + 5b^2$, wäre

man 3 zerlegbar, $3 = \alpha\beta$, so müsste

$9 = N\beta = N\alpha N\beta$ sein, also entweder

$N\alpha = 3, N\beta = 3$, was aber nach (1) unmöglich
ist, oder $N\alpha = 1, N\beta = 9$; dann wäre

aber notwendig $\alpha = \pm 1$, was keine eigentliche
Zerlegung ist. Also unzerlegbar
ist auch $2 \pm \sqrt{5}$ unzerlegbar.

Um die Eindeutigkeit hier wiederherzustellen
hat Hurwitz sog. "starke Teiler eingeführt",
aber erst "bedeutend" hat seinen Begriff
präzisiert und für allgemeine Zahlkörper
die Theorie durchgeführt.

Der Begriff des Ideals \mathfrak{a}^n ist aber auch auf algebraische Funktionen auszuwickeln.

Es sei $P(x)$ der Körper der rationalen Funktionen von x über \mathbb{C} , $P[x]$ Polynomring $P[x, y, z, \dots, \mathfrak{f}]$ sei ein Erweiterungskörper, in welchem $y, z, \dots, \mathfrak{f}$ algebraische Funktionen sind.

Man definiert ganz algebraische Funktionen und Ideale und findet eine eindeutige Zerlegbarkeit von Idealen in Primideale. Die Primideale entsprechen dann eindeutig den Punkten der Riemannschen Fläche.

Ein Primideal wird in der allgemeinen Theorie durch Ungerlegbarkeit durch folgende Eigenschaft charakterisiert: Wenn $\mathfrak{a} \cdot \mathfrak{b}$ durch das Primideal \mathfrak{p} teilbar ist, so ist entweder \mathfrak{a} oder \mathfrak{b} durch \mathfrak{p} teilbar.

Einem vollen Ausgangspunkt b. B. ist die Theorie der hyperkomplexen Zahlen $\alpha = a_0 + a_1 \epsilon + a_2 \epsilon^2 + \dots + a_{r-1} \epsilon^{r-1}$ wo ϵ die r ten Einheitspotenzen des r -ten Kreiskörpers sind. (Frobenius, E. Noether).

Wenn eine Menge M so beschaffen ist, dass mit α, β auch $\alpha \pm \beta, \alpha \beta$ zu M gehören, heißt M ein Ring. (Freilich kann z. B. bei den hyperkomplexen Zahlen die Kommutativität der Multiplikation fehlen.)

Ein System von hyperal. Zahlen heißt ein Ideal, wenn mit α, β auch $\alpha \pm \beta, \alpha \beta, \alpha \gamma$ (γ beliebig) zu ihm gehören. — freilich braucht er nicht kommutativ zu sein.

Wir werden nur jedoch hauptsächlich mit der kommutativen Theorie beschäftigen.

Die allgemeine Idealtheorie soll nun alle diese Standpunkte umfassen.

Literatur 1.) algebraische Zahlkörper:

Deuring, Algebraische Zahlkörper in Gründl. Vorlesungen über Zahlentheorie (Hilbert, Zahltheorie. Leipzig, 1902).

2.) Modulsysteme: Modular Systems, F. S. Macaulay, Camb. Tracts 19.

V. A. Waerden, Multiplikativtheorie, Math. Ann. 90.

3.) Funktorienkörper
Redekind-Ring, Algeb. Funct. einer Veränderlichen, Bell. J. 92.

4.) Allgemeine Theorie:

E. Noether, Idealtheorie in Ringbereichen, Math. Ann. 83

Abstrakter Aufbau ...
Math. Ann. 96.

§ 3. Ringe.

Zählmenge hat zuerst Helmut Hasse betrachtet, Math. Ann. 83, abstrakt bei E. Noether, höherer Algebra I, einfacher bei Hasse.

Ein Ring ist eine Menge von Elementen, in welcher zu a, b aus der Menge $a+b$ und ab definiert sind, alle folgenden Voraussetzungen genügen:

I 1.) $(a+b)+c = a+(b+c)$

2.) $a+b = b+a$

3.) zu jedem a, b existiert $a+x=b$ lösbar

II 1.) $a(bc) = (ab)c$

2.) $ab = ba$

III 1.) $a(b+c) = ab+ac$

2.) $(b+c)a = ba+ca$

Es werden auch Ringe betrachtet, wo II 2.) nicht gilt (nichtkommutative Ringe). Wir beschreiben uns aber auf kommutative Ringe, wo freilich III 2. dann überflüssig ist.

Der Ring bildet also eine Abelsche Gruppe gegenüber Addition; es gibt also eine 0 mit $a+0=a$, ein $-a$ zu jedem a mit $a+(-a)=0$. Dann gibt es genau eine Lösung $a-x=b+a-a=b$

von $b+x=a$. Dann ist weiter

$$(n+m)a = na+ma, \quad n(a+b) = na+nb,$$

$(nm)a = n \cdot (ma)$ (m, n ganze rationale Zahlen), das ist eine direkte Folge unserer Gruppenergebnisse.

Im Prodnkt darf man ausklammern und abkürzen verfahren, endlich Potenzieren mit Potenzen, Exponenten definieren (denn dies folgte im § 2 nur aus den assoziativen und kommutativen Gesetzen): $a^1 = a, a^{n+1} = a^n \cdot a$, nur aus den assoziativen und kommutativen Gesetzen: $a^n a^m = a^{n+m}, (a^n)^m = a^{nm}$,

$$a^n a = a^{n+1}, \quad (a^n)^m = a^{nm},$$

$$(ab)^n = a^n b^n.$$

Auch für Differenzen gilt freilich das distributive Gesetz

$$a(b-c) = ab-ac; \text{ denn}$$

$$\text{es ist } ac + a(b-c) = a(c+b-c) = ab.$$

Weiter erweitert man sofort die Gültigkeit des distributiven Gesetzes auch für Summen und Differenzen mit mehreren Summanden:

$$a(b \pm c \pm d \dots) = ab \pm ac \pm ad \dots$$

auch so:

$$(a+b)(c+d) = ac+bc+ad+bd.$$

Kurz: man darf in der üblichen Weise addieren, subtrahieren und multiplizieren.

Man kann es so aussprechen:
 "Maximale" (im mengentheoretischen Sinn)
 Ideale in \mathcal{O} (mit Einheitsnorm) sind
 Primideale und ihr Restklassenring
 ist ein Körper.

§ 7. Idealtheorie der euklidischen Ringe.

Ein euklidischer Ring ist ein Ring ohne Nullteiler und mit dem Einheitsnorm, wo jedes Ideal Hauptideal ist.

L.B. 1.) Ring der ganzen rationalen Zahlen
 2.) Polynombereich $\Sigma[X]$, wo Σ Körper.

3.) Der Ring der ganzen Ganzzahligen Zahlen $a+bi$ (a, b ganz rational)
Beweis zu 3.) Wenn $\alpha = a+bi, \beta = c+di$
 $\beta \alpha$ (a, b, c, d ganz nat.), so kann man

zwei Ganzzahlige Zahlen ϵ, ρ so finden,
 dass $\alpha = \epsilon\beta + \rho, N(\rho) < N(\beta)$
 Dabei ist $N(\alpha) = |\alpha|^2 = a^2 + b^2$.

Denn: $\frac{\alpha}{\beta} = g+ih, g, h$ rational.
 Ich finde die zu g, h nächsten ganzen nat.
 Zahlen ϵ, f :

$$\frac{\alpha}{\beta} = \epsilon + if + r + i's, \text{ wo } |r| \leq \frac{1}{2}, |s| \leq \frac{1}{2}$$

$$= \epsilon + r + i's \quad (\epsilon \text{ ganze g. Zahl})$$

$$\alpha = \epsilon\beta + \rho, \text{ wo}$$

$$N(\rho) = N(\beta \cdot (r + i's)) \leq N(\beta) \cdot \frac{1}{2} < N(\beta)$$

Man es sei α ein Ideal aus dem Ring der ganzen Ganzzahligen Zahlen, nicht Nullideal. Ich greife eine von seinen Zahlen mit möglichst kleiner positiver Norm β .
 $\epsilon\beta$ sei α diese Zahl; ρ eine andere Zahl von α ; dann gilt es ϵ, ρ (ganz)
 so, dass $\beta = \epsilon\alpha + \rho, N(\rho) < N(\alpha)$;
 weil $\rho \in \alpha$, so muss nach Voraussetzung

Weil die Restklassen ~~von~~^{Prin} bei Primzahlen keine Nullteiler hat, so folgt: falls p Primzahl,
 $ab \equiv 0 \pmod{p}$, so ist entweder
 $a \equiv 0 \pmod{p}$ oder $b \equiv 0 \pmod{p}$.

28
XI

Jedem Element n eines euklidischen Ringes entspricht ein Ideal, nämlich das Ideal (n) , und zwar entspricht denjenigen Zahlen, die sich nur aus Einheiten untersuchen, dasselbe Ideal; umgekehrt, aus $(m) = (n)$ folgt, dass m ein Teiler von n ist und umgekehrt, also $m = \epsilon n$, wo ϵ Einheit; den Primzahlen entsprechen Primideale, und zwar entsprechende Zahlen entsprechen keine Primideale, denn wenn $a = \prod_{i=1}^r p_i$ (keine Einheit) so ist

Wenn \sum die "Hörsper", so sind z. B. die Primzahlen von $\sum [x]$ die irreduziblen Polynome. Cauchy hat über

die komplexen Zahlen durch den Restklassenring mod x^2+1 in dem Ring der Polynome mit reellen Koeffizienten eingeführt.

Satz. Jedes Element eines Euklidischen Ringes lässt sich eindeutig in die Form bringen $a = \epsilon p_1 p_2 \dots p_r$,
 ϵ Einheit

wo p_1, p_2, \dots, p_r keine Einheiten und Primzahlen sind. Das soll bedeuten: in jeder analogen Zerlegung $a = \epsilon' p_1' p_2' \dots p_r'$ ist $p_i' = \epsilon_i p_i$ und ϵ_i auf Abordnung $p_i' = p_i \cdot \epsilon_i$, ϵ_i Einheit.

Beweis: 1.) Endlichkeit beweist man so:

Für $r=1$ (also a Primzahl) ist alles bewiesen. Es sei also die Endlichkeit für diejenigen Zahlen bewiesen, die sich in weniger als r Primfaktoren zerlegen lassen. Dann teilt p_1 das Produkt $p_1' \dots p_r'$, also sind p_1 eine Faktor; z. B. $p_1 = \epsilon_1 p_1'$; weil p_1 Primzahl, so ist $p_1' = \epsilon_1 p_1$, Einheit. Durch Kürzen:

$\epsilon p_2 p_3 \dots p_r = \epsilon_1' p_2' \dots p_r'$; und man ist für diese Zahlen $(r-1$ statt r) schon alles bewiesen.

Wir haben noch zu beweisen: Wenn $f(x)$ in $S[x]$ irreduzibel ist (also auch Einheitsform), so bleibt es in $\Sigma[x]$ irreduzibel - denn eine Zerlegung in $\Sigma[x]$ w"re eine Zerlegung in $S[x]$ auszusprechen.

Folgerung: Wenn Σ ein Körper, so folgt durch Induktion sofort aus letztem Satz:

In $\Sigma[x_1, x_2, \dots, x_n]$ gilt die eindeutige Zerlegung in Primfaktoren, wenn Σ ein Körper,

2
XII

Kapitel II. Körpertheorie.

§ 1. Primkörper.

Ein Körper, der keinen echten Unterkörper enthält, heißt Primkörper.

Satz: Jeder Körper \mathbb{A} enthält einen und nur einen Primkörper \mathbb{P} .

Beweis: Wir nehmen das Einheitselement e von \mathbb{A} und alle Elemente ne (n ganz rational), die bilden einen Ring \mathbb{P} , denn $ne + me = (n+m)e$, $ne me = nme = nme$.

Der Quotientenkörper \mathbb{P} von \mathbb{P} heißt das gewöhnliche: nun jeder Faktorkörper von \mathbb{A} muss e , also auch ne und die Brüche $\frac{ne}{me}$ enthalten, muss also \mathbb{P} enthalten. \mathbb{P} ist der Durchschnitt von allen Unterkörpern von \mathbb{A} .

Es genügt, die Struktur von \mathbb{P} zu beschreiben. \mathbb{P} wird durch die Zuordnung

$$n \mapsto ne$$

Nichtalgebraische Erweiterungen keine transzendente Erweiterungen

Satz: Wenn Σ eine endliche Erweiterung von K ,

Λ eine endliche Erweiterung von Σ ,

so ist auch Λ eine endliche Erweiterung von K .

Λ eine endliche Erweiterung von K .

Und es gilt $(\Lambda/K) = (\Lambda/\Sigma)(\Sigma/K)$.

Beweis: Es sei u_1, \dots, u_r eine

Basis von Σ über K , v_1, \dots, v_s eine

Basis von Λ über Σ . Dann ist, wenn

w aus Λ :

$$w = \sum \alpha_i v_i \quad (\alpha_i \text{ aus } \Sigma)$$

$$= \sum \sum \beta_{ik} u_k v_i \quad (\beta_{ik} \text{ aus } K)$$

Die $u_k v_i$ sind linear unabh. ~~hängig~~ ber. K , denn aus $(\beta_{ik} \text{ aus } K)$

$$\sum \beta_{ik} u_k v_i = 0 \quad \text{folgt}$$

$$\sum_K \beta_{ik} u_k = 0, \quad \text{also } \beta_{ik} = 0,$$

die r_s Zahlen $u_k v_i$ bilden also eine math. lineare Basis von Λ über K , w.z.b.w.

9 XII Es sei $K \subseteq \Sigma \subseteq \Lambda$; Λ algebraisch über Σ , Σ algebraisch über K . Behauptung: Λ ist algebraisch über K .

Beweis: Es sei $w \in \Lambda$; dann ist

$$w^{m_1} + \sigma_{n-1} w^{m_1-1} + \dots + \sigma_0 = 0,$$

wo $\sigma_i \in \Sigma$. Der Körper $K(\sigma_0)$ ist

einfache alg. Erw. von K , also endliche

Erweiterung; $K(\sigma_0, \sigma_1)$ ist eine ~~endliche~~

einfache alg., also endliche Erweiterung

von $K(\sigma_0)$, also nach dem vorangehenden

eine endliche Erweiterung von K ; a.s.w.

Schließlich ist $K(\sigma_0, \sigma_1, \dots, \sigma_{n-1})$ eine endliche

Erweiterung von K ; $K(\sigma_0, \sigma_1, \dots, \sigma_{n-1}, w)$ eine

einfache algbr., also endliche Erweiterung

von $K(\sigma_0, \dots, \sigma_{n-1})$, also eine endliche

Erweiterung von K ; daher ist w

algebraisch über K ; w.z.b.w.

§ 6. Algebraisch abgeschlossene Körper.

Ein Körper heißt algebraisch abgeschlossen, wenn jedes Polynom mit Koeffizienten aus \mathbb{A} in \mathbb{A} vollständig zerfällt.

\mathbb{K} sei ein Körper, \mathbb{A} seine algebraische Erweiterung: wenn in \mathbb{A} alle Polynome aus $\mathbb{K}[X]$ vollständig zerfallen, so ist \mathbb{A} algebraisch abgeschlossen.

Beweis: es sei f algebraisch bes. \mathbb{A} ; dann ist auch f algebraisch bes. \mathbb{K} , also liegt f in \mathbb{A} , so z. B. w.

Wenn \mathbb{A} nur abzählbar viele Elemente hat (was in den Anwendungen meistens der Fall ist), so kann man eine algebraische Erweiterung \mathbb{A} von \mathbb{K} konstruieren, die algebraisch abgeschlossen ist.

Beweis: $f_1(x), f_2(x), \dots$ seien alle (abzählbar viele) Polynome aus $\mathbb{K}[X]$; sie adjungiere zuerst die Nullstellen von $f_1(x)$, dann diejenigen von $f_2(x)$ u. s. w.

Die Vereinigung aller sukzessiven Erweiterungskörper $\mathbb{K}_1, \mathbb{K}_2, \mathbb{K}_3, \dots$ ist eine algebraische Erweiterung von \mathbb{K} , und jedes Polynom $f_n(x)$ zerfällt in \mathbb{K}_n , also unsonst in \mathbb{A} .

Es sei \mathbb{A} eine andere algebraische Erweiterung von \mathbb{K} , die algebraisch abgeschlossen ist. In \mathbb{A} zerfallen wieder alle $f_1(x), f_2(x), \dots$ vollständig; ich habe erst \mathbb{K}_1 durch Adjunktion der Wurzeln in \mathbb{A} von $f_1(x)$; dann adjungiere ich die Wurzeln in \mathbb{A} von $f_2(x)$; so entsteht \mathbb{K}_2 u. s. w. Es ist $\mathbb{K} \supseteq \mathbb{K}_1, \mathbb{K}_2 \supseteq \mathbb{K}_3, \dots$

und zwar ist jeder folgende Term nur als Fortsetzung des vorangehenden bestimmen. Die Vereinigungsmenge ist in \mathbb{A} enthalten und enthält alle \mathbb{K}_n ; \mathbb{A} ist algebraisch abgeschlossen, also ist $\mathbb{A} = \mathbb{A}$; also ist $\mathbb{A} \cong \mathbb{A}(\mathbb{K})$.

Der algebraische Körper über \mathbb{K} , der algebraisch abgeschlossen ist, hat also einen bestimmten Typus bez. \mathbb{K} .

ist $m_i = \binom{k_i}{k_{i-1}}$ oder $m_i < \binom{k_i}{k_{i-1}}$,
 si wachsend a_i separabel ist oder nicht.
 Multiplikation oder m_i gibt die
 Gesamtzahl der Automorphismen.

Folger: Die Eigenschaft der Separabelheit aller
 k_i im Bezug auf k_{i-1} ist unabhängig vom Wahl
 und Reihenfolge der Erweiterungen a_i . Galois-
 ve Automorphismen von separablen Körpern existieren
 einem Körper, in dem alle größeren separabel
 sind (Separabler Erweiterungskörper).
 ist k_p Galois, also mit allen Körpern
 den Körpern in einem beliebigen Erweiterungskörper
 separabel (da er zu jeder Größe auch
 alle Körpergrade enthält, so hat k_p sowohl
 Automorphismen, welche die Elemente von
 K fest lassen, wie der Grad (k_p/k)
 beträgt. (Galoische Gruppe). Diese Automor-
 phismen führen jedes Element in alle Körper-
 grade über.

Ein Element eines separablen Galois-
 Körpers, das mit allen seinen
 Körpergraden identisch ist, liegt im
 Grundkörper K .

Kapitel III Idealtheorie in Polynom- berechnen.

Literatur: S. unter Macaulay und v.d.
 Waerden.

§ 18 Dedekindsche Basisätze.

Man in einem Ring R jedes Ideal eine end-
 liche Basis hat, so sagt man: in R gilt
 die Basisätze. In Körpern, im Endlichkeits-
 Ringen gilt der Basisätze.

Wenn in R der Basisätze gilt, und wenn R
 ein Einheitsideal besitzt, so gilt in
 $R[x]$ der Basisätze.

Bem.: Sei A ein Ideal ~~von~~ in $R[x]$, und A_0
 die Gesamtheit der Koeffizienten der
 höchsten Potenzen von x in allen Polynomen
 von A . A_0 ist ein Ideal, hat also eine
 endliche Basis (a_1, \dots, a_n) , gehörig zu Poly-
 nomen (f_1, \dots, f_n) . Ist n der höchste

Grad der Polynome f_i , so kann man
 mittels (f_1, \dots, f_n) den Grad eines jeden Poly-
 noms einschätzen h_i auf $n-1$. Sei m die
 das Max der Koeffizienten von x^{m-1}
 in allen Polynomen vom Grad $\leq n-1$.

2. Heft.

Von der Wurden: Allgemeine Idealtheorie
Höfster § 10. Nullteilertheorie der Primideale 1927-28

1.) Sei $I = K(x_1, x_2, \dots, x_n)$ ein Erweiterungs-
körper von K , so bilden diejenigen Polynome
 f aus $R = K[x_1, x_2, \dots, x_n]$, für die $f(x_1, x_2, \dots, x_n) = 0$
ist, ein Primideal
Beweis: klar.

2.) Ist P ein Primideal, so ist I dem
Restklassenkörper des Restklassenringes R/P
isomorph, und zwar entsprechen den Rest-
klassen von x_1, \dots, x_n die Elemente ξ_1, \dots, ξ_n .

Beweis: Durch $f(x_1, x_2, \dots, x_n) \rightarrow f(\xi_1, \xi_2, \dots, \xi_n)$
wird R auf $K[\xi_1, \xi_2, \dots, \xi_n]$ surjektiv
abgebildet. Also ist $K[\xi_1, \dots, \xi_n]$ isomorph
dem Restklassenring von R nach dem Ideal
der Polynome f , denen die Null zugeordnet
wird. Jedes Ideal ist aber P . Dann muß es
aber auch die Restklassenring isomorph
sein.

3.) In jedem Primideal $P \neq R$ gibt es einen
Körper $I = K(\xi_1, \dots, \xi_n)$ so dass P besteht
aus allen Polynomen f aus R , für die
 $f(\xi_1, \xi_2, \dots, \xi_n) = 0$.

Beweis: Den Polynom f aus R ordnen

Satz

- (1) (x^2) Enthalten die Ebene $x=0$ zumindest
- (2) (x^2, xy, y^2) Haben mindestens einen Doppelpunkt in allen Punkten der Geraden $x=y=0$.
- (3) $(x^2, xy, y^2, xz, yz, z^2)$ Haben mindestens einen Doppelpunkt in Umgebung
- (4) (x^2, y^2) Berühren die Ebene $y=0$ längs der Geraden $x=y=0$.
- (5) $(x^2, xy, y^2, xz-y)$ Berühren die Fläche $xz-y=0$ längs der Geraden $x=y=0$.
- (6) (x^2, y^2) Haben mindestens einen Doppelpunkt in allen Punkten der Geraden $x=y=0$, während im Fall eines Doppelpunktes der Berührungsebene besteht aus 2 Ebenen, harmonisch zu den Ebenen $x=0, y=0$.
- (7) (x, y, z) Enthalten die Geraden $x=y=0$ und $x=z=0$.

Eigenschaft der Hyperflächen

- (8) (x, y^2, yz) Enthalten die Gerade $x=y=0$ und berühren die Ebene $x=0$ im Punkt $x=y=z=0$
- (9) (x^2, yz) Berühren die Ebene $y=0, z=0$ nach der Geraden $x=y=0, x=z=0$.

Alle diese Ideale erscheinen definiert durch gewisse Relationen zwischen den Hyperflächen (Polynomen) der Ideale und gewissen unveränderlichen Mannigfaltigkeiten.

Abhängig davon: eine primäre Eigenschaft eines Polynoms f in Bezug auf eine unveränderliche Mannigf. M ist eine totale Relation zwischen f und M , die 1.) erhalten bleibt, wenn auf solche Faktoren verzichtet werden, die M nicht enthalten

- 2.) nur dann erfüllt ist, wenn f die Mann. M enthält
- 3.) für jede hinreichend hohe Potenz $L = g^k$ erfüllt ist, sobald g die Mannigfaltigkeit M enthält.

11) Kap V. Quotient algebraische
Gruppen.

Literatur: 2 Bücher, Abstrakter
Algebra ..., Math. Annalen 96 (1926).

$\{ \}$ 2 Moduln in Bezug auf einen Ring.
Ein Modul über eine additiv geschlossene
Abelsche Gruppe M (z.B.). M ist ein Modul
in Multiplikation mit R gegeben, und
eine Multiplikation $r \cdot m = m'$ der Ele-
mente von M mit den Elementen von R
besteht, mit den Eigenschaften

- 1.) $r \cdot m$ ist Element von M
- 2.) $r(m_1 + m_2) = r m_1 + r m_2$
- 3.) $(r \cdot s) \cdot m = r \cdot (s \cdot m)$
- 4.) $(r+s) \cdot m = r \cdot m + s \cdot m$

so nennt man M einen R -Modul.
Untermodul eines R -Moduls sind Unter-
gruppen, die wieder R -Moduln sind,
also die mit m auch $r \cdot m$ enthalten,
wo $r \in R$, und mit m_1 und m_2
auch $m_1 - m_2$. Man kann mit Kongru-

wenn man einem Modul rechnen. $N=0(M)$
heißt: N Untermodul von M (M Teiler,
 N Vielfaches).

Beispiele: Alle Ringe, die R umfassen,
sind R -Moduln. Die Ideale in R sind
 R -Moduln.

Ein R -Modul heißt endlich, wenn er
eine endliche Basis m_1, \dots, m_s besitzt,
so dass alle Elemente von M sich
als Summen $\sum_{i=1}^s r_i m_i + \sum_{j=1}^t n_j m_j$
schreiben lassen.

Der Teilerkettensatz für einen R -Modul
 M besagt die Umgekehrtheit eines unendli-
chen Ketten von Untermoduln

$$M_1 \subset M_2 \subset \dots$$

ist insbesondere $M=R$, so hat man den
Teilerkettensatz für Ideale.

Wie früher ist der Teilerkettensatz äquivalent
mit dem Brauer Satz: Jeder Untermodul
von M (und insbesondere M selbst)
ist endlich.

$$\begin{pmatrix} a & r_1 & \dots & r_n \\ 0 & r_1 - a & \dots & r_m \\ \vdots & \vdots & \ddots & \vdots \\ 0 & r_{n-1} & \dots & r_{m-1} - a \end{pmatrix} = 0.$$

Folgerung 1.) Summe und Produkt zweier ganzen Größen b, c sind wieder ganz.
 Beweis: Sei $b = \sum_{i=1}^k r_i$, $c = \sum_{j=1}^l s_j$

und $bc = \sum_{i=1}^k \sum_{j=1}^l r_i s_j$.

Man wähle für g_1, \dots, g_n alle Produkte $b_i c_j$ ($i=1, \dots, k, j=1, \dots, l$), und $a = b+c$ bzw. $a = b \cdot c$. Dann ist das Kroneckersymbol erfüllt.

2.) Eine Wurzel einer Gleichung $a^k + b_1 a^{k-1} + \dots + b_k = 0$

ist ganz, wenn die Koeffizienten b_1, b_2, \dots, b_k es sind.

Beweis: Sei $b_i = \sum_{j=1}^{k_i} r_{ij}$ ($i=1, \dots, k$).

Man nehme für r_1, \dots, r_n alle Potenzenprodukte $a^i b_1^{j_1} \dots b_k^{j_k}$ ($i, j_1, \dots, j_k \geq 0, \dots$

Dann ist das Kroneckersymbol erfüllt ($k < k_1$).

Beweis: Sind alle Elemente von S ganz in Bezug auf R , und a in Bezug auf S , so auch a in Bezug auf R .

Ein Integralbereich R heißt ganz-abgeschlossen in Kroneckersymbol, wenn jede Potenz aus P , die ganz in Bezug auf R ist, in R liegt.

Gilt in R die eintellige Faktorisierung, so ist R ganz-abgeschlossen.

Beweis: Sei $a^k + r_1 a^{k-1} + \dots + r_k = 0$.

Wäre $a = \frac{r}{s}$ (unvermeidbar), so

$$r^k + r_1 s r^{k-1} + \dots + r_k s^k = 0$$

$$r^k \equiv 0 \pmod{s},$$

also haben r und s doch einen Faktor gemeinsam, aber s ist Einheit, also $a \in R$.

