Algebra Es sei M eine Menge. Eine Abbildung $M \times M \to M$ nennen wir auch eine Operation. Mengen mit Operationen sind uns bekannt: Gruppen, Körper, Vektorräume.

Definition 1 *Ein Ring $(R, +, \cdot)$ ist eine Menge mit zwei Operationen $+$ und $\cdot$.*

Die Operation $+$ ist assoziativ, kommutativ, besitzt ein neutrales Element 0_R, und alle Elemente besitzen inverse Elemente. (d.h. $(R, +)$ ist eine abelsche Gruppe).

Die Operation $\cdot$ ist assoziativ.

Für alle $a, b, c \in R$ gilt:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Die Axiome implizieren, dass

$$0_R \cdot a = 0_R, \quad a \cdot 0_R = 0_R.$$

Wenn die Operation $\cdot$ auch kommutativ ist, so heißt R kommutativ. Wenn diese Operation ein neutrales Element 1_R besitzt, so heißt R ein *unitärer Ring.*

Wenn wir mehrere Ringe betrachten, so bezeichnen wir die Operationen mit $+ = +_R$ und $\cdot = \cdot_R$.

Definition 2 *Es seien R und S Ringe. Eine mengentheoretische Abbildung $\phi : R \to S$ heißt ein Ringhomomorphismus, wenn gilt:*

1. $\phi(0_R) = 0_S$.
2. $\phi(a +_R b) = \phi(a) +_S \phi(b), \quad$ *für alle* $a, b \in R$.
3. $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b), \quad$ *für alle* $a, b \in R$.

Die erste Bedingung folgt hier aus den beiden letzten.

Angenommen R und S sind unitär. Dann muss nicht notwendig $\phi(1_R) = 1_s$ gelten. Wenn das gilt, heißt der Ringhomomorphismus unitär.

Wenn R ein Ring ist, so definiert man der Polynomring $R[T]$. Er besteht aus allen formalen Summen

$$f = \sum_{i=0}^{\infty} a_i T^i, \quad a_i \in R,$$

wobei $a_i = 0$ bis auf endlich viele $i \in \mathbb{Z}$. Man läßt die Koeffizienten welchen Null sind oft fort. Ein von 0 verschiedenes Polynom f kann man schreiben.

$$f = a_n T^n + a_{n-1} T^{n-1} + \ldots + a_1 T + a_0, \quad \text{wo } a_n \neq 0.$$

Man nennt n den Grad $\deg f$ des Polynoms. Der Grad des Nullpolynoms wird als $-\infty$ definiert. Man nennt ein Polynom unitär, wenn $a_n = 1$.

Wenn der Ring R nullteilerfrei (ntf = Definition 5) ist, so gilt für zwei Polynome $f, g \in R[T]$:

$$\deg f + \deg g = \deg(f \cdot g).$$

Daraus folgt insbesondere, dass der Ring $R[T]$ dann ebenfalls ntf. ist.

Konvention: Ab jetzt seien alle vorkommenden Ringe kommutativ!

Die Evaluation: Es sei $R \to S$ ein Ringhomomorphismus. Man hat zu jedem $s \in S$ eine Abbildung (die Evaluation)

$$\epsilon_s : R[T] \to S, \quad \sum_{i=0}^{\infty} a_i T^i \mapsto \phi(a_0) + \sum_{i=1}^{\infty} \phi(a_i) s^i.$$

Hier ist die letzte Summe eine wirkliche Summe im Ring S.

Die Evaluation ist ein Ringhomomorphismus.

Definition 3 *Es sei R ein (kommutativer) Ring. Eine Teilmenge $\mathfrak{a} \subset R$ heißt Ideal, wenn gilt*

1. *Für alle $a, b \in \mathfrak{a}$ gilt $a + b \in \mathfrak{a}$.*
2. *Für alle $a \in \mathfrak{a}$, so gilt $(-a) \in \mathfrak{a}$.*
3. *Für alle $a \in \mathfrak{a}$ und $r \in R$ gilt $r \cdot a \in \mathfrak{a}$.*

Wenn R unitär ist, gilt $(-1_R) \cdot r = (-r)$ für alle $r \in R$. In diesem Fall folgt die Bedingung 2) aus 3).

Es sei $B \subset R$ eine nichtleere Teilmenge. Eine Linearkombination von Elementen aus B ist jede Summe der Form:

$$\sum_{i=1}^{m} r_i b_i,$$

wobei m eine beliebige natürliche Zahl ist und $b_1, \ldots, b_m \in B$ und $r_1, \ldots, r_m \in R$ beliebige Elemente.

Wenn $B = \emptyset$, so ist 0_R nach Definition die einzige Linearkombination von Elementen aus B.

Definition 4 *Es sei R unitär (und kommutativ). Es sei $B \subset R$ ein Teilmenge. Die Menge aller Linearkombinationen von Elementen aus B bezeichen wir mit $< B >$. Das ist ein Ideal von R, nämlich das kleinste Ideal welches B enthält.*

Ein Ideal $\mathfrak{a} \in R$ heißt Hauptideal, wenn $\mathfrak{a} =< B >$, für eine Menge B, die genau ein Element enthält. Es gilt $\mathfrak{a} = Rb$, wo $B = \{b\}$.

Definition 5 *Ein Ring R heißt nullteilerfrei (ntf.), wenn jede Gleichung $a \cdot b = 0$, wo $a, b \in R$, impliziert, dass $a = 0_R$ oder $b = 0_R$.*

Definition 6 *Ein (kommutativer) Ring R heißt Hauptidealring, wenn er unitär und ntf. ist und wenn jedes Ideal $\mathfrak{a} \subset R$ ein Hauptideal ist.*

Satz 7 *Der Ring $\mathbb{Z}$ ist ein Hauptidealring.*

Es sei K ein Körper. Dann ist der Polynomring $K[T]$ ein Hauptidealring.

Es sei R ein (kommutativer) Ring und $\mathfrak{a} \subset R$ ein Ideal. Es sei N die Menge folgender Teilmengen von R:

$$N = \{r + \mathfrak{a} \mid r \in R\}$$

Wir betrachten die Abbildung

$$\pi : R \to N, \quad r \mapsto r + \mathfrak{a}.$$

Dann gilt $\pi(r_1) = \pi(r'_1)$, gdw. $r_1 - r'_1 \in \mathfrak{a}$.

Satz 8 *Es gibt auf N zwei eindeutig bestimmte Operationen $+_N$ und $\cdot_N$, so dass N ein Ring wird, und so dass*

$$\pi : R \to N$$

ein Homomorphismus von Ringen ist. Man nennt N den Faktorring modulo dem Ideal $\mathfrak{a}$. Wir bezeichnen den Ring N mit $R/\mathfrak{a}$.

Primideale und maximale Ideale:

Lemma 9 *Es sei $(M, \geq)$ eine partiell geordnete Menge (siehe Wiki: "poset"). Es sei $M \neq \emptyset$. Wenn jede total geordnete Teilmenge $N \subset M$ eine obere Schranke besitzt, so gibt es in M maximale Elemente.*

Definition 10 *Es sei R ein unitärer Ring.*

Ein Ideal $\mathfrak{p} \subset R$ heißt Primideal, wenn $1_R \notin \mathfrak{p}$, und wenn für alle $a, b \in R$ folgende Implikation gilt:

$$ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}, \ \textit{oder}\ b \in \mathfrak{p}.$$

Ein Ideal $\mathfrak{m} \subset R$ heißt maximales Ideal, wenn $1_R \notin \mathfrak{m}$ und wenn für jedes Ideal $\mathfrak{a}$, so dass

$$\mathfrak{m} \subset \mathfrak{a}, \ \textit{und}\ 1_R \notin \mathfrak{a}$$

gilt, dass $\mathfrak{m} = \mathfrak{a}$.

Ein Element $q \in R$ heißt Primelement, wenn dass von q erzeugte Ideal Rq ein Primideal ist.

Beispiel: Es sei $R = \mathbb{Z}$. Dann ist jede Primzahl p ein Primelement in $\mathbb{Z}$.

Wir nennen eine Ideal $\mathfrak{a} \in R$ eigentlich, wenn $1_R \notin \mathfrak{a}$. Jedes eigentliche Ideal $\mathfrak{a}$ ist in einem maximalen Ideal enthalten. Das Ideal $\mathfrak{a}$ ist genau dann ein Primideal, wenn $R/\mathfrak{a}$ keine Nullteiler hat (ntf.). Es ist genau dann maximal, wenn $R/\mathfrak{a}$ ein Körper ist.

Satz 11 *Es sei R ein Hauptidealring. Es sei $\mathfrak{p} \neq 0$ ein Primideal. Dann ist $\mathfrak{p}$ ein maximales Ideal.*

Definition 12 *Ein unitärer ntf. Ring heißt faktoriell, wenn jedes Element Produkt von Primelementen ist.*

Diese Zerlegung auf folgende Weise eindeutig. Ein Element s eines Ringes R heißt eine *Einheit*, wenn ein Element $t \in R$ existiert, so dass $st = 1$, d.h. s besitzt ein inverses Element bzgl. der Multiplikation in R. Die Menge der Einheiten in R bezeichen wir mit R^*. Es gilt:

1. Für einen Körper K ist $K^* = K \setminus \{0\}$.

2. $\mathbb{Z}^* = \{\pm 1\}$

3. Für einen ntf. Ring gilt $R[T]^* = R^*$.

Zwei Elemente $a, b \in R$ heißen *assoziiert*, wenn ein $s \in R^*$ existiert, so dass $a = sb$ und dass auch $b = s^{-1}a$. Wenn R ein ntf. Ring ist, so sind zwei Elemente a und b genau dann assoziiert, wenn $Ra = Rb$, d.h. die Elemente erzeugen das gleiche Ideal.

Es sei R faktoriell und $a \in R$, $a \neq 0$. Dann gibt es nach Definition eine Zerlegung:

$$a = \epsilon \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_m,$$

wobei $q_1, \ldots, q_m$ Primelemente in R sind und $\epsilon \in R^*$. Wenn man eine weitere Darstellung

$$a = \epsilon' \cdot q'_1 \cdot q_2 \cdot \ldots \cdot q'_{m'},$$

so gilt $m = m'$ und nach Umnumerierung sind q_i und q'_i für $i = 1, \ldots, m$ assoziiert. Wir sagen die Zerlegung ist bis auf Einheiten eindeutig.

Beispiel:

$$6 = 2 \cdot 3 = (-2) \cdot (-3).$$

Es sei R ein ntf. Ring. Es seien $d, a \in R$, wo $d \neq 0$. Wir schreiben $d|a$ (d teilt a.), wenn $a \in Rd$.

Es sei R faktoriell. Es seien $a_1, \ldots, a_n \in R$ Elemente, die nicht alle 0 sind. Wir sagen $t \in R$, $t \neq 0$ ist ein gemeinsamer Teiler dieser Elemente, wenn

$$t|a_1, t|a_2, \ldots, t|a_n.$$

Wir sagen, dass d ein *größter gemeinsamer Teiler* (g.g.T.) ist, wenn d ein gemeinsamer Teiler ist und wenn für jeden anderen gemeinsamen Teiler t gilt, dass $t|d$.

Zwei g.g.T. d und d' sind assoziiert (oder eindeutig modulo Einheiten).

Der g.g.T. existiert in einem faktoriellen Ring R. Man liest ihn aus der Zerlegung in Primelemente genauso ab, wie im Ring der ganzen Zahlen $\mathbb{Z}$. Wenn R ein Hauptidealring ist, so gilt

$$Rd = Ra_1 + Ra_2 + \ldots + Ra_n.$$

Satz 13 *Ein Hauptidealring ist faktoriell.*

Man benutzt das Nothersche Prinzip: In einem Hauptidealring gibt es in jeder nichtleeren Menge von Idealen maximale Elemente.

Es sei R ein (kommutativer) ntf. Ring mit 1. Ein Polynom $f \in R[T]$ vom Grad $\deg f \geq 1$ heißt irreduzibel, wenn es nicht Produkt von zwei Polynomen ist, deren Grad jeweils echt kleiner ist als $\deg f$.

Satz 14 *(Eisensteinkriterium) Es sei R ein ntf. Ring. Es sei*

$$f = a_n T^n + a_{n-1} T^{n-1} + \ldots + a_1 T + a_0 \in R[T]. \tag{1}$$

ein Polynom von Grad $n \geq 1$.

Es sei $\mathfrak{p}$ ein Primideal von R, so dass $a_n \notin \mathfrak{p}$, und $a_i \in \mathfrak{p}$ für $n-1 \geq i \geq 0$. Es sei a_0 nicht Produkt von zwei Elementen aus $\mathfrak{p}$.

Dann ist dass Polynom f irreduzibel.

Definition 15 *Es sei R ein faktorieller Ring. Ein Polynom $f \in R[T]$ heißt primitiv, wenn der größte gemeinsame Teiler seiner Koeffizienten 1_R ist.*

Für ein beliebiges Polynom $f \neq 0$ nennt man einen größten gemeinsamen Teiler der Koeffizienten von f den Inhalt von f.

Satz 16 *(Lemma von Gauß) Es sei R faktoriell. Es seien f und g primitive Polynome. Dann ist das Produkt $f \cdot g$ ein primitives Polynom.*

Wenn $f, g \in R[T]$ zwei von 0 verschiedene Polynome sind, so gilt

$$\text{Inhalt}(f \cdot g) = \text{Inhalt}(f) \cdot \text{Inhalt}(g) \text{ modulo } R^*.$$

Diese Gleichung bedeutet, dass die beiden Elemente von R, die links und rechts vom Gleichheitszeichen stehen, assoziiert sind.

Satz 17 *Es sei R faktoriell. Es sei $f \in R[T]$ ein primitives Polynom. Es sei $g \in R[T]$. Es sei K der Quotientenkörper von R und es gelte in $K[T]$ eine Geleichung:*

$$g = f \cdot h, \quad \textit{wo } h \in K[T].$$

Dann gilt $h \in R[T]$.

Corollary 18 *Es sei R faktoriell. Es sei $f \in R[T]$ ein primitives Polynom. Es sei weiter f als Element von $K[T]$ ein Primelement.*

Dann ist f auch ein Primelement von $R[T]$.

Theorem 19 *Es sei R faktoriell. Dann ist auch $R[T]$ faktoriell.*

Ein Primelement von $R[T]$ ist entweder ein Polynom aus dem letzten Korollar oder ein Primelement $q \in R$, dass man als Polynom vom Grad 0 auffasst.

Es sei R faktoriell und K der Quotientenkörper. Es sei $h \in K[T]$. Dann kann man h schreiben:

$$h = (\frac{u}{v})h_1, \quad \text{wo, } u, v \in R, \ v \neq 0$$

und wo $h_1 \in R[T]$ ein primitives Polynom ist.

Es sei $f \in R[T]$ ein Polynom, welches ein Eisensteikriterium erfüllt, d.h. wie in Satz 1. Dann ist $f \in K[T]$ ein Primelement. In der Tat, sonst findet man aus der Zerlegung in Primelemente in $K[T]$ eine Gleichung

$$f = g \cdot h, \quad g, h \in K[T],$$

wobei die Polynome h, g einen echt kleineren Grad haben als f. Geht man wie oben zu h_1 und g_1 über, so findet man

$$f = (\frac{u}{v})g_1 \cdot h_1,$$

Wenn man mit v multipliziert und die Inhalte nimmt, folgt

$$v\text{Inhalt}(f) = u.$$

Also gilt $f = \text{Inhalt}(f)g_1 \cdot h_1$ und diese Gleichung in $R[T]$ widerspricht dem Eisensteinkriterium, nach dem f irreduzibel ist.

Satz 20 *Es sei R faktoriell. Es sei $f \in R[T]$ ein primitives Polynom, welches einer Eisensteinbedingung genügt (Satz 14). Dann ist f ein Primelement in $R[T]$.*

R-Moduln

Es sei R ein unitärer, nicht notwendig kommutativer Ring. Ein R-Modul M ist genau so definiert wie ein Vektorraum, dh. man hat eine Abbildung

$$R \times M \to M, \quad (r, m) \mapsto rm,$$

mit den bekannten Eigenschaften. Erwähnenswert ist nur die Eigenschaft

$$1_R m = m, \quad m \in M.$$

Beispiel: Es sei $(M, +)$ eine abelsche Gruppe. Es sei t eine natürliche Zahl und $m \in M$. Die Summe mit t Summanden

$$m + m + \ldots + m$$

bezeichnet man mit tm. Man definiert $(-t)m = -(tm)$. Die Abbildung

$$\mathbb{Z} \times M \to M, \quad (g, m) \mapsto gm,$$

macht M zu einem $\mathbb{Z}$-Modul. Daher sind $\mathbb{Z}$-Moduln und abelsche Gruppen ein und dasselbe.

Es sei I eine Menge. Für jedes $i \in I$ sei eine R-Modul N_i gegeben. Man bezeichent mit $\oplus_{i\in I} N_i$ die Menge aller Funktionen $f : I \to \bigcup_{i\in I} N_i$, so dass $f(i) \in M_i$ für alle $i \in I$ und so dass eine endliche Teilemenge $S_f \subset I$ existiert, so dass $f(i) = 0$ für $i \notin S_f$. (Man sagt die Funktion f ist fast überall 0.) Die Struktur eines R-Moduls auf $\oplus_{i\in I} N_i$ ist wie folgt definiert:

$$(f + g)(i) := f(i) + g(i), \quad (rf)(i) = r(f(i)), \quad \text{wo } r \in R.$$

Den R-Modul $\oplus_{i\in I} N_i$ nennt man die direkte Summe.

Wenn $N_i = R$ für alle $i \in I$ so wird die direkte Summe mit $R^{(I)}$ bezeichet. Man schreibt $R^n := R^{([1,n])}$. Das ist der Modul der Spaltenvektoren der Länge n.

Es seien M und N zwei R-Moduln. Wir bezeichnen mit $\mathrm{Hom}_R(M, N)$ die Menge der R-Modulhomomorphismen $\varphi : M \to N$. Wenn R kommutativ ist, so ist $\mathrm{Hom}_R(M, N)$ mit einer R-Modulstruktur versehen. Im allgemeinen ist $\mathrm{Hom}_R(M, N)$ eine abelsche Gruppe. Der Kern $\mathrm{Ker}\,\varphi$ und das Bild $\mathrm{Im}\,\varphi = \varphi(M)$ von φ sind wie in der Theorie der Vektorräume definiert.

Ein R-Modul M heißt *frei*, wenn er isomorph zu einem Modul $R^{(I)}$ ist. Äquivalent dazu ist, das es eine Basis $B \subset M$ in diesem Modul gibt. Wenn $I = [1, n] \subset \mathbb{N}$ so schreibt man $R^n = R^{([1,n])}$. Man sagt M ist frei vom Rang n wenn $M \cong R^n$.

Satz 21 *Es sei R ein unitärer Ring und es sei M ein R-Modul. Es sei I eine Menge. Dann ist die kanonische Abbildung*

$$\kappa : \mathrm{Hom}(R^{(I)}, M) \to \mathrm{Abb}(I, M)$$

eine Bijektion.

Corollary 22 *Es sei $\pi : M \to C$ ein surjektiver R-Modulhomomorphismus. Es sei F ein freier R-Modul und $\varphi : F \to C$ ein R-Modulhomomorphismus.*

Dann gibt es einen R-Modulhomomorphismus $\psi : F \to M$, so dass folgendes Diagramm kommutativ ist:

$$\begin{tikzcd} & F \arrow[dl, "\psi"'] \arrow[d, "\varphi"] \\ M \arrow[r, "\pi"] & C \end{tikzcd}$$

Es seien N, M, C drei R-Moduln. Wir betrachten eine Folge von R-Modulhomomorphismen

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} C \longrightarrow 0. \qquad (2)$$

Hier bezeichnet 0 einen R-Modul, der nur aus dem Nullelement besteht. Die äußeren Pfeile sind die einzig möglichen R-Modulhomomorphismen von oder nach 0.

Definition 23 *Wir sagen, dass (2) eine kurze exakte Sequenz ist, wenn ι injektiv ist, π surjektiv und wenn*

$$\iota(N) = \operatorname{Ker} \pi.$$

Satz 24 *Es sei (2) eine kurze exakte Sequenz. Dann sind die folgenden Bedingungen äquivalent.*

a) Es gibt einen Homomorphismus $\sigma : C \to M$, so dass $\pi \circ \sigma = \mathrm{id}_C$.

b) Es gibt einen Homomorphismus $\varkappa : M \to N$, so dass $\varkappa \circ \iota = \mathrm{id}_N$.

c) Es gibt einen Untermodul $N' \subset M$, so dass $\iota(N) + N' = M$ und $\iota(N) \cap N' = \{0\}$.

Eine kurze exakte Sequenz, die die Bedingungen von Proposition 24 erfüllt, heißt *zerfallend*. Nach Korollar 22 zerfällt eine kurze exakte Sequenz (2), wenn C ein freier R-Modul ist.

Definition 25 *Es sei R ein unitärer Ring. Ein R-Modul M heißt endlich erzeugt, wenn endlich viele Elemente $m_1, \ldots, m_n \in M$ existieren, so dass jedes Element $m \in M$ wie folgt geschrieben werden kann:*

$$m = r_1 m_1 + \ldots + r_n m_n, \quad \textit{wobei } r_1, \ldots, r_n \in R.$$

Wir sagen m ist eine Linearkombination der $m_1, \ldots, m_n$.

Man nennt die Elemente $m_1, \ldots, m_n$ Erzeugende des Moduls M. Wenn zusätzlich aus jeder GLeichung der Form

$$0 = r_1 m_1 + \ldots + r_n m_n, \quad \text{wobei } r_1, \ldots, r_n \in R.$$

folgt dass $r_1 = 0, \ldots, r_n = 0$ (linear unabhängig). So ist der Modul M frei und es ist isomorph zu R^n. Wir sagen dann, dass $m_1, \ldots, m_n$ eine Basis von M ist.

Es sei $\phi : M \to C$ ein surjektiver Homomorphismus von R-Moduln. Wenn $m_1, \ldots, m_n$ Erzeugende von M sind, so sind $\phi(m_1), \ldots, \phi(m_n)$ Erzeugende von C. Insbesondere ist dann C endlich erzeugt.

Definition 26 *Es sei R ntf.. Ein R-Modul M heißt torsionsfrei, wenn jede Gleichung der Form*

$$r \cdot m = 0, \quad r \in R, \ m \in M$$

impliziert, dass $r = 0$ oder $m = 0$.

Satz 27 *Es sei R ein Hauptidealring. Es sei M ein endlich erzeugter torsionsfreier R-Modul. Dann ist M ein freier R-Modul.*

Beweis: Es seien $m_1, \ldots, m_n$ Erzeugende von M. Wir beweisen den Satz nach Induktion durch n.

Der Fall $n = 1$ ist trivial.

Im allgemeinen Fall sei

$$N = \{m \in M \mid \text{exist. } \alpha \in R, \ \alpha \neq 0, \text{ sd. } \alpha m \in R m_1\} \supset R m_1.$$

Man findet eine surjektiven Modulhomomorphismus $\pi : M \to C$ mit dem Kern N, d.h. man hat eine exakte Sequenz:

$$0 \to N \to M \xrightarrow{\pi} C \to 0.$$

Man beweist, dass C torsionsfrei ist. Weil $\pi(m_1) = 0$, sind $\pi(m_2), \ldots, \pi(m_n)$ Erzeugende von C.

Nach Induktionsvoraussetzung ist dann C frei. Es sei $c_1, \ldots, c_r$ eine Basis von C. Wir finden Elemente $\tilde{c}_1, \ldots, \tilde{c}_r \in M$, so dass $\pi(\tilde{c}_i) = c_i$. Es sei $\tilde{C} \subset M$ die Menge aller Linearkombinationen von $\tilde{c}_1, \ldots, \tilde{c}_r$ (lineare Hülle). Das ist ein Untermodul und die Elemente $\tilde{c}_1, \ldots, \tilde{c}_r$ sind linear unabhängig, da ihre

Bilder in C linear unabhängig sind. Also induziert π einen Isomorphismus $\tilde{C} \to C$. Also liegt kein von Null verschiedenes Element von $\tilde{C}$ im Kern von π, d.h. $N \cap \tilde{C} = \{0\}$.

Es folgt, dass jedes $m \in M$ eine eindeutige Zerlegung hat

$$m = u + v, \quad u \in N,\ v \in \tilde{C}.$$

Die Abbildung $m \mapsto u$ ist ein surjektiver R-Modulhomomorphismus $\sigma : M \to N$. Daher ist N endlich erzeugt. Es seien $u_1, \ldots, u_s \in N$ Erzeugende. Nach Definition von N existieren von 0 verschiedene Elemente $\alpha_1, \ldots, \alpha_s \in R$, so dass $\alpha_i \cdot u_i \in Rm_1$.

Es sei $\alpha = \alpha_1 \cdot \ldots \cdot \alpha_s$. Dann folgt $\alpha N \in Rm_1$. Man kann $m_1 \neq 0$ annehmen. Dann ist Rm_1 zu R als R-Modul isomorph. Also ist αN eine freier Modul vom Rang 1, da jedes Ideal ein Hauptideal ist. Wenn αu eine Basis von αN ist, so ist u eine Basis von N, so dass auch N frei ist.

Man sieht leicht, dass $u, \tilde{c}_1, \ldots, \tilde{c}_r$ eine Basis von M ist. Also ist M frei. *Q.E.D.*

Satz 28 *Es sei R ein Hauptidealring. Es sei M ein R-Modul und es seien $m_1, \ldots, m_r \in M$ Erzeugende des Moduls M. Es sei $N \subset M$ ein Untermodul von M.*

Dann gibt es eine natürliche Zahl $s \leq r$ und Elemente $n_1, \ldots, n_s \in N$, die den Modul N erzeugen.

Proof: Es sei $\mathfrak{a}$ die Menge aller Elemente $a \in R$, so dass eine Linearkombination

$$x_1 m_1 + x_2 m_2 + \ldots + x_{r-1} m_{r-1} + a m_r, \quad x_1, \ldots, x_{r-1} \in R, \tag{3}$$

existiert, die in N liegt. Dann ist $\mathfrak{a} = Rd$ ein Hauptideal. Folglich finden wir eine Linearkombination

$$y_1 m_1 + y_2 m_2 + \ldots + y_{r-1} m_{r-1} + d m_r = n_1 \in N.$$

Es sei $M' \subset M$ der Untermodul, der von $m_1, \ldots, m_{r-1}$ erzeugt wird. Es sei $N' = M' \cap N$. Wir schreiben ein Element $n \in N$ in der Form (3). Es sei $z = a/d$. Dann ist

$$n - z n_1 \in M' \cap N = N'.$$

Mittels Induktion finden wir Elemente $n_2, \dots, n_s \in N'$, wo $s \leq r$, die N' erzeugen. Aber dann erzeugen die Elemente $n_1, n_2, \dots, n_s \in N$ den Modul N. *Q.E.D.*

Bemerkung: Es sei M ein freier Modul, und es sei $m_1, \dots, m_r$ eine Basis von M. Dann kann man das Beweisverfahren benutzen, um eine Basis von N zu finden.

Satz 29 *(Elementarteilersatz) Es sei R ein Hauptidealring. Es sei $A \in M(m\times n, R)$. Dann gibt es Matrizen $X \in M(m\times m, R)$ und $Y \in M(n\times n, R)$, die beide invertierbar sind, so dass*

$$XAY = D, \tag{4}$$

wobei D höchstens an den Positionen (i,i) Einträge d_i hat, die von 0 verschieden sein können. Wenn $d_1, \dots, d_r$ die von 0 verschiedenen Einträge bezeichnet, so gilt:

$$Rd_1 \supset Rd_2 \supset \dots \supset Rd_r.$$

Die Zahl r und die Ideale $Rd_1, \dots, Rd_r$ hängen nur von A ab und nicht von der Wahl der Matrizen X und Y.

Definition 30 *Die Elemente $d_1, \dots, d_r \in R$ aus der Proposition nennt man die Elementarteiler der Matrix A. Diese Elemente sind und ihre Reihenfolge sind bis auf Multiplikation mit Einheiten eindeutig bestimmt.*

Wenn also $X'AY' = D'$ ebenfalls den Bedingungen der Proposition genügt, so hat D' an der Position (i,i) für $1 \leq i \leq r$ den Eintrag $d_i\eta_i$, wo $\eta_i \in R^*$ eine Einheit des Ringes R ist. Alle anderen Einträge von D' sind 0.

Es sei K ein Körper. Dann ist $K[T]$ ein Hauptidealring.

Satz 31 *(Frobenius) Es sei K ein Körper. Es sei n eine natürliche Zahl. Es seien $A, B \in M(n \times n, K)$ zwei Matrizen.*

Die Matrizen A, B sind genau dann ähnlich, wenn die beiden Matrizen $E_nT - A, E_nT - B \in M(n \times n, K[T])$ die gleichen Elementarteiler haben.

Determinanten

Es sei R ein kommutativer unitärer Ring. Es sei $n \in \mathbb{N}$. Dann liefert die Leibnizformel (LA vor Proposition 70) eine alternierende Multilinearform

$$\det : R^n \times \dots \times R^n \longrightarrow R$$

wobei links n Faktoren stehen. Jede andere alternierende Multilinearform

$$\vartheta : R^n \times \ldots \times R^n \longrightarrow R$$

ist ein Vielfaches von det, d.h. es existiert ein $\lambda \in R$ mit $\vartheta = \lambda \det$. Wir fassen det auch als eine Abbildung

$$\det : M(n \times n, R) \longrightarrow R$$

auf.

Wenn R ein Körper ist, so ist det aus der linearen Algebra bekannt. Die grundlegenden Rechenregeln für det übertragen sich auf beliebeige Ringe wie folgt. Es seien $A, B \in M(n \times n, R)$. Wir wollen zeigen

$$\det(AB) = \det A \det B \tag{5}$$

Wenn R ntf. so bildet man den *Qutientenkörper* K von R. Es besteht aus allen formalen Brüchen r/s, wo $r, s \in R$ und $s \neq 0$. Dabei sieht man zwei Brüche r_1/s_1 und r_2/s_2 als gleich an, wenn

$$r_1 s_2 = r_2 s_1.$$

Man multipliziert und addiert Brüche wie gewöhnlich.

Da $R \subset K$, kann man (5) auch als eine Gleichung in K auffassen, wo sie bekannt ist (LA Satz 50). Jetzt sei R beliebig, also mit Nullteilern. Man schreibt $A = (a_{ij})$ und $B = (b_{ij})$. Man wählt Unbestimmte x_{ij}, y_{ij} wo $i, j \in [1, n]$, d.h. $2n^2$ Unbestimmte und bildet den Polynomring

$$P := \mathbb{Z}[x_{ij}, y_{ij}].$$

Dieser Ring ist ntf. Man setzt $X = (x_{ij}) \in M(n \times n, P)$ und $Y = (y_{ij}) \in M(n \times n, P)$. Da P ein ntf. Ring ist gilt die Formel

$$\det(XY) = \det X \det Y. \tag{6}$$

Es gibt genau einen Ringhomomorphismus

$$\phi : \mathbb{Z}[x_{ij}, y_{ij}] \longrightarrow R,$$

so dass $\phi(x_{ij}) = a_{ij}$ und $\phi(x_{ij}) = b_{ij}$. Man erhält (5) aus (6), indem man ϕ anwendet.

Satz 32 *Es sei M ein R-Modul und es seien $m_1, \ldots, m_n \in M$ Erzeugende. Gegeben seien n Gleichungen*

$$\sum_{j=1}^{n} a_{ij} m_j = 0, \quad i = 1, \ldots n$$

wobei $(a_{ij}) \in M(n \times n, R)$.

Dann gilt

$$\det(a_{ij}) M = 0.$$

Ganze Elemente

Es sei $\phi : R \to S$ ein Homorphismus kommutativer unitärer Ringe, so dass $\phi(1_R) = 1_S$. Dann sagen wir S ist eine *R-Algebra*.

Beispiel: Es sei R ein unitärer Ring. Die Abbildung $\mathbb{Z} \to R$, die eine ganze Zahl g auf $g1_R$ abbildet (vgl.) ist ein Ringhomomorphismus. Daher ist R automatisch eine $\mathbb{Z}$-Algebra.

Es sei K ein Körper. Dann ist der Kern von $\mathbb{Z} \to K$ ein Primideal. Wenn diese Abbildung den Kern $\{0\}$ hat, so heißt K ein Körper der Charakteristik 0. Wenn der Kern das Primideal $p\mathbb{Z}$ ist, wo p eine Primzahl ist, so heißt K ein Köper der Charakteristik p. Dann ist K eine $\mathbb{F}_p$-Algebra, wobei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Lemma 33 *Es sei p eine Primzahl. Es R eine $\mathbb{F}_p$-Algebra. Dann gilt die binomische Formel*

$$(x + y)^p = x^p + y^p.$$

Es sei S eine R-Algebra. Man erhählt auf der abelschen Gruppe S eine R-Modulstruktur $R \times S \to S$, wenn man setzt:

$$r \cdot s := \phi(r)s$$

wo rechts die Multiplikation in S steht.

Man sagt, dass (S, ϕ) eine *endliche R-Algebra* ist, wenn S als R-Modul endlich erzeugt ist.

Definition 34 *Ein Element $s \in S$ heißt ganz über R, wenn es eine natürliche Zahl $n \geq 1$ gibt und Elemente $a_0, a_1, \ldots, a_{n-1} \in R$, so dass*

$$s^n + \phi(a_{n-1})s^{n-1} + \ldots + \phi(a_1)s + \phi(a_0) = 0.$$

Man sagt, dass $\phi : R \to S$ ganz ist, wenn jedes Element $s \in S$ ganz über R ist.

Beispiel: Es sei $R[T]$ der Polynomring. Es sei $f(T) \in R[T]$ ein unitäres Polynom:

$$f(T) = T^d + a_{d-1}T^{d-1} + \ldots + a_1T^1 + a_0, \quad a_i \in R.$$

Dann ist $R[T]/f(T)R[T]$ eine endliche R-Algebra. Als R-Modul ist $R[T]/f(T)R[T]$ frei mit der Basis

$$1, T, T^2, \ldots, T^{d-1}.$$

Es seien $s_1, \ldots, s_n \in S$. Dann ist

$$R[s_1, \ldots, s_n] = \oplus_{(e_1,\ldots,e_n)\in(\mathbb{Z}_{\geq 0})^n} \; Rs_1^{e_1} \cdot \ldots \cdot s_n^{e_n} \subset S$$

eine Unteralgebra von S. Hier durchläuft $(e_1, \ldots, e_n)$ alle Vektoren deren Einträge nichtnegative ganze Zahlen sind.

Satz 35 *Es sei $s \in S$. Dann sind die folgenden Bedingungen äquivalent:*

(i) Das Element s ist ganz über R.

(ii) Es gibt eine R-Unteralgebra $S' \subset S$, so dass $s \in S'$ und S' eine endliche R-Algebra ist.

(iii) $R[s]$ ist eine endliche R-Algebra.

Corollary 36 *Es seien $s_1, \ldots, s_n \in S$ Elemente, die ganz über R sind. Dann ist $R[s_1, \ldots, s_n]$ ein endlicher R-Modul.*

Insbesondere folgt, dass für zwei Elemente $s_1, s_2 \in S$, die ganz über R sind auch die Elemente s_1s_2 und $s_1 + s_2$ ganz über R sind.

Corollary 37 *Es seien $\phi : R \to S$ und $\psi : S \to T$ Ringhomomorphismen.*
Wenn ϕ ganz ist, und $t \in T$ ganz über S ist, so ist t ganz über R.

Satz 38 *Es sei $\phi : R \to S$ injektiv. Wir nehmen an, dass R und S ntf. sind.*
Dann ist R ein Körper, genau dann wenn S ein Körper ist.

Darstellbarkeit von Funktoren

Die Definitionen von Kategorien und Funktoren stehen in meinem LA-Skript.

Definition 39 *Es sei $\mathcal{C}$ eine Kategorie. Einen Morphismus $\phi : A \to B$ der Kategorie $\mathcal{C}$ nennt man einen* Isomorphismus*, wenn ein Morphismus $\psi : B \to A$ existiert, so dass*

$$\psi \circ \phi = \mathrm{id}_A, \quad \phi \circ \psi = \mathrm{id}_B .$$

Wenn $\mathcal{C}$ die Kategorie der Moduln über einem Ring R ist, so ist $\phi : A \to B$ genau dann eine Isomorphismus, wenn ϕ eine bijektive Abbildung ist.

Definition 40 *Es seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien. Es seien $F, G : \mathcal{C} \to \mathcal{D}$ zwei Funktoren.*

Ein Funktormorphismus (oder natürliche Transformation) Φ ist eine Funktion, die jedem Objekt $X \in \mathcal{C}$ einen Morphismus in $\mathcal{D}$ zuordnet:

$$\Phi_X : F(X) \to G(X).$$

Es wird verlangt, dass für jeden Morphismus $\alpha : X \to Y$ in $\mathcal{C}$ das folgende Diagramm von Morphismen in $\mathcal{D}$ kommutativ ist:

$$\begin{array}{ccc} F(X) & \xrightarrow{\Phi_X} & G(X) \\ {\scriptstyle F(\alpha)}\downarrow & & \downarrow{\scriptstyle G(\alpha)} \\ F(Y) & \xrightarrow{\Phi_Y} & G(Y) \end{array}$$

Mit $\mathrm{Hom}_{Funk}(F, G)$ bezeichen wie die Menge der Funktormorphismen von F nach G.

Man nennt Φ einen Isomorphismus von Funktoren, wenn für alle $X \in \mathcal{C}$ der Morphimus Φ_X in $\mathcal{D}$ ein Isomorphismus ist.

Es sei $\mathcal{C}$ eine Kategorie. Es sei $M \in \mathcal{C}$ ein Objekt. Dann definiert man einen Funktor

$$h_M : \mathcal{C} \to (\text{Mengen})$$

in die Kategorie der Mengen: $h_M(X) = \mathrm{Hom}_{\mathcal{C}}(M, X)$. Wenn $\alpha : X \to Y$ ein Morphimus in $\mathcal{C}$, so definiert man

$$h_M(\alpha) : h_M(X) \to h_M(Y), \quad \rho \mapsto \alpha \circ \rho.$$

Satz 41 *(Yoneda-Lemma) Es sei $F : \mathcal{C} \to$ (Mengen) ein Funktor. Es sei $M \in \mathcal{C}$ ein Objekt. Ein Funktormorphismus $\Phi : h_M \to F$ gibt uns insbesondere eine Abbildung von Mengen $\Phi_M : h_M(M) \to F(M)$. Wir betrachten das Bild $\Phi_M(\mathrm{id}_M) \in F(M)$ von $\mathrm{id}_M \in \mathrm{Hom}_{\mathcal{C}}(M, M) = h_M(M)$.*

Dann ist die Abbildung

$$\mathrm{Hom}_{Funk}(h_M, F) \to F(M), \quad \Phi \mapsto \Phi_M(\mathrm{id}_M)$$

eine Bijektion von Mengen.

Es sei $\alpha : M \to N$ ein Morphismus in $\mathcal{C}$, d.h. $\alpha \in h_M(N)$. Nach Yoneda definiert α eine Funktormorphismus $\alpha^* : h_N \to h_M$. Wir können α^* explizit angeben. Für $\rho \in h_N(X)$ ist

$$\alpha^*(\rho) = \rho \circ \alpha \in h_M(X).$$

Corollary 42 *Es seien M und N Objekte aus $\mathcal{C}$. Dann ist die folgende Abbildung von Mengen bijektiv*

$$\mathrm{Hom}_{\mathcal{C}}(M, N) \to \mathrm{Hom}_{Funk}(h_N, h_M), \quad \alpha \mapsto \alpha^*.$$

Ein Funktor $F : \mathcal{C} \to$ (Mengen) heißt repräsentierbar, wenn es ein Objekt M von $\mathcal{C}$ und einen Funktorisomorphismus

$$\tilde{\xi} : h_M \to F$$

Nach Yoneda ist $\tilde{\xi}$ durch das Element $\xi := \tilde{\xi}_M(\mathrm{id}_M) \in F(M)$ bestimmt. Wir sagen, dass (M, ξ), wo $\xi \in F(M)$ den Funktor F repräsentiert. Wir nennen ξ das universelle Element.

Satz 43 *(Universaleigenschaft) Es sei $F : \mathcal{C} \to$ (Mengen) ein Funktor. Ein Paar (M, ξ), wo $M \in \mathcal{C}$ und $\xi \in F(M)$ repräsentiert genau dann den Funktor F, wenn die folgende Eigenschaft erfüllt ist:*

Für alle Paare (N, η), wo $N \in \mathcal{C}$ und $\eta \in F(N)$ existiert genau ein Morphismus $\tau : M \to N$, so dass

$$F(\tau)(\xi) = \eta.$$

(Man nennt dies die Universaleigenschaft.)

Wenn zwei Paare (M, ξ) und (M', ξ') beide den Funktor F repräsentieren, so existiert ein eindeutig bestimmter Isomorphismus $\tau : M \to M'$, so dass $F(\tau)(\xi) = \xi'$.

Beweis: Weil $\tilde{\xi}_N(\tau) = F(\tau)(\xi)$, besagt die Universaleigenschaft, dass

$$\tilde{\xi}_N : h_M(N) \to F(N)$$

bijektiv ist. *Q.E.D.*

Beispiel 1: Es sei R ein kommutativer Ring. Es sei $\mathcal{C}$ die Kategorie der R-Moduln. Es sei $\alpha : U \to M$ ein Homomorphismus von R-Moduln (= Morphismus in $\mathcal{C}$). Wir definieren einen Funktor $F : \mathcal{C} \to$ (Mengen):

$$F(X) = \{\eta \in h_M(X) \mid \eta \circ \alpha = 0\}.$$

Die 0 bezeichnet den Homomorphismus $U \to X$ der alle Elemente auf das Nullelement von X abbildet (Nullmorphismus).

Es sei $\xi : M \to C$ ein surjektiver Modulhomorphismus, dessen Kern das Bild $\operatorname{Im} \alpha \subset M$ ist. Dann gilt $\xi \in F(C)$. Das Paar (C, ξ) repräsentiert den Funktor F.

Dafür muss man zeigen: Für jeden Homomorphismus $\eta : M \to X$, so dass $\eta \circ \alpha = 0$ exixtiert genau ein Modulhomomorphismus $\tau : C \to X$, so dass folgendes Diagramm kommutativ ist:

$$\begin{tikzcd}
M \arrow[r, "\xi"] \arrow[d, "\eta"'] & C \arrow[dl, "\tau"] \\
X &
\end{tikzcd}$$

Das ist klar. Man nennt (C, ξ) den Kokern von $\alpha : U \to M$.

Beispiel 2: Es sei R ein kommutativer Ring mit 1. Eine R-Algebra ist ein Ringhomomorphismus $\phi : R \to S$, wo S ein kommutativer Ring mit 1 ist. Es sei $\psi : R \to T$ eine weitere R-Algebra.

Definition 44 *Ein R-Algebrahomomorphismus $\chi : S \to T$ ist eine Ringhomomorphismus, so dass $\chi \circ \phi = \psi$. Wir bezeichnen die Menge der R-Algebrahomomorphismen mit*

$$\mathrm{Hom}_{R-Alg}(S, T).$$

Damit bilden die R-Algebren eine Kategorie.

Es sei n eine natürliche Zahl. Wir betrachten den Funktor $F : (R-$Algebren$) \to$ (Mengen):

$$F(S) = S^n$$

Dieser Funktor ist darstellbar durch eine R-Algebra P und das universelle Element $(X_1, \ldots, X_n) \in P^n$. Das ist der Polynomring

$$P = R[X_1, \ldots, X_n].$$

Beispiel 3: Wir betrachten die gleiche Kategorie wie in Beispiel 1. Es sei $M_1, \ldots, M_t$ eine endliche Folge von R-Moduln. Dann definieren wir einen Funktor $T : \mathcal{C} \to$ (Mengen):

$$T(X) = Mult(M_1 \times \ldots \times M_t, X), \quad X \in \mathcal{C},$$

wo rechts die Menge aller multilinearen Abbildungen mit Werten in X steht.

Der Funktor T ist repräsentierbar. Es sei (U, ξ) ein Paar, das T repräsentiert. Man schreibt:

$$M_1 \otimes_R M_2 \otimes_R \ldots \otimes_R M_t := U$$

und für die multilineare Form ξ schreibt man

$$\xi(m_1, m_2, \ldots, m_t) =: m_1 \otimes m_2 \otimes \ldots \otimes m_t.$$

Man nennt das das Tensorprodukt der R-Moduln M_i.

Satz 45 *Wenn $B_i \in M_i$, für $i = 1, \ldots t$, eine Basis von M_i ist, so sind die Elemente*

$$b_1 \otimes b_2 \otimes \ldots \otimes b_t, \quad \text{wo } b_i \in B_i$$

eine Basis des R-Moduls $M_1 \otimes_R M_2 \otimes_R \ldots \otimes_R M_t$.

(vergleiche LA-Skript Satz 64)

Man hat eine Reihe von Rechenregeln für das Tensorprodukt von R-Moduln:

$$(M \otimes_R N) \otimes_R L \cong M \otimes_R (N \otimes_R L). \qquad M \otimes_R N \cong N \otimes_R M.$$

Das Tensorprodukt mit einer dierekten Summe von R-Moduln berechnet sich wie folgt:

$$(\oplus_{i \in I} N_i) \otimes_R M \cong \oplus_{i \in I}(N_i \otimes_R M).$$

Man hat den Isomorphismus $R \otimes_R M \cong M$, $r \otimes m \mapsto rm$. Daraus findet man für jede Menge I den Isomorphismus

$$R^{(I)} \otimes_R M \cong M^{(I)}.$$

Wenn $\phi : N_1 \to N_2$ ein Homomorphismus von R-Moduln ist, so induziert das einen Homomorphismus

$$\begin{array}{rccc} \phi_M : & N_1 \otimes_R M & \longrightarrow & N_2 \otimes_R M \\ & n_1 \otimes m & \mapsto & \phi(n_1) \otimes m \end{array}$$

Wenn

$$N_1 \stackrel{\varkappa}{\to} N_2 \stackrel{\pi}{\to} N_3 \to 0$$

eine exakte Folge von R-Moduln ist und M ein R-Modul, so ist auch die Sequenz

$$N_1 \otimes_R M \stackrel{\varkappa_M}{\to} N_2 \otimes_R M \stackrel{\pi_M}{\to} N_3 \otimes_R M \to 0$$

Wenn $\mathfrak{a} \subset R$ eine Ideal ist, so erhält man

$$(R/\mathfrak{a}) \otimes_R M \cong M/\mathfrak{a}M.$$

Es seien $R_1, \ldots, R_n$ Ringe. Dann definiert man auf der Produktmenge

$$R_1 \times R_2 \times \ldots \times R_n \tag{7}$$

die Struktur eines Ringes mit der folgenden Addition und Multiplikation:

$$\begin{array}{l} (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n) \\ (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 \cdot y_1, \ldots, x_n \cdot y_n), \end{array}$$

wobei $x_i, y_i \in R_i$.

Satz 46 *(Chinesischer Restsatz) Es sei R ein kommutativer unitärer Ring. Es seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Ideale von R. Wie setzen voraus, dass $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$.*

Die Restklassenabbildungen $R \to R/\mathfrak{a}_i$ induzieren einen Ringhomomorphismus

$$R \to (R/\mathfrak{a}_1) \times \ldots \times (R/\mathfrak{a}_n)$$

in das Produkt der Ringe.

Diese Abbildung ist surjektiv.

Definition 47 *Es sei $f \in R$. Man nennt das Element f nilpotent, wenn eine natürliche Zahl s existiert, so dass $f^s = 0$.*

Ein Ring der keine von Null verschiedenen nilpotenten Elemente enthält heißt reduziert.

Satz 48 *Es sei R ein kommutativer unitärer Ring. Es sei $f \in R$ nicht nilpotent. Dann gibt es ein Primideal $\mathfrak{p} \subset R$, so dass $f \notin \mathfrak{p}$.*

Wir definieren jetzt das *Tensorprodukt von R-Algebren.* Es seien $\phi_1 : R \to S_1$ und $\phi_2 : R \to S_2$ zwei R-Algebren. Insbesondere sind dann S_1 und S_2 auch R-Moduln. Daher können wir das Tensorprodukt bilden:

$$S_1 \otimes_R S_2.$$

Es gibt eine eindeutig bestimmte R-bilineare Abbildung

$$S_1 \otimes_R S_2 \times S_1 \otimes_R S_2 \longrightarrow S_1 \otimes_R S_2.$$

die ein Paar $(s_1 \otimes s_2, s_1' \otimes s_2'$ auf $s_1 s_1' \otimes s_2 s_2'$ abbildet. Dadurch wir $S_1 \otimes_R S_2$ ein Ring. Die Abbildung $R \to S_1 \otimes_R S_2$, welche $r \in R$ auf $\phi_1(r_1) \otimes 1 = 1 \otimes \phi_2(r_2)$ abbildet macht $S_1 \otimes_R S_2$ zu einer R-Algebra.

Körpererweiterungen

Es sei K eine Körper. Es sei $\rho : K \to E$ eine K-Algebra, so dass E ein Körper ist. Dann ist ρ automatisch injektiv. Wir nennen E einen Erweiterungskörper von K. Wir schreiben für diese Situation E/K. Man soll sich K als Teilmenge von E vorstellen. Für die Abbildung ρ schreiben wir dann einfach $K \subset E$.

E ist offenbar ein K-Vektorraum. Wenn E ein endlich erzeugter K-Vektorraum ist, so nennen wir E eine endliche Erweiterung von K. Wir schreiben

$$[E : K] = \dim_K E$$

für die Dimension dieses Vektorraums.

Definition 49 *Ein Körper Ω heißt algebraisch abgeschlossen, wenn für jedes unitäre Polynom $f(T) \in \Omega[T]$*

$$f(T) = T^d + a_{d-1}T^{d-1} + \ldots + a_1 T + a_0, \quad a_i \in \Omega.$$

mit $d \geq 1$ Elemente $\alpha_1, \ldots, \alpha_d \in \Omega$ existieren, so dass

$$f(T) = \prod_{i=1}^{d} (T - \alpha_i).$$

Lemma 50 *Ein Köper Ω ist genau dann algebraisch abgeschlossen, wenn für jede Körpererweiterung $\phi : \Omega \to \Theta$, so dass ϕ ganz (Definition 34)ist, ϕ ein Isomorphismus ist.*

Satz 51 *Es sei K ein Körper. Dann gibt es eine Körpererweiterung Ω/K, so dass Ω algebraisch abgeschlossen ist.*

Wenn $K = \mathbb{Q}$ ist, so kann man für Ω den Körper $\mathbb{C}$ nehmen.

Die Menge $\bar{K} \subset \Omega$ aller Elemente $\omega \in \Omega$, die ganz über K sind, bilden einen Körper nach Korollar 36 und Satz 38. Der Körper $\bar{K}$ ist algebraisch abgeschlossen.

Definition 52 *Es sei K ein Körper. Eine Körpererweiterung $\bar{K}/K$ heißt ein algebraischer Abschluss von K, wenn sie ganz (Definition 34)ist und wenn $\bar{K}$ ein algebraisch abgeschlossener Körper ist.*

Satz 53 *Es sei K eine Körper. Es seien $\phi_1 : K \to \Omega_1$ und $\phi_2 : K \to \Omega_2$ zwei algebraische Abschlüsse von K.*

Dann gibt es einen Körperisomorphismus $\alpha : \Omega_1 \to \Omega_2$, so dass $\phi_2 = \alpha \circ \phi_1$, d.h. man hat ein kommutatives Diagramm

$$\begin{tikzcd} K \arrow[r, "\phi_1"] \arrow[d, "\phi_2"'] & \Omega_1 \arrow[dl, "\alpha"] \\ \Omega_2 & \end{tikzcd}$$

Beweis: Man betrachtet die K-Algebra $\Omega_1 \otimes_K \Omega_2$. Sie enthält ein maximales Ideal $\mathfrak{m} \subset \Omega_1 \otimes_K \Omega_2$. Wir erhalten einen Körper $\Omega := (\Omega_1 \otimes_K \Omega_2)/\mathfrak{m}$. Man hat eine kanonische Abbildung

$$\begin{array}{ccccc} \Omega_1 & \xrightarrow{\mathrm{id}\otimes\phi_2} & \Omega_1 \otimes_K \Omega_2 & \to \Omega \\ \omega_1 & \mapsto & \omega_1 \otimes 1 & \end{array} \tag{8}$$

Es sei $\omega_2 \in \Omega_2$. Dann gibt es ein Polynom $f(T) \in K[T]$, so dass $f(\omega_2) = 0$. Aber dann gilt auch $f(1 \otimes \omega_2) = 0$. Wenn wir $\Omega_1 \otimes_K \Omega_2$ als einen Ω_1-Modul via $\mathrm{id}\otimes\phi_2$ ansehen, so wird er von den Elementen $1 \otimes \omega_2$, wo $\omega_2 \in \Omega_2$ erzeugt. Nach Korollar 36 ist daher $\mathrm{id}\otimes\phi_2$ ganz. Nach Korollar 37 ist dann auch das Kompositum $\bar{\phi}_2$ der Abbildungen (8) ganz. Aber dann ist $\bar{\phi}_2$ ein Isomorphismus.

Man erhält eine kommutatives Diagramm:

$$
\begin{tikzcd}
 & \Omega_1 \arrow[dr, "\bar{\phi}_2"] & \\
K \arrow[ur, "\phi_1"] \arrow[dr, "\phi_2"'] & & \Omega \\
 & \Omega_2 \arrow[ur, "\bar{\phi}_1"'] &
\end{tikzcd}
$$

Da $\bar{\phi}_1$ und $\bar{\phi}_2$ Isomorphismen sind, kann man $\alpha = (\bar{\phi}_1)^{-1} \circ \bar{\phi}_2$ nehmen. *Q.E.D.*

Satz 54 *Es sei K ein Körper. Es sei $K \subset \Omega$ ein algebraischer Abschluß von K.*

Es sei L/K eine endliche Erweiterung. Dann sind die folgenden Bedingungen äquivalent:

(i) Es gibt einen Isomorphismus von Ω-Algebren

$$L \otimes_K \Omega \cong \prod \Omega.$$

(ii) Es gibt $[L : K]$ verschiedene K-Algebrahomomorphismen $L \to \Omega$.

(iii) Der Ring $L \otimes_K \Omega$ ist reduziert.

(iv) Für jede endliche Erweiterung E/K ist der Ring $L \otimes_K E$ reduziert.

(iv) Für jede Erweiterung E/K ist der Ring $L \otimes_K E$ reduziert.

Beweis: ((*iii*) $\Rightarrow$ (*i*)): Angenommen $R := L \otimes_K \Omega$ ist reduziert. Es seien $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ maximale Ideale von R. Nach dem Chinesischen Restsatz hat man eine Surjektion von Ω-Algebren

$$R \to \prod_{i=1}^{r} R/\mathfrak{m}_i. \tag{9}$$

Daraus folgt $r \leq [L : K] = \dim_\Omega R$. Deshalb gibt es nur endlich viele maximale Ideale. Wir können voraussetzen, dass wir sie bereits alle aufgezählt haben. Da R eine endlichen Ω-Algebra ist, ist jedes Primideal von R maximal. Also besteht der Kern von (9) aus nilpotenten Elementen. Da R als reduziert vorausgesetzt ist, ist (9) ein Isomorphismus. Da $\Omega \to R/\mathfrak{m}_i$ für jedes i endlich ist und Ω algebraisch abgeschlossen, ist dies ein Isomorphismus. *Q.E.D.*

Beispiel: Es sei $f(T) \in K[T]$ ein irreduzibles unitäres Polynom vom Grad $d \geq 1$. Es sei $L = K[T]/f(T)K[T]$. Dann ist die Anzahl der verschiedenen K-Algebrahomomorphismen $L \to \Omega$ gleich der Anzahl der verschiedenenen Nullstellen von $f(T)$:

$$\sharp \operatorname{Hom}_{K-Alg}(L, \Omega) = \sharp\{\text{verschiedene Nullstellen von } f(T)\}.$$

Insbesondere ist L/K genau dann separabel, wenn $f(T)$ keine mehrfachen Nullstellen hat oder äquivalent dazu wenn die Ableitung $f'(T)$ ein von 0 verschiedenes Polynom ist. In diesem Fall sagen wir auch, dass $f(T)$ ein separables Polynom ist.

Wenn K ein Körper der Charakteristik 0 ist, so ist offensichtlich $f'(T) \neq 0$ und daher L/K stets separabel.

Es sei E/K eine Körpererweiterung. Es sei $\omega \in E$ ein Element, dass ganz über K ist. Wir betrachten den K-Algebrahomomorphismus

$$K[T] \to E, \quad T \mapsto \omega.$$

Der Kern ist eine Primideal, das von einem irreduziblen unitären Polynom $f(T) \in K[T]$ erzeugt wird. Wir nennen f das irreduzible Polynom von ω. Nach Definition gilt $f(\omega) = 0$. Der Körper $K[\omega] \cong K[T]/f(T)K[T]$ ist also genau dann separabel, wenn f separabel ist. Wir sagen dann auch ω ist separabel.

Corollary 55 *(i) Es sei L/K endlich separabel. Es sei Z ein Körper, so dass $K \subset Z \subset L$. (Wir nennen Z/K eine Teilerweiterung von L/K.*

Dann ist T/K separabel.

(ii) Es sei E/K eine endliche Erweiterung und es seien E_i/K, $i = 1, 2$ zwei Teilerweiterungen. Wir nehmen an, dass $E_1 \otimes_K E_2 \to E$ surjektiv ist.

Wenn E_i/K, $i = 1, 2$ separabel sind, so auch E/K.

(iii) Es seien L/K und E/L zwei separable Erweiterungen.

Dann ist E/L separabel.

Definition 56 *Es sei K ein Körper der Charakteristik p. Es sei $K \subset \Omega$ ein algebraischer Abschluss. Wir bezeichnen mit Ω_s die Menge aller $\omega \in \Omega$, die separabel über K sind. Das ist ein Körper. Wir nennen Ω_s den separablen Abschluß von K.*

Wenn $\omega \in \Omega$ so gibt es eine Potenz p^t, so dass $\omega^{p^t} \in \Omega_s$.

Die Einschränkung eines Automorphismus von K-Algebren $\phi : \Omega \to \Omega$ auf Ω_s ist ein K-Algebraautomorphismus $\phi_s : \Omega_s \to \Omega_s$. In der Tat: Es sei $\omega \in \Omega_s$ und $f(T)$ das irreduzible Polynom von ω. Die Nullstellen von $f(T)$ in Ω sind alle separabel und werden von ϕ permutiert. Also gilt $\phi(\omega') = \omega$ für eine Nullstelle ω' von $f(T)$. Also gilt $\omega \in \phi(\Omega_s)$ Also ist ϕ_s ein Automorphismus. Wir schreiben im folgenden einfach ϕ für ϕ_s.

Lemma 57 *Die Einschränkung ist ein Isomorphismus von Gruppen*

$$\mathrm{Aut}_K(\Omega) \longrightarrow \mathrm{Aut}_K(\Omega_s).$$

Hier ist $\mathrm{Aut}_K(\Omega)$ die Gruppe aller Automorphismen der K-Algebra Ω.

Es sei R ein kommutativer unitärer Ring. Es sei $\iota : N \to M$ ein Homomorphismus von R-Moduln. Wir sagen, dass ι ein direkter Summand ist, wenn ein R-Modulhomomorphismus $p : M \to N$ existiert, so dass $p \circ \iota = \mathrm{id}_N$. Dann ist ι injektiv.

Es sei $\phi : R \to S$ ein unitärer Ringhomomorphismus. Wenn $\iota : N \to M$ ein direkter Summand ist, so auch $\breve{\iota} : N \otimes_R S \to M \otimes_R S$, $\breve{\iota}(n \otimes s) := \iota(m) \otimes s$. Insbesondere ist $\breve{\iota}$ injektiv.

Wir sagen, dass ein direkter Summand $\tilde{N} \subset M \otimes_R S$ im Sinne von S-Moduln über R definiert ist, wenn ein direkter Summand $\iota : N \to M$ im Sinne von R-Moduln existiert, so dass $\tilde{N}$ das Bild von $\breve{\iota}$ ist. Dann hat man einen Isomorphismus $N \otimes_R S \cong \tilde{N}$.

Lemma 58 *Es sei R ein Körper. Es sei $\phi : R \to S$ ein unitärer Ringhomomorphismus. Dann ist ϕ injektiv. Es sei V ein R-Vektorraum. Der R-Modulhomomorphismus $\kappa_V : V \to V \otimes_R S$, $\kappa_V(v) = v \otimes 1$ ist injektiv. Es sei $\tilde{W} \subset V \otimes_R S$ ein direkter Summand im Sinne von S-Moduln.*

$\tilde{W}$ ist genau dann über R definiert, wenn Elemente $v_i \in V$, $i \in I$ existieren, so dass $\kappa_V(v_i) \in \tilde{W}$ und diese Elemente $\tilde{W}$ als S-Modul erzeugen.

Beweis Die Elemente v_i erzeugen einen R-Untervektorraum U von V. Dann ist W ein direkter Summand von V und wir bekommen eine Injektion

$$W \otimes_R S \to V \otimes_R S.$$

Das Bild ist $\tilde{W}$, d.h. $W \otimes_R S \cong \tilde{W}$. Wenn man ein Basis von W wählt und sie zu einer Basis von V ergänzt, so sieht man

$$W = \tilde{W} \cap V := \kappa_V^{-1}(\tilde{W}).$$

Q.E.D.

Beweis: Die Elemente v_i erzeugen einen R-Untervektorraum W von V. Dann ist W ein direkter Summand von V und wir bekommen eine Injektion

$$W \otimes_R S \to V \otimes_R S.$$

Das Bild ist $\tilde{W}$, d.h. $W \otimes_R S \cong \tilde{W}$. Wenn man ein Basis von W wählt und sie zu einer Basis von V ergänzt, so sieht man

$$W = \tilde{W} \cap V := \kappa_V^{-1}(\tilde{W}).$$

Satz 59 *(Der Abstieg) Es sei $K \subset \Omega$ ein Homomorphismus von Körpern. Es sei $\mathcal{E}$ eine Menge von K-Algebrahomomorphismen $\Omega \to \Omega$, so dass*

$$K = \{\omega \in \Omega \mid \phi(\omega) = \omega, \textit{ für alle } \phi \in \mathcal{E}\}$$

Es sei V ein K Vektorraum. Dann ist $V \otimes_K \Omega$ ein Ω-Vektorraum.

Für $\phi \in \mathcal{E}$ sei

$$\begin{array}{rccc} \phi_*: & V \otimes_K \Omega & \to & V \otimes_K \Omega \\ & v \otimes \omega & \mapsto & v \otimes \phi(\omega). \end{array}$$

ϕ_* ist eine K-lineare Abbildung. (Aber es ist kein Homomorphismus von Ω-Vektorräumen.)

Ein Ω-Untervektorraum $\tilde{W} \in V \otimes_K \Omega$ ist genau dann über K-definiert, wenn für alle $\phi \in \mathcal{E}$ gilt, dass $\phi_*(\tilde{W}) \subset \tilde{W}$. (vgl. Lemma 58).

Hauptsatz der Galoistheorie

Es sei K ein Körper. Es sei $K \subset \Omega$ ein algebraischer Abschluss von K. Es sei E/K eine separable Erweiterung von K. Es sei $K \subset \Omega$ ein algebraischer Abschluss von K und Ω_s der separable Abschluss.

Es sei $G = \mathrm{Aut}_K(\Omega) = \mathrm{Aut}_K(\Omega_s)$.

Lemma 60

$$K = \{\omega \in \Omega_s \mid \phi(\omega) = \omega \textit{ für alle } \phi \in G\}.$$

Die rechte Seite sind die Elemente von Ω_s die unter G invariant sind. Wir schreiben dafür Ω_s^G.

Wir bezeichnen mit $\mathcal{F}_E$ die Menge der K-Algebrahomomorphismen $E \to \Omega$. (Das Bild liegt auromatisch in Ω_s. Das ist eine endliche G-Menge mit $[E : K]$ Elementen. Wenn $\alpha : L \to E$ ein Homomorphismus von separablen Erweiterungen von K ist, so erhält man eine Abbildung von G-Mengen

$$\alpha^* : \mathcal{F}_E \to \mathcal{F}_L, \quad \alpha^*(\iota) = \iota \circ \alpha : L \to E \to \Omega.$$

Die Zuordnung $E \mapsto \mathcal{F}_E$ ist ein kontravarianter Funktor von der Kategorie der separablen Körpererweiterungen von K in die Kategorie der G-Mengen.

Satz 61 *Die Abbildung*

$$\begin{array}{ccc} \mathrm{Hom}_{K-Alg}(L,E) & \longrightarrow & \mathrm{Hom}_{G-Mengen}(\mathcal{F}_E, \mathcal{F}_L) \\ \alpha & \mapsto & \alpha^* \end{array}$$

ist bijektiv.

Man kann den Körper E wie folgt aus der G-Menge $\mathcal{F}_E$ rekonstruieren. Es sei $\iota \in \mathcal{F}_E$. Der Körper $\iota(E) \subset \Omega_s$ ist zu E isomorph. Es sei

$$G(\iota) = \{g \in G \mid g\iota = \iota\}$$

der Stabilisator in G von ι. Dann ist $G(\iota)$ die Menge der Automorphismen der $\iota(E)$-Algebra Ω_s. Daher gilt nach Lemma 60, dass

$$\iota(E) = \Omega_s^{G(\iota)}. \tag{10}$$

Theorem 62 *Es sei E/K eine separabel Erweiterung. Es sei $u : \mathcal{F}_E \to \mathcal{F}$ eine Surjektion von G-Mengen.*

Dann gibt es einen K-Algebrahomomorphismus $\alpha : L \to E$ und einen Isomorphismus von G-Mengen $\tau : \mathcal{F} \to \mathcal{F}_L$, so dass folgendes Diagramm kommutativ ist

$$\begin{tikzcd} \mathcal{F}_E \arrow[rr, "u"] \arrow[dr, "\alpha^*"'] & & \mathcal{F}, \arrow[dl, "\tau"] \\ & \mathcal{F}_L & \end{tikzcd}$$

wobei τ ein Isomorphismus von G-Mengen ist.

Bemerkung: Wir wählen eine Einbettung $\iota \in \mathcal{F}_E$. Es sei $\kappa := u(\iota)$ und $\lambda = \alpha^*(\iota)$. Da τ ein Isomorphismus ist haben wir gleiche Stabilisatoren.

$$\Omega_s^{G(\lambda)} = \Omega_s^{G(\kappa)} \subset \Omega_s^{G(\iota)}.$$

Die letzte Inklusion gilt weil $G(\iota) \subset G(\kappa)$. Daher gilt nach (10)

$$\lambda(L) = \Omega_s^{G(\kappa)} \subset \iota(E).$$

Das zwingt uns für α die Inklusion zu nehmen

$$L := \iota^{-1}(\Omega_s^{G(\kappa)}) \subset E. \tag{11}$$

Wenn wir die entsprechende Abbildung $\alpha^* : \mathcal{F}_E \to \mathcal{F}_L$ betrachten, so ist nach (11) das Kompositum $L \to E \xrightarrow{\iota} \Omega_s$ invariant unter $G(\kappa)$. Daher erhält man eine Abbildung von G-Mengen $\tau : \mathcal{F} \to \mathcal{F}_L$. Der Satz behauptet, dass dies ein Isomorphismus ist.

Wir können das auch so ausdrücken: Wir betrachten die Abbildung von G-Mengen $G/G(\iota) \to \mathcal{F}_E$, die g auf $g\iota$ abbildet. Man bekommt man ein kommutatives Diagramm

$$\begin{array}{ccc} G/G(\iota) & \longrightarrow & \mathcal{F}_E \\ \downarrow & & \downarrow \\ G/G(\kappa) & \longrightarrow & \mathcal{F} \end{array}$$

dessen horizontale Pfeile bijektiv sind.

Deshalb kann man den letzten Satz 62 in Termen von $E' = \iota(E)$ und $L' = \iota(L)$ auch so formulieren

Corollary 63 *Es sei $E' \subset \Omega_s$ eine separable Erweiterung von K. Es sei $I = \mathrm{Aut}_{E'}(\Omega) \subset G$. Es sei H eine Untergruppe von G, so dass $I \subset H \subset G$.*

Dann gibt es eine Köpererweiterung L'/K, so dass $K \subset L' \subset E'$ und so dass $H = \mathrm{Aut}_{L'}(\Omega)$.

Vor dem Beweis von Satz 62 erklären wir eine elementare Variante. Es sei dafür Ω ein beliebiger Körper. Es sei A eine endliche Menge. Dann betrachten wir den Ring (7)

$$R = \Omega^A = \Omega \times \ldots \times \Omega,$$

wobei rechts $|A|$-Exemplare stehen. Um die Bezeichnungen zu vereinfachen nehmen wir $A = [1, n]$ an. Wir schreibe ein Element $\underline{\omega} \in R$ als Zeilenvektor $\underline{\omega} = (\omega_1, \dots, \omega_n)$. Wenn $I \subset \Omega$ so bezeichnen wir mit $e_I \in R$ den Zeilenvektor $\underline{\omega}$, so dass $\omega_i = 1$ für $i \in I$ und $\omega_j = 0$ für $j \notin I$.

Der Ringhomomorphismus

$$\Omega \to R, \quad \omega \to (\omega, \omega, \dots, \omega)$$

macht R zu einer Ω-Algebra.

Wenn $i \in A$, so sei $p_i : R \to \Omega$ die Abbildung $p_i(\underline{\omega}) = \omega_i$. Das ist ein Ω-Algebrahomomorphismus.

Lemma 64

$$\mathcal{F}_R := \mathrm{Hom}_{\Omega-Alg}(R, \Omega) = \{p_i \mid i \in A\}$$

Hier steht links die Menge der Algebrahomomorphismen, die wir mit $\mathcal{F}_R$ bezeichnen. Insbesondere ist $|\mathcal{F}_R| = \dim_\Omega R$ die Dimension des Vektorraums R.

Satz 65 *Es sei $S \subset R = \Omega^A$ ein Ω-Unteralgebra. Dann existiert eine Zerlegung von A in disjunkte nichtleere Teilmengen*

$$A = I_1 \cup I_2 \cup \ldots \cup I_m,$$

so dass $e_{I_1}, \ldots e_{I_m}$ eine Basis des S-Vektorraumes Ω ist.

Wir schreiben die Zerlegung mit Hilfe ihrer klassifizierenden Abbildung

$$u : A \to C = \{I_1, I_2 \ldots I_m\},$$

Dann können den letzten Satz wie folgt formulieren:

Corollary 66 *Die Ω-Unteralgebren von $R = \Omega^A$ entsprechen bijektiv den surjektiven Abbildungen $u : A \to C$.*

Dabei entspricht u der folgenden Algebra

$$S = \{\underline{\omega} \in R \mid p_i(\underline{\omega}) = p_j(\underline{\omega}) \textit{ für alle } i, j \in A \textit{ so dass } u(i) = u(j)\}.$$

Die Einschränkung von p_i auf S ist ein Ω-Algebrahomorphismus $S \to \Omega$. Das definiert eine Abbildung $\rho : \mathcal{F}_R \to \mathcal{F}_S$. Diese Abbildung faktorisiert über eine Bijektion τ:

$$\begin{tikzcd} A = \mathcal{F}_R \arrow[rr, "\rho"] \arrow[dr, "u"'] & & \mathcal{F}_S \arrow[dl, "\tau"] \\ & C & \end{tikzcd}$$

Man hat einen Isomorphismus

$$S \to \Omega^{\mathcal{F}_S}, \quad s \mapsto (\ldots, q(s), \ldots),$$

wobei $q \in \mathcal{F}_S$ alle Elemente durchläuft.

Beweis des Hauptsatzes 62
Man hat

$$\mathcal{F}_E := \mathrm{Hom}_{K-Alg}(E, \Omega) \cong \mathrm{Hom}_{\Omega-Alg}(E \otimes_K \Omega, \Omega).$$

Die Abbildung u entspricht einer Unteralgebra $\tilde{L} \subset E \otimes_K \Omega$. Nach Voraussetzung ist der Ω-Untervektorraum $\tilde{L} \subset E \otimes_K \Omega$ über K definiert. Also gibt es einen K-Untervektorraum $L \subset E$, so dass $\tilde{L} = L \otimes_K \Omega$. Es gilt:

$$L = \tilde{L} \cap E = \{v \in E \otimes_K \Omega \mid g(v) = v, \text{ für alle } g \in G\}.$$

Daraus sieht man, dass L eine K-Algebra ist.

Man hat

$$\mathcal{F}_L := \mathrm{Hom}_{K-Alg}(L, \Omega) = \mathrm{Hom}_{\Omega-Alg}(\tilde{L}, \Omega) = \mathcal{F},$$

wo die letzte Gleichung die Definition von $\tilde{L}$ ist. Das beendet den Beweis.

Traditionelle Form der Galoistheorie.

Ein Teilkörper $N \subset \Omega_s$ heißt normal, wenn für alle $g \in G$, gilt dass $gN \subset N$.

Wenn E/K eine separable Erweiterung ist, so ist das Kompositum der Körper $\phi(E)$, wo $\phi \in \mathcal{F}_E$ ein Normalkörper. Man hat eine Surjektion

$$G \to \mathrm{Aut}_K(N).$$

Man hat eine Bijektion zwischen den Untergruppen $H \subset \mathrm{Aut}_K(N)$ und der Teilkörperen $L \subset N$:

$$L = N^H, \quad H = \mathrm{Aut}_L(N).$$