Algebra 1

B. Herzog
Leipzig 2013/2014

Mo. 15.15-16.45 Hs. 11
Di. 13.15-14.45 Hs 5

Zu den Prüfungen

- Jede Woche werden Übungsaufgaben ins Netz gestellt, die in der nächsten Woche in den Seminaren abzugben sind und die mit Punkten bewertet werden.
- Zur Erlangung des Übungsscheins werden fünfzig Prozent der maximalen Punktzahl benötigt.
- Nach dem Ende der Vorlesung findet eine mündliche Prüfung statt. Der Übungsschein gilt als Zulassung zu dieser Prüfung.

Prüfungstage:
Fr. der 21.2.2014
Mo. der 24.3.2014
Fr. der 4.4.2014

Bezeichnungen

A_n	alternierende Gruppe, vgl.1.2.1
Aut(G)	Gruppe der Automorphismen der Gruppe G, vgl. 1.1.1
C(G)	Zentrum der Gruppe G, vgl. 1.1.10
det A	Determinante der quadratischen Matrix A, vgl. 1.1.5
E_{ij}	Elementarmatrix mit einer Eins in der Position (i,j) und Nullen in allen übrigen Positionen, vgl. 2.2.1 Beispiel 3.
G(K/k)	Galois-Gruppe der Galois-Erweiterung K/k, vgl. 3.7.1
GL(n, K)	allgemeine lineare Gruppe der umkehrbaren n×n-Matrizen über dem Körper K, vgl. 1.1.3
GL(V)	allgemeine lineare Gruppe des Vektorraums V, vgl. 1.1.3
Im(h)	Bild des Homomorphismus h, 1.1.11
Ker(h)	Kern des Homomorphismus h, 1.1.11
O(V)	orthogonale Gruppe des Vektorraums V mit Bilinearform, vgl. 1.1.6
O(x)	Orbit des Elements x bei einer Gruppen-Operation, vgl. 1.2.14
S(M)	Gruppe der Permutationen der Menge M, vgl. 1.1.2
S_n	Gruppe der Permutationen der Menge {1,2,...,n}, vgl. 1.1.2
SL(n,K)	spezielle lineare Gruppe über dem Körper K, vgl. 1.1.4
SL(V)	spezielle lineare Gruppe des Vektorraums V, vgl. 1.1.4
Sp(V)	symplektische Gruppe des symplektischen Vektorraums V, vgl. 1.1.7
U(n)	unitäre Gruppe, vgl. 1.1.8
U(V)	unitäre Gruppe des hermitischen Vektorraums V, vgl. 1.1.8
AB	Produkt zweier Teilmengen einer Gruppe, vgl. 1.3.3.
G'×G"	direktes Produkt der Gruppen G' und G", vgl. 1.1.12
(G:U)	der Index von U in G, d.h. die Anzahl der Nebenklassen der Gruppe G modulo der Untergruppe U, vgl. 1.3.2
$[K:k]_s$	Separabilitätsgrad der endlichen Körpererweiterung K/k, vgl. 3.5.1
#M	Anzahl der Elemente der Menge M, vgl. 1.1.2
R*	Gruppe der Einheiten des Rings R mit Eins, vgl. 1.1.9
<M>	die von der Menge M erzeugte Untergruppe, vgl. 1.2.4

$\langle g \rangle$	die vom Element g erzeugte zyklische Gruppe, vgl. 1.2.5
G/U	die Menge der Linksnebenklassen von G modulo U, vgl. 1.3.1 und 1.3.4
U\G	die Menge der Rechtsnebenklassen von G modulo U, vgl. 1.3.1 und 1.3.4
G_m	Stabilisator des Elements m bei der Operation der Gruppe G, vgl. 1.6.2

0. Einleitung

Wie Sie im vergangenen Studienjahr gelernt haben, besteht Mathematik im Verstehen und Finden von Beweisen.

Das Finden von Beweisen lernt man, indem man sich Beweise anderer Mathematiker ansieht und diese versucht zu verstehen.

Ihre bisherige Kenntnis beschränkt sich allerdings mehr auf Beweis-Fragmente oder einfache Fakten und Theorien, die mehr oder weniger durch das systematische Sammeln mehr oder weniger offensichtlicher Fakten gewonnen wurden.

Wer wirklich zu verstehen will, was Mathematik ist, sollte mindestens einmal einem Mathematiker oder noch besser der mathematischen Gemeinde bei der Lösung eines echten Problems zugesehen haben, d.h. bei der Lösung eines Problems, das eine zeitlang offen war und von dem nicht nach einer kurzen Analyse klar war, wie es zu lösen ist.

Beim jetzigen Aufbau des Mathematik-Studiums haben sie maximal zwei solche Gelegenheiten. Die eine Gelegenheit bietet diese Vorlesung, die andere werden Sie haben, wenn Sie die Spezialisierungsrichtung Funktionalanalysis wählen und in den zugehörigen Vorlesungen die Theorie der Soboljev-Räume und die Lösung der Laplace-Gleichung

$$\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial x^2}\right) f = u$$

kennenlernen. Es geht dabei darum, zu zeigen, daß die Lösung f dieser Gleichung existiert (und unendlich oft differenzierbar ist, falls u diese Eigenschaft besitzt). In der Mitte des 19. Jahrhunderts wurden diese Aussage von Riemann bei der Entwicklung der komplexen Analysis benötigt, d.h. die Theorie der komplexwertigen (differenzierbaren) Funktionen einer komplexen Veränderlichen. Riemann selbst konnte diese Aussage nicht beweisen, so daß eine der schönsten mathematischen Theorien ca. 80 Jahre lang auf schwachen Füßen stand. In gewisser Weise kann man sagen, die Funktionalanalysis wurde in der ersten Hälfte des 20. Jahrhunderts entwickelt um dieses Problem zu lösen.

Die vorliegende Vorlesung behandelt die Lösung einiger klassischer Probleme die zum Teil bereits in der antiken Mathematik gestellt, über Jahrhunderte offen waren und erst in der Neuzeit gelöst wurden. Der größte Teil der Vorlesung befaßt sich mit der Bereitstellung der zur Lösung benötigten algebraischen Konstruktionen.

0.1 Die Probleme

Zu den betrachteten Problemen gehören die folgenden.

Die Dreiteilung eines Winkels
Die Quadratur des Kreises
Das Delische Problem
Die Frage nach der Lösungsformel für eine algebraische Gleichung eines Grades größer als 4

Die Dreiteilung eines Winkels
Ein gegebener Winkel soll mit Zirkel und Lineal in drei gleiche Teile geteilt werden.

Die Quadratur des Kreises
Zu einem gegebenen Kreis soll ein Quadrat mit demselben Flächeninhalt konstruiert werden. Hat der Kreis in einer geeigneten Längeneinheit den Radius 1, so ist also ein Quadrat mit der Kantenlänge

$$\sqrt{\pi}$$

zu konstruieren.

Das Delische Problem
Als sich die Delier wegen einer überstandenen Pest an das Orakel von Delphi wandten und fragten, wie sie sich für ihr Überleben bedanken könnten, erhielten sie von Apollon den Antwort, sie sollten dessen Altar zu verdoppeln. Der Altar des Apollon ist ein Würfel aus Gold. Hat dieser Würfel in irgendeiner Längeneinheit die Kantenlänge 1, so besteht die Aufgabe also darin, einen Würfel mit dem Volumeninhalt 2 zu konstruieren, d.h. mit der Kantenlänge

$$\sqrt[3]{2}$$

zu konstruieren. Diese Konstruktion ist, wie bei den alten Griechen üblich, mit Zirkel und Lineal auszuführen.

Lösungsformeln für algebraische Gleichungen großen Grades
Wir wissen, eine quadratische Gleichung

$$x^2 + px + q = 0$$

besitzt die Lösungen

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}\,.$$

Das Problem besteht darin, eine ähnliche Lösungsformel für algebraische Gleichungen höheren Grades zu finden. Genauer: gesucht ist eine Formel für die Nullstellen eines Polynoms, in welcher außer den vier Grundrechenarten nur noch Wurzelausdrücke vorkommen. Ausdrücke dieser Gestalt nennt man auch Radikale. Man spricht deshalb auch von der Lösung algebraischer Gleichungen durch Radikale.

Bei allen angegeben Problemen haben sich über Jahrhunderte die jeweils besten Mathematiker ihrer Zeit vergeblich bemüht eine Lösung zu finden. Als das schwierigste aller Probleme erwies sich das zuletzt aufgeführte. Man fand ziemlich schnell Lösungsformeln für Gleichungen dritten und vierten Grades, aber dann gab es über Jahrhunderte überhaupt keinen Fortschritt.

Erst gegen Ende des 19. Jahrhunderts hatte ein junger Mathematiker die entscheidene Idee (wahrscheinlich bereits im Alter von 16. Jahren) und hat damit die Mathematik revolutioniert: der französische Mathematiker Evariste Galois. Leider ist es ihm nicht gelungen, die damaligen mathematischen Autoritäten (wie zum Beispiel Cauchy oder Poisson) von seiner Idee zu überzeugen. Cauchy hat vermutlich Galois' zur Veröffentlichung eingereichte Arbeiten ungelesen in den Papierkorb geworfen - möglicherweise aus politischer Feindschaft - Cauchy war Royalist und Galois war Republikaner. Poisson hat die Arbeit mit der Bemerkung zurückgeschickt, daß er sie nicht verstehe und Galois doch seine Aussagen erst einmal ordentliche aufschreiben solle. Man muß dazu sagen, Galois war kein ausgebildeter Mathematiker und hat nie ein ordentliches Mathematik-Studium absolviert. Auf der Ecole Polytechnique wurde er abgeleht - er soll währende der Aufnahmeprüfung dem Prüfer ein Tintenfaß an den Kopf geworden haben - aus Wut über dessen triviale Fragen.

Galois wurde mit 21 Jahren in ein Duell verstrickt und ist dabei gestorben. Er glaubte wohl, für die Ehre einer Dame einzustehen. Von der wurde aber bekannt, daß es nur ein Lockvogel seiner politschen Gegner war.

In der Nacht vor dem Duell schrieb Galois seine Lösung des Problems noch einmal auf. Sei Bruder schickte dieses Schriftstücke an alle bekannten Mathematiker der damaligen Zeit. Unter anderem auch an Gauß. Aber vergeblich, auch von Gauß ist keine Reaktion bekannt. Galois war auch Jahre nach seinem Tod als Mathematiker völlig unbekannt.

Seine Beweisschrift wurde später durch Zufall in einer Bibliothek entdeckt und durch Jordan und Liouville in eine allgemein verständliche Sprache übersetzt und bekannt gemacht.

0.2 Der Lösungsansatz für die geometrischen Probleme

Die Lösung aller genannten Aufgaben besteht darin, zu zeigen, daß es keine Lösung gibt.

Die Beweis-Idee besteht darin, die Körper zu betrachten, die von den Kordinaten der interessierenden Punkte erzeugt werden.

Bezeichnungen

Seien K ein Körper und $k \subseteq K$ ein Teilkörper. Dann heißt K auch Erweiterungskörper von k und man spricht von einer Körpererweiterung K/k. Für jede Körpererweiterung K/k heißt die Dimension

$$[K:k] := \dim_k K,$$

welche K als Vektorraum über k hat auch Grad der Körpererweiterung K/k. Ist dieser Grad endlich, so heißt K/k auch endliche Körpererweiterung.

Seien K/k eine Körpererweiterung und

$$a_1, \dots, a_n \in K$$

irgendwelche Elemente des großen Körpers. Dann bezeichnet

$$k(a_1, \dots, a_n)$$

den kleinsten Teilkörper von K, der den Körper k und die Elemente $a_1, \dots, a_n$ enthält.[1] Es ist nicht schwer, zu zeigen, ein solcher Körper existiert stets.[2] Er heißt der über k von $a_1, \dots, a_n$ erzeugte Körper. Allgemeiner bezeichnet man für beliebige Punkte

$$p_1, \dots, p_n \in K^d$$

mit

$$k(p_1, \dots, p_n),$$

den von allen Koordinaten aller p_i über k erzeugte Körper. Man nennt ihn auch den über k von den Punkten p_i erzeugten Körper.

---

[1] Er soll in jedem Teilkörper von K enthalten sein, der den Körper k und alle a_i enthält. Formal kann man ihn als Durchschnitt aller Teilkörper von K definieren, welche k und alle a_i enthalten.

[2] Es wird in derselben Weise gezeigt, wie man die Existenz des kleinsten linearen Unterraums bewiesen wird, der eine gegeben Menge von Vektoren enthält.

Der erste Lösungsschritt besteht darin, die Körper

$$K := k(p_1, \dots, p_n)$$

zu beschreiben, die von Punkten erzeugt werden, welche man mit Hife von Zirkel und Lineal konstruieren kann, d.h. durch die folgenden Operationen:

1) Ziehen einer Geraden durch zwei gegebene Punkte.
2) Schlagen eines Kreises um einen gegebenen Punkt mit einem Radius, der gleich dem Abstand zweier gegebener Punkte ist.
3) Hinzufügen zu den gegebenen Punkten des Schnittpunkts zweier Geraden wie in 1.
3) Hinzufügen zu den gegebenen Punkten der Schnittpunkte einer Geraden wie in 1 mit einem Kreis wie in 2.
4) Hinzufügen zu den gegebenen Punkten der Schnittpunkte zweier Kreise wie in 2.

Dies wird im wesentlichen in den Übungsaufgaben der ersten Serie getan. Der wesentliche Punkt ist bei den geometrischen Aufgaben der Körpergrad der zugehörigen Erweiterung K/k. In den Übungsaufgaben wird gezeigt, daß dieser Körpergrad eine Potenz von 2 sein muß.

Die Lösung der geometrischen Probleme besteht im Beweis der Tatsache, daß die Koordinaten der gesuchten Punkte in keiner Erweiterung von $\mathbb{Q}$ liegen können, deren Grad eine Potenz von 2 ist.

Am leichtesten ist dies beim Delischen Problem: eine einfache Untersuchung zeigt, die zugehörige Erweiterung hat den Grad 3 und kann deshalb in keiner Erweiterung liegen, deren Grad eine Potenz von 2 ist.

Bei den anderen Problemen kommen transzendente Zahlen ins Spiel. In diesen Fällen sind die hier angegebenen Beweise unvollständig, weil wir aus Zeitgründen auf den Transzendenzbeweis zum Beispiel für die Zahl π verzichten müssen.

0.3 Lösungsansatz für das algebraische Problem

Am schwierigsten ist der Beweis für die Unlösbarkeit des Problems im Fall der Lösbarkeit von polynomialen Gleichungen durch Radikale. Hier werden wir jedoch den Beweis in allen Einzelheiten angeben und insbesondere die Theorie von Galois beschreiben.

Sei

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

ein Polynom in einer Unbestimmten x mit Koeffizienten aus einem Körper k. Seien weiter

$$\alpha_1, \dots, \alpha_r$$

die Nullstellen, die p (in irgendeinem Erweiterungskörper) hat und sei

$$L = k(\alpha_1, \dots, \alpha_r)$$

der von diesen Nullstellen erzeugte Erweiterungskörper.

Die Frage besteht darin, ob sich die α_i durch Rechenausdrücke in den Elementen von k darstellen lassen, in denen neben den vier Grundrechenarten noch Wurzelzeichen vorkommen dürfen.

Bezeichnung

Sei K/k eine endlich Körpererweiterung. Man sagt K wird über k durch Radikale erzeugt oder auch K/k ist eine Erweiterung durch Radikale, wenn es eine endlich Folge von Zwischenkörpern gibt, sage wir

$$k = K_0 \subseteq K_1 \subseteq ... \subseteq K_n = K$$

mit

$$K_i = K_{i-1}(\sqrt[n_i]{d_i})$$

wobei n_i eine natürliche Zahl und d_i ein Element von K_{i-1} ist.

Die zu lösende Frage ist hier die Frage, wann die zum Polynom p gehörige Erweiterung L/k eine Teilerweiterung einer Erweiterung durch Radikale ist,

$$L \subseteq K \text{ mit } K/k \text{ Erweiterung durch Radikale.}$$

Wie oben kommt es auf eine geeignete Charakterisierung der Erweiterungen K/k durch Radikale an. Mit Dimensionsberechnungen kommt man hier aber nicht weiter. Die Charakterisierung ist viel raffinierter. Stattdessen muß man hier die Automorphismengruppe

$$G = Aut_k K = \{ f: K \longrightarrow K \mid f \text{ ist k-linear, } f(xy) = f(x)f(y) \text{ für } x,y \in L, f(c) = c \text{ für } c \in k\}$$

der betrachteten Erweiterung untersuchen. Man muß Folgen von Untergruppen

$$\{1\} = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

betrachten und die zugehörigen Faktorgruppen G_i/G_{i-1}. An diesen kann man ablesen, ob die Gruppe von einer Erweiterung durch Radikal kommt. Die zugehörige Gruppen-Eigenschaft nennt man Auflösbarkeit und spricht von auflösbaren Gruppen.

Das erste Drittel dieser Vorlesung hat das Ziel, den Begriff der auflösbaren Gruppe zu definieren.

0.4 Zusammenfassung

Damit stehen zwei Bestandteile der Vorlesung fest:

Gruppentheorie
Körpertheorie

und außerdem der Bestandteil der sich mit dem Zusammenhang zwischen Gruppen und Körpern beschäftigt:

Galoistheorie

Um Körpertheorie zu betreiben braucht man noch einen weiteren vorbereitenden Bestandteil: da Körper speziellen Ringe sind und Ringe bei der Konstruktion von Körpern eine Rollen spielen, müssen wir uns auch mit

Ringtheorie

beschäftigen. Damit steht der grobe Aufbau der Vorlesung fest:

1. Gruppen
2. Ringe
3. Körper

1. Gruppen

1.1. Definition und Beispiele

1.1.1 Gruppen und Gruppenhomomorphismen

Eine Gruppe G ist eine Menge zusammen mit einer Abbildung

$$G\times G \longrightarrow G, (x,y) \mapsto xy,$$

genannt Gruppenoperation, mit den folgenden Eigenschaften.

(i) Die Gruppenoperation ist assoziativ,

$$(xy)z = x(yz) \text{ für } x,y,z\in G.$$

(ii) Sie besitzt ein neutrales Element e,

$$ex = xe = x \text{ für } x\in G.$$

(iii) Jedes Element x der Gruppe besitzt ein Inverses x^{-1},

$$xx^{-1} = x^{-1}x = e.$$

Die Gruppe heißt abelsch oder auch kommutativ, falls außerdem das Kommutativgesetz gilt,

$$xy = yx \text{ für } x,y\in G.$$

Ein (Gruppen-) Homomorphismus ist eine Abbildung

$$h: G \longrightarrow G'$$

einer Gruppe G in eine Gruppe G' mit h(xy) = h(x)h(y). Ein (Gruppen-) Homomorphismus h: $G\longrightarrow G'$, für welchen es einen (Gruppen-) Homomorphismus g: $G'\longrightarrow$ G gibt mit

$$h\circ g = Id \text{ und } g\circ h = Id,$$

heißt (Gruppen-) Isomorphismus. Ein Automorphismus der Gruppe G ist ein Isormorphismus $G \longrightarrow G$. Die Menge der Automorphismen von G wird mit

$$Aut(G)$$

bezeichnet.

Bemerkungen

(i) In nichtabelschen Gruppen schreibt man die Operation im Allgemeinen als Multiplikation, in abelschen Gruppen als Addition. Das neutrale Element bezeichnet man im ersten Fall auch mit 1 und redet vom Einselement, und im letzteren Fall mit 0 und redet vom Nullelement. Im additiven Fall spricht man analog vom Negativen eines Elements x anstatt von dessen Inversen und schreibt -x anstelle von x^{-1},

(ii) Sind x und y Elemente mit

$$xy = e,$$

so sagt man, x ist linksinvers zu y und y ist rechtsinvers zu x. Anstelle von Gruppenaxiom (iii) kann man auch fordern, jedes Element x besitzt ein Linksinverses x' und ein Rechtsinverses x". Es ist dann nämlich automatisch

$$x' = x'e = x'(xx") = (x'x)x" = ex" = x".$$

(iii) Ein Gruppenhomomorphismus h: $G \longrightarrow G'$ überführt das neutrale Element ins neutrale Element,

$$h(e) = e'.$$

Wegen ee = e gilt nämlich h(e)h(e) = h(e), also

$$e' = h(e)h(e)^{-1} = h(e)h(e)h(e)^{-1} = h(e)e' = h(e).$$

(iv) Ein Homomorphismus ist genau dann ein Isomorphismus, wenn er bijektiv ist.

(v) Die Anzahl der Elemente von G heißt Gruppenordnung und wird bezeichnet mit

$$\#\, G := \text{Anzahl der Elemente von } G.$$

(vi) Die Menge Aut G der Automorphismen ist eine Gruppe mit der Komposition von Abbildungen als Gruppenoperation.

1.1.2 Permutationsgruppen

Sei M eine Menge und

$$S(M) = \{ f:M \longrightarrow M \mid f \text{ bijektiv} \}$$

die Menge aller bijektiven Abbildungen $M \longrightarrow M$. Dann ist S(M) ein Gruppe mit der Zusammensetzung von Abbildungen als Gruppenoperation. Diese Gruppe heißt symmetrische Gruppe. Im Fall

$$M = \{1,...,n\}$$

(= Menge der ersten n natürlichen Zahlen) schreibt man auch

$$S_n = S(M).$$

Gruppenordnung ist gleich

$$\# S_n = n!$$

Beispiel 1
$S_1 = \{(1)\}$ ist die kleinstmögliche Gruppe. Sie heißt triviale Gruppe.

Beispiel 2
$S_2 = \{ (1), (12)\}$ ist eine abelsche Gruppe.

Beispiel 3
$S_3 = \{ (1), (12), (13), (23), (123), (321) \}$ ist eine nicht-abelsche Gruppe.

1.1.3 Die allgemeine lineare Gruppe

Seien n eine natürliche Zahl und K ein Körper. Dann ist die Menge

$$GL(n, K) = \{ A \in K^{n \times n} \mid A \text{ umkehrbar} \}$$

der umkehrbaren quadratische n-reihigen Matrizen zusammen mit der gewöhnlichen Matrizen-Multiplikation eine Gruppe. Sie heißt allgemeine lineare Gruppe über K. Analog definiert man

$$GL(V)$$

für jeden K-Vektorraum V als Menge der bijektiven K-linearen Abbildungen $V \longrightarrow V$ mit der Zusammensetzung von Abbildungen als Gruppenoperation.

1.1.4 Die spezielle lineare Gruppe

Seien n eine natürliche Zahl und K ein Körper. Dann ist die Menge

$$SL(n, K) = \{ A \in K^{n \times n} \mid \det A = 1 \}$$

der quadratische n-reihigen Matrizen mit der Determinante 1 zusammen mit der gewöhnlichen Matrizen-Multiplikation eine Gruppe. Sie heißt spezielle lineare Gruppe über K. Analog definiert man

$$SL(V)$$

für jeden endlich-dimensionalen K-Vektorraum V.

1.1.5 Die Determinante als Gruppenhomomorphismus

Die Abbildung

$$\det: GL(n, V) \longrightarrow GL(1, V), A \mapsto \det(A),$$

ist auf Grund des Multiplikationssatzes für Determinanten ein Gruppenhomomorphismus.

1.1.6 Die Orthogonale Gruppe

Sei V ein Vektorraum über dem Körper mit der nicht-entarteten symmetrischen Bilinearform $< , >. V \times V \longrightarrow K$. Dann ist die Menge

$$O(V) := \{ f \in GL(V) \mid <f(x), f(y)> = <x,y> \text{ für } x,y \in V \}$$

zusammen mit der gewöhnlichen Matrizenmultiplikation eine Gruppe, welche orthogonale Gruppe.

Im Fall $V = K^n$ schreibt man auch

$$O(n, K) := O(K^n).$$

Im Fall $V = \mathbb{R}^n$, $n = r + s$, und

$$< \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \dots \\ y_n \end{pmatrix} > = x_1 y_1 + \dots + x_r y_r - x_{r+1} y_{r+1} - \dots - x_n y_n$$

schreibt man auch

$$O(r,s) := O(r,s, \mathbb{R}).$$

Die klassische orthogonale Gruppe ist die Gruppe $O(n, \mathbb{R})$.

Die Gruppe $O(1, 3, \mathbb{R})$ heißt auch Lorenz-Gruppe. Es ist die Gruppe der Relativitätstheorie.

1.1.7 Die Symplektische Gruppe

Seien K ein Körper, V ein K-Vektorraum (endlicher Dimension) mit einer nicht-entarteten schiefsymmetrischen Bilinearform

$$\omega: V \times V \longrightarrow K.$$

Dann besitzt

$$Sp(V) := \{ f \in GL(V) \mid \omega(fx, fy) = \omega(x,y) \text{ für } x,y \in V \}$$

die Struktur einer Gruppe mit der Zusammensetzung von Abbildungen als Gruppenoperation. Die Gruppe heißt symplektische Gruppe von V.

1.1.8 Die unitäre Gruppe

Seien V ein $\mathbb{C}$-Vektorraum (endlicher Dimension) mit einem hermitischen Skalarprodukt

$$< , > : V \times V \longrightarrow \mathbb{C}.$$

Dann besitzt

$$U(V) := \{ f \in GL(V) \mid <fx, fy> = <x, y> \text{ für } x,y \in V \}$$

die Struktur einer Gruppe mit der Zusammensetzung von Abbildungen als Gruppenoperation. Diese Gruppe heißt unitäre Gruppe von V. Im Fall

$$V = \mathbb{C}^n$$

und

$$< \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \dots \\ y_n \end{pmatrix} > = x_1 \overline{y}_1 + \dots + x_n \overline{y}_n$$

schreibt man auch

$$U(n) := U(V).$$

1.1.9 Einheitengruppen

Sei R ein Ring mit Einselement $1 \in R$. Ein Element $r \in R$ heißt Einheit von R, wenn es ein Element $r' \in R$ gibt mit

$$rr' = r'r = 1.$$

Die Menge der Einheiten von R ist bezüglich der Multiplikation von R eine Gruppe. Diese Gruppe wir mit

$$R^*$$

bezeichnet und heißt multiplikative Gruppe von R.

Beispiel 1

Für jeden Körper ist

$$GL(n, K) = (K^{n \times n})^*.$$

Insbesondere ist

$$GL(1, K) = K^*.$$

Beispiel 2

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

Beispiel 3

Sei

$$\Gamma := \mathbb{Z} + \mathbb{Z}i := \{ a + bi \mid a,b \in \mathbb{Z} \}$$

die Menge der komplexen Zahlen mit ganzzahligen Real- und Imaginärteil. Diese Menge ist ein Ring mit 1, wobei die Ringoperationen gerade die gewöhnliche Addition bzw. Multiplikation komplexer Zahlen seien. Dieser Ring heißt Ring der ganzen Gaußschen Zahlen. Es gilt

$$\Gamma^* = \{ \pm 1, \pm i\}$$

1.1. 10 Das Zentrum einer Gruppe

Für jede Gruppe G ist

$$C(G) := \{ g \in G \mid gx = xg \text{ für jedes } x \in G \}$$

mit der Multiplikation von G eine Gruppe. Diese Gruppe heißt Zentrum von G.

Beispiel

$$C(GL(n,K)) = \{c \bullet Id \mid c \in K^*\}$$

ist die Gruppe der Skalar-Matrizen (zu den Null verschiedenen Skalaren).

1.1.11 Bilder und Kerne

Sei $h: G \longrightarrow G'$ ein Gruppenhomomorphismus. Dann ist der Kern von h,

$$\text{Ker } h := \{ g \in G \mid h(g) = e' \}$$

mit der Multiplikation von G eine Gruppe. Außerdem ist das Bild von h,

$$\text{Im } h := \{ h(g) \mid g \in G \}$$

mit der Multiplikation von G' eine Gruppe.

Bemerkung

Ein Gruppenhomomorphismus $h: G \longrightarrow G'$ ist genau dann injektiv, wenn dessen Kern trivial ist, d.h. Ker $h = \{e\}$ gilt.

Beispiel

Für jede Gruppe G ist die Abbildung

$$G \longrightarrow \text{Aut}(G),\ g \mapsto (x \mapsto gxg^{-1}),$$

ein Gruppenhomomorphismus. Das Bild dieses Homomorphismus heißt Gruppe der inneren Automorphismen von G. Die Abbildung

$$\sigma_g : G \longrightarrow G,\ x \mapsto gxg^{-1},$$

heißt auch Konjugation mit g.
Der Kern dieses Homomorphismus ist gerade das Zentrum von G,

$$C(G) = \mathrm{Ker}(G \longrightarrow \mathrm{Aut}(G),\ g \mapsto (x \mapsto gxg^{-1})).$$

1.1.12 Direkte Produkte

Seien G' und G" zwei Gruppen. Dann ist

$$G' \times G'' = \{(x', x'') \mid x' \in G',\ x'' \in G''\}$$

bezüglich der Gruppenoperation

$$(x', x'') \bullet (y', y'') := (x'x'', y'y'')$$

eine Gruppe. Diese Gruppe heißt direktes Produkt von G' und G" oder auch äußeres direktes Produkt.
Seien G eine Gruppe und G', G" $\subseteq$ G zwei Untergruppen mit der Eigenschaft, daß die Abbildung

$$G' \times G'' \longrightarrow G,\ (x', x'') \mapsto x'x'',$$

ein Gruppen-Homomorphismus ist, der außerdem auch noch bijektiv ist. Dann schreibt man ebenfalls

$$G = G' \times G''$$

und sagt, G zerfällt in das innere direkte Produkt der beiden Untergruppen G' und G".

1.1.13 Endliche Gruppen, Multiplikationstabellen

Für jede endliche Gruppe

$$G = \{ g_1, \ldots, g_n \}$$

kann man die Gruppenstruktur vollständig durch eine Multiplikationstabelle bestimmen.

	...	g_i	...
...			
g_j		$g_j g_i$	
.....			

Mit Hilfe der Gruppentabelle lassen sich die letzten beiden Gruppenaxiome leicht überprüfen.

Das dritte Gruppenaxiom bedeutet im wesentlichen, in jeder Zeile und Spalte des rechten unteren Teils der Tabelle kommt jedes Gruppenelement genau einmal vor.

Aufwendig gestaltet sich im allgemeinen die Überprüfung des ersten Gruppenaxioms. Fragen wir zum Beispiel nach Gruppen der Ordnung 4,

$$G = \{ e, a, b, c \} \text{ (e das Einselement).}$$

Die Grupentabellen hat die Gestalt

	e	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*		*1*	
b	*b*			
c	*c*			

Die bereits eingetragenen Werte beschreiben, die Tatsache, daß e das Einselement sein soll. In der Position 1 kann weder a noch b stehen (da a bzw. b in der Zeile bzw. Spalte bereits vorkommt. Es gibt also nur die Möglichkeiten

$$1 = e \text{ bzw. } 1 = c.$$

Betrachten wir den ersten Fall.

	e	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*		*e*	
b	*b*		*2*	
c	*c*		*1*	

In der neuen Position 1 können e, b und c nicht vorkommen, d.h. es ist

$$1 = a$$

In der Position 2 muß dann aber c stehen,

$$2 = c.$$

Für alle übrigen Positionen stehen nach derselben Argumentation die Einträge auch fest:

	e	***a***	***b***	***c***
e	***e***	***a***	***b***	***c***
a	***a***	***c***	***e***	***b***
b	***b***	***e***	***c***	***a***
c	***c***	***b***	***a***	***e***

Dies ist gerade die Additionstabelle der Restklassen modulo 4 mit

$e = 0, a = 1, b = 3, c = 2$

	0	*1*	*3*	*2*
0	*0*	*1*	*3*	*2*
1	*1*	*2*	*0*	*3*
3	*3*	*0*	*2*	*1*
2	*2*	*3*	*1*	*0*

Betrachten wir den zweiten Fall. Wie wir gesehen haben erhalten wir im Fall, daß das Produkt von zwei verschiedenen Elementen $\neq e$ gleich e ist, die Restklassen modulo 4, also nichts Neues. Wir schließen diesen Fall aus und erhalten:

	e	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*		*c*	*b*
b	*b*	*c*		*a*
c	*c*	*b*	*a*	

Dieselbe Argumentationsweise wie oben liefert:

	e	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*c*	*b*
b	*b*	*c*	*e*	*a*
c	*c*	*b*	*a*	*e*

Dies ist gerade die Multiplikationstabelle des direkten Produkts aus den Restklassen modulo 2 mit sich selbst

$$\{0, 1\} \times \{0,1\} = \{(0,0), (0,1), (1,0), (1,1)\}$$

mit $e = (0,0), a = (0,1), b = (1,0), c = (1,1)$. Diese Gruppe ist abelsch und heißt Kleinsche Vierergruppe.

1.1.14 Die Operation einer Gruppe auf einer Menge

Eine (Links-) Operation einer Gruppe G auf einer Menge M ist ein (Gruppen-) Homomorphismus

$$h: G \longrightarrow S(M).$$

Bemerkungen

(i) Eine solche Operation definiert eine Abbildung

$$h':G\times M \longrightarrow M, (g,m) \mapsto gm,$$

mit

1. $(g'g'')m = g'(g''m)$ für $g',g''\in G$ und $m\in M$
2. $em = m$ für $m\in M$.

Man kann nämlich

(1) $$gm = h(g)(m)$$

setzen. Die Relationstreue von h, d.h.

$$h(g'g'') = h(g')h(g'')$$

übersetzt sich dann gerade in Bedingung 1. Bedingung 2 ist die Übersetzung der Aussage $h(e) = Id$.

(ii) Jede Abbildung

$$h': G \times M \longrightarrow M,$$

welche den Bedingungen 1 und 2 genügt, kommt von einer eindeutig bestimmten Operation

$$h: G \longrightarrow S(M).$$

Die Eindeutigkeit von h ergibt sich aus (1). Interpretiert man (1) als Definition für h, so folgt

$h(g'g'')(m)$	$= (g'g'')m$	(nach Definition von h)
	$= g'(g''m)$	(nach Bedingung 1)
	$= h(g')(h(g'')(m))$	(nach Definition von h)

also

$$h(g'g'') = h(g')\circ h(g''),$$

d.h. h ist relationstreu. Wir haben noch zu zeigen, h ist korrekt definiert, d.h.

$$h(g): M \longrightarrow M$$

ist eine bijektive Abbildung für jedes $g\in G$. Es gilt

$$h(g)h(g^{-1})(m) = h(gg^{-1})(m) = h(e)m = em = m$$
$$h(g^{-1})h(g)(m) = h(g^{-1}g)(m) = h(e)m = em = m$$

Es ist also

$$h(g)h(g^{-1}) = h(g^{-1})h(g) = Id,$$

d.h. h ist bijektiv.

.

(iii) Aus (i) und (ii) ergibt sich, die Angabe einer Operation von G auf M ist äquivalent zur Angabe einer Abbildung h', die den Bedingungen 1 und 2 genügt. Deshalb spricht man auch bei der Abbildung h' von einer (Links-) Operation.

(iv) Eine Rechtsoperation einer Gruppe G auf einer Menge M ist eine Abbildung

$$M \times G \longrightarrow M, (m, g) \mapsto mg,$$

mit

1. $m(g'g'') = (mg')g''$
2. $me = m$.

(v) Ist eine Rechtsoperation gegeben, so ist

$$G\times M \longrightarrow M, (g,m) \mapsto mg^{-1},$$

eine Linksoperation. Ist umgekehrt

$$G \times M \longrightarrow M, (g,m) \mapsto gm,$$

eine Linksoperation, so ist

$$M \times G \longrightarrow M, (m,g) \mapsto g^{-1}m,$$

eine Rechtsoperation. Linksoperationen und Rechtsoperationen stehen also in einer eineindeutigen Korrespondenz. Deshalb werden wir uns im allgemeinen auf die Betrachtung von (Links-) Operationen beschränken.

(vi) Operiert G auf M und ist $m\in M$, so heißt

$$O(m) = Gm = \{ gm \mid g\in G \}$$

Orbit von m bezüglich der gegebenen Operation. Die Bezeichnung kann man mit der Vorstellung verbinden, daß die Zeit auf den Punkten einer Raketenbahn operiert und so die Rakete entlang des zugehörigen Orbits bewegt.

(v) Je zwei Orbits sind identisch oder disjunkt. Aus $m \in O(m')\bigcap O(m'')$ folgt nämlich die Existenz von Gruppenelementen $g',g''\in G$ mit

$$g'm' = m = g''m''.$$

Für jedes $g\in G$ gilt deshalb

$$gm' = gg'^{-1}g'm' = gg'^{-1}g''m''\in O(m''),$$

d.h. es gilt $O(m') \subseteq O(m'')$. Aus Symmetriegründen gilt dann aber auch die umgekehrte Inklusion, d.h. es ist

$$O(m') = O(m'').$$

Beispiel 1: Linkstranslationen
Sei G eine Gruppe. Dann operiert G auf sich selbst durch Multiplikation von links oder auch Linkstranslationen,

$$G \times G \longrightarrow G, (g,x) \mapsto gx.$$

Beispiel 2: Rechtstranslationen
Außerdem operiert G auf sich selbst durch Multiplikation von rechts oder auch Rechtstranslationen,

$$G \times G \longrightarrow G, (g, x) \mapsto xg^{-1}.$$

Beispiel 3: Konjugation
Weiter operiert G auf sich selbst durch Konjugation oder auch innere Automorphismen,

$$G \times G \longrightarrow G, (g,x) \mapsto gxg^{-1}.$$

Die zugehörigen Orbits sind die Mengen der Gestalt

$$O(x) = \{gxg^{-1} \mid g \in G\}$$

unf heißen Konjugationsklassen von G.

Beispiel 4: Operation der GL(n, K) auf den n×n-Matrizen
Seien K ein algebraisch abgeschlossener Körper und n eine natürliche Zahl. Dann operiert die allgemeine lineare Gruppe GL(n, K) durch Konjugation auf dem K-Vektorraum der n×n-Matrizen.

$$GL(n, K) \times K^{n\times n} \longrightarrow K^{n\times n}, (g, x) \mapsto gxg^{-1}.$$

Jedes Orbit besteht dann gerade aus allen Matrizen mit ein und derselben Jordanschen Normalform.

Spezialfall: Operation durch Automorphismen

Die Gruppe G operiere von links oder rechts auf der Menge M, und M sei ebenfalls eine Gruppe, oder ein Vektorraum oder allgemein ein Objekt irgendeiner Kategorie $\mathcal{C}$. Falls dann für jedes g∈G die Abbildung

$$M \longrightarrow M,\ m \mapsto gm \text{ (bzw. } m \mapsto mg),$$

ein Automorphismus von Gruppen, von Vektorräumen bzw. der gegebenen Kategorie $\mathcal{C}$ ist, so sagt man, G operiert durch Automorphismen auf M (von links bzw. von rechts)

1.1.15 Halbdirekte Produkte

Seien G' und G" zwei Gruppen und G' operiere auf G" von rechts durch Automorphismen,

$$G" \times G' \longrightarrow G",\ (x, g) \mapsto x^g,$$

Dann ist[3]

$$G' \rtimes G" := \{ (x', x") \mid x' \in G' \text{ und } x" \in G" \}$$

mit der folgenden Operation eine Gruppe. Diese Gruppe heißt halbdirektes Produkt von G' und G".

$$(x', x") \bullet (y', y") := (x'y', (x")^{y'} \bullet y").$$

Bemerkungen

(i) Das Einselement des halbdirekten Produkts ist gerade (e', e").

(ii) Das zu (x', x") inverse Element (y', y") genügt den Bedingungen

$$x'y' = e',\ \ x"^{\,y'} \bullet y" = e",$$

d.h. es ist

$$y' = x'^{-1}$$

und

$$y" = (x"^{\,y'})^{-1} = (x"^{-1})^{\,y'} = (x"^{-1})^{x'^{-1}}$$

d.h.

$$(x', x")^{-1} = (x'^{-1}, (x"^{-1})^{x'^{-1}})$$

(iii) Wir betrachten den Fall

$$G" = G,\ G' = \mathrm{Aut}\, G \text{ und } G \times \mathrm{Aut}(G) \longrightarrow G,\ (g, \sigma) \mapsto \sigma^{-1}(g).$$

und identifizieren G mit einer Teilmenge des halbdirekten Produkts mittels

$$G \longrightarrow \mathrm{Aut}\, G \rtimes G,\ x \mapsto (\mathrm{Id}, x).$$

Dann entspricht das Anwenden des Automorphismus h∈Aut G auf ein Element x∈G gerade der Konjugation mit dem Element (h,e):

$$(h, e)(\mathrm{Id}, x)(h,e)^{-1} = (h, x)\,(h^{-1}, e) = (\mathrm{Id}, h(x))$$

---

[3] Das Symbol

$$\rtimes$$

kann man sich als Zusammensetzung

$$\times\ i$$

aus einem Kreuz und einem 'i' enstanden denken, wobei das 'i' bedeuteden soll, daß der rechte Faktor des halbdirekten Produkts eine invariante Untergruppe ist. Analog bezeichnet

$$G' \ltimes G"$$

ein halbdirektes Produkt zweier Untergruppen, wobei jedoch diesmal der zweite Faktor auf dem ersten durch Automorphismen operiert (und entsprechend G' ein Normalteiler im halbdirekten Produkt G'⋉G" ist).

Die Automorphismen von G lassen sich also zu inneren Automorphismen des halbdirekten Produkts fortsetzen.

(iv) Seien G' und G" zwei Gruppen, wobei G" auf G' von links durch Automorphismen auf G' operiere,

$$G"\times G' \longrightarrow G', (g, x) \mapsto {}^{g}x.$$

Dann ist

$$G'\ltimes G" \longrightarrow \{(x', x") \mid x'\in G' \text{ und } x"\in G"\}$$

mit der folgenden Operation eine Gruppe.

$$(x', x")\bullet(y', y") = (x'({}^{x"}y') \ , x"y").$$

1.2 Untergruppen und Normalteiler

1.2.1 Definitionen

Eine Teilmenge $U \subseteq G$ einer Gruppe heißt Untergruppe, wenn U mit den Operationen von G die Struktur einer Gruppe hat. Die Untergruppe U von G heißt Normalteiler oder auch invariante Untergruppe, wenn die folgende Implikation besteht.

$$u\in U \text{ und } g\in G \Rightarrow gug^{-1} \in U.$$

Bemerkungen

(i) Für jedes $g\in G$ setzen wir

$$gUg^{-1} := \{gug^{-1} \mid u\in U\}$$

Dann gilt für jede Untergruppe U von G,

$$U \text{ ist Normalteiler von } G \Leftrightarrow gUg^{-1} \subseteq U \text{ für jedes } g\in G.$$

(ii) Die Bedingung an U, Normalteiler zu sein, bedeutet gerade, alle inneren Automorphismen von G überführen die Elemente von U in Elemente von U, d.h. U ist invariant gegenüber inneren Automorphismen. Daher der Name "invariante Untergruppe".

(iii) Jede Untergruppe U einer abelschen Gruppe ist ein Normalteiler:

$$gUg^{-1} = gg^{-1}U = eU = U.$$

Beispiel für einen Normalteiler

Der Kern eines Homomophismus $h: G \longrightarrow G'$ ist eine invariante Untergruppe: für $u\in \text{Ker } h$ und $g\in G$ gilt

$$h(gug^{-1}) = h(g)h(u)h(g)^{-1} = h(g)e'h(g)^{-1} = h(g)h(g)^{-1} = e',$$

d.h. $gug^{-1} \in \text{Ker } h$. Die Untergruppeneigenschaft von Ker h werden wir mit Hilfe des nachfolgenden Kriteriums nachweisen.

Beispiel 1

Die Menge

$$U := \{ (1), (12)\}$$

ist eine Untergruppe von $S_3 = \{ (1), (12), (13), (23), (123), (321)\}$ jedoch kein Normalteiler, denn das Element

$$(23)U(23)^{-1} = \{ (1), (13)\}$$

liegt nicht in U. Insbesondere kann U unmöglich der Kern eines auf S_3 definierten Homomorphismus sein.

Beispiel 2

Die Teilmenge

$$A_n \subseteq S_n$$

der geraden Permutationen der symmetrischen Gruppe S_n ist mit den Operationen von S_n eine Gruppe und heißt alternierende Gruppe. Insbesondere ist A_n eine Untergruppe von S_n. Als Kern des Homomorphismus

$$\text{sign: } S_n \longrightarrow \{\pm 1\},$$

welcher jede Permutation auf ihr Vorzeichen abbildet, ist A_n sogar ein Normalteiler.

1.2.2 Untergruppenkriterium

Seien G eine Gruppe und $U \subseteq G$ eine Teilmenge. Dann sind folgende Aussagen äquivalent.

(i) U ist eine Untergruppe von G.

(ii) U ist nicht leer und für je zwei Elemente $x,y \in U$ gilt $xy^{-1} \in U$.

(iii) Es sind die folgenden drei Bedingungen erfüllt.

(a) $e \in U$.

(b) $x,y \in U \Rightarrow xy \in U$.

(c) $x \in U \Rightarrow x^{-1} \in U$.

Beweis. (i) $\Rightarrow$ (ii). Da U eine Gruppe ist, enthält U das neutrale Element, ist also nicht leer. Sind $x,y \in U$ Elemente von U, so muß auch

$$y^{-1} \in U$$

gilt (da U eine Gruppe ist), also $xy^{-1} \in U$.

(ii) $\Rightarrow$ (iii). Nach Voraussetzung ist U nicht leer. Es gibt also ein Element $x \in U$. Dann git aber nach Voraussetzung auch

$$e = xx^{-1} \in U,$$

d.h. Bedingung (a) ist erfüllt. Mit $x \in U$ gilt nach Voraussetzung auch

$$x^{-1} = ex^{-1} \in U,$$

d.h. Bedingung (c) ist erfüllt. Mit $x, y \in U$ gilt, wie gerade gezeigt auch $x, y^{-1} \in U$, also

$$xy = x(y^{-1})^{-1} \in U,$$

d.h. Bedingung (b) ist erfüllt.

(iii) $\Rightarrow$ (i). Auf Grund von Bedingung (b) definiert die Gruppenoperation von G eine Abbildung

$$U \times U \longrightarrow U, (x,y) \mapsto xy.$$

Da die Gruppenoperation von G assoziativ ist, gilt dasselbe auch die auf U induzierte Operation. Nach Bedingung (a) gilt $e \in U$, d.h. U besitzt ein neutrales Element. Nach Bedingung (c) gilt mit $x \in U$ auch $x^{-1} \in U$, d.h. jedes Element von U besitzt in U ein Inverses. Damit ist U eine Gruppe,
QED.

1.2.3 Beispiel: der Kern eines Homomorphismus

Sei $h: G \longrightarrow G'$ ein Homomorphismus. Dann ist Ker h eine Untergruppe (also ein Normalteiler.

Beweis.

Wegen e∈Ker h ist Ker h nicht leer. Für x,y∈Ker h gilt

$$h(xy^{-1}) = h(x)h(y^{-1}) = h(x)h(y)^{-1} = e'\bullet e'^{-1} = e',$$

also $xy^{-1} \in$ Ker h.
QED.

1.2.4 Beispiel: endliche Untergruppen

Seien G eine Gruppe und $U \subseteq G$ eine nichtleere endliche Teilmenge mit

$$x, y \in U \Rightarrow xy \in U.$$

Dann ist U eine Untergruppe von G.

Beweis. Seien x,y∈U zwei Elemente. Es reicht zu zeigen,

$$xy^{-1} \in U.$$

Nach Voraussetzung ist die Abbildung

$$\varphi: U \longrightarrow U,\ u \mapsto uy,$$

wohldefiniert. Diese Abbildung ist injektiv, denn die Zusammensetzung mit der Abbildung

$$u \mapsto uy^{-1}$$

ist die identische Abbildung: $(uy)y^{-1} = u(yy^{-1})$ ue = u. Das Bild der Abbildung φ besteht also aus genau so vielen Elementen wie U selbst, d.h.

$$\varphi \text{ ist bijektiv.}$$

Insbesondere gibt es ein u∈U mit

$$x = \varphi(u) = uy.$$

Multiplikation von links mit y^{-1} liefert

$$xy^{-1} = u \in U.$$

QED.

1.2.5 Beispiel: Untergruppen der S_4

Die folgenden Teilmengen von
S_4 = { (1),
(12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (Ordnung 2)
(123), (124), (134), (234), (Ordnung 3)
(321), (421), (431), (432),
(1234), (1342), (1423), (Ordnung 4)
(1432), (1243), (1324) }

sind Untergruppen.
Ordnung 1: {(1)}
Ordnung 2:
{ (1), (12)}, {(1), (13)} , {(1),(14)}, {(1), (23)}, {(1),(24)}, {(1), (34),}
{(1), (12)(34)}, {(1), (13)(24)}, {(1), (14)(23)}
Ordnung 3:
{ (1), (123), (321)}, { (1), (124),(421)}, { (1), (134),(431)}, { (1), (234), (432)}
Ordnung 4:
{ (1), (1234), (13)(24),(4321)}
{ (1), (1342), (14)(23),(2431)}
{ (1), (1423), (12)(34),(3241)}
{ (1),), (12)(34), (13)(24), (14)(23)} = V_4

Ordnung 6:

$\{ (1), (12), (13), (123), (321)\} = S_3$ (= <(12)>⋊<(123)>)

$\{ (1), (12), (14), (124), (421)\}$

$\{ (1), (13), (14), (134), (431)\}$

$\{ (1), (23), (24), (234), (432)\}$

Ordnung 8:[4]

$\{ (1), (12)(34), (13)(24), (14)(23), (1234), (4321), (13), (24)\}$

$\{ (1), (12)(34), (13)(24), (14)(23), (1342),(2431), (23), (14)\}$

$\{ (1), (12)(34), (13)(24), (14)(23), (1423),(3241), (12), (34)\}$

Ordnung 12:

$\{ (1), (12)(34), (13)(24),(14)(23),$
$(123), (124), (134), (234),$
$(321), (421), (431), (432)\} = A_4$

Ordnung 24: S_4

Wir werden später sehen, es gibt keine weiteren Untergruppen. Die einzigen Normalteiler sind:

$\{(1)\}, V_4 , A_4 , S_4$

1.2.6 Beispiel: Durchschnitte von Untergruppen

Seien G ein Gruppe und $\{G_\alpha\}_{\alpha\in I}$ eine beliebige Familie von Untergruppen G_α von G. Dann ist

$$U := \bigcap_{\alpha\in I} G_\alpha$$

eine Untergruppe von G.

Beweis. Die Menge U ist nicht leer, denn $e \in G$ liegt in jedem G_α, also auch in U. Seien jetzt zwei Elemente $x,y\in U$ gegeben. Es reicht zu zeigen,

$$xy^{-1}\in U.$$

Zumindest gilt $x,y\in G_\alpha$ für jedes α, also $xy^{-1}\in G_\alpha$, da die G_α Untergruppen sind. Dann ist aber auch $xy^{-1}\in U$.

QED.

1.2.7 Endliche Gruppen als Untergruppen der endlichen symmetrischen Gruppen

Seien G eine (endliche) Gruppe und

$$h: G \longrightarrow S(G), g \mapsto (x \mapsto gx),$$

die Operation von G auf sich durch Linkstranslationen. Der Homomophismus h ist injektiv, d.h er identifiziert G mit dem Bild von h in S(G).

Insbesondere kann man jede (endliche) Gruppe mit einer Untergruppe einer (endlichen) Permultationsgruppe identifizieren.

Beweis (der Injektivität von h). Ist $g\in$ Ker(h), so ist die Abbildung

---

[4] Jede Untergruppe der Ordnung 4 liegt in einer 2-Sylow-Untergruppe. V_4 liegt deshalb in jeder 2-Sylow-Untergruppe. Die 2-Sylow-Untergruppen werden deshalb von V_4 und einer weiteren Untergruppe der Ordnung 4 erzeugt.

$$G \longrightarrow G,\ x \mapsto gx,$$

die identische Abbildung, d.h. gx = x für jedes x. Speziell für x = e folgt

$$g = ge = e.$$

Wir haben gezeigt, Ker (h) = {e} ist trivial, d.h. h ist injektiv.
QED.

1.2.8 Erzeugendensysteme, zyklische Gruppen

Seien G eine Gruppe und $M \subseteq G$ eine Teilmenge von G. Dann wird der Durchschnitt aller Untergruppen von G, die die Menge M enthalten, mit

$$< M> := <m \mid m \in M> := \bigcap_{M \subseteq U \subseteq G, U \text{ Untergruppe}} U$$

bezeichnet und heißt die von M erzeugte Untergruppe von G. Falls <M> = G gilt, so heißt M auch Erzeugendensystem von G. Eine Gruppe mit einem einelementigen Erzeugendensystem heißt zyklisch. Eine Gruppe mit endlichem Erzeugendensystem heißt endlich erzeugt.

Bemerkungen

(i) Sei G = <g> eine zyklische Gruppe. Dann ist

$$\{ g^n \mid n \in \mathbb{Z} \}$$

eine Untergruppe, welche das Element g enthält. Da G die kleinste Gruppe ist mit dieser Eigenschaft, gilt

$$G = \{ g^n \mid n \in \mathbb{Z} \},$$

d.h. jede zyklische Gruppe besteht aus den Potenzen eines festen Elements. Insbesondere ist jede zyklische Gruppe abelsch.

(ii) Sei G eine Gruppe und $g \in G$ ein Element. Dann ist

$$<g> = \{ g^n \mid n \in \mathbb{Z} \}$$

die von g in G erzeugte zyklische Gruppe. Die Ordnung dieser Untergruppe heißt auch Ordnung von g,

$$\text{ord } g := \# \{ g^n \mid n \in \mathbb{Z} \}$$

Beispiel
Für jede Gruppe G ist G ein Erzeugendensystem von G,

$$G = <G>.$$

Beispiel

Wie wir aus der linearen Algebra wissen, ist jede Permutation $\sigma \in S_n$ ein Produkt von Transpositionen der Gestalt

$$(12), (13), \ldots, (1n).$$

Anders ausgedrückt, diese Permutationen bilden ein Erzeugendensystem von S_n,

$$S_n = < (12), (13), \ldots, (1n) >$$

Man beachte, es gilt

$$(1i)(ij)(1i) = (1j)$$

d.h.

$$(ij) = (1i)(1j)(1i).$$

Beispiel

Die von $(12) \in S_n$, $n \geq 2$ erzeugte Gruppe besteht aus den Potenzen von (12),

$$< (12) > = \{ (1), (12) \},$$

d.h. (12) ist ein Element der Ordnung 2 von S_n.

Beispiel

Die von $(123) \in S_n$, $n \geq 3$ erzeugte Gruppe besteht aus den Potenzen von (123),

$$< (123) > = \{ (1), (123), (321) \},$$

d.h. (123) ist eine Element der Ordnung 2 von S_n.

Analog sieht man, ein r-Zyklus $(a_1 ... a_t)$ ist ein Element der Ordnung r.

Beipiel

$$S_3 = <(12), (13)>$$

Es gibt kein Erzeugendensystem aus weniger Elementen, denn dann wäre die Gruppe zyklisch, also abelsch, was nicht der Fall ist..

Beispiel

$\mathbb{Z}$ ist mit der gewöhnlichen Addition ganzer Zahlen eine zyklische Gruppe.

1.2.9 Untergruppen zyklischer Gruppen

Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis. Sei G eine zyklische Gruppe,

$$G = <g> = \{ g^n \mid n \in \mathbb{Z} \}$$

und $U \subseteq G$ eine Untergruppe. O.B.d.A. sei $U \neq \{e\}$. Dann enthält U eine Potenz g^n von g mit $g^n \neq e$, d.h. $n \neq 0$,

$$e \neq g^n \in U, n \neq 0.$$

Weil U eine Untergruppe ist, liegt mit g^n auch $(g^n)^{-1} = g^{-n}$ in U, d.h. wir können annehmen,

$$n > 0.$$

Sei

$$n_0 := \min \{ n \in \mathbb{N} \mid g^n \in U \}.$$

Die Menge, deren Minimum wir nehmen, ist nicht leer, d.h. n_0 ist eine wohldefinierte natürliche Zahl. Nach Konstruktion gilt $g^{n_0} \in U$, also

$$U \supseteq < g^{n_0} >.$$

Zum Beweis der Behauptung reicht es zu zeigen, es gilt sogar "=". Sei also ein beliebiges Element von U gegeben,

$$g^m \in U.$$

Es reicht zu zeigen, g^m ist eine Potenz von g^{n_0}, d.h. es reicht zu zeigen, n_0 ist ein Vielfaches von m. Jedenfalls gilt

$$m = q \bullet n_0 + r$$

mit ganzen Zahlen q und r, wobei gilt

(1) $$0 \leq r < n_0.$$

Es gilt

$$g^r = g^{m - qn_0} = g^m (g^{n_0})^{-q} \in U.$$

Nach Definition von n_0 und wegen (1) muß dann aber r = 0 gelten, d.h. m ist ein Vielfaches von n_0.

QED.

1.2.10 Untergruppen abelscher Gruppen

Sei A eine (additiv geschriebene) abelsche Gruppe. Dann ist die Teilmenge

$$A_{tor} := \{a \in A \mid na = 0 \text{ für ein } n \in \mathbb{N}\}$$

der Elemente endlicher Ordnung eine Untergruppe von A und heißt Torsionsuntergruppe von A. Sei n eine natürliche Zahl. Dann ist die Teilmenge

$$A_n := \{a \in A \mid n^r a = 0 \text{ für ein } r \in \mathbb{N}\}$$

der Elemente, die von einer n-Potenz annulliert werden, eine Untergruppe und heißt n-Torsionsuntergruppe.

1.3 Faktorgruppen, die Isomorphiesätze und Anwendungen

1.3.1 Nebenklassen

Seien G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann operiert U auf G durch Multplikation von links,

$$U \times G \longrightarrow G, (u, g) \mapsto ug.$$

Die zugehörigen Orbits sind die Mengen der Gestalt

$$O(x) = Ux := \{ux \mid u \in U\}$$

und heißen Rechtsnebenklassen von G modulo U. Die Menge der Rechtsnebenklassen von G modulo U wird mit

$$U\backslash G$$

bezeichnet.
Weiter operiert U auf G durch Multiplikation von rechts,

$$U \times G \longrightarrow G, (u, g) \mapsto gu^{-1}.$$

Die zugehörigen Orbits sind die Mengen der Gestalt

$$O(x) = xU := \{xu \mid u \in U\}$$

und heißen Linksnebenklassen von G modulo U. Die Menge Linksnebenklassen von G modulo U wird mit

$$G/U$$

bezeichnet.

Bemerkungen

(i) Je zwei Links- (bw. Rechts-) Nebenklassen sind identisch oder disjunkt.
(ii) Je zwei Nebenklassen modulo U lasen sich bijektiv aufeinander abbilden.
(iii) Für jede Untergruppe U von G sind folgende Aussagen äquivalent.
1. U ist ein Normalteiler.
2. $gUg^{-1} = U$ für jedes $g \in G$.
3. $G/U = U\backslash G$.

Falls diese Bedingungen erfüllt sind, schreibt man für jedes $g \in G$ auch

$$g \bmod U := gU = Ug$$

Beweis. Zu (i). Das gilt, wie wir gesehen haben, allgemeiner für je zwei Oribts.

Zu (ii). Die Abbildung

$$U \longrightarrow Ug, u \mapsto ug,$$

ist wohldefiniert und bijektiv: die inverse Abbildung ist durch $u \mapsto ug^{-1}$ gegeben. Analog ist

$$U \longrightarrow gU, u \mapsto gu,$$

bijektiv. Also laßt sich jede Nebenklasse modulo U bijektiv auf U abbilden. Also lassen sich je zwei Nebenklassen modulo U bijektiv aufeinander abbilden.

Zu (iii). $1 \Rightarrow 2$. Nach Voraussetzung gilt

(1) $$gUg^{-1} \subseteq U \text{ für jedes } g \in G.$$

Insbesondere gilt (1) auch für g^{-1} anstelle von g, d.h. es ist

$$g^{-1}Ug \subseteq U.$$

Multiplikation von links mit g und von rechts mit g^{-1} liefert

$$U \subseteq gUg^{-1},$$

d.h. es gilt in (1) sogar das Gleichheitszeichen.

1. $\Leftarrow$ 2. trivial.

2 $\Rightarrow$ 3. Nach Voraussetzung gilt $gUg^{-1} = U$ für jedes $g \in G$. Multiplikation von rechts mit g liefert

$$gU = Ug,$$

d.h. die Menge der Linksnebenklassen ist gleich der Menge der Rechtsnebenklassen.

3. $\Rightarrow$ 2. Nach Voraussetzung gibt es für jedes $g \in G$ ein $g' \in G$ mit

$$gU = Ug'.$$

Durch Multiplikation von rechts mit g^{-1} folgt

$$gUg^{-1} = Ug'g^{-1}.$$

Rechts steht eine Rechtsnebenklasse, die das Element e enthält. Das ist aber auch der Fall für die Rechtsnebenklasse Ue = U. Also steht auf der rechten Seite U,

$$gUg^{-1} = U.$$

Dies gilt für jedes $g \in G$, d.h. es gilt 2.
QED.

1.3.2 Satz von Lagrange

Seien G eine endliche Gruppe und $U \subseteq G$ eine Untergruppe. Dann ist die Ordnung von U ein Teiler der Ordnung von G.
Genauer gilt

$$\#G = \#U \bullet \#G/U = \#U \bullet \#U\backslash G.$$

Beweis. Nach 1.3.1 Bemerkung (i) ist G die disjunkte Vereinigung seiner Links-Nebenklassen, sagen wir

$$G = g_1U \bigcup g_2U \bigcup \ldots \bigcup g_rU,\ G/U = \{ g_1U, g_2U, \ldots, g_rU \}.$$

Damit ist

$$\#G = \#g_1U + \#g_2U + \ldots + \#g_rU \text{ mit } r := \#G/U.$$

Nach 1.3.1 Bemerkung (ii) enthält jede Nebenklassen genau so viele Elemente wie U, d.h.

$$\#G = r \bullet \#U,\ r = \#G/U.$$

Die Aussage über die Rechtsnebenklassen wird analog bewiesen.
QED.

Bemerkung
Die Zahl

$$\#G/U = \#U\backslash G$$

heißt Index der Untergruppe U in G und wird mit

$$(G:U)$$

bezeichnet.

1.3.3 Bezeichnung: Produkte von Teilmengen

Seien G eine Gruppe und $A,B \subseteq G$ zwei Teilmengen. Wir setzen

$$A \bullet B := \{ab \mid a \in A, b \in B\}$$

Ist $A = \{a\}$ eine einelementige Menge, so schreiben wir auch

$$aB = AB \text{ und } Ba = BA.$$

Diese Definition ist mit früheren Definitionen für Ausdrücke der Gestalt aB bzw. Ba bzw. aBc verträglich.

Bemerkungen

(i) Auf Grund des Assoziativgesetzes für die Gruppenoperation gilt für je drei Teilmenge $A,B,C \subseteq G$,

$$(AB)C = A(BC).$$

(ii) Ist A oder B ein Normalteiler von G, so gilt $AB = BA$.

Beweis von (ii). Sei zum Beispiel A ein Normalteiler. Dann gilt

$b^{-1}Ab = A$ für jedes $b \in B$,

also

$$Ab = bA.$$

Damit gilt aber

$$AB = \bigcup_{bPB} Ab = \bigcup_{bPB} bA = BA.$$

QED.

1.3.4 Die Gruppenstruktur von G/N im Fall eines Normalteilers N

Seien G eine Gruppe und $N \subseteq G$ ein Normalteiler. Dann ist

$$G/N = N\backslash G$$

bezüglich der in 1.3.3 definierten Multiplikation von Mengen eine Gruppe. Die Menge G/N mit dieser Gruppenstruktur heißt Faktorgruppe von G modulo N.

Die natürliche Abbildung

$$\rho: G \longrightarrow G/N,\ g \mapsto gN,$$

ist dann ein Gruppenhomomorphismus (und heißt deshalb auch natürlicher Homomorphismus). Es gilt

$$\text{Ker } \rho = N.$$

Beweis. Für $g', g'' \in G$ gilt

(1) $$(g'N)(g''N) = g'NNg'' = g'Ng'' = g'g''N \in G/N,$$

d.h. die Multiplikation von Teilmengen definiert eine Abbildung

$$G/N \times G/N \longrightarrow G/N,\ (g'N, g''N) \mapsto g'g''N.$$

Das Assoziativgesetz gilt auf Grund von Bemerkung (i) von 1.3.3. Die Menge N spielt die Rolle des neutralen Elements: für $g \in G$ gilt

$$N \bullet gN = gNN = gN$$
$$gN \bullet N = gN$$

Die Existenz des inversen Elements: für $g \in N$ gilt

$$gN \bullet g^{-1}N = gg^{-1}N = eN = N$$
$$g^{-1}N \bullet gN = g^{-1}gN = eN = N.$$

Auf Grund von (1) gilt

$$\rho(g'g'') = g'g''N = (g'N)(g''N) = \rho(g')\rho(g'').$$

Schließlich ist

$$g \in \text{Ker } h \Leftrightarrow h(g) = h(e) \Leftrightarrow gN = eN \Leftrightarrow g \in N$$

QED.

Beispiel

Für jedes $n \in \mathbb{N}$ ist $n\mathbb{Z}$ eine Untergruppe der additiven Gruppe $\mathbb{Z}$ und

$$\mathbb{Z}/n\mathbb{Z} = \{\ \overline{g} := g + n\mathbb{Z} \mid g \in \mathbb{Z}\ \}$$

besteht gerade aus den Restklassen modulo n:

$$\begin{aligned}
\overline{g} = \overline{g'} &\Leftrightarrow \overline{g} - \overline{g'} = \overline{0} \\
&\Leftrightarrow \overline{g-g'} = n\mathbb{Z} \\
&\Leftrightarrow 0 \in \overline{g-g'} = g-g' + n\mathbb{Z} \quad \text{(Restkl. sind identisch oder disj.)} \\
&\Leftrightarrow \text{Es gibt ein } k \in \mathbb{Z} \text{ mit } 0 = g-g' + nk \\
&\Leftrightarrow \text{Es gibt ein } k \in \mathbb{Z} \text{ mit } g'-g = nk \\
&\Leftrightarrow g' \equiv g \pmod{n}.
\end{aligned}$$

1.3.5 Normalteilereigenschaft und Gruppenstrukur

Seien G eine Gruppe, $U \subseteq G$ eine Untergruppe und

$$\rho: G \longrightarrow G/U,\ g \mapsto gU,$$

die natürliche Abbildung. Dann sind folgende Eigenschaften äquivalent.

(i) G/U besitzt eine solche Gruppenstruktur, daß ρ ein Homomorphismus ist.

(ii) U ist ein Normalteiler von G.

Die analoge Aussage gilt auch mit U\G anstelle von G/U.,

Beweis. (ii) ⇒ (i). Folgt aus 1.3.4.

(i) ⇒ (ii). Es gelte (i). Für jedes g∈G gilt dann

$$gUg^{-1} \subseteq (gUg^{-1})U = \rho(g)\rho(g^{-1}) = \rho(gg^{-1}) = \rho(e) = eU = U,$$

d.h.

$$gUg^{-1} \subseteq U.$$

Mit anderen Worten, U ist ein Normalteiler.
QED.

1.3.6 Der Homomorphiesatz

Seien G eine Gruppe, $N \subseteq G$ ein Normalteiler, h: G⟶G' ein Gruppen-Homomorphismus und

$$\rho: G \longrightarrow G/N$$

der natürliche Homomorphismus. Dann sind die beiden folgenden Aussagen äquivalent.

(i) $N \subseteq \operatorname{Ker} h$.

(ii) Es gibt einen Homomorphismus $\tilde{h}: G/N \longrightarrow G'$ mit der Eigenschaft, daß das folgende Diagramm kommutativ ist.

$$\begin{array}{ccc} G & \xrightarrow{h} & G' \\ \rho\downarrow & \nearrow \tilde{h} & \\ G/N & & \end{array}$$

Falls die beiden Bedingungen erfüllt sind, so gilt außerdem:

(iii) $\tilde{h}$ ist durch h eindeutig festgelegt. Es gilt $\tilde{h}(gN) = h(g)$ für jedes g∈G.

(iv) $\operatorname{Im} \tilde{h} = \operatorname{Im} h$.

(v) $\operatorname{Ker} \tilde{h} = \operatorname{Ker} h/N$.

Beweis. (ii) $\Rightarrow$ (i). Nach Voraussetzung gilt

$$h = \tilde{h} \circ \rho.$$

Für $g \in N$ gilt also

$$h(g) = \tilde{h}(\rho(g)) = \tilde{h}(gN) = \tilde{h}(eN).$$

Man beachte, wegen $g \in N$ gilt $g^{-1} \in N$, also $e = gg^{-1} \subseteq gN$, d.h. gN und eN haben das Element e gemeinsam, sind also identische Nebenklassen. Damit ist

$$h(g) = \tilde{h}(\rho(e)) = h(e) = e',$$

d.h.

$$g \in \mathrm{Ker}(h).$$

Zu (iii). Wir beweisen die Eindeutigkeit von $\tilde{h}$ unter der Voraussetzung, daß (ii) gilt. Wegen

$$h = \tilde{h} \circ \rho.$$

gilt für jedes $g \in G$:

$$\tilde{h}(gN) = \tilde{h}(\rho(g)) = h(g),$$

d.h. $\tilde{h}(gN)$ ist eindeutig festgelegt.

(i) $\Rightarrow$ (ii). Wir haben die Existenz von $\tilde{h}$ zu beweisen. Wir definieren

$$\tilde{h}(gN) := h(g).$$

Diese Definition ist korrekt (d.h. unabhängig von der speziellen Wahl von g): mit

$$gN = g'N$$

gilt nämlich

$$g = ge \in gN = g'N,$$

d.h. $g = g'n$ für ein $n \in N$, d.h.

$$h(g) = h(g'n) = h(g')h(n) = h(g')$$

wegen $n \in N \subseteq \mathrm{Ker}\ h$. Damit ist $\tilde{h}$ korrekt definiert. Wir haben noch zu zeigen, $\tilde{h}$ hat alle geforderten Eigenschaften:

1. $\tilde{h}$ ist ein Homomorphismus.

2. $h = \tilde{h} \circ \rho$.

Zu 1:

$$\tilde{h}(g'N \bullet g''N) = \tilde{h}(g'g''N) = h(g'g'') = h(g')h(g'') = \tilde{h}(g'N)\,\tilde{h}(g''N).$$

Zu 2.

$$\tilde{h}(\rho(g)) = \tilde{h}(gN) = h(g).$$

Zu (iv).

$$\mathrm{Im}\,\tilde{h} = \{\, \tilde{h}(gN) \mid g \in G \,\} = \{\, h(g) \mid g \in G \,\} = \mathrm{Im}\,h.$$

Zu (v).

$$\begin{aligned} \mathrm{Ker}\,\tilde{h} &= \{\, gN \mid \tilde{h}(gN) = e' \,\} \\ &= \{\, gN \mid h(g) = e' \,\} \\ &= \{\, gN \mid g \in \mathrm{Ker}\,h \,\} \\ &= \mathrm{Ker}\,h / N. \end{aligned}$$

QED.

1.3.7 Der 0-te Isomorphiesatz

Sei h: G$\longrightarrow$G' ein Gruppenhomomorphismus. Dann ist der zum Normalteiler

$$N := \operatorname{Ker} h$$

gehörige Homomorphismus

$$\tilde{h} : G/\operatorname{Ker} h \longrightarrow G',\ gN \mapsto h(g),$$

injektiv, definiert also einen Isomorphismus

$$\tilde{h} : G/\operatorname{Ker} h \longrightarrow \operatorname{Im} h,\ gN \mapsto h(g).$$

Beweis. Es gilt

$$\operatorname{Ker} \tilde{h} = \operatorname{Ker} h / \operatorname{Ker} h = \{ gN \mid g \in N \} = \{N\} = \text{triviale Gruppe},$$

d.h. $\operatorname{Ker} \tilde{h}$ ist trivial, d.h. $\tilde{h}$ ist injektiv.
QED.

1.3.8 Der erste Isomorphiesatz

Seien G eine Gruppe, $N \subseteq G$ ein Normalteiler und $U \subseteq G$ eine Untergruppe. Dann ist

$$U \bigcap N$$

ein Normalteiler von U und die Abbildung

$$U/U\bigcap N \longrightarrow UN/N,\ u\ U\bigcap N \mapsto uN,$$

ein Gruppen-Isomorphismus.
Beweis. Wir betrachten den natürlichen Homomorphismus

$$\rho: G \longrightarrow G/N,\ g \mapsto gN.$$

Seine Einschränkung

$$h := \rho|_U : U \longrightarrow G/N,\ u \mapsto uN,$$

auf die Untergruppe U ist ein Homomorphismus mit dem Bild

$$\begin{aligned} \operatorname{Im}(h) &= \{ h(u) \mid u \in U \} \\ &= \{uN \mid u \in U\} \\ &= \{unN \mid u \in U,\ n \in N\} \\ &= \{ xN \mid x \in UN \} \\ &= UN/N \end{aligned}$$

und dem Kern

$$\operatorname{Ker}(h) = \{u \in U \mid u \in \operatorname{Ker} h \} = \{u \in U \mid u \in N \} = U \bigcap N.$$

Insbesondere ist $U\bigcap N$ ein Normalteiler in U. Die Isomorphie-Aussage folgt jetzt aus dem 0-ten Isomorphiesatz.
QED.

1.3.9 Der zweite Isomorphiesatz

Seien G eine Gruppe und $N', N'' \subseteq G$ zwei Normalteiler mit

$$N' \subseteq N''.$$

Dann ist N''/N' ein Normalteiler in G/N' und die Abbildung

$$(G/N')/(N''/N') \longrightarrow G/N'',\ \bar{g}\,(N''/N') \mapsto gN'',$$

(mit $\bar{g} := gN'$) ist ein Gruppen-Isomorphismus.
Beweis. Wir betrachten den natürlichen Homomorphismus

$$\rho: G \longrightarrow G/N'',\ g \mapsto gN''.$$

Da N' in dessen Kern N'' liegt, gibt es nach dem Homomorphiesatz den Homomorphismus

$$\tilde{\rho}: G/N' \longrightarrow G/N'',\ gN' \mapsto \rho(g) = gN''.$$

Mit ρ ist auch $\tilde{\rho}$ surjektiv. Für den Kern erhalten wir

$$\operatorname{Ker} \tilde{\rho} = \operatorname{Ker} \rho/N' = N''/N'.$$

Deshalb induziert $\tilde{\rho}$ (nach dem 0-ten Isomorphiesatz) einen Isomorphismus

$$(G/N')/\operatorname{Ker} \tilde{\rho} \longrightarrow \operatorname{Im} \tilde{\rho} = G/N'',\ \text{Restklasse von } gN' \mapsto \tilde{\rho}(gN') = \rho(g) = gN''.$$

Wegen $\operatorname{Ker} \tilde{\rho} = N''/N'$ ist das gerade die Behauptung.
QED.

1.4. Zyklische Gruppen

1.4.1 Die Menge der zyklischen Gruppen bis auf Isomorphie

Jede zyklische Gruppe ist isomorph zu einer Gruppe der Gestalt $\mathbb{Z}/n\mathbb{Z}$. Dabei bezeichne $\mathbb{Z}$ die additive Gruppe der ganzen Zahlen und

$$n\mathbb{Z} := \{ng \mid g \in \mathbb{Z}\}$$

den Normalteiler der durch n teilbaren ganzen Zahlen.

In einer multiplikativ geschriebenen zyklischen Gruppe $G = \langle g \rangle$ der Ordnung n gilt

1. $g'^n = e$ für jedes $g' \in G$.
2. $g^k = e \Leftrightarrow n \mid k$.

Bemerkungen

(i) Man beachte, es gilt $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$.

(ii) Umgekehrt sind alle additiven Gruppen der Gestalt $\mathbb{Z}/n\mathbb{Z}$ zyklisch,

$$\mathbb{Z}/n\mathbb{Z} = \langle 1 + n\mathbb{Z} \rangle = \{ g + n\mathbb{Z} \mid g \in \mathbb{Z} \}$$

Beweis. Sei $G = \langle g \rangle$ eine zyklische Gruppe, d.h.

$$G = \{ g^n \mid n \in \mathbb{Z} \}.$$

Dann ist die Abbildung

$$h: \mathbb{Z} \longrightarrow G,\ n \mapsto g^n,$$

ein sujektiver Homomorphismus der additiven Gruppe $\mathbb{Z}$ auf die multiplikative Gruppe G,

$$h(a + b) = h(a)h(b)$$

und

$$\operatorname{Im} h = G.$$

Auf Grund des 0-ten Isomorphiesatzes ist damit

$$\mathbb{Z}/\operatorname{Ker} h \longrightarrow G,\ g \bullet \operatorname{Ker} h \mapsto h(g),$$

ein Isomorphismus. Es reicht also zu zeigen,

$$\operatorname{Ker} h = n\mathbb{Z} \text{ für ein } n \in \mathbb{Z}.$$

Im Fall $\operatorname{Ker} h = \{0\}$ ist die Aussage trivial: $\operatorname{Ker} h = 0\mathbb{Z}$. Sei also

$$\operatorname{Ker} h \neq \{0\}.$$

Dann gibt es ein von Null verschiedenes Element

$$n \in \operatorname{Ker} h - \{0\}.$$

Mit n liegt aber auch -n in Ker h. Wir können also annehmen,

$$n \in \mathbb{N}$$

ist eine natürliche Zahl. O.B.d.A sei n die kleinste natürliche Zahl, die in Ker h liegt,

$$n := \min \{ m \in \text{Ker } h \mid m > 0 \}.$$

Es reicht zu zeigen, daß dann

$$\text{Ker } h = n\mathbb{Z}$$

gilt. Wegen $n \in \text{Ker } h$ gilt zumindest

$$\text{Ker } h \supseteq n\mathbb{Z}.$$

Beweisen wir die umgekehrte Inklusion. Sei $x \in \text{Ker } h$. Wir schreiben x in der Gestalt

$$x = qn + r$$

mit ganzen Zahlen q mit

(1) $$0 \leq r < n.$$

Wegen $x \in \text{Ker } h$ und $n \in \text{Ker } h$ gilt

$$\begin{aligned} h(r) &= h(x) / h(qn) \\ &= h(x) / h(n)^q \\ &= e / e^q \\ &= e, \end{aligned}$$

d.h. $r \in \text{Ker } h$. Wegen (1) und der Minimalitätseigenschaft von n folgt $r = 0$, d.h.

$$x = qn,$$

d.h. $x \in n\mathbb{Z}$. Wir haben gezeigt, es besteht auch die umgekehrte Inklusion $\text{Ker } h \subseteq n\mathbb{Z}$.

Der zweite Teil der Behauptung ist eine direkte Übersetzung der entsprechenden (offensichtlichen) Eigenschaften von $\mathbb{Z}/n\mathbb{Z}$. Zum Beispiel entspricht Aussage 1 der Tatsache, daß in $\mathbb{Z}/n\mathbb{Z}$ das n-fache jeden Elements gleich der Nullrestklasse ist.
QED.

1.4.2 Untergruppen zyklischer Gruppen zu vorgegebener Ordnung

Seien $n \in \mathbb{Z}$ eine natürliche Zahl und m ein Teiler von n,

$$n = q\,m \text{ für ein } q \in \mathbb{N}.$$

Dann ist die Abbildung

(1) $$\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z},\ g \bmod m\mathbb{Z} \mapsto qg \bmod n\mathbb{Z},$$

ein wohldefinierter injektiver Homomorphismus.

Insbesondere besitzt die zyklische Gruppe der Ordnung n zu jedem Teiler m von n eine Untergruppe der Ordnung m.

Beweis. Wir betrachten die Abbildung

$$h: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z},\ g \mapsto qg \bmod n\mathbb{Z}.$$

Diese Abbildung ist ein Homomorphismus,

$$\begin{aligned} h(g'+g'') &= (qg' + qg'') \bmod n \\ &= (qg' \bmod n) + (qg'' \bmod n) \\ &= h(g') + h(g''). \end{aligned}$$

Berechnen wir den Kern von h. Für $g \in \mathbb{Z}$ gilt:

$$\begin{aligned} g \in \text{Ker } h &\Leftrightarrow qg \equiv 0 \bmod n \\ &\Leftrightarrow qm = n \mid qg \\ &\Leftrightarrow m \mid g \end{aligned}$$

$\Leftrightarrow g \in m\mathbb{Z}$.

Es gilt also Ker h = $m\mathbb{Z}$. Nach dem 0-ten Isomorphiesatz ist die Abbildung

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\text{Ker } h \longrightarrow \text{Im } h\ (\subseteq \mathbb{Z}/n\mathbb{Z}),\ g \pmod m \mapsto h(g) = qg \pmod n,$$

ein Isomorphismus, d.h. (1) ist ein injektiver Isomorphismus (wie behauptet).
QED.

1.4.3 Die Anzahl der Untergruppen einer zyklischen Gruppe

Seien G eine endliche zyklische Gruppe und m ein Teiler der Gruppenordnung

$$n := \#G.$$

Dann gibt es genau eine Untergruppe der Ordnung m von G.
Beweis. Sei

$$G = < g > = \{ g^x \mid x \in \mathbb{Z} \}\ (\cong \mathbb{Z}/n\mathbb{Z})$$

und

$$n = m\,q.$$

Man beachte, es gilt dann[5]

(1) $$g^x = e \Leftrightarrow n \mid x.$$

Nach 1.3.11 gibt es mindestens eine Untergruppe der Ordnung m, nämlich

$$U = < g^q >.$$

Sei jetzt U' eine beliebige Untergruppe der Ordnung m von G. Nach 1.2.5 ist U' zyklisch,

$$U' = < g^h >.$$

Als zyklische Gruppe der Ordnung m ist U' isomorph zu $\mathbb{Z}/m\mathbb{Z}$, d.h. es gilt

$$(g^h)^m = 1.$$

Wegen (1) ist damit

$$qm = n \mid hm$$

also

$$q \mid h.$$

Dann ist aber $g^h \in < g^q > = U$, also $U' \subseteq U$, also U' = U.
QED.

1.4.4 Produkte zyklischer Gruppen

Seien m und n teilerfremde ganze Zahlen,

$$ggT(m,n) = 1.$$

Dann ist die Abbildung

$$\mathbb{Z}/(mn) \longrightarrow \mathbb{Z}/(m) \times \mathbb{Z}/(n),\ (a \pmod{mn}) \mapsto (a \pmod m, a \pmod n)$$

ein Isomorphismus.

Insbesondere ist das Produkt zweier zyklischer Gruppen mit teilerfremder (endlicher) Ordnung wieder zyklisch.
Beweis. Wir betrachten den Homomorphismus

$$h: \mathbb{Z} \longrightarrow \mathbb{Z}/(m) \times \mathbb{Z}/(n),\ a \mapsto (a \pmod m, a \pmod n).$$

Nach dem 0-ten Isomorphiesatz reicht es zu zeigen,

1. Ker h = $mn\mathbb{Z}$.
2. Im h = $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$.

---

[5] Als zyklische Gruppe der Ordnung n ist G isomorph zur additiven Gruppe $\mathbb{Z}/n\mathbb{Z}$, wobei g der Restklasse von 1 entspricht. Das x-fache dieser Restklasse ist genau dann gleich 0, wenn x ein Vielfaches von n ist.

Zu 1. Die Inklusion "$\supseteq$" ist trivial: Vielfache von mn sind durch m und durch n teilbar.

Beweisen wir "$\subseteq$". Sei a$\in$ Ker h. Dann gilt

$$a \pmod m = 0 \pmod m \text{ und } a \pmod n = 0 \pmod n,$$

d.h. m | a und n | a. Da m und n teilerfremd sind, folgt

$$mn \mid a,$$

d.h. $a \in mn\mathbb{Z}$.

Zu 2. Wegen 1. induziert h einen Isomorphismus

$$\mathbb{Z}/(mn) = \mathbb{Z}/\mathrm{Ker}(h) \xrightarrow{\tilde{h}} \mathrm{Im}(\tilde{h}) = \mathrm{Im}(h) \quad (\subseteq \mathbb{Z}/(m) \times \mathbb{Z}/(n)\ ).$$

Das Bild dieses Isomorphismus besteht also aus mn Elementen. Deshalb gilt

$$\mathrm{Im}(h) = \mathrm{Im}(\tilde{h}) = \mathbb{Z}/(m) \times \mathbb{Z}/(n).$$

QED.

Bemerkungen

(i) Unser nächstes Ziel ist eine vollständig Beschreibung der endlich erzeugten abelschen Gruppen. Eine wichtige Aussage in diesem Kontext, ist die Aussage, daß jede Untergruppe einer endlich erzeugten abelschen Gruppe wieder endlich erzeugt ist.

(ii) Der Beweis dieser Aussage läßt sich am besten in einem Kontext führen, der eine gemeinsame Verallgemeinerung der Begriffe der abelschen Gruppe und des Vektorraums darstellt: dem Begriff des Moduls.

(iii) Der Begriff des Moduls ist dem Begriff der Vektorraums sehr ähnlich, und viele Aussagen über Vektorräume gelten auch für Moduln und werden in derselben Weise wie für Vektorräume bewiesen. Wir werden uns deshalb im folgenden meistens die Wiederholung der Vektorraum-Beweise ersparen.

1.5 Moduln

1.5.1 Definition

Sei R ein Ring mit 1. Ein (linker) R-Modul ist eine (additiv geschriebene) abelsche Gruppe M zusammen mit einer Abbildung

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

welche Multiplikation des Moduls heißt und den folgenden Bedingungen genügt.

(i) $r\bullet(m + n) = r\bullet m + s\bullet m$ und $(r + s)\bullet m = r\bullet m + s\bullet m$ für $r, s\in R$ und $m,n\in M$

(ii) $(r\bullet s)\bullet m = r\bullet(s\bullet m)$ für $r,t \in R$ und $m \in M$

(iii) $1\bullet m = m$ für $m \in M$.

Sind M und M' zwei R-Moduln, so ist eine R-lineare Abbildung

$$f: M \longrightarrow M'$$

eine Abbildung mit

$$f(rm + sn) = rf(m) + sf(n) \text{ für } r,s \in R \text{ und } m,n \in M.$$

Ein rechter R-Modul ist eine abelsche Gruppe M zusammen mit einer Abbildung

$$M \times R \longrightarrow M, (m, r) \mapsto m\bullet r,$$

so daß die folgenden Bedingungen erfüllt sind.

(i') $(m+n)\bullet r = m\bullet r + n\bullet r$ und $m\bullet(r+s) = m\bullet r + m\bullet s$ für $r,s\in R$ und $m,n\in M$.

(ii') $m\bullet(r\bullet s) = (m\bullet r)\bullet s$ für $m \in M$ und $r,s \in R$

(iii') $m\bullet 1 = m$ für $m \in R$.

Sind M und M' zwei rechte R-Moduln, so ist eine R-lineare Abbildung

$$f: M \longrightarrow M'$$

eine Abbildung mit

$$f(mr + ns) = f(m)\bullet r + f(n)\bullet s \text{ für } r,s \in R \text{ und } m,n \in M.$$

Bemerkungen

(i) Die R-Moduln bilden mit den R-linearen Abbildungen eine Kategorie

$$R\text{-Mod}.$$

Analog bilden die rechten R-Moduln mit den R-linearen Abbildungen eine Kategorie

$$\text{Mod-}R.$$

(ii) Sei R ein Körper. Dann stimmt der Begriff des R-Moduls mit dem Begriff des R-Vektorraums überein.

(iii) Sei $R = \mathbb{Z}$. Dann stimmt der Begriff des R-Moduls mit dem Begriff der abelschen Gruppe überein.

(iv) Seien R ein Ring mit 1 und R^{op} der zu R entgegengesetzte Ring, d.h. als Menge ist

$$R^{op} := R,$$

die Addition von R^{op} ist dieselbe wie die von R, und für die Multiplikation $\bullet^{op}$ von R^{op} gilt

$$a\bullet^{op}b := b\bullet a.$$

Dann ist jeder linke R-Modul ein rechter R^{op}-Modul und jeder rechte R-Modul ein linker R^{op}-Modul. Wegen

$$(R^{op})^{op} = R$$

reicht es deshalb, wenn wir uns auf die Untersuchung von (linken) R-Moduln beschränken.

(v) Im Fall kommutativer Ringe R mit 1 fallen die beiden Begriffe linker und rechter R-Modul zusammen.

1.5.2 Teilmoduln

Seien R ein Ring mit 1 und M ein R-Modul. Ein R-Teilmodul von M ist eine Teilmenge

$$N \subseteq M,$$

welche mit den Operationen von M ein R-Modul ist.

Bemerkungen

(i) Eime Teilmenge $N \subseteq M$ ist genau dann ein R-Teilmodul von M, wenn die folgenden Bedingungen erfüllt sind.
(a) N ist nicht leer.
(b) Mit je zwei Elemente n', n" ∈ N gilt auch n'-n" ∈ N.
(c) Mit n ∈ N und r ∈ R gilt auch r•n ∈ R.

Dieses Teilmodulkriterion wird in derselben Weilse bewiesen wie das entsprechende Kriterium für lineare Unterräume von Vekotrräumen.

(ii) Für jede Familie $\{N_i\}_{i\in I}$ von Teilmodduln N_i von M ist auch

$$\bigcap_{i\in I} N$$

ein Teilmodul von M.

Der Beweis erfolgt in derselben Weise wie im Fall von Vektorräumen.

(iii) Für jede R-lineare Abbildung f: M $\longrightarrow$ M' ist das Bild dieser Abbildung ein R-Teilmodul von M' (und wird mit Im(f) bezeichnet).

(iv) Für jede R-lineare Abbildung f: M $\longrightarrow$ M' ist der Kern dieser Abbildung,

$$\mathrm{Ker}(f) := \{m \in M \mid f(m) = 0\}$$

ein R-Teilmodul von M.

1.5.3 Erzeugendensysteme und Basen

Seien R ein Ring mit 1, M ein R-Modul und $S \subseteq M$ eine Teilmenge. Dann wird der Durchschnitt aller Teilmoduln von M, die die Menge S enthalten mit

$$< S > = < s \mid s\in S > := \bigcap \{N \subseteq M \mid N \text{ ist Teilmodul von M mit } S \subseteq M\}$$

bezeichnet und heißt der von S erzeugte Teilmodul von M oder auch Erzeugnis von S über R. Im Fall

$$M = < S >$$

heißt S Erzeugendensystem von M über R. Ist S endlich, so sagt man M ist über R endlich erzeugt.

Bemerkungen

(i) Wie im Fall von Vektorräumen sieht man, das Erzeugnis < S > von S über R besteht aus allen (endlichen) R-Linearkombinationen von Elementen aus S,

$$< S > = \{ \sum_{s\in S} r_s \bullet s \mid r_s \in R \text{ für jedes } s \in S, r_s = 0 \text{ für fast alle } s\}$$

Man schreibt deshalb auch

$$< S > = \sum_{s\in S} R\bullet s$$

bzw.

$$< S > = R\bullet S.$$

(ii) Der Begriff der linearen Unabhängigkeit von Elementen von M wird in derselben Weise definiert wie im Fall von Vektorräumen, d.h. eine Teilmenge $S \subseteq M$ heißt linear unabhängig über R, wenn nur die trivialen Linearkombinationen von je endlich vielen Elementen von S gleich Null sind.

(iii) Ein linear unabhängiges Erzeugendensystem eines Moduls heißt auch Basis dieses Moduls.

(iv) Nicht jeder R-Modul besitzt eine Basis. Zum Beispiel ist

$$M := \mathbb{Z}/2\mathbb{Z}$$

ein Modul über $R := \mathbb{Z}$. Für jedes $m \in M$ gilt aber $2m = 0$, d.h. kein von Null verschiedenes Element kann einer Basis angehören.

(v) Ein R-Modul, der eine Basis besitzt heißt frei.

(vi) Wie im Fall von Vektorräumen definiert man die direkte Summe und das direkte Produkt einer Familie $\{M_i\}_{i\in I}$ von R-Moduln.

$$\times_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i \text{ für alle } i \in I\}$$

$$\oplus_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i \text{ für alle } i \in I, \text{ fast alle } m_i \text{ sind gleich } 0\}$$

Operationen:

$$(m'_i)_{i\in I} + (m'_i)_{i\in I} = (m''_i + m''_i)_{i\in I}$$

$$r\bullet(m_i)_{i\in I} := (r\bullet m_i)_{i\in I}.$$

(vii) Ein R-Modul ist genau dann frei, wenn er isomorph ist zu einer direkten Summe von Exemplaren des R-Moduls R.

(viii) Sie Exaktheit von Sequenzen von Moduln wird in derselben Weise definiert wie im Fall von Vektorräumen, d.h.

$$\ldots \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow \ldots$$

heißt <u>exakt</u> an der Stelle M, wenn Im(f) = Ker(g) gilt.

Sei

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

eine exakte Sequenz von R-Moduln. Weiter seien

$$\{m'_i\}_{i\in I}$$

ein Erzeugendensystem von M' und

$$\{m''_j\}_{j\in J}$$

eine Familie von Elementen aus M mit der Eigenschaft, daß die Bilder $g(m''_j)$ ein Erzeugendensystem von M'' bilden. Dann bilden die beiden Familien zusammen ein Erzeugendensystem von M.

(x) Aussage (viii) gilt auch für Basen anstelle von Erzeugendensystemen.

(x) Sind die Moduln M' und M'' der exakten Sequenz von (viii) endlich erzeugt, so gilt dasselbe für M.

Alle Beweise erfolgen in derselben Weise wie im Fall von Vektorräumen.

1.5.4 Faktormoduln

Seien R ein Ring mit 1, M ein R-Modul und $N \subseteq M$ ein Teilmodul. Dann besitzt die Menge

$$M/N := \{m + N \mid m \in M\}$$

auf genau eine Weise die Struktur eines R-Moduls, für welche die natürliche Abbildung

$$\rho: M \longrightarrow M/N,\ m \mapsto m + N,$$

eine R-lineare Abbildund ist.

Bemerkungen

(i) Die Abbildung ρ ist surjektiv und hat den Kern N.

(ii) Eine R-lineare Abbildung $f: M \longrightarrow M'$ faktorisiert sich genau dann über ρ, wenn $M \subseteq \mathrm{Ker}(f)$ gilt. Die Faktorisierung ist dann eindeutig bestimmt, d.h. des gibt dann genau eine R-lineare Abbildung $\tilde{f}: M/N \longrightarrow M'$ für welche das Diagramm

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ {\scriptstyle\rho}\downarrow & \nearrow_{\tilde{f}} & \\ M/N & & \end{array}$$

kommutativ ist.

(iii) Falls $\tilde{f}$ existiert, so gilt

$\mathrm{Im}(\tilde{f}) = \mathrm{Im}(f)$

$\mathrm{Ker}(\tilde{f}) = \mathrm{Ker}(f)/N.$

(iv) Wie im Fall von Vektorräumen und Gruppen gelten die Isomorphiesätze 0-2.

$M/Ker(f) \cong Im(f)$, Restklasse von $m \mapsto f(m)$,

$N'/N' \bigcap N'' \cong N'+N''/N''$ für je zwei Teilmoduln $N', N'' \subseteq M$

$(M/N')/(N''/N') \cong M/N''$ für je zwei Teilmoduln $N', N'' \subseteq M$ mit $N' \subseteq N''$

1.5.5 Tensorprodukte

Seien R ein kommutativer Ring mit 1, M ein rechter und N ein linker R-Modul. Das Tensor-Produkt von M und N über R wird mit

$$M \otimes_R N$$

bezeichnet und ist definiert als eine abelsche Gruppe zusammen mit einer Abbildung

$$b: M \times N \longrightarrow M \otimes_R N, (m, n) \mapsto m \otimes n,$$

mit folgenden Eigenschaften.

(i) Die Abbildung b ist R-bilinear, d.h. es gilt

(a) $b(m'+m'', n) = b(m',n) + b(m'',n)$ für $m', m'' \in M$ und $n \in N$.

(b) $b(m, n'+ n'') = b(m,n') + b(n,m'')$ für $m \in M$ und $n', n'' \in N$.

(c) $b(m \bullet r, n) = b(n, r \bullet n)$ für $m \in M, n \in N, r \in R$.

(ii) Die Abbildung b ist universell bezüglich der Eigenschaft (i), d.h. für jede bilineare Abbildung

$$b': M \times N \longrightarrow A$$

mit Werten in einer abelschen Gruppe A gibt es genau einen Gruppen-Homomorphismus

$$\tilde{b}': M \otimes_R N \longrightarrow A$$

mit $b' = \tilde{b}' \circ b$.

Bemerkungen

(i) $M \otimes_R R = M$ und $R \otimes_R N = N$.

(ii) $(\oplus_{i \in I} M_i) \otimes_R N = \oplus_{i \in I} (M_i \otimes_R N)$

$M \otimes_R (\oplus_{i \in I} N_i) = \oplus_{i \in I} (M \otimes_R M_i)$

(iii) Der Übergang zum Tensorprodukt definiert Funktoren

$$\otimes_R N: \text{Mod-R} \longrightarrow \text{Ab}, M \mapsto M \otimes_R N$$

$$M \otimes_R: \text{R-Mod} \longrightarrow \text{Ab}, N \mapsto M \otimes_R N$$

(iv) Für jede kurze exakte Seqenz von rechten R-Moduln

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

erhält man durch Anwenden des Funktors $\otimes_R N$ eine exakte Seqenz von abelschen Gruppen

$$M' \otimes_R N \longrightarrow M \otimes_R N \longrightarrow M'' \otimes_R N \longrightarrow 0$$

(v) Für jede kurze exakte Seqenz von (linken) R-Moduln

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

erhält man durch Anwenden des Funktors $M \otimes_R$ eine exakte Seqenz von abelschen Gruppen

$$M\otimes_R N' \longrightarrow M\otimes_R N \longrightarrow M\otimes_R N'' \longrightarrow 0$$

(vi) Ist der Modul, mit dem in (iv) bzw. (v) tensoriert wird frei, so kann bleiben die tensorierten Sequenzen auch exakt, wenn man die links fehlende Null-Abbildung '$0 \longrightarrow$' hinzufügt. Im allgemeinen ist dies jedoch nicht der Fall. Zum Beispiel definiert im Fall $R = \mathbb{Z}$ die Multiplikation mit 2 eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Durch Tensorieren mit $\mathbb{Z}/2\mathbb{Z}$ über $\mathbb{Z}$ erhält man eine Sequenz

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{2} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

welche nicht mehr exakte ist, denn die Multiplikation mit 2 ist jetzt die Null-Abbildung und insbesondere nicht mehr injektiv.

(vii) Ist $R \longrightarrow S$ ein Homomorphismus von kommutativen Ringen mit 1, so ist

$$M\otimes_R S$$

ein rechter S-Modul mit

$$(m\otimes s)\bullet t = m\otimes(st) \text{ für } m\in M,\ s,t \in S,$$

und

$$S\otimes_R N$$

ein linker S-Modul mit

$$s\bullet(t\otimes n) = (s\bullet t)\otimes n.$$

(viii) Sind $R \longrightarrow S$ und $R \longrightarrow T$ zwei Homomorphismen von kommutativen Ringen mit 1, so ist

$$S\otimes_R T$$

eine R-Algebra mit

$$(s\otimes t)\bullet(s'\otimes t') = (ss')\otimes(tt') \text{ und}$$
$$r\bullet(s\otimes t) = (rs)\otimes t = s\otimes(rt)$$

Die Beweise der obigen Aussagen erfolgen in derselben Weise wie im Fall von Vektorräumen.

1.5.6 Noethersche Moduln und Ringe

Seien R ein Ring mit 1 und M ein R-Modul. Der Modul M heißt noethersch über R, wenn jeder Teilmodul von M endlich erzeugt ist. Der Ring R heißt noethersch, wenn R als R-Modul noethersch ist.

Bemerkungen

(i) Sei R ein Körper. Die einzigen Teilmoduln des 1-dimensionalen R-Vektorraum R sind dann {0} und R. Beide sind endlich erzeugt. Also ist jeder Körper ein noetherscher Ring.

(ii) Betrachten wir den Ring $R = \mathbb{Z}$ der ganzen Zahlen. Die Teilmoduln von $\mathbb{Z}$ sind gerade die Untergruppen von $\mathbb{Z}$, also von der Gestalt

$$n\mathbb{Z} = < n > \text{ mit } n \in \mathbb{Z}.$$

Insbesondere sind alle Teilmoduln von $\mathbb{Z}$ endlich erzeugt (sogar einfach erzeugt), d.h. $\mathbb{Z}$ ist ein noetherscher Ring.

(iii) Seien R ein Ring mit 1 und

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

eine exakte Sequenz von R-Moduln. Dann sind folgende Aussagen äquivalent.
(a) M ist noethersch.
(b) M' und M'' sind noethersch.

(iv) Seien R ein Ring mit 1 und M' und M" zwei noethersche R-Moduln. Dann ist auch die direkte Summe M'⊕M" noethersch.

Beweis von (iii). (a) ⇒ (b). Sei M noethersch. Wir können M' mit einem Teiilmodul von M identifizieren. Teilmoduln von M' werden dann zu Teilmoduln von M. Mit M ist somit auch M' noethersch. Sei jetzt ein Teilmodul von M" gegeben, sagen wir

$$N'' \subseteq M''.$$

Dann ist $g^{-1}(N'')$ ein Teilmodul von M, besitzt also ein endliches Erzeugendensystem. Wir wenden g auf ein solches Erzeugendensystem an und erhalten ein endliches Erzeugendensystem von N". Also ist N" endlich erzeugt.

(b) ⇒ (a). Seien M' und M" noethersch und

$$N \subseteq M$$

ein Teilmodul. Wir haben zu zeigen, N ist endlich erzeugt. Wir schränken g auf N ein und erhalten eine exakte Sequenz

$$0 \longrightarrow \mathrm{Ker}(g|N) \longrightarrow N \xrightarrow{g|N} g(N) \longrightarrow 0 \qquad (1)$$

Das Bild g(N) ist als Teilmodul des noetherschen Moduls M" endlich erzeugt.

Weiter gilt

$$\begin{aligned} \mathrm{Ker}(g|N) &\subseteq \mathrm{Ker}(g) \\ &= \mathrm{Im}(f) && \text{(wegen der Exaktheit der Sequenz der M)} \\ &\cong M'. && \text{(weil f injektiv ist)} \end{aligned}$$

Wir können also Ker(g|N) mit einem Teilmodul des noetherschen Moduls M' identifizieren. Als solcher ist Ker(g|N) endlich erzeugt.

Wir haben gezeigt, die beiden äußeren Moduln der exakten Sequenz (1) sind endlich erzeugt. Nach Bemerkung 1.5.3 (x) ist dann aber auch N endlich erzeugt.

QED.

Beweis von (iv). Man wende Aussage (iii) auf die exakte Sequenz

$$0 \longrightarrow M' \xrightarrow{f} M'\oplus M'' \xrightarrow{g} M'' \longrightarrow 0$$

mit

$$f(m') := (m',0)$$

und

$$g(m',m'') := m''$$

an.

QED.

1.5.7 Basissatz von Hilbert

Sei R kommutativer Ring mit 1. Ist R noethersch, so gilt dasselbe auch für den Polynomring R[x].

Bezeichnung:

Die Teilmoduln des R-Moduls R heißen auch Ideale [6] von R.

Beweis. Sei

$$I \subseteq R[x]$$

ein Ideal des Polynomrings. Wir haben zu zeigen, I besitzt ein endliches Erzeugendensystem. Wir können ohne Beschränkung der Allgemeinheit annehmen,

$$I \neq \{0\}.$$

---

[6] Im nicht-kommutativen Fall spricht man von linksseitigen Idealen oder auch Linksidealen.

Nach Voraussetzung ist R ein noetherscher Ring. Damit ist jede endliche direkte Summe von Exemplaren von R ein noetherscher R-Modul, und dasselbe gilt von jedem Teilmodul einer solchen endlichen direkten Summen.

Insbesondere ist für jede natürliche Zahl n der R-Modul

$$I(n) := \{ f \in I \mid \deg f \leq n\} \text{ noethersch als R-Modul} \qquad (1)$$

(als R-Teilmodul von $\{f \in R[x] \mid \deg f \leq n\} \cong R^{n+1}$).

Für jedes Polynom

$$f(x) = f_0 + f_1 x + f_2 x^2 + ... + f_i x^i + ...$$

mit Koeffizienten $f_i \in R$ sei

$$c(f)$$

der höchste von Null verschiedene Koeffizient des Polynoms f im Fall $f \neq 0$ und sei gleich Null, falls $f = 0$ ist. Wir setzen

$$\tilde{I} := \{c(f) \mid f \in I\}$$

Sind a, b zwei Elemente aus $\tilde{I}$ und A, B $\in$ I zwei Polynome mit dem höchsten Koeffizienten a bzw. b, so können wir A und B so mit geeigneten x-Potenzen multiplizieren, daß diese Polynome denselben Grad bekommen. Wir können also annehmen,

$$\deg A = \deg B.$$

Durch bilden von R-Linearkombinationen von A und B sehen wir, daß beliebige R-Linearkombinationen von a und b in $\tilde{I}$ liegen. Mit anderen Worten,

$$\tilde{I} \text{ ist ein Ideal von R.}$$

Als Ideal von R ist $\tilde{I}$ endlich erzeugt. Wir wählen Polynome

$$g_1,...,g_m \in I$$

mit

$$\tilde{I} = R \bullet c(g_1) + ... + R \bullet c(g_m) \qquad (2)$$

Weiter fixieren wir eine natürliche Zahl d mit

$$\deg g_1 \leq d \text{ , ... , } \deg g_m \leq d.$$

Zu Beweis der Behauptung reicht es zu zeigen

$$I = I(d) + R[x] \bullet g_1 + ... + R[x] \bullet g_m, \qquad (3)$$

denn dann bilden die g_i zusammen mit einem beliebigen endlichen Erzeugendensystem des noetherschen R-Moduls I(d) ein endliches Erzeugendensystem des Ideals I. Nach Definition von I(d) und der g_i besteht zumindest die Inklusion '$\supseteq$' (weil I ein R[x]-Modul ist). Wir haben also nur die Inklusion '$\subseteq$' zu beweisen.

Sei $f \in I$. Im Fall $f = 0$ ist nichts zu beweisen. Sei also $f \neq 0$.

Wir führen den Beweis durch Induktion nach dem Grad von f.

<u>Induktionsanfang</u>: $\deg f \leq d$.

Nach Definition (1) gilt dann $f \in I(d)$ und f liegt trivialerweise in der rechten Seite von (3).
Induktionsschritt. $d < \deg f$.

Nach Definition von $\tilde{I}$ und der Wahl der g_i können wir den höchsten Koeffizienten von f in der folgenden Gestalt schreiben (vgl (2)).

$$c(f) = r_1 \bullet c(g_1) + ... + r_m \bullet c(g_m) \text{ mit } r_i \in R \text{ für alle i.}$$

Nach Voraussetzung ist

$$n_i := \deg f - \deg g_i \geq \deg f - d > 0$$

für jedes i eine natürliche Zahl. Deshalb ist

$$\sum_{i=1}^{m} r_i \bullet x^{n_i} \bullet g_i \in I$$

ein wohldefiniertes Polynom mit demselben Grad wie f und demselben höchsten Koeffizienten wie f. Insbesondere ist der Grad von

$$f - \sum_{i=1}^{m} r_i \bullet x^{n_i} \bullet g_i$$

kleiner als der Grad von f. Nach Induktionsvoraussetzung liegt damit diese Differenz in der rechten Seite von (3). Dann liegt aber auch f selbst in der rechten Seite von (3).
QED.

1.6 Endlich erzeugte abelsche Gruppen, Elementarteilersatz

1.6.1 Erzeugendensysteme abelscher Gruppen

Seien A eine (additiv geschriebene) abelsche Gruppe und

$$\{a_i\}_{i \in I}$$

ein Erzeugendensystem von A. Dann gilt

$$A = \{ \sum_{i \in I} g_i a_i \mid g_i \in \mathbb{Z}, \text{ fast alle } g_i = 0 \}.$$

Beweis. Dies ist ein Spezialfall von Bemerkung 1.5.2(i) (mit $R := \mathbb{Z}$).
QED.

Bemerkungen: elementare Operationen mit Erzeugendensystemen

(i) Wir denken uns im folgenden die Indexmenge I mit irgendeiner Ordnung versehen, d.h. die a_i seien in irgendeiner Reihenfolge gegeben. Die Eigenschaft, Erzeugendensystem zu sein hängt jedoch nicht von dieser Reihenfolge ab: durch Abänderung der Ordnung von I geht ein Erzeugendensystem in ein Erzeugendensystem von A über.

(ii) Ersetzt man ein a_i durch $a_i + g a_j$ mit $i, j \in I$ und j verschieden von i, erhält man wieder ein Erzeugendensystem von A.

(iii) Sei A eine endlich erzeugte abelsche Gruppe. Dann bezeichnen wir mit

$$\mu(A)$$

die minimale Anzahl von Elementen, die ein Erzeugendensystem von A haben kann.

(iv) Beispiel: Ist p eine Primzahl und

$$A = \mathbb{Z}/(p) \oplus .... \oplus \mathbb{Z}/(p) \text{ (n -mal)}$$

eine direkte Summe von n Exemplaren von $\mathbb{Z}/(p)$, so gilt

$$\mu(A) = n.$$

(Beweis siehe unten).

(v) Die mininale Erzeugenzahl kann nicht größer werden, wenn man von A zu einer Faktorgruppe A/B übergeht,

$$\mu(A) \geq \mu(A/B),$$

denn aus jedem Erzeugendensystem von A erhält man durch Übergang zu den Restklassen modulo B ein Erzeugendensystem von A/B.

(vi) Seien p eine Primzahl und die Gruppe A eine direkte Summe von endlich vielen zyklischen Gruppen von p-Potenzordnung,

$$A = \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus ... \oplus \mathbb{Z}/p^{n_r}\mathbb{Z} \text{ (alle } n_i > 0).$$

Dann ist

$$\mu(A) = r$$

gleich der Anzahl der direkten Summanden.

Beweis von (iv). Die Elemente von A lassen sich mit ganzen Zahlen $g \in \mathbb{Z}$ multiplizieren,

$$g \bullet (\overline{g}_1, ... , \overline{g}_n) = (g\overline{g}_1, ... , g\overline{g}_n),$$

wobei das Produkt Null ist, wenn g ein Vielfaches der Primzahl p ist. Das bedeutet, das Produkt hängt nicht von der ganzen Zahl g sondern nur von deren Restklasse modulo p ab. Wir haben damit eine Multplikation der Elemente des Körpers

$$\mathbb{F}_p = \mathbb{Z}/(p)$$

mit dem Elementen der Gruppe A definiert. Die Gruppe A wird dadurch zu einem $\mathbb{F}_p$-Vektorraum, und es gilt

$$\mu(A) = \dim_{\mathbb{F}_p} A = n.$$

QED.

Beweis von (vi).

Sei

$$e_i \in A$$

das Element von A, dessen i-te Koordinate die Restklasse von 1 und dessen übrige Koordinaten Nullrestklassen sind. Dann ist jedes Element von A eine ganzzahlige Linearkombination von $e_1,...,e_r$, d.h. die e_i bilden ein Erzeugendensystem von A und es gilt

$$\mu(A) \leq r.$$

Außerdem gilt

$$\begin{aligned} A/pA &= \left(\bigoplus_{i=1}^{r} \mathbb{Z}/p^{n_i}\mathbb{Z}\right)/p\bullet\left(\bigoplus_{i=1}^{r} \mathbb{Z}/p^{n_i}\mathbb{Z}\right) \\ &\cong \bigoplus_{i=1}^{r} (\mathbb{Z}/p^{n_i}\mathbb{Z}) / (p\mathbb{Z}/p^{n_i}\mathbb{Z}) \\ &\cong \bigoplus_{i=1}^{r} \mathbb{Z}/p\mathbb{Z} \end{aligned}$$

Damit ist aber auch

$$\mu(A) \geq \mu(A/pA) = r.$$

QED.

1.6.2 Die Gruppe der Relationen zu einem Erzeugendensystem

Seien A eine (additiv geschriebene) abelsche Gruppe und

$$a := \{a_i\}_{i\in I}$$

ein Erzeugendensystem von A. Dann ist die Menge

$$R(a) := \{ \{g_i\}_{i\in I} \mid g_i\in\mathbb{Z}, \text{ fast alle } g_i = 0, \sum_{i\in I} g_i a_i = 0 \}$$

eine abelsche Gruppe bezüglich der Operation

$$\{g'_i\}_{i\in I} + \{g''_i\}_{i\in I} := \{ g'_i + g''_i\}_{i\in I}.$$

Die Elemente von R(a) heißen Relationen von a.

Beweis. Die angegeben Operation definiert eine Abbildung

$$R(a) \times R(a) \longrightarrow R(a).$$

Diese ist assoziativ, da in der additiven Gruppe $\mathbb{Z}$ das Assoziativgesetz gilt. Die Familie

$$\{g_i\}_{i\in I} \text{ mit } g_i = 0 \text{ für alle } i$$

spielt die Rolle des Nullelements, die Familie

$$\{ - g_i\}_{i\in I}$$

die Rolle des Negativen von $\{g_i\}_{i\in I}$.

QED.

Bemerkungen

(i) Bezeichne $\mathbb{Z}^{(I)}$ die direkte Summe der Gruppen der Familie $\{\mathbb{Z}\}_{i\in I}$, d.h.

$$\mathbb{Z}^{(I)} = \{ \{g_i\}_{i\in I} \mid g_i\in\mathbb{Z}, \text{ fast alle } g_i = 0\}$$

mit koordinatenweiser Addition,

$$\{g'_i\}_{i\in I} + \{g''_i\}_{i\in I} := \{ g'_i + g''_i\}_{i\in I}.$$

Dann ist die Abbildung

$$\mathbb{Z}^{(I)} \longrightarrow A, \{g_i\}_{i\in I} \mapsto \sum_{i\in I} g_i a_i ,$$

ein surjektiver Gruppenhomomorphismus mit dem Kern R(a). Insbesondere ist

(1) $$A \cong \mathbb{Z}^{(I)}/R(a).$$

(ii) Unser Ziel ist es, in diesem Abschnitt zu verschiedenen abelschen Gruppen A ein Erzeugendensystem zu finden, für welches R(a) eine möglichst einfache Gestalt besitzt. Der Isomorphismus liefert dann eine besonders einfache Beschreibung der Gruppe A.

(iii) Gruppen, die isomorph sind zu Gruppen der Gestalt $\mathbb{Z}^{(I)}$, heißen freie abelsche Gruppen

1.6.3 Das Verhalten der Gruppe R(a) bei elementaren Operationen

Seien A eine abelsche Gruppe und $a = \{a_i\}_{i\in I}$ ein Erzeugendensystem von A. Dann gilt:

(i) Für jede bijektive Abbildung f: I $\longrightarrow$ I ist auch $a' := \{a_{f(i)}\}_{i\in I}$ ein Erzeugendensystem und die Abbildung

$$f_*: R(a) \longrightarrow R(a'), \{g_i\}_{i\in I} \mapsto \{g_{f(i)}\}_{i\in I},$$

ist ein Isomorphismus abelscher Gruppen.

(ii) Seien $i_o, j_0 \in I$ verschieden und $g \in \mathbb{Z}$. Die Familie $a' := \{a'_i\}_{i\in I}$ entstehe aus a, indem man a_{i_0} durch $a_{i_o} + g a_{j_0}$ ersetzt, d.h.

$$a'_i := \begin{cases} a_i & \text{falls } i \neq i_o \\ a_{i_o} + g a_{j_o} & \text{falls } i = i_o \end{cases} .$$

Dann ist a' ein Erzeugendensystem und die Abbildung

$$f_*: R(a) \longrightarrow R(a'), \{g_i\}_{i\in I} \mapsto \{g'_i\}_{i\in I'}$$

mit

$$g'_i := \begin{cases} g_i & \text{falls } i \neq j_o \\ g_{j_o} - g g_{i_o} & \text{falls } i = j_o \end{cases}$$

ist ein Isomorphismus abelscher Gruppen.

Beweis. Die Aussagen sind trivial. Man beachte im Fall (ii) gilt

$$\begin{aligned} \sum_{i\in I} g_i a_i &= \ldots + g_{i_o} a_{i_o} + \ldots + g_{j_o} a_{j_o} + \ldots \\ &= \ldots + g_{i_o} (a_{i_o} + g\, a_{j_o}) + \ldots + (g_{j_o} - g g_{i_o}) a_{j_o} + \ldots \\ &= \sum_{i\in I} g'_i a'_i \end{aligned}$$

QED.

Bemerkung zu Erzeugendensystemen bei Isomorphismen

Seien $h: G \longrightarrow G'$ ein Isomorphismus von Gruppen und $\{g_i\}_{i\in I}$ ein Erzeugendensystem von G. Dann ist $\{h(g_i)\}_{i\in I}$ ein Erzeugendensystem von G'.

1.6.4 Elementarteilersatz

Sei A eine endlich erzeugte abelsche Gruppe. Dann besitzt A ein endliches Erzeugendensystem

$$a = \{a_i\}_{i\in I}, I = \{1,\ldots,n\},$$

mit endlich vielen Relationen

$$r_1, \ldots, r_s, (s \leq n),$$

so daß gilt

1. $R(a) = \langle r_1, \ldots, r_s \rangle = \mathbb{Z} r_1 + \ldots + \mathbb{Z} r_s$

2. $r_j = \{ r_{ji} \}_{i\in I} = \begin{pmatrix} d_1 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & d_s & \ldots & 0 \\ 0 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}$ mit $d_i > 0$.

2. $d_i \mid d_{i+1}$ für $i = 1, \ldots, s-1$.

Die d_i heißen Elementarteiler von A.

Die Folge der Elementarteiler hängt nur von der Gruppe A und nicht vom Erzeugendensystem a ab.

Bemerkungen

(i) Weil $a_1, \dots, a_n \in A$ ein Erzeugendensystem von A ist, ist die $\mathbb{Z}$-lineare Abbildung

$$\mathbb{Z}^n \xrightarrow{f} A, \begin{pmatrix} g_1 \\ \dots \\ g_n \end{pmatrix} \mapsto \sum_{i=1}^{n} g_i a_i ,$$

surjektiv. Nach Definition von R(a) gilt

$$R(a) := \mathrm{Ker}(f).$$

Betrachten wir die Matrix

$$r = (r_1,\dots,r_s) = \begin{pmatrix} d_1 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & d_s & \dots & 0 \\ 0 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix},$$

deren Spalten die Erzeuger r_i von R(a) sind, und die zugehörige $\mathbb{Z}$-lineare Abbildung

$$\mathbb{Z}^s \xrightarrow{g} \mathbb{Z}^n, x = \begin{pmatrix} x_1 \\ \dots \\ x_s \end{pmatrix} \mapsto rx = \sum_{i=1}^{n} r_i x_i .$$

Das Bild von g ist dann gerade das Erzeugnis R(a) der $r_i = d_i e_i$,

$$\mathrm{Im}(g) = R(a) = \mathbb{Z}d_1e_1 + \dots + \mathbb{Z}d_re_r .$$

Wir erhalten so eine exakte Sequenz von $\mathbb{Z}$-linearen Abbildungen

$$\mathbb{Z}^s \xrightarrow{g} \mathbb{Z}^n \xrightarrow{f} A \longrightarrow 0.$$

(ii) Wegen der Surjektivität der Abbildung f gilt

$$\begin{aligned} A &\cong \mathbb{Z}^n/\mathrm{Ker}(f) \\ &= \mathbb{Z}^n/\mathrm{Im}(g) \\ &= \mathbb{Z}^n/(\mathbb{Z}d_1e_1 + \dots + \mathbb{Z}d_re_r) \\ &= (\mathbb{Z}/d_1\mathbb{Z})\oplus\dots\oplus(\mathbb{Z}/d_s\mathbb{Z}) \oplus \mathbb{Z}^{n-s} \end{aligned}$$

Wie wir sehen werden, ist die Zahl n-s unabhängig von der speziellen Wahl der angegebenen Zerlegung von A in eine direkte Summe zyklischer Gruppen. Diese Zahl heißt Rang von A.

(iii) Die Isomorphie von (ii) bedeutet gerade, es gibt ein Erzeugendensystem

$$e_i = (0 \bmod d_1,\dots, 0 \bmod d_{i-1}, 1 \bmod d_i, 0 \bmod d_{i+1}, \dots, 0 \bmod d_s)$$

(i = 1, ... , s) von A mit der Eigenschaft, daß eine ganzzahlige Linearkombination genau dann gleich Null ist,

$$n_1 \bullet e_1 + n_2 \bullet e_2 + \dots + n_s \bullet e_s = 0,$$

wenn für jedes i der i-te Koeffizient kongruent Null modulo d_i ist,

$$n_i \in d_i\mathbb{Z} \text{ für } i = 1, \dots, s.$$

Beweis. Wir fixieren irgendein endliches Erzeugendensystem

$$a = \{a_i\}_{i\in I} \text{ von } A, I = \{1,\dots,n\}$$

und ein Erzeugendensystem

$$r = \{r_j\}_{j\in J} \text{ von } R(a).$$

Weil R(a) ein $\mathbb{Z}$-Teilmodul von $\mathbb{Z}^n$ ist (und $\mathbb{Z}^n$ ein noetherscher $\mathbb{Z}$-Modul), können wir annehmen, das Erzeugendensystem von R(a) ist endlich, sagen wir

$$J = \{1,\dots,s\}.$$

Weiter führen wir Bezeichnungen für die Koordinaten der Erzeuger r_j ein,

$$r_j = \begin{pmatrix} r_{j1} \\ \dots \\ r_{jn} \end{pmatrix} = (r_{ji})_{i\in I}.$$

und betrachten die Matrix

$$r = (r_1,\dots,r_s) = (r_{ji})_{i\in I, j\in J}, = \begin{pmatrix} r_{11} \dots r_{s1} \\ \dots \dots \dots \\ r_{1n} \dots r_{sn} \end{pmatrix}$$

mit den Spalten r_j.

Das gesuchte Erzeugendensystem werden wir im wesentlichen durch elementare Operationen im Sinne von 1.5.3 aus dem gegebene Erzeugendensystem gewinnen. Den nachfolgend beschriebenen Algorithmus kann man in gewissem Sinne als eine Verallgemeinerung des Gaußschen Algortihmus auffassen.

Vorbemerkung 1: elementare Zeilenoperationen:
Auf Grund von 1.5.3 können wir das Erzeugendensystem a so abändern, daß sich dabei die Reihenfolge der Koordinaten der r_j in vorgegebener Weise abändert.
Außerdem können wir durch Abändern des Erzeugendensystems a erreichen, daß die r_{j,i_o} durch $r_{j,i_o} - g r_{j,j_0}$ ersetzt werden mit vorgegebenen $i_o, j_o \in I$ und $g\in\mathbb{Z}$. (und $i_o \neq j_o$).

Mit anderen Worten, wir können
1. die Zeilen von r permutieren.
2. ein ganzzahliges Vielfaches einer Zeile von r zu einer anderen addieren

ohne daß die Familie der r_j aufhört ein Erzeugendensystem eines R(a) zu einem endlichen Erzeugendensystem von A zu sein.

Vorbemerkung 2: elementare Spaltenoperationen:
Wir können natürlich auch die Reihenfolge der r_j abändern und ein ganzzahliges Vielfaches eines r_j zu einem anderen addieren, ohne daß die Familie der r_j aufhört,

Erzeugendensystem von R(a) zu sein. Mit anderen Worten, die oben angegebenen Operationen können wir auch mit den Zeilen von r anstelle der Spalten ausführen.

Beschreibung eines Algorithmus.

1. Falls alle $r_{ji} = 0$ sind, endet der Algorithmus: es ist dann n = s = 0. Die Zahl der Elementarteiler ist Null, R(a) = {0} ist trivial und A ist eine freie abelsche Gruppe.

2. Wir suchen in (r_{ji}) eine ganze Zahl $r_{j_0 i_0} \neq 0$, deren Betrag minimal ist unter allen Beträgen aller von Null verschiedener r_{ji}. Durch Divison mit Rest, d.h. durch Abziehen von ganzzahligen Vielfachen erreichen wir, daß alle Einträge in der j_0-ten Zeile und i_0-ten Spalte betragmäßig kleiner sind als $r_{j_0 i_0}$. Wir können das Verfahren solange fortsetzen, wie wir auf diese Weise betragskleinere von Null verschiedene Einträge gewinnen können. Wir finden so ein neues Erzeugendensystem a und ein Erzeugendensystem $\{r_j\}$ derart, daß die zugehörige Matrix r der r_{ij} einen Eintrag $r_{j_0 i_0}$ mit folgenden Eigenschaften besitzt:

   a) O.B.d.A. ist $j_0 = i_0 = 1$.

   b) $r_{j_0 i_0}$ ist der einzige Eintrag in seiner Zeile und Spalte, der ungleich Null ist.

   c) $r_{j_0 i_0}$ ist betragsmäßig minimal unter allen von Null verschiedenen Einträgen der Matrix r.

3. In der Situation von 2 können wir annehmen,

$$a = r_{j_0 i_0}$$

befindet sich in der ersten Zeile und ersten Spalte von r. Falls es in r noch einen Eintrag

$$b = r_{ji}$$

gibt, der kein Vielfaches von $r_{j_0 i_0}$ ist, so können wir die erste Spalte von r zur j-ten addieren und anschließend ein Vielfaches der ersten Zeile von der i-ten Zeile abziehen, so daß in der Position (j,i) ein Eintrag entsteht der betragskleiner ist als $r_{j_0 i_0}$ und ungleich Null.

$$\begin{pmatrix} a & \dots & 0 & \dots \\ \dots & \dots & \dots & \dots \\ 0 & \dots & b & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \mapsto \begin{pmatrix} a & \dots & a & \dots \\ \dots & \dots & \dots & \dots \\ 0 & \dots & b & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \mapsto \begin{pmatrix} a & \dots & a & \dots \\ \dots & \dots & \dots & \dots \\ -ga & \dots & b-ga & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

Indem wir wie in 2. fortfahren erreichen wir die dort beschrieben Situation (mit verkleineten $r_{j_0 i_0}$). Durch Wiederholtes Anwenden von 2 und 3 erhalten wir eine Matrix mit

a) einem Eintrag $d_1 := r_{j_0 i_0} \neq 0$ in der Position (1,1)

b) Nullen in allen anderen Positionen der ersten Zeile und ersten Spalte.

c) Einträgen in allen anderen Positionen, die entweder 0 sind oder Vielfache von $d_1 = r_{j_o i_o}$.

4. In der Situation von 3 streichen wir die erste Zeile und erste Spalte und wiederholen das Verfahren mit der verbleibenden Matrix. Wir erhalten nacheinander ganze Zahlen

$$d_1 , d_2 , d_3 , ...$$

mit

$$d_i \mid d_{i+1}$$

wobei alle weiteren Einträge r_{ji} durch alle d_i teilbar sind.

Das Ende des Algorithmus.

Da die Zahl der Spalten von r endlich ist, endet das Verfahren nach endlich vielen, sagen wir s, Schritten mit einem gewissen Erzeugendensystem a und einer Familie von Relationen r_j mit $j \in J$ wobei gilt

$$r_j = \{ r_{ji} \}_{i \in I} \text{ mit } r_{ji} = d_j \delta_{ji} \text{ für } j = 1, ... ,s$$

und die Koordinaten aller weiteren r_j sind sämtlich Null.

$$r = (r_1,...,r_s) = \begin{pmatrix} d_1 & ... & 0 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & ... & d_s & ... & 0 \\ 0 & ... & 0 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & ... & 0 & ... & 0 \end{pmatrix},$$

Beweis der Unabhängigkeit der Elementarteiler von der speziellen Wahl der Zerlegung in eine direkte Summe.

Für

$$A \cong \mathbb{Z} / d_1 \mathbb{Z} \oplus ... \oplus \mathbb{Z} / d_s \mathbb{Z} \oplus \mathbb{Z}^{n-s} \qquad (1)$$

gilt

$$A_{tor} \cong \mathbb{Z} / d_1 \mathbb{Z} \oplus ... \oplus \mathbb{Z} / d_s \mathbb{Z}$$

Auf Grund der Übungsaufgaben sind die Zahlen s und d_i durch die Gruppe A_{tor} und damit durch A eindeutig festgelegt.
Wir haben zu zeigen, daß auch der Rang n-s durch A eindeutig fesgelegt ist. Dazu betrachten wir die Faktorgruppe

$$A/A_{tor} \cong \mathbb{Z}^{n-s}.$$

Dies ist eine endlich erzeugte freie abelsche Gruppe. Wir tensorieren mit $\mathbb{Q}$ über $\mathbb{Z}$ und erhalten

$$(A/A_{tor}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Z}^{n-s} \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q})^{n-s}.$$

Dies ist ein $\mathbb{Q}$-Vektorraum der Dimension n-r, d.h.

$$n-s = \dim_{\mathbb{Q}} (A/A_{tor}) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Die Zahl n-s hängt also nicht von der speziellen Wahl der Zerlegung von A ab, sondern nur von A selbst.

QED.

Bemerkungen

(i) Zum Beweis der Unabhängigkeit des Rangs von A von der Wahl der Zerlegung hätten wir auch mit $\mathbb{Z}/p\mathbb{Z}$ statt mit $\mathbb{Q}$ tensorieren können und hätten dann die folgende Formen für den Rang gefungen.

$$\text{rk } A := \dim_{\mathbb{Q}} (A/A_{tor})\otimes_{\mathbb{Z}}\mathbb{Q} = \dim_{\mathbb{F}_p} (A/A_{tor})\otimes_{\mathbb{Z}}\mathbb{F}_p$$

(i) Für den Rang einer endlich erzeugte abelschen Gruppe A gilt

$$\text{rk } A = \dim_{\mathbb{Q}} A\otimes_{\mathbb{Z}}\mathbb{Q}$$

Beweis von (ii).

Die Multiplikation mit der ganzen Zahl d definiert eine exakte Sequenz

$$0 \longrightarrow \mathbb{Z} \xrightarrow{d} \mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z} \longrightarrow 0.$$

Durch Tensorieren mit $\mathbb{Q}$ über $\mathbb{Z}$ erhalten wir daraus die exakte Sequenz

$$\mathbb{Q} \xrightarrow{d} \mathbb{Q} \xrightarrow{\alpha} (\mathbb{Z}/d\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Q} \longrightarrow 0.$$

Nun ist aber die Multiplikation mit d im $\mathbb{Q}$-Vektorraum $\mathbb{Q}$ ein Isomorphismus, d.h. es gilt

$$(\mathbb{Z}/d\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Q} = \text{Im}(\alpha) = \mathbb{Q}/\text{Ker}(\alpha) = \mathbb{Q}/\text{Im}(\mathbb{Q} \xrightarrow{d} \mathbb{Q}) = \mathbb{Q}/\mathbb{Q} = 0.$$

Durch Tensorieren von (1) mit $\mathbb{Q}$ über $\mathbb{Z}$ erhalten wir damit

$$\begin{aligned} A\otimes_{\mathbb{Z}}\mathbb{Q} &\cong (\mathbb{Z}/d_1\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Q}\oplus\ldots\oplus(\mathbb{Z}/d_s\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Q}\oplus(\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q})^{n-s} \\ &\cong 0 \oplus \ldots \oplus 0 \oplus \mathbb{Q}^{n-s} \\ &\cong \mathbb{Q}^{n-s} \end{aligned}$$

also

$$\dim_{\mathbb{Q}} A = n\text{-}s.$$

QED.

1.6.5 Zerlegung in direkte Summen zyklischer Gruppen von Primzahlpotenzordnung

Sei A eine endlich erzeugte abelsche Gruppe. Dann gibt es (nicht notwendig verschiedene) Primzahlen $p_1,\ldots,p_r$ und natürliche Zahlen $n_1, \ldots, n_r$ und s mit

$$A \cong \mathbb{Z}^s \oplus \oplus_{i=1}^{r} \mathbb{Z}/p_i^{n_i}\mathbb{Z}$$

Beweis. Wir fixieren eine Zerleung

$$A \cong \mathbb{Z}/d_1\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}/d_s\mathbb{Z}\oplus\mathbb{Z}^s \text{ mit } s = \text{rk } A$$

wie in 1.6.4 und schreiben jeden der Elementarteiler $d = d_i$ als Produkt von paarweise teilerfremden Primzahlpotenzen. Nach 1.4.4 läßt sich jede der zyklischen Gruppen

$$\mathbb{Z}/d\mathbb{Z}$$

als direktes Produkt von zyklischen Gruppen von Primzahl-Potenz-Ordnung schreiben.

QED.

Bemerkungen

(i) A ist genau dann endlich, wenn s = 0 ist, und es gilt dann

$$\#A = \prod_{i=1}^{r} p_i^{n_i}$$

(ii) Die Potenzen $p_i^{n_i}$ sind durch die Elementarteiler d_i (bis auf die Reihenfolge) eindeutigbestimmt und damit durch die Gruppe A.

(iii) Umgekehrt sind die d_i durch die Potenzen $p_i^{n_i}$ festgelegt:

d_s ist das Produkt der $p_i^{n_i}$ mit n_i maximal zu gegebenen p_i und

d_{s-1} ist das Produkt der $p_i^{n_i}$ mit n_i maximal nachdem man ein maximales n_i gestrichen hat usw.

Beispiel

Wegen $12 = 2^2 \cdot 3$ sind die nachfolgend aufgezählten Gruppen bis auf Isomorphie die einzigen abelschen Gruppen der Ordnung 12.

$$\mathbb{Z}/(3) \oplus \mathbb{Z}/(2^2), \mathbb{Z}/(3) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2),$$

Im ersten Fall hat man nur einen Elementartteiler

$$d_1 = 3 \cdot 2^2 = 12$$

im zweiten Fall erhält man

$$d_2 = 3 \cdot 2 = 6 \text{ und } d_1 = 2.$$

1.6.6 Untergruppen zu vorgegebener Ordnung

Seien A eine endliche abelsche Gruppe der Ordnung n und m ein Teiler von n. Dann gibt es eine Untergruppe $U \subseteq A$ der Ordnung m von A.

Beweis. Nach 1.6.5 können wir annehmen, es ist

$$A = \oplus_{i=1}^{r} \mathbb{Z}/p_i^{n_i}\mathbb{Z} \text{ mit } n = \prod_{i=1}^{r} p_i^{n_i}.$$

Dann hat m die Gestalt

$$m = \prod_{i=1}^{r} p_i^{m_i} \text{ mit } m_i \leq n_i \text{ für jedes i.}$$

Es reicht deshalb zu zeigen, $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$ hat eine Untergruppe U_i der Ordnung $p_i^{m_i}$ (die direkte Summe der U_i ist dann eine Untergruppe der gesuchten Ordnung). Wir können also annehmen

$$A = \mathbb{Z}/p^a\mathbb{Z}, n = p^a, m = p^b \text{ mit } b \leq a.$$

Dann gilt aber die Behauptung auf Grund von 1.4.2.
QED.

1.6 Sylow-Gruppen

1.6.1 p-Gruppen, p-Untergruppen und Sylow-Untergruppen

Sei p eine Primzahl. Eine p-Gruppe ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist.

Sei G eine Gruppe. Eine p-Untergruppe von G ist eine Untergruppe von G von p-Potenzordnung. Eine p-Sylow-Untergruppe von G ist eine Untergruppe

$$U \subseteq G$$

mit $\# U = p^n$, wobei p^n die höchste Potenz von p ist, die die Ordnung von G teilt,

$$p^n \mid \#G \text{ und } p^{n+1} \ncong \#G.$$

Eine natürliche Zahl $m \in \mathbb{N}$ heißt Exponent der Gruppe G, wenn für jedes $g \in G$ gilt

$$g^m = e.$$

Bemerkungen

(i) Jede endliche Gruppe $G = \{ g_1,...,g_n\}$ (mindestens einen) Exponenten. Jedes Element g_i von G erzeugt nämlich eine zyklische Untergruppe von endlicher Ordnung m_i , und es ist

$$(g_i)^{m_i} = e.$$

Mit $m = m_1 \bullet ... \bullet m_n$ gilt dann aber $g^m = e$ für jedes $g \in G$.

(ii) Wir werden die Existenz der p-Sylow-Untergruppen nachweisen. Zunächst benötigen wir aber eine Beschreibung der Orbits von Gruppenoperationen.

1.6.2 Stabilisatoren und Orbits

Seien

$$G \times M \longrightarrow M, (g,m) \mapsto gm,$$

eine Operation einer Gruppe G auf einer Menge M und $m \in M$ ein Element. Dann ist der Stabilisator

$$G_m = \{ g \in G \mid gm = m \}$$

von m in G eine Untergruppe und die Abbildung

$$\varphi: G/G_m \longrightarrow O(m), g \mapsto gm,$$

ist wohldefiniert und bijektiv.

Beweis. Die Untergruppeneigenschaft des Stabilisators. Es gilt $e \in G_m$. Mit $g', g'' \in G_m$ gilt

$$(g'g'')m = g'(g''m) = g'm = m,$$

also $g'g'' \in G_m$. Mit $g \in G_m$ gilt schließlich $gm = m$, also

$$m = em = (g^{-1}g)m = g^{-1}(gm) = g^{-1}m,$$

also $g^{-1} \in G_m$.

Die Korrektheit der Definition von φ. Sei $g'G_m = g''G_m$. Wir haben zu zeigen

$$g'm = g''m.$$

Wegen $g'G_m = g''G_m$ gilt $g'' \in g'G_m$, d.h.

$$g'' = g's \text{ mit } s \in G_m.$$

Es folgt

$$g''m = (g's)m = g'(sm) = g'm.$$

Bijektivität von φ. Surjektiv ist die Abbildung nach Definition des Orbits. Zeigen wir die Injektivität. Es gelte

$$\varphi(g' G_m) = \varphi(g'' G_m).$$

Dann ist $g'm = g''m$, also

$$(g'^{-1}g'')m = g'^{-1}(g''m) = g'^{-1}(g'm) = (g'^{-1}g')m = em = m,$$

also $g'^{-1}g'' \in G_m$, also $g'' \in g'G_m$, also $g''G_m = g'G_m$.

QED.

1.6.3 Konjugationsklassen

Seien G eine Gruppe und $g \in G$ ein Element. Dann heißt die Menge

$$C(g) := \{x^{-1}gx \mid x \in G\}$$

Konjugationsklasse von g in G. Die Konjugationsklasse heißt trivial, wenn sie aus nur einem Element besteht.

Bemerkungen

(i) Die Konjugationsklassen der Gruppe G sind gerade die Orbit bezüglich der Operation

$$G \times G \longrightarrow G, (x, g) \mapsto xgx^{-1},$$

von G auf sich durch innere Automorphismen.

(ii) Die Konjugationsklasse des Elements $g \in G$ ist genau dann trivial, wenn g im Zentrum

$$C(G) := \{g \in G \mid xg = gx \text{ für } x \in G\}$$

der Gruppe G liegt.

1.6.4 Die Klassenformel

Sei G eine endliche Gruppe mit dem Zentrum

$$C = C(G)$$

und den nicht-trivialen Konjugationsklassen

$$C_1, \ldots, C_r.$$

Dann gilt

$$\#G = \#C + \sum_{i=1}^{r} \#C_i .$$

Außerdem ist die Ordnung jeder Konjugationsklasse ein Teiler der Gruppenordnung,

$$\#C_i \mid \#G.$$

Beweis. Wir betrachten die Operation

$$G \times G \longrightarrow G, (x, g) \mapsto xgx^{-1},$$

von G auf sich durch Konjugation. Seien

$$O_1,\ldots,O_r,\ldots,O_s$$

die Orbits dieser Operation, wobei die ersten r Orbits gerade nicht-trivialen Orbits seien, d.h. diejenigen mit mehr als einem Element. Dann gilt

$$\#G = \sum_{i=1}^{s} \#O_i = \sum_{i=r}^{r} \#O_i + \text{Anzahl der trivialen Orbits.}$$

Nach Bemerkung 1.6.3 (i) sind die nicht-trivialen Orbits aber gerade die nicht-trivialen Konjugationsklassen und nach 1.6.3(ii) ist die Anzahl der trivialen Orbits gerade die Ordnung des Zentrums. Die noch verbleibende Teilbarkeitsaussage ergibt sich aus der Tatsache, daß sich nach 1.6.2 jedes Orbit mit einer Menge der Gestalt

$$G/G_g$$

identifizieren läßt.

QED.

1.6.5 Die Existenz der p-Sylow-Untergruppen

Seien G eine endliche Gruppe und p eine Primzahl, welche die Gruppenordnung teilt,

$$p \mid \#G.$$

Dann besitzt G eine p-Sylow-Untergruppe.

Beweis. Wir führen den Beweis durch Induktion nach der Gruppenordnung $n = \#G$. Im Fall $n = 1$ ist die Aussage trivial. Falls n eine Primzahl ist, ist die Aussage ebenfalls trivial.

Nehmen wir jetzt an, die Aussage gilt für alle Gruppen mit einer Ordnung $< n$.

1. Fall: G enthält eine echte Untergruppe U mit #G/U teilerfremd zu p.

Nach Induktionsvoraussetzung besitzt U eine p-Sylow-Untergruppe. Diese ist aber auch eine p-Sylow-Untergruppe von G, d.h. eine solche existiert.

2. Fall: Jede Untergruppe U von G besitzt einen durch p teilbaren Index,

$$p \mid \#G/U.$$

Seien $C_1,...,C_r$ die nicht-trivialen Konjugationsklassen von G. Dann gilt nach der Klassenformel

$$\# G = \# C + \sum_{i=1}^{r} \# C_i .$$

Für jede Untergruppe U von G ist die Ordnung # G/U ein Vielfaches von p. Insbesondere sind die Ordnungen # G und # C_i Vielfache von p. Dasselbe muß also auch für die Ordnung des Zentrums gelten,

$$p \mid \# C.$$

Insbesondere ist das Zentrum von G nicht trivial (und abelsch). Nach 1.5.6 gibt es eine Untergruppe der Ordnung p in C(G),

$$U \subseteq C(G), \#U = p.$$

Weil U ganz im Zentrum von G liegt, ist U ein Normalteiler. Betrachten wir den natürlichen Homomorphismus

$$h: G \longrightarrow G/U.$$

Sei p^n die höchste p-Potenz, die #G teilt. Dann ist p^{n-1} die höchste p-Potenz, die #G/U teilt. Nach Induktionsvoraussetzung gibt es eine p-Sylow-Untergruppe von G/U,

$$\overline{S} \subseteq G/U, \# \overline{S} = p^{n-1}.$$

Es reicht zu zeigen,

$$S := h^{-1}(\overline{S})$$

ist eine p-Sylow-Untergruppe von G.

Aus der Untergruppeneigenschaft von $\overline{S}$ (und dem Untergruppenkriterium) ergibt sich sofort die Untergruppeneigenschaft von S. Es reicht also zu zeigen,

$$\# S = p^n.$$

Die Einschränkung des natürlichen Homomorphismus h auf S ist nach Definition von S ein surjektiver Homomorphismus

$$h': S \twoheadrightarrow \overline{S}.$$

Nach Definition von S liegt der Kern U von h ganz in S, d.h. es gilt

$$\text{Ker } h' = U.$$

Damit ist nach dem 0-ten Isomorphiesatz

$$p^{n-1} = \# \overline{S} = \# \text{ Im } h' = \# S/\text{Ker } h' = \# S/U = \# S / \#U = \#S / p.$$

Also gilt $\#S = p^n$.
QED.

1.6.6 Eigenschaften von Sylow-Untergruppen

Seien G eine endliche Gruppe und p ein Primteiler der Gruppenordnung. Dann gelten die folgenden Aussagen.

(i) Jede p-Untergruppe von G liegt ganz in einer p-Sylow-Untergruppe.

(ii) Je zwei p-Sylow-Untergruppen S und S' von G sind konjugiert, d.h. es gibt ein $g \in G$ mit $S' = gSg^{-1}$.

(iii) Für die Anzahl n der p-Sylow-Untergruppen von G gilt $n \equiv 1 \pmod{p}$.

Beweis. Bezeichne

$$S$$

die Menge der p-Sylow-Gruppen. Die Gruppe G operiert durch Konjugation auf S,

$$G \times S \longrightarrow S, (g, P) \mapsto gPg^{-1}, \tag{1}$$

denn Konjugation mit $g \in G$ ist ein Isomorphismus von G, d.h. das Konjugierte einer p-Sylow-Gruppe von G ist wieder eine p-Sylow-Untergruppe. Wir fixieren ein Element von S, sagen wir

$$P \in S.$$

Sei

$$G_P = \{ g \in G \mid gPg^{-1} = P \}$$

der Stabilisator von P und

$$O(P) := \{gPg^{-1} \mid g \in G\}$$

das Orbit von P. Dann gilt

$$P \subseteq G_P,$$

d.h. G/G_P läßt sich mit einer Faktorgruppe von G/P identifizieren. Insbesonder ist

$$\# O(P) = \#G/G_P \mid \#G/P .$$

Die Ordnung ganz rechts ist aber teilerfremd zu p (da P eine p-Sylow-Untergruppe ist, d.h.

$$\#O(P) = \#G/G_P \text{ ist teilerfremd zu p.} \tag{2}$$

Die Orbits der Operation (1) besitzen also eine zu p teilerfremde Ordnung.

<u>Zu (i)</u>. Sei U eine p-Untergruppe von G. Wir können annehmen,

$$\#U > 1.$$

Die Untergruppe U operiert durch Konjugation auf dem Orbit von P,

$$U \times O(P) \longrightarrow O(P), (u, gP\, g^{-1}) \mapsto ugPg^{-1}u^{-1} = (ug)P(ug)^{-1}.$$

Für jedes $x \in O(P)$ haben wir eine Bijektion

$$U/U_x \longrightarrow Ux.$$

Da die Ordnung von U eine p-Potenz ist, gilt dasselbe von $\#U/U_x = \#Ux$. Die Ordnungen der Orbits von U auf O(P) sind also p-Potenzen. Wegen (2) sind diese Ordnungen aber nicht alle durch p teilbar, d.h. mindestens ein Orbit hat die 0-te p-Potenz zur Ordnung ,

$$\# Ux = 1 \text{ für mindestens ein } x \in O(P).$$

Sei $x = gPg^{-1} =: P'$ ein solches x. Zum Beweis der Behauptung reicht es zu zeigen, es gilt dann

$$U \subseteq P' \tag{3}$$

Weil das U-Orbit von $x = P'$ aus nur einem Element besteht, gilt
Dann gilt

$$uP'u^{-1} = P' \text{ für jedes } u \in U. \tag{4}$$

also uP' = P'u für jedes u∈U, also

$$UP' = P'U. \tag{5}$$

Insbesondere ist

$$UP' := \{ ug \mid u \in U, g \in P' \}$$

eine Untergruppe von G:

1. $e = ee \in UP'$, d.h. $UP' \neq \emptyset$.

2, Mit ug , u'g'∈UP' gilt

$$ug(u'g')^{-1} = ugg'^{-1}u'^{-1} \in UP'U = UUP' \text{ (wegen (4)} = UP'.$$

Wegen (4) ist P' ein Normalteiler in UP', und es ist

$$UP'/P' \equiv P'/U \bigcap P',$$

d.h. die Faktorgruppe hat p-Potenzordnung. Dann hat aber auch UP' eine p-Potenzordnung. Da P' maximale p-Potenzordnung hat und ganz in UP' liegt, folgt P' = UP',

$$\text{also } U \subseteq P'.$$

Zu (ii). Die obigen Betrachtungen kann man insbesondere für den Fall machen, wenn U eine p-Sylow-Untergruppe ist. Aus der Inklusion $U \subseteq P'$ ergibt sich dann aber, weil U maximale p-Potenzordnung hat,

$$U = P' = gPg^{-1},$$

d.h. U ist konjugiert zu der fest gewählten p-Sylow-Gruppe P.
Zu (iii). Die obigen Betrachtungen gelten auch für den Spezialfall U = P. Insbesondere gibt es ein Orbit von U = P in O(P) mit nur einem Element,

$$Px = \{x\}.$$

Alle anderen Orbits besitzen jedoch mehr als ein Element[7]. Alle anderen Orbits haben also eine durch p teilbare Ordnung. Damit gilt

$$\#\, O(P) \equiv 1 \pmod p.$$

Nach (ii) ist aber O(P) = S die Menge aller p-Sylow-Untergruppen, d.h. es gilt

$$\#\, S \equiv 1 \pmod p.$$

QED.

1.6.7 Beispiel

S_5 ist von der Ordnung $5! = 2^3 \cdot 3 \cdot 5$, besitzt aber keine Untergruppe der Ordnung 15.

Mit anderen Worten, die Umkehrung des Satzes von Lagrange ist im allgemeinen falsch!

Beweis. Sei $H \subseteq S_5$ eine Untergruppe der Ordnung 15. Dann besitzt H Untergruppen H_3 und H_5 der Ordnungen 3 bzw. 5 (die Sylow-Untergruppen).

$$H_3 \subseteq H \,,\, H_5 \subseteq H.$$

Diese Untergruppen sind von Primzahlordnung, also zyklisch. Wir können annehmen,

$$H_5 = <(12345)>$$

und es gilt

$$H_3 = <(abc)>.$$

Der Dreierzyklus entsteht aus (12345) durch Streichen von zwei Elementen. Wir können annehmen, eins der gestrichenen Elemente ist 5, d.h.

---

[7] Nach (3): wir haben in (i) gezeigt, aus # Ux = 1 mit $x = gPg^{-1} = P'$ folgt $U \subseteq P'$ (also U = P').

$$\{a,b,c\} \subseteq \{1,2,3,4\}$$

1. Fall: $4 \notin \{a,b,c\}$
Es gilt (abc) = (123) oder (abc) = (321). Wir annehmen an, (abc) = (123). Der andere Fall wird analog behandelt. Konjugation mit (12345) liefert

$$(234) \in H$$

also liegt (234)(123) = (13)(24) in H, d.h. H enthält ein Element der Ordnung 2, was nicht möglich ist.

Es verbleiben noch die Fälle $3 \notin \{a, b, c\}$, $2 \notin \{a, b, c\}$ unf $1 \notin \{a, b, c\}$. Diese werden in derselben Weise behandelt:

2. Fall: $3 \notin \{a,b,c\}$
Wir können annehmen, (abc) = (124). Konjugation mit (12345) liefert

$$(235), (341) \in H$$

also liegt (124)(134) = (13)(24) in H, d.h. H enthält ein Element der Ordnung 2, was nicht möglich ist.

3. Fall: $2 \notin \{a,b,c\}$

Wir können annehmen, (abc) = (134). Konjugation mit $(12345)^{-1}$ liefert

$$(523), (412) \in H$$

also liegt (124)(134) = (13)(24) in H, d.h. H enthält ein Element der Ordnung 2, was nicht möglich ist.

4. Fall: $1 \notin \{a,b,c\}$

Wir können annehmen, (abc) = (234). Konjugation mit $(12345)^{-1}$ liefert

$$(123) \in H$$

also liegt (234)(123) = (13)(24) in H, d.h. H enthält ein Element der Ordnung 2, was nicht möglich ist.
QED.

1.7 Auflösbare Gruppen

1.7.1 Definitionen

Sei G eine Gruppe. Ein Gruppenturm von G ist eine echt absteigende Folge von Untergruppen,

$$G = G_0 \supset G_1 \supset \ldots \supset G_m .$$

Dabei heißt m Länge des Turms. Eine Verfeinerung eines Gruppenturms ist ein Gruppenturm, der durch Einfügen einer endlichen Anzahl von Untergruppen entsteht zwischen schon vorhandene Gruppen.

Der Turm heißt normal oder auch Normalreihe, wenn G_{i+1} Normalteiler ist in G_i für jedes i. Eine Normalreihe heißt abelsch, wenn G_i/G_{i+1} abelsch ist für jedes i. Sie heißt zyklisch, wenn G_i/G_{i+1} zyklisch ist. Die Gruppen der Gestalt G_i/G_{i+1} heißen Faktoren der Normalreihe.

Eine Kompositionsreihe ist eine Normalreihe, die trivial endet (d.h. $G_m = \{e\}$) und für welche est keine Normalreihe gibt, die eine (echte) Verfeinerung ist.

Eine Gruppe heißt auflösbar, wenn es eine abelsche Normalreihe gibt , die trivial endet.

Eine Gruppe heißt nilpotent, wenn es eine abelsche Normalreihe gibt, die trivial endet und die aus lauter Normalteilern von G besteht.
Seien zwei trivial endende Normalreihen gegeben.

$$G = G_0 \supset G_1 \supset \ldots \supset G_r = \{e\} .$$

$$G = H_0 \supset H_1 \supset \ldots \supset H_s = \{e\}.$$

Diese Normalreihen heißen äquivalent, wenn gilt

1. $r = s$
2. Es gibt eine Permutation $\sigma \in S_{r-1}$ mit

$$G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$$

für $i = 1,\ldots,r-1$.

Eine Gruppe G heißt einfach, wenn sie nicht-trivial ist und außer G und {e} keine Normalteiler besitzt.

Bemerkungen

(i) Seien $h: G \longrightarrow G'$ ein Homomorphismus und

$$G' = G'_0 \supset G'_1 \supset \ldots \supset G'_m$$

eine Normalreihe von G'. Dann ist

$$G_0 \supset G_1 \supset \ldots \supset G_m$$

mit $G_i := h^{-1}(G_i)$ eine Normalreihe von G. Ist die urprüngliche Reihe abelsch oder zyklisch, so gilt dasselbe auch für die neue Reihe.

(ii) Jede abelsche Normalreihe einer endlichen Gruppe besitzt eine zyklische Verfeinerung.

Beweis. Zu (i). Die Abbildung

$$\varphi: G_i \longrightarrow G'_i/G'_{i+1} \text{ , } g \mapsto h(g) \bmod G'_{i+1} ,$$

ist ein Gruppenhomomorphismus mit

$$g \in \operatorname{Ker} \varphi \Leftrightarrow h(g) \in G'_{i+1} \Leftrightarrow g \in h^{-1}(G'_{i+1}) \Leftrightarrow g \in G_{i+1} ,$$

d.h. es gilt $\operatorname{Ker} \varphi = G_{i+1}$. Nach dem 0-ten Isomorphiesatz gilt

$$G_i/G_{i+1} = G_i/\operatorname{Ker} \varphi \cong \operatorname{Im} \varphi \subseteq G'_i/G'_{i+1} .$$

Mit der Faktorgruppe rechts ist also auch die Faktorgruppe links abelsch bzw. zyklisch.
Zu (ii): Sei

$$G = G_0 \supset G_1 \supset \ldots \supset G_m$$

eine abelsche Normalreihe. Es reicht für fest vorgegebenes i zu zeigen, zwischen G_i und G_{i+1} gibt es Untergruppen H_j, sagen wir

(1) $$G_i = H_1 \supset \ldots \supset H_{n+1} = G_{i+1}$$

mit H_j/H_{j+1} zylisch für jedes j. Es reicht deshalb, die Normalreihe

$$G_i \supset G_{i+1}$$

zu betrachten. O.B.d.A sei also

$$m = 1.$$

Betrachten den natürlichen Homomorphismus

$$\rho: G \longrightarrow G/G_1 =: \overline{G}.$$

Zum Beweis der Behauptung reicht es, die folgenden beiden Aussagen zu beweisen.

1. Besitzt $\overline{G}$ eine zyklische Verfeinerung, so auch G.
2. $\overline{G}$ besitzt eine zyklische Verfeinerung.

Aussage 1 ist eine direkte Konsequenz von (i). Beweisen wir Aussage 2. Nach Konstruktion ist $\overline{G}$ abelsch, also ein endlich abelsche Gruppe, also direkte Summe endlich vieler endlicher zyklischer Gruppen, sagen wir

$$\overline{G} = \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_r}.$$

Betrachten wir die Untergruppen

$$\overline{G}_i := \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_i}$$

von $\overline{G}$. Es gilt

$$\overline{G} = \overline{G}_r \supset \overline{G}_{r-1} \supset ... \supset \overline{G}_1 \supset \overline{G}_0 = \{0\} \qquad (1)$$

und

$$\overline{G}_{i+1}/\overline{G}_i \cong \mathbb{Z}_{d_{i+1}},$$

d.h. (1) ist die gesuchte Verfeinerung.

QED.

1.7.2 Nilpotenz der p-Gruppen

Sei G eine endliche p-Gruppe. Dann ist G nilpoten (also insbesondere auch auflösbar). Falls G nicht-trivial ist, so hat G ein nicht-triviales Zentrum.

Beweis. 1. Schritt. Falls $G \neq \{e\}$ ist, ist auch $C:=C(G) \neq \{e\}$.
Wir lassen G durch Konjugation auf sich selbst operieren,

$$G \times G \longrightarrow G,\ (g,x) \mapsto gxg^{-1}$$

und schreiben G als disjunkte Vereinigung von Orbits,

(1) $$G = O(g_1) \bigcup ... \bigcup O(g_r) \text{ (disjunkte Vereinigung).}$$

Nach 1.6.2 gilt

(2) $$\#O(g_i) = [G/G_{g_i}] = \text{Teiler von } \#G = \text{p-Potenz.}$$

Wegen (1) ist die Summe dieser p-Potenzen gleich #G, also durch p teilbar,

(3) $$p \mid \sum_{i=1}^{r} \#O(g_i)$$

Ist $O(g_i)$ das Orbit des neutralen Elements, so gilt

$$\#O(g_i) = \#O(e) = \#\{geg^{-1} \mid g \in G\} = \#\{e\} = 1.$$

Es gibt also mindestens einen Summanden auf der rechten Seite von (3), der nicht durch p teilbar ist. Dann muß es aber noch einen weiteren Summanden geben, der ebenfalls nicht durch p teilbar ist. Wegen (2) ist dieser Summand gleich 1. Es gibt also ein $g \in G$ mit

$$1 = \#O(g) = \#\{xgx^{-1} \mid x \in G\},\ g \neq e,$$

d.h. es ist

$$xgx^{-1} = x \text{ für jedes } x \in G \text{ und } g \neq e,$$

d.h.

$$e \neq g \in C(G).$$

Mit anderen Worten, das Zentrum von G ist nicht trivial.

2. Schritt. Auflösbarkeit von G.
Wir führen den Beweis durch Induktion nach der Gruppenordnung

$$n = \# G.$$

Im Fall n = 1 ist die Aussage trivial. Sei also n > 1. Nach dem ersten Schritt ist das Zentrum

$$C := C(G)$$

eine nicht-triviale (abelsche) Untergruppe von G,

$$\# C > 1.$$

Auf Grund der Defintion von C ist C sogar ein Normalteiler von G, d.h.

$$G/C$$

ist eine Gruppe der Ordnung

$$\#G/C = \#G / \#C < n.$$

Insbesondere ist die Ordnung von C ein Teiler der Ordnung von G, also eine p-Potenz. Nach Induktionsvoraussetzung gibt es eine abelsche Normalreihe von G/C, die trivial endet,

$$G/C = \overline{G}_0 \supset \overline{G}_1 \supset \ldots \supset \overline{G}_m = \{ \overline{e} \}$$

und die aus lauter Normalteilern von G/C besteht.
Bezeichne

$$\rho: G \longrightarrow G/C$$

den natürlichen Homomorphismus und sei

$$G_i = \rho^{-1}(\overline{G}_i).$$

das Urbild des Normalteilers $\overline{G}_i$. Man beachte, G_i ist ein Normalteiler von G.

Dann ist

$$G = G_0 \supset G_1 \supset \ldots \supset G_m \ (= C) \supset \{e\}$$

eine abelsche Normalreihe von G, die trivial endet (nach Bemerkung (i) von 1.7.1 und wegen $C/\{e\} \cong C$ abelsch).
QED.

1.7.3 Das Schmetterlingslemma (von O. Schreier)

Seien G eine Gruppe,

$$U, V \subseteq G$$

zwei Untergruppen von G und

$$u \subseteq U \text{ und } v \subseteq V$$

Normalteiler in U bzw. V. Dann gelten die folgenden Aussagen.

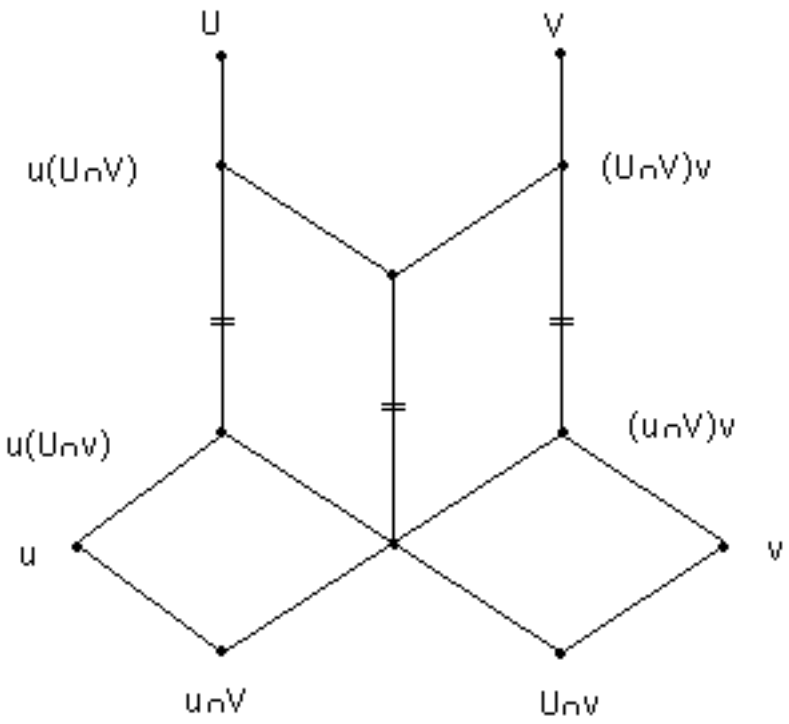
(i) $u(U \cap v)$ ist Normalteiler in $u(U \cap V)$.

(ii) $(u \cap V)v$ ist Normalteiler in $(U \cap V)v$

(iii) Die zu (i) und (ii) gehörigen Faktorgruppen sind isomorph:

$$u(U \cap V)/\ u(U \cap v) \cong (U \cap V)v/(u \cap V)v.$$

Die in der Formulierung des Lemmas auftretenden Gruppen und Faktorgruppen lassen sich durch die folgende Skitze illustrieren, von der das Lemma seinen Namen hat.


U
V
u(U∩V)
(U∩V)v
u(U∩v)
(u∩V)v
u
v
u∩V
U∩v

Beweis (nach Zassenhaus). Wir beschränken uns auf eine Beweisskitze. In der obigen Zeichnung sind U, V, u, v vorgegeben. Die gekennzeichneten Ecken sollen für die angegebenen Untergruppen stehen.

Die übrigen Ecken stehen für Untergruppen, welche durch die folgenden beiden (generell geltenden) Regeln definiert sind.

Der Schnitt von zwei Kanten, die nach unten verlaufen steht für den Durchschnitt der beiden Gruppen an deren oberen Ende.

Der Schnitt zweier Kanten, die nach oben verlaufen steht für das Produkt der beiden Gruppen an deren untern Ende (d.h. für die kleinste Untergruppe, die beide enthält).

Betrachten wir die beiden oberen Parallelogramme, die die Flügel des Schmetterlings bilden. Wir wollen zeigen, gegenüberliegende Seiten der Parallelogramme stehen für isomorphe Faktorgruppen.

Dazu bestimmen wir zunächst die Untergruppen, welche zum oberen und unteren Punkt in der Mitte des Diagramms gehören.

1 Der obere Punkt in der Mitte gehört zum Durchschnitt $U \bigcap V$.

Wegen $u(U \bigcap V) \subseteq U$ und $(U \bigcap V)v \subseteq V$ gilt einerseits

$$u(U \bigcap V) \ \bigcap \ (U \bigcap V)v \ \subseteq \ U \bigcap V$$

Andererseits ist $U \bigcap V \subseteq u(U \bigcap V)$ und $U \bigcap V \subseteq (U \bigcap V)v$, also auch

$$U \bigcap V \subseteq u(U \bigcap V) \ \bigcap \ (U \bigcap V)v.$$

2. Der untere Punkt in der Mitte gehört zum Produkt $(u \bigcap V)(U \bigcap v)$.

Wegen $(u \bigcap V)(U \bigcap v) \subseteq u(U \bigcap v)$ und $(u \bigcap V)(U \bigcap v) \subseteq (u \bigcap V)v$ gilt einerseits

$$(u \bigcap V)(U \bigcap v) \subseteq u(U \bigcap v) \ \bigcap \ (u \bigcap V)v. \qquad (1)$$

Sei andererseits x ein Element aus dem Durchschnitt aus der rechten Seite. Dann läßt sich x ín der folgenden Gestalt schreiben.

$x = x_u \bullet y$ mit $x_u \in u$ und $y \in U \bigcap v$

$x = z \bullet x_v$ mit $z \in u \bigcap V$ und $x_v \in v$.

Es folgt $x_v = z^{-1} x_u \bullet y \in u \bullet U \bigcap v$ und $x_v \in v$ also

$$x_v \in (u \bullet U \bigcap v) \bigcap v \subseteq U \bigcap v.$$

Zusammen folgt

$$x = z \bullet x_v \in (u \bigcap V)(U \bigcap v).$$

Damit besteht auch die zu (1) umgekehrte Inklusion.

$$u(U \bigcap v) \bigcap (u \bigcap V)v \subseteq u(U \bigcap v) \bigcap uv \subseteq u(U \bigcap V)$$

3. Bestimmung des Faktors zur Strecke in der Mitte.

Wir setzen

$$H := U \bigcap V \text{ und } N := u(U \bigcap v)$$

Dann gilt

$$H \bigcap N = (U \bigcap V) \bigcap u(U \bigcap v) = (U \bigcap V \bigcap u)(U \bigcap v) = (u \bigcap V)(U \bigcap v) \qquad (2)$$

und

$$NH = u(U \bigcap v)(U \bigcap V) = u(U \bigcap V) \qquad (3)$$

Weil u Normalteiler in U ist, operiert U durch Konjugation auf u. Dann operiert aber auch $U \bigcap V$ durch Konjugation auf u. Insbesondere gilt

$$x \bullet u = u \bullet x \text{ für } x \in U \bigcap V \qquad (4)$$

und

$$u(U \bigcap V) = (U \bigcap V)u,\ u(U \bigcap v) = (U \bigcap v)u$$

und diese Produkte sind Untergruppen von G.

Weil v ein Normalteiler von V ist, operiert V durch Konjugation auf v. Also operiert $U \bigcap V$ auf $U \bigcap v$ durch Konjugation. Es folgt

$$x \bullet U \bigcap v = U \bigcap v \bullet x \text{ für } x \in U \bigcap V.$$

Zusammen mit (4) erhalten wir

$$x \bullet u(U \bigcap v) = u(U \bigcap v) \bullet x \text{ für } x \in U \bigcap V.$$

d.h. $U\bigcap V$ operiert auf $u(U\bigcap v)$ durch Konjugation. Weiter gilt für $x \in u$

$$x \bullet u(U\bigcap v) = u(U\bigcap v) = (U\bigcap v)u = (U\bigcap v)u \bullet x,$$

d.h. auch u operiert durch Konjugation auf $u(U\bigcap V)$. Zusammen erhalten wir, daß $u(U\bigcap V)$ auf $u(U\bigcap v)$ durch Konjugation operiert. Damit ist Aussage (i) der Behauptung bewiesen. Aus Symmetriegründen folgt Aussage (ii).

Nach dem ersten Isomorphiesatz gilt

$$H/H\bigcap N \cong HN/N$$

und insbesondere ist N ein Normalteiler in HN. Es folgt HN = NH und der Isomorphiesatz bekommt wegen (2) und (3) die Gestalt

$$U\bigcap V/ (u\bigcap V)(U\bigcap v) \cong u(U\bigcap V)/u(U\bigcap v)$$

Der Faktor zur Kante in der Mitte des Schmetterling ist somit isomoph zum Faktor der Kante links. Aus Symmetriegründen gilt dasselbe bezüglich der Kante rechts.

Damit ist der Faktor zur linken Kante isomorph zum Faktor der rechten Kante, d.h. es gilt die Behauptung.

QED.

1.7.4 Satz von Schreier

Sei G eine Gruppe. Dann lassen sich je zwei Normalreihen von G, die trivial enden, so verfeinern, daß die entstehenden Normalreihen äquivalent sind.

Beweis. Seien zwei Normalreihen der beschriebenen Art gegeben, sagen wir

$$G = G_0 \supset G_1 \supset \ldots \supset G_r = \{e\} .$$

$$G = H_0 \supset H_1 \supset \ldots \supset H_s = \{e\}.$$

Vorbemerkung

Bei den zu konstruierenden Verfeinerungen können wir zulassen, daß benachbarte Gruppen nicht notwendig verschieden sind. Auf Grund der paarweise isomorphen Faktoren hat die Gültigkeit des Gleichheitszeichens in der einen Reihe die eines Gleichheitszeichens in der anderen zur Folge. Wenn wir also in der einen Reihe eine Gruppe weglassen können, so gilt dasselbe in der anderen. Nach dem Weglassen doppelt auftretender Untergruppen sind die konstruierten Reihen weiter äquivalent.

Wir setzen für i = 1,...,r-1 und j = 1,..., s-1

$$G_{ij} := G_{i+1}(H_j\bigcap G_i).$$

Dann gilt

$$G_{i0} = G_i \, , G_{ij} \supseteq G_{ij+1} \, , G_{is} = G_{i+1}$$

und wir erhalten die folgende Verfeinerung des ersten Gruppenturms,

$$... \supseteq G_{i-1,s} (= G_i) = G_{i0} \supseteq G_{i2} \supseteq ... \supseteq G_{is} (= G_{i+1}) = G_{i+1,0} \supseteq ...$$

Analog setzen wir

$$H_{ji} := H_{j+1}(G_i \cap H_j)$$

und erhalten so eine Verfeinerung des zweiten Gruppenturms. Jede der beiden Verfeinerungen besteht aus (r+1)(s+1) Gruppen. Auf Grund des Schmetterlingslemmas bestehen die Isomorphismen

$$G_{ij}/G_{i,j+1} \cong H_{ji}/H_{j,i+1},$$

d.h. die beiden verfeinerten Normalreihen sind äquivalent.
QED.

1.7.5 Satz von Jordan-Hölder

Sei G eine Gruppe. Dann sind je zwei Kompositionsreihen von G, d.h. je zwei Normalreihen, welche trivial enden und einfache Faktoren haben,

$$G = G_0 \supset G_1 \supset ... \supset G_m = \{e\}, G_i/G_{i+1} \text{ einfach},$$

äquivalent.
Beweis. Wegen der Einfachheit der Faktoren besitzen die Normalreihen keine Verfeinerungen, die von den Ausgangsreihen verschieden sind. Nach dem Satz von Schreier besitzen sie aber äquivalente Verfeinerungen. Also sind sie selbst schon äquivalent.
QED.

1.7.6 Beispiel: die Kompositionsreihen von S_4

Die Gruppen in der Reihe

$$S_4 \supset A_4 \supset V_4 \supset U \supset \{(1)\} \qquad (1)$$

mit U := { (1), (12)(34) } haben die Ordnungen 24, 12, 4, 2 und 1, die sykzessiven Faktoren haben also die Ordnungen

$$2, 3, 2, 2,$$

d.h. sie haben Primzahlordnungen, sind also zyklisch.
Die Reihe ist eine Normalreihe:
A_4 hat den Index 2 in S_4, ist also Normalteiler.
V_4 enthält alle Doppel-Zweier-Zyklen von S_4, ist also Normalteiler in S_4, also erst recht in A_4.
Da V_4 abelsch ist, sind alle Untergruppen Normalteiler.

Insbesondere sehen wir, S_4 ist auflösbar.

Bemerkungen

(i) Da alle Faktoren von (1) zyklisch sind, ist (1) eine Kompositionsreihe von S_4.

(ii) Wir schreiben $V_4 = \{1, a, b, c\}$. Ersetzt man in (1) die Untergruppe U durch eine der Gruppen

$$U = \{1, a\}, U = \{1, b\}, U = \{1, c\}$$

weitere Kompositionsreihen von S_4.

(iii) Es gibt keine weiteren Kompositionsreihen von S_4.

Beweis von (iii).

Nach dem Satz von Jordan-Hölder sind die Faktoren jeder Normalreihe von S_4 mit einfachen Faktoren zyklisch von der Ordnung 2 oder 3. Es ist nicht schwer, zu zeigen, die Untergruppen von S_4 sind gerade die in 1.25 angebenen.

Der einzige Normalteiler N vom Index 2 in S_4 ist A_4. Es gilt

$$\#N = \#A_4 / 2 = 12 = 2^2 \cdot 3$$

enthält N eine 3-Sylow-Untergruppe, welche die Ordnung 3 besitzt und insbesondere zyklisch ist. Die einzigen Elemente der Ordnung 3 von S_4 sind die Dreierzyklen, d.h. U enthälten einen Dreierzyklus. Als Normalteiler enthält damit N alle 8 Dreierzyklen und damit 8 gerade Permutationen.
Wäre $N \neq A_4$, so enthielte N eine ungerade Permutation σ und die Abbildung

$$N \longrightarrow N, x \mapsto \sigma x,$$

wäre eine Bijektion, die gerade in ungerade und ungerade in gerade Permutionen überführt, Insbesondere enthielte N genau 12/2 = 6 gerade und 6 ungerade Permutationen, was nicht der Fall ist.

S_4 besitzt keine Normalteiler N vom Index 3. Angenommen doch. Dann gilt

$$\#N = \# A_4 / 3 = 8,$$

d.h. N ist eine 2-Sylow-Untergruppe. Die Zahl der Sylow-Untergruppen ist aber 3 (jede wird von V_4 und einer zyklischen Gruppe der Ordnung 4 erzeugt). Je zwei 2-Sylow-Untergruppen sind aber konjugiert, also keine Normalteiler.

Wir haben damit gezeigt, jede Normalreihe von S_4 mit einfachen Faktoren beginnt wie folgt.

$$S_4 \supset A_4.$$

Die nächste Untergruppe hat den Index 2 oder 3 in A_4, also die Ordnung 6 oder 4.

Der einzige Normalteiler N vom Index 3 in A_4 ist V_4. Es gilt

$$\#N = \#A_4/3 = 12/3 = 4.$$

Insbesondere ist N eine 2-Sylow-Untergruppe von A_4. Das gilt insbesondere für $N=V_4$, d.h. N ist konjugiert zu V_4. Weil V_4 Normalteiler ist, folgt $N = V_4$.
A_4 besitzt keine Normalteiler N vom Index 2. Angenommen doch. Dann gilt

$$\#N = 12/2 = 6.$$

Insbesondere besitzt N Sylow-Untergruppen der Ordnungen 2 und 3, und enthält somit einen Zweier-Zyklus und einen Dreier-Zyklus. Durch geeignete Wahl der Bezeichnungen können wir annehmen

$$(123) \in N,$$

Durch Konjugation mit $(12)(34) \in A_4$ ergibt sich

$$(124) \in N.$$

Damit enthält N alle Dreierzyklen der Gestalt (12k). Da diese A_4 erzeugen, folgt $N=A_4$ im Widerspruch zu #N = 6.

Damit haben wir gezeigt, jede Kompositionsreihe von S_4 hat die Gestalt

$$S_4 \supset A_4 \supset V_4 \supset U \supset \{e\}$$

mit einer Untergruppe U der Ordnung 2 von $V_4 = \{ e, a, b, c\}$. Für U gibt es die folgenden Möglichkeiten.

$$U = \langle a \rangle , U = \langle b \rangle, U = \langle c \rangle.$$

Es gibt also insgesamt drei Normalreihen von S_4 mit einfachen Faktoren.

1.7.7 Beispiel: A_n ist einfach für $n \geq 5$

Die alternierende Gruppe A_n ist für $n \geq 5$ einfach. Insbesondere ist

$$S_n \supset A_n \supset \{e\} \quad (n \geq 5)$$

die einzige Normalreihe mit einfachen Faktoren. Die Gruppen S_n und A_n sind für $n \geq 5$ nicht auflösbar.

Beweis. Es reicht, die Einfachheit von A_n zu beweisen. Jede Normalreihe mit einfachen Faktoren beginnt dann nämlich wie folgt

$$S_n \supseteq N$$

mit einem Normalteiler N der Ordung 12 oder 2. Die Untergruppen der Ordnung 2 werden von einem Zweierzyklus und der identischen Abbildung gebildet und sind keine Normalteiler. Wäre N ein von A_n verschiedenener Normalteiler der Ordnung 12, so enthielte N mindestens eine ungerade Permutation. Multiplikation mit dieser überführt gerade Permutationen in ungerade und ungerade in gerade. Also besteht N zu Hälfte aus geraden und zur anderen Hälfte aus ungerade Permutationen, d.h.

$$A_n \bigcap N$$

wäre eine Untergruppe aus n!/4 Elementen und es wäre ein Normalteiler von A_n im Widerspruch zur Einfachheit von A_n.

Beweis der Einfachheit von A_n.

1. Schritt. Wenn ein Normalteiler N von A_n (n>2) einen Dreizyklus enthält, so gilt $N = A_n$.

Wir können ohne Beschränkung der Allgemeinheit annehmen $(123) \in N$. Dann gilt auch

$$(321) = (123)^2 \in N$$

und

$$\sigma \bullet (321) \bullet \sigma^{-1} \in N \text{ für jedes } \sigma \in A_n .$$

Für $\sigma = (12)(3k)$ erhalten wir

$$(12k) \in N$$

(mit $k > 3$ beliebig). Die Zyklen der Gestalt (12k) erzeugen aber A_n, d.h. es gilt $N = A_n$.

2. Schritt. Abschluß des Beweises.

Angenommen, es gibt einen von {e} und A_n verschiedenen Normalteiler A_n. Wir haben zu zeigen, dies ist nicht möglich. Angenommen doch. Wir wählen dann ein

$$\tau \in N - \{e\},$$

und zwar derart, daß τ eine maximale Anzahl von Elementen von $[1,n] := \{1,2,...,n\}$ in sich abbildet.

1. Fall. τ bildet genau vier Elemente [1,n] nicht in sich ab.
Wir können o.B.d.A. annehmen, die Elemente, die von τ nicht festgelassen werden, sind gerade 1, 2, 3 und 4, d.h.

$$\tau \in S_4.$$

Die einzigen geraden Permutationen von S_4, die kein Element von S_4 fest lassen sind aber die Doppel-Zweier-Zyklen (vgl. Beispiel 1.2.5)[8]. Durch geeignete Wahl der Bezeichnung können wir erreichen,

$$\tau = (12)(34).$$

Wegen $n \geq 5$ können wir τ mit (345) konjugieren und erhalten

$$\tau' = (12)(45) \in N,$$

also

$$N \ni \tau\tau' = (345).$$

Das steht aber im Widerspruch zu der Annahme des hier behandelten ersten Falls, daß jedes Element von N mindestens 4 Elemente nicht fest läßt.
2. Fall. τ bildet mehr als vier Elemente [1,n] nicht in sich ab.
Wir schreiben τ als Produkt von elementfremden Zyklen, wobei wir mit dem längsten Zyklus anfangen. Durch geeignete Wahl der Bezeichnungen erreichen wir,
(a) $\tau = (1234...)...$
oder, wenn der längste Zyklus ein Dreierzyklus ist,
(b) $\tau = (123)(456)...$
(c) $\tau = (123)(45)...$
oder, wenn nur Zweierzyklen vorkommen,
(d) $\tau = (12)(34)(56)...$
Wir konjugieren τ mit $\sigma = (234)$ und erhalten in den beschriebenen drei Fällen

(a) $\tau' = (1342...)... \in N$

(b) $\tau' = (134)(256)... \in N$

(c) $\tau' = (134)(25)... \in N$

(d) $\tau' = (13)(42)(56)... \in N.$

In allen drei Fällen gilt $\tau \neq \tau'$, also

$$\tau^{-1}\tau' \neq (1).$$

Im ersten und im letzten Fall gilt

$$\tau'(k) = \tau(k) \text{ für jedes } k > 4$$

also $\tau^{-1}\tau'(k) = k$ für jedes $k > 4$, d.h. $\tau^{-1}\tau'$ läßt genau 4 Elemente nicht fest, was nach dem 1. Fall nicht möglich ist. Verbleiben die Fälle (b) und (c). Es gilt

$$\tau^{-1}\tau' = (321)(654)(134)(256) = (12436) \text{ im Fall (b)}$$

$$\tau^{-1}\tau' = (321)(54)(134)(25) = (12435) \text{ im Fall (c).}$$

Da aber, wie eben gesehen, der Fall (a) nicht möglich ist, sind auch diese beiden Fällen nicht möglich.

3. Fall. τ bildet höchsten drei Elemente nicht in sich ab.
Dann muß τ aber genau drei Elemente nicht in sich abbilden, denn $\tau \neq (1)$ und τ kann als gerade Permutation kein Zweierzyklus sein. Also ist τ ein Dreierzyklus. Nach dem ersten Schritt gilt dann aber $N = A_n$.

QED.

---

[8] A_4 besteht aus den 3 Doppel-Zweier-Zyklen, allen 8 Dreierzyklen und (1).

2. Ringe

2.1 Definitionen und Beispiele

2.1.1 Definitionen

Ein Ring ist eine Menge R zusammen mit zwei Abbildungen

$$+: R \times R \longrightarrow R, (r,s) \mapsto r+s,$$

$$\bullet: R \times R \longrightarrow R, (r,s) \mapsto rs,$$

genannt Addition und Multiplikation von R, wobei die folgenden Bedingungen erfüllt sind.

(i) R ist mit der Operation eine + eine abelsche Gruppe.

(ii) Die Multiplikation ist assoziativ, d.h.

$$a(bc) = (ab)c \text{ für } a,b,c \in R.$$

(iii) Es gelten die Distributivgesetze, d.h.

$$a(b+c) = ab + ac \text{ und } (a+b)c = ac + bc \text{ für } a,b,c \in R.$$

Ein Ring-Homomorphismus ist eine Abbildung

$$h: R \longrightarrow R'$$

eines Rings R in einen Ring R', welche die Addition und die Multiplikation von respektiert, d.h.

$$h(a+b) = h(a) + h(b) \text{ und } h(ab) = h(a)h(b) \text{ für } a,b \in R.$$

Im Fall R'=R sagt man auch, h ist ein Ring-Endomorphismus.
Ein Ring-Isomorphismus ist ein bijektiver Ring-Homomorphismus (dessen Umkehrung dann automatisch auch ein Ring-Homomorphismus ist). Im Fall R' = R spricht man auch von einem Ring-Automorphismus.
Der Ring heißt kommutativ, wenn gilt

$$ab = ba \text{ für beliebige } a,b \in R.$$

Ein Element e eines Rings R heißt Einselement oder einfach nur Eins und wird mit

$$e = 1$$

bezeichnet, wenn gilt

$$1 \bullet r = r \bullet 1 = r \text{ für jedes } r \in R.$$

Ein Ring mit Einselement (oder auch Ring mit 1) ist ein Ring R, welcher ein Einselement besitzt.

Ein Homomorphismus von Ringen mit 1 ist ein Ring-Homomorphismus

$$h: R \longrightarrow R',$$

wobei R und R' Ringe mit 1 sind, für welchen zusätzlich gilt

$$h(1) = 1',$$

wenn 1 und 1' die Einselemente von R bzw. R' bezeichnen. Man sagt in dieser Situation auch, R' ist eine R-Algebra. (mit dem Struktur-Homomorphismus h).
Analog werden die Begriffe Isomorphismus, Endomorphismus und Automorphismus von Ringen mit 1 definiert.

Sei R ein Ring mit 1. Eine Einheit ist ein Element $e \in R$, für welches es ein Element $e' \in R$ gibt mit

$$ee' = e'e = 1.$$

Das Element e' heißt dann zu e inverses Element.

Sei R ein Ring. Ein Element $n \in R-\{0\}$ heißt Linksnullteiler, falls es ein $n' \in R - \{0\}$ gibt mit

$$nn' = 0$$

und es heißt Rechtsnullteiler, falls es ein $n' \in R - \{0\}$ gibt mit

$$n'n = 0.$$

Ein Element heißt Nullteiler, falls es Linksnullteiler oder Rechtsnullteiler ist. Ein Ring R heißt nullteilerfrei, falls es in R keine Nullteiler gibt.
Ein Integritätsbereich ist ein kommutativer und nullteilerfreier Ring mit 1. Ein Körper ist ein kommutativer Ring mit 1, indem jedes von 0 verschiedene Element eine Einheit ist.

Sei R ein Ring. Ein Teilring von R ist eine nicht-leere Teilmenge von R, die mit den Operationen von R ein Ring ist.

Bemerkungen

(i) Sind 1 und 1' Einselemente von R, so gilt

$$1 = 1 \cdot 1' = 1'.$$

(ii) Sind e' und e" zu e inverse Elemente, so gilt

$$e' = e' \cdot 1 = e'ee" = 1 \cdot e" = e".$$

(iii) Falls es zu $e \in R$ ein Linksinverse e' und ein Rechtsinverses e" gibt, d.h.

$$e'e = 1 = ee",$$

so gilt (auf Grund der Rechnung von (ii)) e' = e", d.h. e' = e" invers zu e.

2.1.2 Beispiele für Integritätsbereiche

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ und $\mathbb{H}$ sind Integritätsbereiche.

Jeder Körper ist ein Integritätsbereich.

2.1.3 Matrizenalgebren

Für jeden Ring R (mit 1) ist die Menge

$$M_n(R) = R^{n \times n}$$

der n×n-Matrizen mit Einträgen aus R ein Ring (mit 1) bezüglich der gewöhnlichen Addition und Multiplikation von Matrizen. Im Fall $n > 1$ ist dieser Ring nicht kommutativ und besitzt sowohl Links- als auch Rechtnullteiler.

Durch die Abbildung

$$R \longrightarrow M_n(R), r \mapsto r \cdot Id,$$

welche jedes Element von R in die zugehörige Skalar-Matrix von $M_n(R)$ abbildet, ist $M_n(R)$ eine R-Algebra.

2.1.4 Polynomalgebren

Sei R ein Ring mit 1. Dann ist die Menge

$$R[x] := \{ r_0 + r_1 x^2 + \ldots + r_n x^n \mid r_0, r_1, \ldots, r_n \in R, n = 0,1,2,\ldots \}$$

$$= \{ \sum_{i=0}^{\infty} r_i x^i \mid r_i \in R, \text{ fast alle } r_i = 0 \}$$

der Polynome in der Unbestimmten x mit Koeffizienten aus R mit den folgenden Operationen ein Ring mit 1.

$$\sum_{i=0}^{\infty} r_i x^i + \sum_{i=0}^{\infty} s_i x^i := \sum_{i=0}^{\infty} (r_i + s_i) x^i$$

$$(\sum_{i=0}^{\infty} r_i x^i)\bullet(\sum_{i=0}^{\infty} s_i x^i) := \sum_{i=0}^{\infty}(\sum_{j+k=i} r_j s_k)x^i.$$

Man sagt auch R[x] entsteht aus R durch Adjunktion der Unbestimmten x.

Bemerkungen

(i) Die r_i heißen Koeffizienten und r_0 heißt Absolutglied des Polynoms

$$f(x) = \sum_{i=0}^{\infty} r_i x^i.$$

Im Fall $f \neq 0$ heißt der Index des höchsten von Null verschiedenen Koeffizienten Grad von f und wird mit

$$\deg \sum_{i=0}^{\infty} r_i x^i = \max \{ i \mid r_i \neq 0 \}$$

bezeichnet. Der Grad von $f = 0$ ist nach Vereinbarung 0.

(ii) Zwei Polynome sind genau dann gleich, wenn alle einander entsprechenden Koeffizienten gleich sind. Man kann deshalb R[x] mit der Menge der Familien

$$\{r_i\}_{i=0}^{\infty} \text{ mit } r_i \in R \text{ und } r_i = 0 \text{ für fast alle i}$$

identifizieren. Als R-Modul ist R[x] eine direkte Summe von Exemplaren von R.

(iii) R[x] ist genau dann kommutativ, wenn R kommutativ ist.

(iv) Sei $f(x) = r_0 + r_1 x^2 + ... + r_n x^n$ ein Polynom des Grades n. Dann heißt

$$\ell(f) := r_n$$

höchster Koeffizient von f. Es gilt

$$\ell(f) = 0 \Leftrightarrow f = 0.$$

Falls R ein Integritätsbereich ist, gilt außerdem für je zwei Polynom f und g,

$$\ell(fg) = \ell(f)\bullet\ell(g).$$

Ist R ein Integritätsbereich, so gilt dasselbe für R[x], denn aus $f \neq 0$ und $g \neq 0$ folgt $\ell(f) \neq 0$ und $\ell(g) \neq 0$, also $0 \neq \ell(f)\,\ell(g) = \ell(fg)$, also $fg \neq 0$.

(v) Die Abbildung

$$R \longrightarrow R[x],\ r \mapsto r := r\bullet x^0,$$

die jedem Element r von R das Polynom des Grades 0 mit dem Absolutglied r zuordnet, ist ein injektiver Ringhomomorphismus. Der Polynomring R[x] ist auf diese Weise eine Algebra über R. Wegen der Injektivität des Struktur-Homomorphismus kann man R mit dem Teilring der Polynome des Grades 0 identifizieren.

(vi) Durch wiederholtes Adjungieren von Unbestimmten, sage wir $x_1, ..., x_n$ erhält man aus R eine Polynomalgebra in diesen Unbestimmten, welche auch mit

$$R[x_1, ..., x_n] = R[x_1][x_2] ... [x_n]$$

bezeichnet wird. Diese Bezeichnung betont, daß es bei der Adjunktion (bis auf Isomorphie) nicht auf die Reihenfolge der Unbestimmten ankommt. Man identifiziert alle so entstehenden Ringe und schreibt

$$R[x_1, ..., x_n] = \{ \sum_{I} r_I x^I \mid r_I \in R, r_I = 0 \text{ für fast alle I}\}$$

Die Summation wird hier über alle n-Tupel $I = (i_1,...,i_n)$ nicht-negativer ganzer Zahlen erstreckt und wir benutzen hier die folgende Multi-Index-Schreibweise.

$$x^I = x_1^{i_1}\bullet...\bullet x_n^{i_n}.$$

Die Polynome der Gestalt $r_I x^I$ heißen Monome, die Zahl

$$|I| = i_1 + \ldots + i_n$$

heißt ihr Grad. Der maximale Grad der Monome von $f = \sum_I r_I x^I$ mit von Nullverschiedenen Koeffizienten heißt Grad von f und wird mit

$$\deg f = \max \{ |I| : r_I \neq 0 \}.$$

bezeichnet. Das Nullpolynom hat wieder nach Vereinbarung den Grad 0. Ein Polynom heißt homogen, wenn es Summe von Monomen desselben Grades ist.

(vi) Ist

$$f(x) = \sum_I r_I x^I$$

und $a = (a_1,\ldots,a_n)$ ein Tupel von Elementen aus R, so sei

$$f(a) = \sum_I r_I a^I$$

das Element von R, welches man erhält, indem man in dem Rechenausdruck $\sum_I r_I x^I$ die Unbestimmte x_i überall durch a_i ersetzt. Die so definierte Abbildung

$$R[x_1, \ldots, x_n] \longrightarrow R,\ f(x) \mapsto f(a),$$

ist ein Homomorphismus von Ringen mit 1 und heißt Auswertungsabbildung an der Stelle a.

(vii) Die Polynom-Ringe lassen sich durch eine Universalitätseigenschaft charakterisieren:
1. $S := R[x_1, \ldots, x_n]$ ist eine R-Algebra welche die Menge der Unbestimmten x_i als Teilmenge enthält,

$$\{x_1, \ldots, x_n\} \subseteq S,$$

wobei sich jede auf dieser Teilmengen definierte Abbildung

$$\{x_1, \ldots, x_n\} \longrightarrow S'$$

mit Werten in einer R-Algebra S' auf genau eine Weise zu einem Homomorphismus von R-Algebren

$$S \longrightarrow S'$$

fortsetzen läßt.
2. Jede R-Algebra S, welche die Unbestimmten x_i enthält und die Eigenschaft 1 besitzt, ist als R-Algebra isomorph zu $R[x_1, \ldots, x_n]$.

2.1.5 Der Ring der ganzen Gaußschen Zahlen

Die Menge

$$\Gamma = \mathbb{Z}+\mathbb{Z}i := \{a+bi \in \mathbb{C} \mid a,b \in \mathbb{Z}\}$$

ist ein Teilring des Körpers der komplexen Zahlen und heißt Ring der ganzen Gaußschen Zahlen. Als Teilring von $\mathbb{C}$ ist Γ ein Integritätsbereich. Er enthält die ganzen Zahlen als Teilring und ist eine $\mathbb{Z}$-Algebra.

2.1.6 Der Ring $\mathbb{Z}+\mathbb{Z}\sqrt[3]{2}+\mathbb{Z}(\sqrt[3]{2})^2$

Die Menge

$$\mathbb{Z}+\mathbb{Z}\sqrt[3]{2}+\ \mathbb{Z}\ (\sqrt[3]{2})^2 := \{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2 \in \mathbb{R} \mid a,b,c\in\mathbb{Z}\}$$

ist ein Teilring des Körpers der reellen Zahlen. Man beachte, es gilt zum Beispiel

$$\sqrt[3]{2}\bullet(\sqrt[3]{2})^2 = 2$$

$$(\sqrt[3]{2})^2\bullet(\sqrt[3]{2})^2 = 2\bullet\sqrt{2}$$

Als Teilring von $\mathbb{R}$ ist dies ein Integritätsbereich. Er enthält die ganzen Zahlen als Teilring und ist eine $\mathbb{Z}$-Algebra.

2.1.7 Erzeugendensysteme für Teilalgebren

Seien S ein kommutativer Ring mit 1, $R \subseteq S$ ein Teilring mit $1\in R$ und

$$a_1,...,a_n \in S$$

endlich viele Elemente. Dann ist

$$R[a_1,...,a_n] := \{ f(a_1,...,a_n) \mid f\in R[x_1, ... , x_n] \text{ (=Polynomring)}\}$$

ein Teilring von S , welcher R als Teilring enthält (also eine R-Algebra). Es ist der kleinste Teilring von S, welcher R und die Elemente $a_1,...,a_n$ enthält und heißt deshalb die von

$$a_1,...,a_n$$

über R <u>erzeugte Teilalgebra</u> von S.

Ist $M \subseteq S$ eine beliebige Teilmenge von S, so ist

$$R[M] := \bigcup \{R[a_1,...,a_n] : a_1,...,a_n\in M, n = 1,2,3, ...\}$$

ein Teilring von S, welcher R und alle Elemente von M enthält. Es ist der kleinste Teilring von S mit dieser Eigenschaft und heißt deshalb die von M über R erzeugte Teilalgebra von S.

Beispiel 1

Γ ist die von i über $\mathbb{Z}$ erzeugte Teilalgebra von $\mathbb{C}$,

$$\Gamma = \mathbb{Z}+\mathbb{Z}i = \mathbb{Z}[i].$$

Beispiel 2

$\mathbb{Z}+\mathbb{Z}\sqrt[3]{2}+\mathbb{Z}\ (\sqrt[3]{2})^2$ ist die von $\sqrt[3]{2}$ über $\mathbb{Z}$ erzeugte Teilalgebra von $\mathbb{R}$,

$$\mathbb{Z}+\mathbb{Z}\sqrt[3]{2}+\ \mathbb{Z}\ (\sqrt[3]{2})^2 = \mathbb{Z}[\sqrt[3]{2}].$$

Beispiel 3

Seien S kommutativer Ring mit 1, $R \subseteq S$ ein Teilring mit $1\in R$, $\alpha\in S$ ein Element, welches Nullstelle eines <u>normierten</u> Polynoms

$$f(x) = x^n + r_1x^{n-1}+...+r_0 \in R[x]$$

mit Koeffizienten aus R ist (d.h. der höchste Koeffizient ist 1). In dieser Situation sagt man, α ist <u>ganz</u> über R. Es ist dann

$$R\bullet 1+ R\bullet\alpha + ... + R\bullet\alpha^{n-1} = R[\alpha]$$

Dieses Beispiel verallgemeinert die beiden ersten Beispiele. In Beispiel 1 ist

$$R = \mathbb{Z}, S = \mathbb{C}, f(x) = x^2+1, n = 2,$$

in Beispiel 2 ist

$$R = \mathbb{Z}, S = \mathbb{R}, f(x) = x^3 - 2, n = 3.$$

In den beiden Beispielen sind außerdem zwei “Polynome des Grades < n in α" genau dann gleich, wenn einander entsprechende Koeffizienten gleich sind (d.h. $1, \alpha, \ldots, \alpha^{n-1}$ sind “linear unabhängig” über R).

2.2 Faktorringe

2.2.1 Ideale und Restklassen-Mengen

Seien R ein Ring. Ein Linksideal von ist eine nicht-leere Teilmenge I von R mit

1. $x-y \in I$ für beliebige $x,y \in I$
2. $rx \in I$ für beliebige $r \in R$ und $x \in I$

Ein Rechtsideal von R ist eine nicht-leere Teilmenge I von R mit

1. $x-y \in I$ für beliebige $x,y \in I$
2. $xr \in I$ für beliebige $r \in R$ und $x \in I$

Ein Ideal von R oder auch zweiseitiges Ideal von R ist eine Teilmenge von R, die sowohl Linksideal als auch Rechtsideal ist.

Bemerkungen

(i) Ist R kommutativ, so sind die Begriffe Linksideal, Rechtsideal und Ideal äquivalent.

(ii) Ist R ein Ring mit 1, so kann man die erste Bedingung durch die folgende ersetzen.

1’ $x+y \in I$ für beliebige $x,y \in I$

Gilt nämlich 1’ und $x,y \in I$, so gilt (im Fall der Linksideale) auch $-y = (-1)y \in I$, also auch

$$x-y = x + (-y) \in I.$$

Gilt umgekehrt 1. und $x,y \in I$, so gilt auch $-y = (-1)y \in I$, also auch

$$x + y = x - (-y) \in I.$$

Analog argumentiert man im Fall der Rechtsideale.

Beispiel 1

Für jede ganze Zahl g ist $g\mathbb{Z}$ ein Ideal von $\mathbb{Z}$. Jedes Ideal von $\mathbb{Z}$ hat diese Gestalt, denn jedes Ideal ist insbesondere auch eine Untergruppe der additiven Gruppe von $\mathbb{Z}$.

Beispiel 2

Sei K ein Körper. Dann sind {0} und K die einzigen Ideale von K.

Ist nämlich I ein von {0} verschiedenes Ideal, so gibt es ein $x \in I-\{0\}$. Wegen $x^{-1} \in K$ folgt $1 \in I$, d.h. für jedes $c \in K$ gilt

$$c = c \cdot 1 \in I,$$

d.h. es gilt I = K.

Beispiel 3

Seien K ein Körper, $R = K^{n \times n}$ der Ring der n×n-Matrizen und $\ell \leq n$ eine natürliche Zahl. Weiter sei

$$I := \{ (a_{ij}) \in K^{n \times n} \mid a_{ij} = 0 \text{ für } j = \ell+1,\ldots,n\} = \left\{ \begin{pmatrix} * & \ldots & * & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ * & \ldots & * & 0 & \ldots & 0 \end{pmatrix} \right\}$$

(ℓ mal)

die Menge der Matrizen, die nur in den ersten ℓ Spalten von 0 verschiedene Einträge haben können. Dann ist I ein Linkideal, denn Multiplikation von links mit Matrizen liefert Matrizen, deren Zeilen Linearkombinationen der Zeilen der Ausgangsmatrix sind.

Analog sei

$$I' := \{ (a_{ij}) \in K^{n\times n} \mid a_{ij} = 0 \text{ für } i = \ell+1,...,n\} = \left\{ \begin{pmatrix} * & \dots & * \\ \dots & \dots & \dots \\ * & \dots & * \\ 0 & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 0 \end{pmatrix} \right\}$$

die Menge der Matrizen, die nur in den ersten ℓ Zeilen von 0 verschiedene Einträge haben können. Dann ist I ein Rechtsideal.

Der volle Matrizenring $R = K^{n\times n}$ hat wie die Körper nur die (zwei-seitigen) Ideale 0 und R. Um das einzusehen, nehmen wir an,

$$I \subseteq R$$

sei ein von 0 verschiedenes Ideal. Dann gibt es eine von der Nullmatrix verschiedene Matrix A in I, sagen wir

$$0 \neq A \in I.$$

Der Eintrag von A in der Position (u,v) sei

$$a \neq 0.$$

Durch Multiplikation mit 1/a erreichen wir[9]

$$a = 1.$$

Bezeichne E_{ij} die n×n-Matrix, deren Eintrag in der Position (i,j) gleich Eins und deren übrige Einträge gleich Null sind. Es gilt dann

$$E_{ij} \bullet E_{i'j'} = \begin{cases} E_{ij}, & \text{im Fall } j = i' \\ 0 & \text{sonst} \end{cases}$$

Wir denken uns A als K-Linearkombination der E_{ij} geschrieben und erhalten mit Hilfe dieser Relationen

$$a \bullet E_{uv} = E_{uu} \bullet A \bullet E_{vv} \in I,$$

also

$$E_{uv} \in I,$$

da a = 1 ist.
Für beliebige i und beliebige j folgt

$$E_{ij} = E_{iu} E_{uv} E_{vj} \in I.$$

Da jede Matrix K-Linearkombination der Matrizen E_{ij} ist, folgt $K^{n\times n} \subseteq I$, also

$$I = K^{n\times n}.$$

Beispiel 4

Sei $h: R \longrightarrow R'$ ein Ringhomomorphismus. Dann ist

$$\text{Ker } h := \{x \in R \mid h(x) = 0\}$$

ein zweiseitiges Ideal.

---

[9] genauer: durch Multiplikation mit einer geeigneten Multiplikationsmatrix.

Wegen $h(0) = 0$ gilt $0 \in \text{Ker } h$, d.h. Ker h ist nicht leer. Mit $x,y \in \text{Ker } h$ gilt

$$h(x-y) = h(x) - h(y) = 0 - 0 = 0,$$

also $x-y \in \text{Ker } h$. Mit $r \in R$ und $x \in \text{Ker } h$ gilt

$$h(rx) = h(r)h(x) = h(r) \bullet 0 = 0$$

und

$$h(xr) = h(x)h(r) = 0 \bullet h(r) = 0$$

also $rx \in \text{Ker } h$ und $xr \in \text{Ker } h$.

Beispiel 5

Seien R ein kommutiver Ring mit 1 und $M \subseteq R$ eine Teilmenge von R. Dann ist

$$I := \{ r_1m_1+...+r_nm_n \mid r_1,...,r_n \in R , m_1,...,m_n \in R, n = 1,2,3,... \}$$

ein Ideal von R. Es ist das kleinste Ideal von R, welches M enthält und heißt das von M erzeugte Ideal. Bezeichnung:

$$(M) = (M)R = I.$$

Im Fall $M = \{ m_1,...,m_n \}$ scheibt man auch

$$(m_1,...,m_n) = (m_1,...,m_n)R = (M).$$

2.2.2 Die Ringstruktur von R/I

Seien R ein Ring und I ein zweiseitiges Ideal von R. Dann gilt

(i) Die Menge

$$R/I := \{ r + I \mid r \in R \}$$

der Restklassen modulo I ist ein Ring bezüglich der Operationen

$(r + I) + (s + I) := (r+s) + I$

$(r + I) \bullet (s + I) := (r \bullet s) + I$

(ii) Die natürliche Abbildung

$$\rho: R \longrightarrow R/I, r \mapsto r + I,$$

ist ein Ringhomomorphismus.

(iii) Ist R ein Ring mit 1, so gilt dasselbe für R/I und ρ ist ein Homomorphismus von Ringen mit 1.

(iv) Ist R kommutativ, so gilt dasselbe für R/I.

Beweis. Zu (i). Mit der angegebene Addition ist R/I eine abelsche Gruppe, denn I ist ein Normalteiler der additiven Gruppe von R. Die Definition der Multiplikation von R/I ist korrekt, denn aus

$$r + I = r' + I \text{ und } s + I = s' + I$$

folgt

$$r-r' \in I \text{ und } s-s' \in I$$

also

$$rs - r's' = (r-r')s + r'(s-s') \in I$$

also

$$rs + I = r's' + I.$$

Die Ringaxiome überprüft man durch direktes Nachrechnen (bzw. unter Verwendung der Relationstreue der natürlichen Abbildung von (ii).

Zu (ii). Es gilt

$\rho(r+s) = (r+s)+I = (r+I)+(s+I) = \rho(r) + \rho(s)$

$\rho(r \bullet s) = (r \bullet s)+I = (r+I) \bullet (s+I) = \rho(r) \bullet \rho(s),$

d.h. ρ ist relationstreu. Man beachte, daraus (und aus der Surjektivität von ρ) ergeben sich die bisher noch nicht bewiesenen Ringaxiome, zum Beispiel das Assoziativitätsgesetz der Multiplikation:

$$(\rho(r)\bullet\rho(s))\bullet\rho(t) = \rho(rs)\bullet\rho(t) = \rho((rs)t) = \rho(r(st)) = \rho(r)\bullet\rho(st) = \rho(r)\bullet(\rho(s)\bullet\rho(t)).$$

Analog beweist man die Distribitivgesetze, zum Beispiel:

$$\rho(r)\bullet(\rho(s)+\rho(t)) = \rho(r)\rho(s+t) = \rho(r(s+t)) = \rho(rs+rt) = \rho(rs)+\rho(rt)$$
$$= \rho(r)\bullet\rho(s) + \rho(r)\bullet\rho(t).$$

Wir verwenden hier die Tatsache, daß jedes Element von R/I die Gestalt $\rho(x)$ mit $x\in R$ beseitzt.

Zu (iii). Es gilt

$$\rho(1)\rho(r) = \rho(1\bullet r) = \rho(r)$$

und

$$\rho(r)\rho(1) = \rho(r\bullet 1) = \rho(r),$$

d.h. 1+I ist ein Einselement von R.

Zu (iv). Es gilt

$$\rho(r)\rho(s) = \rho(rs) = \rho(sr) = \rho(s)\rho(r).$$

QED.

Beispiel

Sei K ein Körper. Dann ist der Polynomring R = K[x] nullteilerfrei, $I = x^2K[x]$ ist eine Ideal und R/I ist nicht nullteilerfrei.

Weil nämlich x nicht in I liegt, wohl aber x^2, so ist $\overline{x} := x + I$ ein von Nullverschiedenes Element von R/I. Das Quadrat jedoch,

$$\overline{x}^2 = (x+I)(x+I) = x^2 + I = I,$$

ist Null. Die Eigenschaft der Nullteilerfreiheit bleibt also nicht erhalten beim Übergang zu einem Faktorring.

2.2.3 Der Homomorphiesatz

Seien R ein Ring, $I \subseteq R$ ein Ideal und $h: R \longrightarrow R'$ ein Ring-Homomorphismus und

$$\rho: R \longrightarrow R/I, r + I,$$

der natürliche Homomorphismus. Dann sind folgende Aussagen äquivalent.

(i) $I \subseteq \text{Ker } h$.

(ii) Es gibt einen Homomorphismus $\tilde{h}: R/I \mapsto R'$ mit der Eigenschaft, daß das folgende Diagramm kommutativ ist.

$$\begin{array}{ccc} R & \overset{h}{\longrightarrow} & R' \\ \rho\downarrow & \nearrow \tilde{h} & \\ R/I & & \end{array}$$

Falls die beiden Bedingungen erfüllt sind, so gilt außerdem:

(iii) $\tilde{h}$ ist durch h eindeutig festgelegt. Es gilt $\tilde{h}(r+I) = h(r)$ für jedes $r\in R$.

(iv) $\text{Im } \tilde{h} = \text{Im } h$.

(v) $\text{Ker } \tilde{h} = \text{Ker } h/I$.

Beweis. Man benutzt dieselben Argumente wie beim Beweis des Homomorphiesatzes für Gruppen.

QED.

2.2.4 Der 0-te Isomorphiesatz

Sei $h: R \longrightarrow R'$ ein Ring-Homomorphismus. Dann ist der zum Ideal

$$I := \operatorname{Ker} h$$

gehörige Homomorphismus

$$\tilde{h} : R/\operatorname{Ker} h \longrightarrow R', g+I \mapsto h(g),$$

injektiv, definiert also einen Isomorphismus

$$\tilde{h} : G/\operatorname{Ker} h \longrightarrow \operatorname{Im} h, gN \mapsto h(g).$$

Beweis. Vgl. den Beweis von 1.3.7.
QED.

2.2.5 Der erste Isomorphiesatz

Seien R ein Ring,, und $I \subseteq R$ ein Ideal und $S \subseteq R$ ein Teilring. Dann ist

$$I \cap S$$

ein Ideal von S und die Abbildung

$$S/S \cap I \longrightarrow S+I/I, s + S \cap I \mapsto s+I,$$

ein Ring-Isomorphismus.
Beweis. vgl. 1.3.8
QED.

2.2.6 Der zweite Isomorphiesatz

Seien R ein Ring und $I, J \subseteq R$ zwei Ideale von R mit $I \subseteq J$. Dann ist J/I ein Ideal von R/I und die Abbildung

$$R/J \longrightarrow (R/I)/(J/I), r + J \mapsto (r + I) + J/I.$$

ist wohldefiniert und ein Isomorphismus von Ringen.
Beweis. vgl. 1.3.9. Die hier angegebene Abbildung ist gerade die inverse Abbildung zu der in 1.3.9.
QED.

2.2.7 Maximale Ideale und Primideale

Seien R ein kommutativer Ring mit 1 und I ein echtes Ideal von R (d.h. $I \neq R$). Dann heißt I <u>Primideal</u> von R, wenn die folgende Implikation besteht.

$$x,y \in , xy \in I \Rightarrow x \in I \text{ oder } y \in I.$$

Das Ideal I heißt <u>maximal</u>, wenn für jedes echte Ideal J von R die folgende Implikation besteht.

$$I \subset J \Rightarrow I = J.$$

2.2.8 Existenz maximaler Ideale

Seien R ein kommutativer Ring mit 1 und I ein echtes Ideal von R. Dann gibt es ein maximales Ideal M von R mit $I \subseteq M$.

Beweis. Wir betrachten die Menge

$$\mathcal{M} := \{ J \subseteq R \mid J \text{ ist echtes Ideal von R mit } I \subseteq J\}.$$

Diese Menge ist nicht leer, denn es gilt

$$I \in \mathcal{M}.$$

Sie ist halbgeordnet bezüglich der Inklusion '$\subseteq$' von Mengen (d.h. '$\subseteq$' ist reflexiv, antisymmetrisch und transitiv). Es reicht zu zeigen, M besitzt ein bezüglich dieser Halbordnung maximales Element. Dazu reicht es zu zeigen, $\mathcal{M}$ genügt den Bedingungen des Zornschen Lemmas. Sei also

(1) $$\{J_i\}_{i \in A}$$

eine linear geordnete Kette in $\mathcal{M}$. Es reicht zu zeigen,

$$J := \bigcup_{i \in A} J_i$$

ist wieder ein Element von $\mathcal{M}$. Für jedes $i \in A$ gilt

$$I \subseteq J_i \subseteq J.$$

Es reicht also zu zeigen, J ist ein echtes Ideal von R. Weil jedes der Ideale J_i echt ist, gilt

$$1 \notin J_i$$

(denn andernfalls wäre $R = R \bullet 1 \subseteq J_i$, d.h. $R = J_i$ und J_i nicht echt). Also gilt auch

$$1 \notin J.$$

Es reicht also zu zeigen, J ist ein Ideal. Seien

$$x, y \in J$$

zwei vorgegebene Elemente von J. Nach Definition von J gibt es $i,j \in A$ mit

$$x \in J_i \text{ und } y \in I_j .$$

Da (1) eine Kette ist, gilt $J_i \subseteq J_j$ oder $J_i \supseteq J_j$ O.B.d.A. bestehe die erste Inklusion. Dann gilt

$$x\text{-}y \in J_j \subseteq J$$

also $x - y \in J$.

Seien $x \in I$ und $r \in R$ vorgegeben. Dann gibt es ein $i \in A$ mit $x \in J_i$. Dann ist aber auch

$$rx = xr \in J_i \subseteq J$$

also $rx = xr \in J$. Wir haben gezeigt, J ist ein Ideal von R.
QED.

2.2.9 Charakerisierung der maximalen Ideale

Seien R ein kommutativer Ring mit 1 und I ein echtes Ideal von R. Dann sind folgende Bedingungen äquivalent.
(i) I ist ein maximales Ideal von R.
(ii) R/I ist ein Körper.

Beweis. (i) $\Rightarrow$ (ii). Sei x + I ein von Null verschiedenes Element von R. Wir haben zu zeigen, x + I besitzt ein Inverses. Da x + I ungleich Null sein soll, gilt

$$x \notin I.$$

Wir betrachten die Menge

$$I' := I + xR := \{ i + rx \mid i \in I, r \in R \}.$$

Diese Menge ist ein Ideal und enthält I als echte Teilmenge. Weil I maximal sein soll, folgt

$$I' = R.$$

Es gibt also ein $i \in I$ und ein $r \in R$ mit

$$i + r\,x = 1.$$

Damit ist aber

$$1 + I = (i + I) + (r+I)(x+I) = (r+I)(x+I).$$

Mit anderen Worten r + I ist invers zu x+I.

(ii) $\Rightarrow$ (i). Sei J ein Ideal von R, welches I als echte Teilmenge enthält. Wir haben zu zeigen,

$$J = R.$$

Nach Voraussetzung gibt es ein Element

$$x \in J - I.$$

Dann ist die Restklasse x + I ungleich Null in R/I, d.h. es gibt ein zu x+I inverses Element y + I in R/I, d.h.

$$1 + I = (x+I)(y+I) = xy + I.$$

Insbesondere ist $1 - xy \in I \subseteq J$. Wegen $x \in J$ folgt

$$1 = (1-xy) + xy \in J.$$

Damit gilt aber auch für jedes $r \in R$,

$$r = r \bullet 1 \in J,$$

d.h. $R \subseteq J$, d.h. $R = J$.

QED.

2.2.10 Charakterisierung der Primideale

Seien R ein kommutativer Ring mit 1 und I ein echtes Ideal von R. Dann sind folgende Bedingungen äquivalent.

(i) I ist ein Primideal von R.

(ii) R/I ist ein Integritätsbereich.

Beweis. (i) $\Rightarrow$ (ii). Weil R kommutativ mit 1 ist, gilt dasselbe für R/I. Wir haben noch zu zeigen, R/I besitzt keine Nullteiler. Seien x + I und y+I von Null verschiedene Elemente. Wir haben zu zeigen,

(1) $$(x+I)(y+I) = xy + I$$

ist von Null verschieden. Nach Voraussetzung gilt $x \notin I$ und $y \notin I$. Da I Primideal ist, folgt $xy \notin I$, also ist das Element (1) ungleich Null.

(ii) $\Rightarrow$ (i). Seien $x,y \in R$ Element mit $xy \in I$. Wir haben zu zeigen, einer der Faktoren liegt in I. Wegen $xy \in I$ gilt in R/I.

$$(x + I)(y+I) = xy + I = I = \text{Nullelement von } R/I.$$

Weil R/I ein Integritätsbereich ist, folgt

$$x + I = I \text{ over } y+I = I,$$

d.h. $x \in I$ oder $y \in I$.

QED.

Beispiel 1

Sei R ein Integritätsbereich. Dann ist das Nullideal (0) = {0} ein Primideal von R.

Beispiel 2.

Seien R ein Integritätsbereich und S := R[x] ein Polynomring über R und I = xS die Menge der Vielfachen von x. Dann ist I ein Ideal von S mit

$$S/I \cong R.$$

Insbesondere ist I ein Primideal von R. Falls R kein Körper ist, so ist I kein maximales Ideal.

Im Fall

$$R = K[x,y] \text{ und } I = (x)$$

(und K ein Körper) ist

$$K[x,y]/(x) \cong K[y],$$

d.h. (x) ist Primideal aber nicht maximales Ideal.

2.3 Quotientenringe

2.3.1 Vorbemerkung

In diesem Abschnitt wollen wir zu einen gegebenen kommutativen Ring R (mit 1) neue Ringe konstruieren, deren Elemente die Gestalt

$$\frac{a}{b} \text{ mit } a,b \in R,\ b \neq 0,$$

haben. Wir haben zu diesem Zweck vor allem die Frage zu klären, was man unter dem Symbol a/b zu verstehen hat. Wir halten zunächst fest:

(i) Für je zwei Quotienten $\frac{a}{b}$ und $\frac{a'}{b'}$ sollte auch

$$\frac{a}{b} \bullet \frac{a'}{b'} = \frac{aa'}{bb'}$$

ein Element des betrachteten Rings sein. Mit anderen Worten, falls b und b' als Nenner auftreten, so sollte auch das Produkt bb' ein Nenner sein, d.h. die Menge der Nenner ist multiplikativ abgeschlossen.

(ii) Zwei Quotienten $\frac{a}{b}$ und $\frac{a'}{b'}$ sollten gleich sein, falls gilt ab' = a'b,

$$\frac{a}{b} = \frac{a'}{b'} \text{ falls } ab' = a'b \text{ gilt.}$$

Außerdem sollte gelten

$$\frac{a}{b} = \frac{as}{bs}$$

für jeden Nenner s. Man beachte, mit $\frac{as}{bs}$ sollte auch $\frac{b}{1} \bullet \frac{as}{bs} = \frac{abs}{bs} = \frac{as}{s}$ ein Element des betrachteten Rings sein, d.h. s ist ein Nenner.

(iii) Die beiden Bedingungen von (ii) kann man zu einer Bedingung zusammenfassen:

$$\frac{a}{b} = \frac{a'}{b'} \text{ falls es einen Nenner s gibt mit } s(ab' - a'b) = 0.$$

(iv) Zur formalen Konstruktion der Quotienten brauchen wir die Begriffe der Äquivalenzrelation und der Äquivalenzklasse.

2.3.2 Äquivalenzrelationen und Äquivalenzklassen

Eine Äquivalenzrelation auf einer Menge M ist eine Relation R auf M mit folgenden Eigenschaften.

(i) R ist reflexiv, d.h. xRx für jedes x∈M.
(ii) R ist symmetrisch, d.h. mit xRy gilt auch yRx.
(iii) R ist transitive, d.h. mit xRy und yRz gilt auch xRz.

Eine Äquivalenzklasse bezüglich der gegebenen Äquivalenzrelation R ist eine Menge der Gestalt

$$[x] = \{ y \in M \mid yRx \} \text{ mit } x \in M.$$

Diese Menge heißt auch Äquivalenzklasse des Elements x. Die Menge der Äquivalenzklassen bezüglich R wird mit

$$M/R = \{ [x] \mid x \in M \}$$

bezeichnet.

Beispiel 1

Die Gleichheit ist eine Äquivalenzrelation auf jeder Menge. Die Äquivalenzklassen sind einelementig, d.h. man kann M/R mit M identifizieren.

Beispiel 2

Seien G eine Gruppe und $U \subseteq G$ eine Untergruppe. Wir definieren für Elemente g,h∈G:

$$g \sim h \text{ falls } g^{-1}h \in U.$$

Dann ist '~' eine Äquivalenzrelation auf G und die Äquivalenzklassen sind gerade die Linksnebenklassen,

$$G/\sim = G/U.$$

Analoge Aussagen gelten auch für die Rechtsnebenklassen bzw. für die Restklassen eines Rings bezüglich eines Ideals.

Beispiel 3

Die Gruppe G operiere auf der Menge M. Wir definieren für die Elemente m',m"∈M:

$$m' \sim m" \text{ falls es ein } g \in G \text{ gibt mit } m" = gm'.$$

Dann ist '~' eine Äquivalenzrelation auf M und die Äquivalenzklassen sind gerade die die Orbits der gegebenen Gruppenoperation..

Bemerkungen

(i) Je zwei Äquivalenzklassen sind identisch oder disjunkt.

(ii) Insbesondere ist M disjunkte Vereinigung der Äquivalenzklassen bezüglich einer gegebenen Äquivalenzrelation.

Beweis von (i). Seien [x'] und [x"] nicht disjunkt, d.h. es existiere ein $x \in [x'] \cap [x"]$. Für jedes $y \in [x']$ gilt dann

$$yRx' \text{ und } x'Rx \text{ und } xRx".$$

Also gilt auch yRx", d.h. $y \in [x"]$. Wir haben gezeigt,

$$[x'] \subseteq [x"].$$

Die umgekehrte Inklusion folgt analog.

QED.

2.3.3 Konstruktion

Sei R ein kommutativer Ring. Eine nicht-leere Teilmenge $S \subseteq R$ heißt <u>multiplikativ abgeschlossen</u>, wenn die folgende Implikation besteht.

$$a \in S \text{ und } b \in S \Rightarrow ab \in S.$$

Seien R ein kommutativer Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Ein <u>Quotient</u>

$$\frac{a}{s} \text{ mit } a \in R \text{ und } s \in S$$

von Elementen aus R bezüglich der Nennermenge S ist definiert als die Äquivalenzklasse des Paares

$$(a,s) \in R \times S$$

in der Menge R×S bezüglich der folgenden Äquivalenzrelation '~'.

$$(a',s') \sim (a",s") \text{ falls es ein } t \in S \text{ gibt mit } t(a's" - a"s') =^{10} 0.$$

Die zugehörige Menge der Äquivalenzklassen wird mit

$$S^{-1}A := A_S := \{ \frac{a}{s} \mid a \in R, s \in S \}$$

bezeichnet und heißt <u>Quotientenring</u> von R bezüglich S.

Bemerkungen

(i) '~' ist tatsächlich eine Äquivalenzrelation.

(ii) R_S ist mit den folgenden (wohldefinierten) Operationen ein kommutativer Ring mit 1..

---

[10] Ohne den Faktor t auf der rechten Seite dieser Identät wäre '~' im allgemeinen keine Äquivalenzrelation. Im Fall von Integritätsbereichen kann man jedoch diesen Faktor weglassen.

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'}$$
$$\frac{a}{s} \bullet \frac{a'}{s'} = \frac{aa'}{ss'}$$

(iii) Die Abbildung

$$R \longrightarrow R_S\ ,\ a \mapsto \frac{as}{s},$$

ist unabhängig von der speziellen Wahl von s und ist ein Homomorphismus von Ringen. Sie heißt natürlicher Homomorphismus in den Quotientenring.

Beweis. Zu (i). Reflexivität: Es gilt $s(a's' - a's') = 0$, also

$$(a',s') \sim (a',s')$$

Symmetrie: Aus $(a',s') \sim (a'',s'')$ folgt $t(a's'' - a''s') = 0$ für eine $t \in S$, also auch

$$t(a''s' - a's'') = 0,$$

also $(a'',s'') \sim (a',s')$.

Transitivität: Aus $(a,s) \sim (a',s')$ und $(a',s') \sim (a'',s'')$ folgt

$$t(as' - a's) = 0$$

und

$$t'(a's'' - a''s') = 0$$

für gewisse $t,t' \in S$. Wir multiplizieren die erste Identität mit $t's''$ und die zweite mit ts und bilden die Summe. Wir erhalten

$$0 = t's''tas' - tst'a''s' = tt's'(as'' - a''s).$$

Wegen $tt's' \in S$ folgt $(a,s) \sim (a'',s'')$.

Zu (ii). Die Ringaxiome von R_S bezüglich der angegebenen Operationen sind leicht nachzuweisen und folgenen aus den Ringaxiomen von R. Wir beschränken uns hier auf den Nachweis, daß die Operationen korrekt definiert sind. Aus den Definitionen folgt dann auch, das s/s die Rolle eines Einselements in R_S spielt.

Korrektheit der Addition. Seien $\frac{a}{s} = \frac{b}{t}$ und $\frac{a'}{s'} = \frac{b'}{t'}$. Dann gibt es Elemente $u,u' \in S$ mit

(1) $u(at - bs) = 0$

und

(2) $u'(a't' - b's') = 0.$

Wir haben zu zeigen, es gilt $\frac{as' + a's}{ss'} = \frac{bt' + b't}{tt'}$, d.h. es gibt ein $v \in S$ mit

(3) $v(as'tt' + a'stt' - bt'ss' - b'tss') = 0$

Wir multiplizieren (1) mit $u's't'$ und (2) mit uts und bilden die Summe. Wir erhalten

$$0 = uu'ats't' - uu'bss't' + uu'a't'ts - uu'b's'ts$$
$$= uu'(as'tt' + a'stt' - bt'ss' - b'tss'),$$

d.h. (3) gilt mit $v := uu'$.

Korrektheit der Multiplikation. Seien $\frac{a}{s} = \frac{b}{t}$ und $\frac{a'}{s'} = \frac{b'}{t'}$, d.h. es gebe Elemente $u,u' \in S$, so daß die Identitäten (1) und (2) bestehen. Wir haben zu zeigen, $\frac{aa'}{ss'} = \frac{bb'}{tt'}$, d.h. es gibt ein $w \in S$ mit

(4) $w(aa'tt' - bb'ss') = 0.$

Wir multiplizieren (1) mit $u'a't'$ und (2) mit ubs und bilden die Summe. Wir erhalten

$$0 = uu'ata't' - uu'b's'bs = uu'(aa'tt' - bb'ss'),$$

d.h. (4) gilt mit $w = uu'$.

Zu (iii). Die Relationstreue der Abbildung folgt unmittelbar aus den Definitionen der Ringoperationen von R_S. Für je zwei Elemente $s,s' \in S$ gilt

$$as/s = as'/s'$$

(wegen s(ass' - as's) = 0), d.h. die Abbildung ist unabhängig von der speziellen Wahl von s∈S.
QED.

2.3.4 Beispiel: der volle Quotientenring, Quotientenkörper

Sei R ein kommutativer Ring. Dann ist die Menge

$$S := \{ s \in R \mid \text{für jedes } x \in R - \{0\} \text{ gilt } sx \neq 0 \}$$

der Nicht-Nullteiler von R eine multiplikativ abgeschlossene Menge. Der zugehörige Quotientenring

$$Q(R) := S^{-1}R$$

heißt voller Quotientenring.

Bemerkungen

(i) Ist R ein nullteilerfrei, so ist Q(R) ein Körper.

(ii) Der Quotientenkörper von $\mathbb{Z}$ ist $Q(\mathbb{Z}) = \mathbb{Q}$.

(iii) Für jeden Körper K ist der Quotientenkörper des Polynomrings $K[X_1,...,X_n]$ gerade der Körper

$$Q(K[X_1,...,X_n]) = K(X_1,...,X_n)$$

der rationalen Funktionen mit Koeffizienten aus K.

Beweis. Zu (i). Ist R nullteilerfrei, so ist die Menge der Nicht-Nullteiler von R gerade gleich

$$S = R - \{0\},$$

d.h.

$$Q(R) = \{ \frac{a}{b} \mid a \in R, b \in R - \{0\} \}.$$

Ist $\frac{a}{b} \neq \frac{0}{b}$ ungleich dem Nullelement, d.h. $a \neq 0$, so ist $\frac{b}{a}$ ein Element von Q(R), d.h. $\frac{a}{b}$ ist eine Einheit.

Zu (ii). Das gilt nach Definition von $\mathbb{Q}$.

Zu (ii). Das gilt nach Definition des Begriffs der rationalen Funktion.

QED.

2.3.5 Die Universalitätseigenschaft der Quotientenringe

Seien R ein kommutativer Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Menge. Dann gelten folgende Aussagen.

(i) Der natürliche Homomorphismus $\rho: R \longrightarrow S^{-1}R, r \mapsto (rs)/s$ überführt jedes Element von R in eine Einheit von $S^{-1}R$.

(ii) Für jeden Homomorphismus $h: R \longrightarrow R'$ mit Werten in einem kommutativen Ring R' mit 1, der die Elemente von S in Einheiten abbildet, gibt es genau einen Homomorphismus

$$\tilde{h}: S^{-1}R \longrightarrow R'$$

von Ringen mit 1 derart, daß das folgende Diagramm kommutativ ist.

$$\begin{array}{ccc} R & \xrightarrow{h} & R' \\ \rho\downarrow & \nearrow \tilde{h} & \\ S^{-1}R & & \end{array}$$

Beweis. Zu (i). Für jedes $s \in S$ besitzt $\rho(s) = s^2/s$ ein Inverses, nämlich s/s^2, ist also eine Einheit.

Zu (ii). Eindeutigkeit von $\tilde{h}$. Falls $\tilde{h}$ exisitiert, so gilt für jedes Element a/s aus $S^{-1}R$:

$$h(s)\tilde{h}(a/s) = \tilde{h}(\rho(s))\,\tilde{h}(a/s) = \tilde{h}(s^2/s \bullet a/s) = \tilde{h}((as^2)/(s^2)) = \tilde{h}(\rho(a)) = h(a).$$

Da h(s) eine Einheit in R' ist, folgt

(1) $\tilde{h}(a/s) = h(s)^{-1}h(a)$.

Diese Formel zeigt, $\tilde{h}$ ist durch h eindeutig festgelegt.

Existenz von $\tilde{h}$. Wir definieren $\tilde{h}$ durch die Formel (1) und zeigen zunächst, daß diese Definition korrekt ist. Sei also

$$a/s = a'/s'.$$

Wir haben zu zeigen, dann gilt

(2) $$h(s)^{-1}h(a). = h(s')^{-1}h(a').$$

Nach Voraussetzung gibt es ein $t \in S$ mit

$$t(as' - a's) = 0.$$

Wir wenden h an und erhalten

$$h(t)(h(a)h(s') - h(a')h(s)) = 0.$$

Da h(t) eine Einheit ist, können wir mit deren Inversen multiplizieren und erhalten

$$h(a)h(s') = h(a')h(s).$$

Multiplikation mit dem $h(s')^{-1}h(s)^{-1}$ liefert (2) (da R' ein kommutativer Ring ist).
QED.

2.3.6 Lokale Ringe

Seien R ein kommutativer Ring mit 1 und $P \subseteq R$ ein Primideal. Dann ist

$$S := R - P$$

eine multiplikative abgeschlossene Menge und

$$R_P := S^{-1}R$$

ein Ring mit genau einem maximalen Ideal. Solche Ringe heißen lokale Ringe.
Bezeichne

$$\gamma: R \longrightarrow R_P$$

den natürlichen Homomorphismus. Dann ist das maximale Ideal von R_P gleich

$$m(R_P) := PR_P \text{ (:= das von } \gamma(P) \text{ in } R_P \text{ erzeugte Ideal).}$$

Beweis. Die Multiplikativität der Menge S folgt unmittelbar aus der Primidealeigenschaft von P. Betrachten wir die Teilmenge

$$M := \{ \frac{r}{s} \mid r \in P, s \in S\}$$

von R_P. Diese Menge ist ein Ideal:

1. Für $\frac{r}{s}, \frac{r'}{s'} \in M$, d.h. $r,r' \in P$ und $s,s' \in S$, gilt

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'} \in M.$$

2. Fur $\frac{r}{s} \in R_P$ und $\frac{r'}{s'} \in M$, d.h. $r \in R$, $r' \in P$, $s,s' \in S$, gilt

$$\frac{r}{s} \bullet \frac{r'}{s'} = \frac{rr'}{ss'} \in M.$$

Weiter ist M ein echtes Ideal: läge das Einselement von R_P in M, $\frac{s}{s} = \frac{r}{s}$ für ein $r \in P$ und ein $s \in S$, so gäbe es ein $t \in S$ mit $t(s^2 - rs) = 0$, d.h. $ts^2 = trs \in P$. Weil P Primideal ist und sowohl s als auch t nicht in P liegen, ist dies nicht möglich.

Zeigen wir, M ist das einzige maximale Ideal von R_P. Dazu reicht es zu zeigen, jedes echte Ideal von R_P liegt ganz in M. Sei I ein Ideal, welches nicht ganz in M liegt. Es reicht zu zeigen, I ist der ganze Ring. Weil I nicht ganz in M liegt, gibt es ein Element

$$\frac{r}{s} \in I \text{ mit } r \notin P, s \in S,$$

Es gilt dann $r \in R-P = S$, d.h. $\frac{s}{r}$ ist ein Element von R_P. Dann ist aber

$$\frac{s}{r} \bullet \frac{r}{s} = \frac{sr}{rs}$$

ein Element von I. Dieses Element ist aber das Einselement von R_P. Deshalb gilt $I = R_P$.

Wir haben noch zu zeigen, das maximale Ideal M wird von $\gamma(P)$ erzeugt. Für jedes $p \in P$ gilt

$$\gamma(p) = \frac{ps}{s} \in M.$$

Deshalb gilt $\gamma(P) \subseteq M$ und das von $\gamma(P)$ erzeugte Ideal liegt ganz in M,

$$PR_P \subseteq M.$$

Umgekehrt läßt sich jedes Element von M in der Gestalt

$$\frac{r}{s} = \frac{rs}{s} \bullet \frac{1}{s} = \gamma(r) \bullet \frac{1}{s} \in \gamma(r)R_P \text{ mit } r \in P, s \in S,$$

schreiben. Deshalb besteht auch die umgekehrte Inklusion.
QED.

Bemerkung
Der Name "lokaler Ring" kommt daher, daß man Ringe dieser Art benutzen kann, um geometrische Objekte in der Umgebung eines Punkt zu beschreiben, d.h. "lokal" zu beschreiben.

2.4 Euklidische Ringe

2.5.1 Definition

Eine wohlgeordnete Menge ist eine Menge, die mit einer reflexiven[11], anti-symmetrischen[12], transitiven[13] und linearen[14] Relation "$\leq$" versehen ist, mit der Eigenschaft, daß jede Teilmenge von M ein kleinstes Element besitzt.

Beispiel
Die Menge $\mathbb{N}$ der natürlichen Zahlen ist bezüglich der gewöhnlichen $\leq$-Relation wohlgeordnet. Dasselbe gilt für die Menge

$$\mathbb{Z}_{\geq 0} := \{ n \in \mathbb{Z} \mid n \geq 0 \}$$

---

[11] es gilt $x \leq x$ für jedes $x \in M$

[12] Aus $x \leq y$ und $y \leq x$ folgt $x = y$.

[13] Aus $x \leq y$ und $y \leq z$ folgt $x \leq y$.

[14] Je zwei Elemente $x,y \in M$ sind vergleichbar, d.h. es gilt $x \leq y$ oder $y \leq x$.

der nicht-negativen ganzen Zahlen.

Ein Integritätsbereich R heißt euklidischer Ring, wenn es eine Abbildung

$$N: R - \{0\} \longrightarrow M$$

mit Werten in einer wohlgeordneten Menge so daß folgendes gilt.

Für je zwei Elemente $x, y \in R - \{0\}$ gibt es Element $q,r \in R$ mit

$$x = qy + r,$$

wobei entweder $r = 0$ oder $N(r) < N(y)$ gilt.

Bemerkungen

(i) Mit anderen Worten, ein Euklidischer Ring ist ein Integritätsbereich, in welchem Division mit Rest möglich ist.

(ii) Die in der Definition auftretende Abbildung N wird manchmal auch als Höhenfunktion oder auch als Norm des Euklidischen Rings bezeichnet.

2.5.2 Beispiel: $\mathbb{Z}$

Der Ring der ganzen Zahlen ist mit der Höhenfunktion

$$N: \mathbb{Z} - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}\ ,\ n \mapsto |n|,$$

ein euklidischer Ring. Dabei bezeichne $\mathbb{Z}_{\geq 0}$ die Menge der nicht-negativen ganzen Zahlen mit der gewöhnlichen "$\leq$"-Beziehung als Wohlordnung.

2.5.3 Beispiel: der Polynomring K[X] über einem Körper K

Seien K ein Körper und X eine Unbestimmte. Dann ist der Polynomring K[X] ein euklidischer Ring bezüglich der Höhenfunktion

$$K[X] - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}\ ,\ f(x) \mapsto \deg f(x).$$

2.5.4 Beispiel: Ring der ganzen Gaußschen Zahlen

Der Ring $\Gamma = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i\ (\subseteq \mathbb{C})$ ist ein euklidischer Ring bezüglich der Höhenfunktion

$$N: \Gamma - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}\ ,\ a + bi \mapsto a^2+b^2 = (a+bi)(a-bi) = |a+bi|^2.$$

Beweis. Seien zwei ganze Gaußsche Zahlen $z, w \in \Gamma - \{0\}$ gegeben. Wir wollen zeigen, wir können in Γ die Division von z durch w mit Rest durchführen. Dazu betrachten wir die komplexe Zahl

$$\frac{z}{w} = \alpha + \beta i \in \mathbb{C}$$

und wählen eine ganze Gaußsche Zahl $q \in \Gamma$, die möglichst nahe bei z/w liegt. Wir können auf jeden Fall erreichen, daß Real- und Imaginärteil von q um höchstens den Wert 1/2 vom Real- bzw. vom Imaginärteil von z/w abweicht, d.h. es gibt ein

$$q = q'+q''i \in \Gamma \text{ mit } \left|\frac{z}{w} - q\right| = \sqrt{(\alpha-q')^2 + (\beta-q'')^2}\ \leq \sqrt{\frac{1}{4}+\frac{1}{4}} = \frac{1}{2}\sqrt{2}.$$

Wir setzen

$$r := z - qw \in \Gamma.$$

Dann gilt

$$z = qw + r$$

und

$$|r| = |z - qw| = |w| \cdot \left|\frac{z}{w} - q\right| \leq \frac{1}{2}\sqrt{2}\,|w| < |w|,$$

also

$|r|^2 < |w|^2$,
d.h. $N(r) < N(w)$.
QED.

2.5.5 Der Euklidische Algorithmus

Seien R ein euklidischer Ring mit der Höhenfunktion

$$H: R - \{0\} \longrightarrow M$$

und $a,b \in R - \{0\}$ zwei Elemente. Wir setzen

$$a_0 := a, a_1 = b.$$

Angenommen, wir hätten bereits die Elemente

$$a_0, \ldots, a_n \in R - \{0\}$$

konstruiert. Nach Voraussetzung gibt es Elemente $q,r \in R$ mit

$$a_{n-1} = q \bullet a_n + r,$$

wobei $r = 0$ oder

$$N(r) < N(a_n).$$

Falls $r = 0$ ist, so endet der Algorithmus. Im Fall $r \neq 0$ setzen wir

$$a_{n+1} := r,$$

so daß gilt

(1) $$a_{n-1} = q \bullet a_n + a_{n+1} \text{ und } N(a_{n+1}) < N(a_n).$$

Bemerkungen

(i) Weil M wohlgeordnet ist, bricht der euklidische Algorithmus nach endlich vielen Schritten ab, denn andernfalls erhielten wir eine unendliche Teilmenge

$$\{ N(a_i) \mid i = 1,2,3, \ldots \}$$

von M, die kein kleinstes Element besitzt.

(ii) Teilbarkeit. Für zwei Elemente $a,b \in R$ bedeute

$$a \mid b$$

(in Worten: a teilt b), daß es ein Element $c \in R$ gibt mit

$$b = a \bullet c.$$

2.5.6 Der größte gemeinsame Teiler

Seien R ein euklidischer Ring und

$$a,b \in R - \{0\}.$$

Dann gibt es ein Element $d \in R - \{0\}$ mit folgenden Eigenschaften.

(i) $d \mid a$ und $d \mid b$.

(ii) Für jedes Element $d' \in R$ mit $d' \mid a$ und $d' \mid b$ gilt $d' \mid d$.

Dieses Element ist bis auf Multiplikation mit Einheiten aus R eindeutig bestimmt und heißt größter gemeinsamer Teiler von a und b. Es gilt außerdem:

(iii) Es gibt Elemente $a',b' \in R$ mit

$$d = aa' + bb'.$$

Beweis. Wir wenden auf a und b den Euklidischen Algorithmus an und erhalten Elemente

$$a_0, \ldots, a_n \in R - \{0\}$$

Wir werden zeigen, $d = a_n$ hat die Eigenschafen (i) und (ii). Den Beweis führen wir durch Induktion nach n.
Im Fall $n = 1$ endet der Algorithmus bereits nach dem 0-ten Schritt, d.h. es gilt

$$a = qb + r \text{ mit } r = 0,$$

Dann hat aber $d = b = a_1$ tatsächlich die geforderten Eigenschaften.

Sei jetzt $n > 1$. Wir schreiben

(1) $$a = qb + r$$

mit ($a = a_0$, $b = a_1$ und) $r = a_2$. Durch Anwenden des Euklidischen Algorithmus auf b und r erhalten wir die Folge

$$a_1, \dots, a_n \in R - \{0\}.$$

Diese Folge besteht aus einem Element weniger als die ursprüngliche Folge (denn a_0 fehlt). Nach Induktionsvoraussetzung genügt $d = a_n$ den beiden folgenden

(i') d teilt b und r

(ii') Jeder gemeinsame Teiler von b und r ist ein Teiler von d.

Es reicht zu zeigen, d genügt auch den Bedinungen (i) und (ii).

Zu (i). Wegen (i') gilt

$$d \mid a = qb+r \text{ und } d \mid b.$$

Zu (ii). Ist d' ein gemeinsamer Teiler von a und b, so gilt

$$d' \mid b \text{ und } d' \mid r = a - qb.$$

Nach (ii') gilt $d' \mid d$.

Zu (iii). Die eben durchgeführte Induktion zeigt im Fall $n = 1$, d.h. im Fall $a = qb$, daß für den größten gemeinsamen Teiler $d = b$ gilt

$$d = 0 \bullet a + 1 \bullet b,$$

d.h. d ist eine ganzzahlige Linearkombination von a und b (wie behauptet). Im Fall $n > 1$ können wir annehmen, der größte gemeinsame Teiler d von b und r ist eine ganzzahlige Linearkombination von b und r, sagen wir

$$d = b \bullet b' + r \bullet r'.$$

Nun ist aber d auch ein größter gemeinsamer Teiler von a und b, und es gilt

$$\begin{aligned} d &= b \bullet b' + (a - qb) \bullet r' \\ &= a \bullet r' + b \bullet (b' - q \bullet r'). \end{aligned}$$

Wir haben gezeigt, ein größter gemeinsamer Teiler von a und b ist eine ganzzahlige Linearkombination von a und b.

Zum Abschluß des Beweises bleibt noch zu zeigen, daß die Eindeutigkeitsaussage gilt.

Zur Eindeutigkeit von d. Sei d' ein Element von $R-\{0\}$, das denselben Bedingungen wie d genügt. Weil d ein gemeinsamer Teiler von a und b ist, gilt dann

$$d' \mid d$$

und weil d' ein gemeinsamer Teiler von a und b ist, gilt

$$d \mid d'.$$

Es gibt also Elemente $e,f \in R$ mit

$$d' = ed \text{ und } d = fd'.$$

Damit gilt

$$(1 - ef)d = d - fd' = d - d = 0,$$

also $1 - ef = 0$, also $ef = 1$. Die Elemente e und f sind somit zueinander inverse Einheiten.

QED.

Bemerkungen

(i) Für je zwei größte gemeinsame Teiler d', d" von a und b gibt es, wie eben gezeigt, eine Einheit $e \in R$ mit

$$d" = ed' \text{ und } d' = e^{-1}d".$$

Wir führen die Bezeichnung

$$ggT(a,b)$$

für irgendeinen dieser größten gemeinsamen Teiler ein.

(ii) Die Definition von ggT ist zugegebenermaßen etwas ungenau. Eine fomal korretke (aber unbequeme) Definition wäre die folgende.

$$ggT(a,b) = dR^* \in R/R^*.$$

Dabei sei d irgendein größter gemeinsamer Teiler von a und b,

$$R/R^*$$

bezeichne die Menge der Orbits bezüglich der Operation

$$R^*\times R \longrightarrow R,\ (e,r) \mapsto er,$$

und

$$dR^* = R^*d = \{ed \mid e\in R^*\}$$

das Orbit des Elements d.

Beweis. Zu (i). trivial.

Zu (ii). Wir haben zu zeigen, die Abbildung

$$ggT: R \longrightarrow R/R^*,$$

hängt nicht von der speziellen Wahl des jeweiligen größten gemeinsamen Teilers ab.

Seien d' und d" zwei größte gemeinsame Teiler von a und b. Dann gibt es eine Einheit e mit

$$d" = ed'.$$

Also gilt

$$d"R^* = d'eR^* = d'R^*,$$

denn für Einheiten e gilt $eR^* = R^*$.

QED.

2.5 Hauptidealringe

2.6.1 Definition

Ein Hauptideal in einem kommutativen Ring R mit 1 ist ein Ideal, welches von nur einem Element erzeugt wird, d.h. ein Ideal von der Gestalt

$$I = aR \text{ mit } a\in R.$$

Ein Hauptidealring ist ein Integritätsbereich, dessen sämtliche Ideale Hauptideale sind.

2.6.2 Beispiel: Euklidische Ringe

Jeder Euklidische Ring ist ein Haupidealring.

Beweis. Sei R ein Euklidischer Ring mit der Höhenfunktion

$$H: R-\{0\} \longrightarrow M$$

und sei $I \subseteq R$ ein Ideal von R. Wir haben zu zeigen, I ist ein Hauptideal. O.B.d.A. sei I nicht das Nullideal,

$$I \neq \{0\}\ (= 0R).$$

Wir betrachten die Teilmenge

$$\{ H(x) \mid x\in I - \{0\} \}$$

von M. Da I nicht das Nullideal ist, ist diese nicht leer. Auf Grund der Definition des Euklidischen Rings besitzt diese Menge ein kleinstes Element, d.h. es gibt ein Element

(1) $$a \in I - \{0\} \text{ mit } H(a) \leq H(x) \text{ für jedes } x \in I - \{0\}.$$

Es reicht zu zeigen,

$$I = aR.$$

Wegen $a\in I$ gilt trivialerweise $I \supseteq aR$. Angenommen die umgekehrte Inklusion wäre falsch, d.h. es gibt ein Element in

$$I - aR.$$

Dann ist die Teilmenge

$$\{ H(x) \mid x \in I - aR \}$$

von M nicht-leer, enthält also ein kleinstes Element. Es gibt also ein Element

(2) $a' \in I-aR$ mit $H(a') \leq H(x)$ für jedes $x \in I - aR$.

Nach Definition des Euklidischen Rings gibt es Elemente $q, r \in R$ mit

$$a' = qa + r \text{ mit } r = 0 \text{ oder } H(r) < H(a).$$

Nach Konstruktion gilt

$$r = a' - qa \in I.$$

Nach Wahl von a nimmt H in allen Elementen von I-{0} einen Wert $\geq H(a)$ an (vgl. (1)). Wäre $r \neq 0$, so wäre der Wert von H in r aber kleiner. Also ist

$$r = 0.$$

also $a' = qa \in aR$ im Widerspruch zu (2). Dieser Widerspruch zeigt, I- aR muß leer sein, d.h. es gilt

$$I = aR.$$

QED.

2.6.3 Beispiel: $K[X_1,...,X_n]$ mit $n \geq 2$

Sei K ein Körper. Dann ist der Polynomring

$$R := K[X_1,...,X_n]$$

im Fall $n \geq 2$ kein Hauptidealring, also auch nicht Euklidisch.

Beweis. Es reicht zu zeigen,

$$I := (X_1,X_2) = X_1R + X_2R$$

ist kein Hauptideal. Angenommen, doch, d.h.

$$I = pR$$

mit einem Polynom $p \in R - \{0\}$. Dann gilt

$$X_1 , X_2 \in I = pR,$$

d.h. es gibt Polynome $q_1, q_2 \in R$ mit

$$X_1 = pq_1 \text{ und } X_2 = pq_2.$$

Als Polynom in X_i mit $i > 1$ hat X_1 den Grad 0, also hat auch pq_1 diesen Grad. Insbesondere hat p hat in X_i den Grad 0,

d.h.

$$\deg_{X_i} p = 0 \text{ für } i = 2,...,n.$$

Aus der zweiten Identität liest man in analoger Weise ab, daß p auch als Polynom in X_1 den Grad 0 hat. Insgesamt erhalten wir

$$p \in K - \{0\}$$

ist ein konstantes Polynom. Die Polynome von

$$I := (X_1,X_2) = X_1R + X_2R$$

sind aber sämtlich Polynome mit dem Absolutglied 0. Da p mit seinem Absolutglied übereinstimmt, folgt

$$p = 0.$$

Dann ist aber pR das Nullideal, also von $I := (X_1,X_2)$ verschieden.

Das steht aber im Widerspruch zur Wahl von p, d.h. zu I = pR.
QED.

Bemerkung
Der Nachweis der Existenz von Hauptidealringen, die nicht Euklidisch sind, ist schwieriger und wird hier nicht erbracht.

2.6 ZPE-Ringe

2.7.1 Definitionen

Sei R ein Integritätsbereich. Eine Nicht-Einheit $r \in R - \{0\}$ heißt zerlegbar oder auch reduzibel, wenn sie Produkt von zwei Nichteinheiten ist ,

$$r = ab \text{ mit } a,b \in R - R^*.$$

Andernfalls heißt r unzerlegbar oder auch irreduzibel. Eine Nicht-Einheit $r \in R- \{0\}$ heißt prim in R oder auch Primelement von R, wenn für beliebige Elemente $a,b \in R$ die folgende Implikation besteht.

$$r \mid ab \Rightarrow r \mid a \text{ oder } r \mid b.$$

Dabei bezeichne $a \mid b$ für zwei Elemente $a,b \in R$ die Teilbarkeit von b durch a, d.h es soll ein Element $c \in R$ geben mit $b = ac$.

Zwei Primelemente $a,b \in R$ heißen assoziiert, wenn es eine Einheit $e \in R^*$ gibt mit

$$a = eb.$$

Ein Integritätsbereich R heißt ZPE-Ring, wenn jede Nicht-Einheit von $R-\{0\}$ Produkt von endlich vielen Primelementen ist.

Bemerkungen

(i) Jedes Primelement ist unzerlegbar.

(ii) Ist R ein ZPE-Ring, so ist auch umgekehrt jedes unzerlegbare Element ein Primelement.

(iii) Eine Nicht-Einheit $r \in R - \{0\}$ eines Rings R ist genau dann ein Primelement, wenn das von r erzeugte Ideal $(r) = rR$ ein Primideal ist.

(iv) Seien zwei Zerlegungen einer Nicht-Einheit $r \in R-\{0\}$ in Produkte von Primelementen gegeben,

$$p_1 \bullet \ldots \bullet p_r = r = q_1 \bullet \ldots \bullet q_s .$$

Dann gilt r = s und es gibt eine Permutation $\sigma \in S_r$ mit

$$q_i \text{ assoziiert zu } p_{\sigma(i)} \text{ für } i = 1,\ldots,r.$$

Die Zerlegung in Primfaktoren ist somit, falls sie existiert, eindeutig bis auf die Reihenfolge der Primfaktoren und bis auf den Übergang zu assoziierten Primelementen. Dies ist auch der Grund für die Bezeichnung: ZPE bedeutet, die Zerlegung in Primelement ist eindeutig.

(v) In ZPE-Ringen kann man die Begriffe des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen (eindeutig bis auf die Multiplikation mit Einheiten) definieren. Es ist jedoch im allgemeinen nicht richtig, daß der größte gemeinsame Teiler zweier Elemente a, b Linearekombination von a und b ist.

Beweis Zu (i). Sei p Primelement und p = ab in R. Dann teilt p einen der Faktoren a oder b, sagen wir

$$p \mid a,$$

d.h.

$$a = pa' \text{ mit } a' \in R.$$

Es folgt

$$(1-a'b)p = p - pa'b = p - ab = 0.$$

Wegen $p \neq 0$ folgt $1 - a'b = 0$, d.h. $a'b = 1$, d.h. b ist Einheit.
Zu (ii). Sei a ein unzerlegbares Element. Da R ZPE-Ring sein soll, gibt es eine Zerlegung von a in Primfaktoren,

$$a = p_1 \bullet \ldots \bullet p_r.$$

Da a unzerlegbar ist, müssen alle Faktoren rechts mit höchstens einer Ausnahme Einheiten sein. Da Einheiten keine Primelemente sind, folgt r = 1. Also ist

$$a = p_1 ,$$

ein Primelement.

Zu (iii). Die Nicht-Einheit $r \in R - \{0\}$ ist genau dann ein Primelement, wenn die folgende Implikation besteht (für Elemente aus R):

$$r \mid ab \Rightarrow r \mid a \text{ oder } r \mid b.$$

Nun ist aber $x \mid y$ gleichbedeutend mit $y \in xR$. Die Implikation läßt sich also in der folgenden Gestalt schreiben.

$$ab \in rR \Rightarrow a \in rR \text{ oder } b \in rR.$$

In dieser Gestalt bedeutet die Implikation aber gerade, daß rR ein Primideal ist.

Zur Eindeutigkeitsaussage von (iv). Wir führen den Beweis durch Induktion nach r. Im Fall r = 1 , d.h.

$$p_1 = q_1 \bullet \ldots \bullet q_s ,$$

gilt wegen der Unzerlegbarkeit des Primelements p_1 (nach (i)) $s = 1$[15] also

$$p_1 = q_s.$$

Die Eindeutigkeitsaussage gilt hier also sogar in verschärfter Form.

Sei jetzt r > 1. Die Primzahl p_r teilt einen Faktor auf der rechten Seite, sagen wir $p_r \mid q_s$, d.h.

$$q_s = ap_r.$$

Da q_s als Primelement unzerlegbar ist, ist

$$a \in R^*$$

eine Einheit. Kürzen des gemeinsamen Faktors liefert

$$p_1 \bullet \ldots \bullet p_{r-1} = q_1 \bullet \ldots \bullet q_{s-2}(aq_{s-1}).$$

Der letzte Faktor aq_{s-1} rechts ist ein Primelement. Nach Induktionsvoraussetzung gilt

$$r - 1 = s - 1$$

und die Primelemente $p_1, \ldots, p_{r-1}$ sind assoziiert zu einer Permutation der Primelemente

$$q_1, \ldots, q_{s-2}(aq_{s-1}),$$

also auch zu einer Permutation der Primelemente $q_1, \ldots, q_{s-1}$. Mit anderen Worten, es gilt die Behauptung.

---

[15] weil Einheiten keine Primelemente sind.

QED.

2.7.2 Beispiel: Hauptidealringe

Jeder Hauptidealring ist ein ZPE-Ring.

Beweis. Sei R ein Hauptidealring.

1. Schritt. Jedes unzerlegbare Element von R ist Primelement.
Angenommen, die Aussage ist falsch. Dann gibt es eine Nicht-Einheit

$$r \in R - \{0\},$$

die unzerlegbar ist aber kein Primelement. Insbesondere ist

$$rR$$

kein Primideal, d.h. es gibt Elemente $a,b \in R$ mit

$$ab \in rR,\ a \notin rR,\ b \notin rR.$$

Die Ideale

$$I := (r,a) = rR + aR \text{ und } J := (r,b) = rR + bR$$

enthalten rR als echte Teilmenge. Zeigen wir, es gilt sogar

(1) $$rR \subset I \subset R \text{ und } rR \subset J \subset R.$$

Keines dieser beiden größeren Ideale ist gleich R, denn im Fall J = R wäre zum Beispiel IJ = IR = I. Auf jeden Fall wäre

$$IJ = \text{eines der beiden Ideale I oder J}$$

(welche das Ideal rR echt enthalten). Insbesondere wäre

$$IJ \supset rR \text{ (echte Inklusion).}$$

Es gilt aber

$$IJ = (r,a)(r,b) = (r^2, ar, rb, ab) \subseteq rR,$$

ein Widerspruch. Damit ist (1) bewiesen.

Da R ein Hauptidealring ist, gilt

$$I = sR \text{ für ein } s \in R,$$

d.h.

$$r \in rR \subset sR,$$

also

$$r = sx \text{ für ein } x \in R.$$

Das Element s ist keine Einheit, denn das Ideal sR = I ist von R verschieden. Das Element x ist keine Einheit, denn rR = sxR ist von sR verschieden. Damit ist aber r kein unzerlegbares Element. Dieser Widerspruch beweist die Aussage des ersten Schritts.

2. Schritt. Jede Nicht-Einheit ist Produkt von endlich vielen Primelementen.

Auf Grund des ersten Schritts reicht es zu zeigen, jede Nicht-Einheit ist das Produkt von endlich vielen unzerlegbaren Elementen. Wir führen die folgende Bezeichnung ein.

Ein schlechtes Element von R sei eine Nicht-Einheit, welche nicht als Produkt von endlich vielen unzerlegbaren Elementen geschrieben werden kann.

Wir haben zu zeigen, es gibt in R keine schlechten Elemente. Angenommen doch. Sei

$$r_1$$

ein schlechtes Element. Wir betrachten das Ideal

(2) r_1R

von R. Das Element r_1 muß zerlegbar sein (andernfalls wäre es Produkt unzerlegbarer Elemente, wobei die Anzahl der Faktoren gleich 1 ist),

(3) $r_1 = ab$ mit $a,b \in R\text{-}R^*$.

Mindestens einer der Faktoren a , b muß wieder schlecht sein. Sagen wir

$$r_2 = a$$

ist schlecht. Wegen $r_1 = ab = r_2b$ gilt

$$r_1R \subseteq r_2R.$$

Die Inklusion ist echt, denn andernfalls gibt es ein $c \in R$ mit

$$r_2 = r_1c = abc = r_2bc,$$

d.h. $0 = r_2 (1 - bc)$, d.h. $0 = 1 - bc$, d.h. b wäre eine Einheit im Widerspruch zu (3). Es gilt also

$$r_1R \subset r_2R.$$

Wir haben gezeigt, für jedes schleichte Element r_1 gibt es ein schlechtes Element r_2 mit

$$r_1R \subset r_2R.$$

Wir wenden diese Tatsache wiederholt an und erhalten eine unendliche echt aufsteigenden Kette von Idealen von R,

$$r_1 R \subset r_2R \subset ... \subset r_iR \subset ...$$

Das steht im Widerspruch zu der Tatsache, daß R als Hauptidealring noethersch ist. Es gibt also tatsächlich keine schlechten Elemente.

QED.

2.7.3 Beispiel: $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$

Der Ring

$$R = \mathbb{Z}+\mathbb{Z}\sqrt{-5} \cong \mathbb{Z}[X]/(X^2 + 5).$$

ist kein ZPE-Ring, also auch kein Hauptidealring und insbesondere kein Euklidischer Ring.

Beweis. Es gilt in R

(*) $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

2 ist keine Einheit von R. Es gilt

$$R/2R = \mathbb{Z}[X]/(2, X^2 + 5) = \mathbb{F}_2[X]/(X^2+\overline{5}),$$

und $X^2+\overline{5}$ ist als Polynom positiven Grades keine Einheit von $\mathbb{F}_2[X]$.

3 ist keine Einheit von R.

$$R/3R = \mathbb{Z}[X]/(3, X^2 + 5) = \mathbb{F}_3[X]/(X^2+\overline{5}),$$

und $X^2+\overline{5}$ ist als Polynom positiven Grades keine Einheit von $\mathbb{F}_3[X]$.

Unzerlegbarkeit von 2. Angenommen

$$2 = (a+b\sqrt{-5})(c - d\sqrt{-5}) \text{ mit } a,b,c,d \in \mathbb{Z}.$$

Dann gilt

$$2 = ac + 5bd$$

$$0 = bc - ad$$

.Insbesondere sind die Paare (a,b) und (c,d) proportional,

$$(c,d) = q(a,b) \text{ mit } q \in \mathbb{Q},$$

d.h.

$$2 = q\,(a^2 + 5b^2) \text{ und } 2q = c^2 + 5d^2$$

Wir schreiben q als Quotient teilerfremder ganzer Zahlen. Aus der ersten Identität folgt, der Zähler von q ist 1 oder 2.Aus der zweiten Identität folgt, der Nenner von q ist 1 oder 2. Für q gibt es also nur folgende Möglichkeiten.

$$q = 2,\ q = 1,\ q = 1/2.$$

Im ersten Fall folgt

$$1 = a^2 + 5b^2$$

also $b = 0$, $a = \pm 1$, d.h. $a+b\sqrt{-5}$ ist Einheit.
Im zweiten Fall folgt

$$2 = a^2 + 5b^2,$$

also $b = 0$, $2 = a^2$ was nicht möglich ist.
Im dritten Fall folgt

$$1 = c^2 + 5d^2,$$

also $d = 0$, $c = \pm 1$, d.h. $c - d\sqrt{-5}$ ist Einheit.
Unzerlegbarkeit von 3 . Der Beweis ist analog zum obigen Unzerlegbarkeitsbeweis für 2. Angenommen

$$3 = (a+b\sqrt{-5})(c - d\sqrt{-5}) \text{ mit } a,b,c,d \in \mathbb{Z}.$$

Dann gilt

(1) $3 = ac + 5bd$
(2) $0 = bc - ad$

.Insbesondere sind die Paare (a,b) und (c,d) proportional,

$$(c,d) = q(a,b) \text{ mit } q \in \mathbb{Q},$$

d.h.

$$3 = q\,(a^2 + 5b^2) \text{ und } 3q = c^2 + 5d^2$$

Wir wir schreiben q als Quotient teilerfremder ganzer Zahlen. Aus der ersten Identität folgt, der Zähler von q ist 1 oder 3.Aus der zweiten Identität folgt, der Nenner von q ist 1 oder 3. Für q gibt es also nur folgende Möglichkeiten.

$$q = 3,\ q = 1,\ q = 1/3.$$

Im ersten Fall folgt

$$1 = a^2 + 5b^2$$

also $b = 0$, $a = \pm 1$, d.h. $a+b\sqrt{-5}$ ist Einheit.
Im zweiten Fall folgt

$$3 = a^2 + 5b^2,$$

also $b = 0$, $3 = a^2$ was nicht möglich ist.
Im dritten Fall folgt

$$1 = c^2 + 5d^2,$$

also $d = 0$, $c = \pm 1$, d.h. $c - d\sqrt{-5}$ ist Einheit.
Abschluß des Beweises.
Angenommen R ist ein ZPE-Ring. Dann sind 2 und 3 Primelemente. Insbesondere müßte einer der Faktoren auf der rechten Seite von (*) durch 2 teilbar sein, d.h.

$$\frac{1}{2} + \frac{1}{2}\sqrt{-5} \text{ oder } \frac{1}{2} - \frac{1}{2}\sqrt{-5}$$

würde in $R = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ liegen, was offensichtlich[16] nicht der Fall ist.

---

[16] Eine komplexe Zahl $a + b\sqrt{-5}$ liegt genau dann in R, wenn a und b ganze Zahlen sind (denn 1 und $\sqrt{-5}$ sind linear unabhängig über $\mathbb{Z}$.

QED.

Bemerkung

Unser nächstes Ziel ist der Beweis der ZPE-Eigenschaft für Polynomringe in mehreren Unbestimmten über einem Körper. Wir werden die allgemeinere Aussage beweisen, daß für jeden ZPE-Ring R auch die Polynom-Algebra R[X] ein ZPE-Ring ist.

Der Beweis erfordert einige Vorbereitungen. Wir werden dabei ganz wesentlich benutzen, daß Q(R)[X] euklisch, also insbesodere ein ZPE-Ring ist.

2.7.4 Die Ordnung eines Elements des

Seien R ein ZPE-Ring, K = Q(R) dessen Quotientenkörper und

$$p$$

eine Primelement von R. Da R ein ZPE-Ring ist, also nullteilerfrei, so ist die natürliche Abbildung

$$R \longrightarrow K, r \mapsto r/1,$$

injektiv, d.h. R läßt sich mit einem Teilring des Körpers K identifizieren (was wir im folgenden tun werden). Da R ein ZPE-Ring ist, hat jedes Element $x \in K-\{0\}$ die Gestalt

$$x = e \bullet p_1^{n_1} \bullet \ldots \bullet p_r^{n_r}$$

mit einer Einheit $e \in R^*$, paarweise nicht-assoziierten Primelementen p_i und ganzen Zahlen $n_i \in \mathbb{Z}$. Dabei sind die p_i bis auf die Reihenfolge und bis auf den Übergang zu assoziierten Primelementen eindeutig bestimmt. Für gegebenes p_i ist der Exponent n_i eindeutig festgelegt.

Ist p ein Primelement von R, welches zu p_i assoziert ist, so schreiben wir

$$\mathrm{ord}_p(x) = n_i$$

und nennen diese ganze Zahl auch <u>Ordnung</u> von x bezüglich p. Im Fall x = 0 setzen wir

$$\mathrm{ord}_p(x) = \infty.$$

Bemerkungen

(i) Für jedes $x \in R$ ist $\mathrm{ord}_p(x)$ die größte ganze Zahl n mit $p^n \mid x$,

$$\mathrm{ord}_p(x) = \sup \{ n \in \mathbb{Z} \mid p^n \mid x \}.$$

(ii) Nach Definiton gilt

$$\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y).$$

(iii) Durch die beiden Eigenschaften (i) und (ii) ist die Ordnungsfunktion eindeutig bestimmt. Sie bieten also die Möglichkeit einer alternativen Definiton.

(iv) Die Ordnungsfunktionen zu assoziierten Primelementen sind gleich, d.h.

$$\mathrm{ord}_p(x) = \mathrm{ord}_{p'}(x) \text{ für alle } x$$

falls p und p' assoziierte Primideale sind.

(v) Bezeiche $\mathbb{P}(R)$ die Menge der Klassen assoziierter Primelemente von R. Dann kann man die Ordnungsfunktion für gegebenes $x \neq 0$ als Abbildung

$$\mathbb{P}(R) \longrightarrow \mathbb{Z}, x \mapsto \mathrm{ord}_p(x),$$

(vi) Für jedes Element $x \in K - \{0\}$ gilt

$$x = e \bullet \prod_{\wp = [p] \in \mathbb{P}(R)} p^{\mathrm{ord}_p x}.$$

Dabei durchlaufe $\wp$ die Menge der Klassen äquivalenter Primelemente von R und p bezeichne ein irgendwie gewähltes Element von $\wp$. Der Faktor e bezeichne eine Einheit von R (die von der speziellen Wahl der Repräsentanten p von $\wp$ abhängt.

(v) Die Formel von (vi) kann man auch auf den Fall $x = 0$ verallgemeinern, wenn man vereinbart

$$p^{\infty} = 0.$$

2.7.5 Der größte gemeinsame Teiler

Seien R ein ZPE-Ring, K = Q(R) dessen Quotientenkörper und

$$x_1, \dots, x_r \in K$$

endlich viele Elemente. Wir schreiben jedes x_i in der Gestalt

$$x_i = e \bullet \prod_{\wp=[p]\in\mathbb{P}(R)} p^{\operatorname{ord}_p x_i}.$$

und definieren

$$n(p) := \min \{\operatorname{ord}_p x_i \mid i = 1,\dots,r\}.$$

Das Element

$$(1) \qquad \operatorname{ggT}(x_1, \dots, x_r) := \prod_{\wp=[p]\in\mathbb{P}(R)} p^{n(p)}$$

heißt dann <u>größter gemeinsamer Teiler</u> von $x_1, \dots, x_r$.

Bemerkungen

(i) Die Definition des größten gemeinsamen Teilers hängt von der Wahl der Repräsentanten p der Klassen $\wp$ im Produkt (1) ab und ist nur bis auf einen Faktor, der eine Einheit in R ist, eindeutig.

(ii) Eine korrektere Definiton wäre

$$(1) \qquad \operatorname{ggT}(x_1, \dots, x_r) := \prod_{\wp=[p]\in\mathbb{P}(R)} p^{n(p)} \bmod R^*$$

Dabei bezeichne der Ausdruck recht gerade das Orbit des Elements (1) bei der Operation

$$R^* \times K \longrightarrow K, (e, x) \mapsto ex.$$

(iii) Wenn man sich auf die Definition des ggT von Elementen aus der multiplikativen Gruppe $K^* := K - \{0\}$ beschränkt, so kann man den ggT auch definieren als das Bild von (1) beim natürlichen Gruppen-Homomorphismus

$$K^* \longrightarrow K^*/R^*.$$

(iv) Wir werden hier die naive Definiton (1) benutzen, müssen aber stets beachten, der ggT ist nur bis auf Multiplikation mit einer Einheit festgelegt. Wir geben hier noch einige (offensichtliche) Eigenschaften des größten gemeinsamen Teilers an.

(v) Nach Konstruktion gilt, falls mindestens ein x_i von Null verschieden ist:

1. $\operatorname{ggT}(x_1, \dots, x_r) \neq 0$.

2. $x_i / \operatorname{ggT}(x_1, \dots, x_r) \in R$ für $i = 1,\dots,r$.

(vi) $\operatorname{ggT}(x_1, \dots, x_r)$ liegt in R, falls jedes x_i in R liegt.

(vii) $\operatorname{ggT}(cx_1, \dots, cx_r) = c \bullet \operatorname{ggT}(x_1, \dots, x_r)$.

(viii) $\operatorname{ggT}(x_1, \dots, x_r)$ ist im allgemeinen keine Linearkombination der $x_1, \dots, x_r$.

2.7.6 Der Inhalt eines Polynoms

Seien R ein ZPE-Ring, K := Q(R) dessen Quotientenkörper und

$$f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$$

ein Polynom mit Koeffizienten aus K. Dann heißt

$$I(f) := ggT(a_0,...,a_n) \in K$$

Inhalt des Polynoms f.

Bemerkungen

(i) Der Inhalt eines Polynom ist nur bis auf einen Faktor aus R* festgelegt.

(ii) Für jedes von Null verschiedene Polynom $f(X) \in K[X]$ gilt

$$f(X)/I(f) \in R[X]$$

2.7.7 Lemma von Gauß

Seien R ein ZPE-Ring, K := Q(R) dessen Quotientenkörper und

$$f, g \in K[X]$$

zwei Polynome einer Unbestimmten mit Koeffizienten aus K. Dann gilt

$$I(fg) = I(f) \bullet I(g).$$

Bemerkungen

(i) Die Aussage ist so zu interpretiern, daß die beiden Seiten sich nur um einen Faktor aus R* unterscheiden.

(ii) Alternativ können man auch sagen, die Definition von einem der drei auftretenden Inhalt läßt sich so um einen Faktor aus R* abändern, daß die behauptete Gleichheit gilt.

Beweis des Lemmas. Wir schreiben

$$f = \alpha f_1 \text{ und } g = \beta g_1 \text{ mit } \alpha = I(f) \text{ und } \beta = I(g).$$

Dann gilt

$$I(f_1) = 1 = I(g_1)$$

und

$$I(fg) = I(\alpha\beta f_1 g_1) = \alpha\beta \bullet I(f_1 g_1).$$

Es reicht also zu zeigen, daß $f_1 g_1$ den Inhat 1 hat. Wir können also annehmen, die Polynome

$$f(X) = a_n X^n + ... + a_0 \quad \text{mit } a_n \neq 0$$

$$g(X) = b_m X^m + ... + b_0 \text{ mit } b_m \neq 0$$

haben den Inhalt 1 (und liegen damit insbesondere in R[X]). Wir haben zu zeigen fg hat den Inhalt 1, d.h. es gibt kein Primelement p, das alle Koeffizienten von fg teilt.

Angenommen, es gibt doch ein solches Primelement $p \in R$. Wir führen folgende Bezeichnungen ein.

$$r := \max \{ i \mid a_i \neq 0 \text{ und } p \nmid a_i \}$$

$$s := \max \{ j \mid b_j \neq 0 \text{ und } p \nmid b_j \}$$

Da f den Inhalt 1 hat, also nicht alle Koeffizienten Vielfache von p sind, ist r wohldefiniert. Analog ist auch s wohldefiniert. Betrachten wir den Koeffizienten c_{r+s} von X^{r+s} in fg. Es gilt

$$c_{r+s} = ... + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + ...$$

Nach Konstruktion sind alle Summanden rechts durch p teilbar, ausgenommen der Summand $a_r b_s$.[17] Deshalb ist c_{r+s} nicht durch p teilbar, im Widerspruch zur Wahl von p.
QED.

2.7.8 Faktorzerlegung von Polynomen über R und über Q(R)

Seien R ein ZPE-Ring, K:=Q(R) dessen Quotientenkörper und

$$f(X) \in R[X] - \{0\}$$

ein Polynom. Besitzt f(X) eine Zerlegung in Faktoren kleineren Grades über K,

$$f(X) = g(X)h(X) \text{ mit } g(X), h(X) \in K[X] - K,$$

so besitzt f(X) auch eine solche Zerlegung über R. Genauer, es gilt

$$f(X) = c \bullet g_1(X)h_1(X)$$

mit

$$g_1(X) := g(X)/I(g) \in R[X]$$

$$h_1(X) := h(X)/I(h) \in R[X]$$

$$c := I(g)I(h) \in R.$$

Beweis. Die einzige nicht-triviale Aussage ist die Aussage, daß c in R liegt. Diese folgt aber aus dem Lemma von Gauß, nach welchem c bis auf einem Faktor aus R* gleich

$$I(gh) = I(f)$$

ist. Der Inhalt eines Polynoms über R liegt aber in R.
QED.

2.7.9 Die ZPE-Eigenschaft beim Übergang zu Polynomringen

Sei R ein ZPE-Ring mit dem Quotientenkörper K = Q(R).Dann ist auch der Ring

$$R[X]$$

der Polynome über R in einer Unbestimmten X ein ZPE-Ring. Die Primelemente von R[X] sind gerade die Primelement von R zusammen mit den Polynomen

$$p(X) \in R[X]$$

die den folgenden beiden Bedingungen genügen..

1. $I(p) = 1$.
2. p ist als Element von K[X] irreduzibel.

Beweis. Sei f(X) ein Element von R[X]. Unter Verwendung der Zerlegung in Primfaktoren in K[X] erhalten wir eine Zerlegung

(1) $$f(X) = c \bullet p_1(X) \bullet \ldots \bullet p_r(X).$$

mit $c \in K$ und Primelementen $p_i(X)$ von K[X]. Indem wir $p_i(X)$ durch $p_i(X)/I(p_i)$ und c durch $cI(p_i)$ ersetzen, erreichen wir, daß gilt

$$I(p_i) = 1$$

also insbesondere

$$p_i(X) \in R[X].$$

---

[17] Alle Summanden links von $a_r b_s$ sind durch p teilbar, weil der erste Faktor es ist. Alle Summanden rechts von $a_r b_s$ sind durch p teilbar, weil der zweite Faktor es ist.

Nach dem Lemma von Gauß gilt dann in der Zerlegung (1) auch

$$c = I(\text{RHS von (1)}) = I(\text{LHS von (1)}) = I(f) \in R,$$

d.h. (1) ist eine Faktorzerlegung über R. Da R ein ZPE-Ring ist, können wir c auch als Produkt von Primelementen aus R schreiben.
Wir haben gezeigt, jedes Element von R[X] - {0} ist Produkt von endlich vielen Elementen, die nach der Aussage des Satzes Primelement sind.
Zum Abschluß des Beweises reicht es also zu zeigen, die angegebenen Elemente sind tatsächlich Primelemente und es gibt keine weiteren. Zu zeigen sind also folgende Aussagen:

1. Jedes Primelement von R ist auch eines von R[X].
2. Jedes irreduzible Polynom $p \in K[X]$ mit dem Inhalt 1 ist ein Primelement von R[X].
3. Es gibt keine weiteren Primelemente in R[X].

Zu 1. Sei p ein Primelement von R und sei $p \mid fg$ mit $f,g \in R[X]$. Dann gilt

$$p \mid I(fg) = I(f)I(g)$$

(nach dem Lemma von Gauß), also $p \mid I(f)$ oder $p \mid I(g)$, also $p \mid f$ oder $p \mid g$.
Zu 2. Da K[X] ein ZPE-Ring ist, ist p ein Primelement von K[X]. Wegen I(p) = 1 gilt außerdem

$$p \in R[X].$$

Sei jetzt

$$p \mid fg \text{ mit } f,g \in R[X].$$

Dann gilt, weil p Primelement von K[X] ist,

$$p \mid f \text{ oder } p \mid g \text{ (in K[X])},$$

d.h. f oder g hat eine Faktorzerlegung über K, wobei einer der Faktoren gleich p ist. Nach 2.7.8 gibt es dann aber auch eine Faktorzerlegung von f bzw. g über R, wobei einer der Faktoren p ist. Mit anderen Worten,

$$p \mid f \text{ oder } p \mid g \text{ (in R[X])}.$$

Also ist p ein Primelement von R[X].
Zu 3. Sei p ein Primelement von R[X], wie wir oben gezeigt haben, gibt es dann eine Darstellung von p als Produkt von Primelementen der in 1 und 2 beschriebenen Typen. Weil p selbst Primelement ist, muß die Anzahl der Faktoren in dieser Zerlegung gleich 1 sein, d.h. p ist Primelement eines in 1 oder 2 beschriebenen Typs.
QED.

2.7.10 Polynomringe über einem Körper

Für jeden Körper K ist der Polynomring

$$K[X_1,...,X_n]$$

ein ZPE-Ring.
Beweis. Das folgt unmittelbar aus 2.7.9 und der Tatsache, daß Polynomringe in einer Unbestimmten über K Euklidische Ring sind.
QED.

2.7.11 Eisenstein-Polynome

Seien R ein ZPE-Ring,

$$p \in \mathbb{P}(R)$$

ein Primelement von R und

$$f(X) = a^nX^n + a_{n-1}X^{n-1} + ... + a_0 \in R[X]$$

ein Polynom des Grades n mit Koeffizienten aus R. Dann heißt R Eisenstein-Polynom bezüglich p,
wenn die folgenden Bedingungen erfüllt sind.

1. $p^2 \nmid a_0$.
2. $p \mid a_i$ für $i = 0, 1, \ldots, n-1$.
3. $p \nmid a_n$,

Ein Polynom von R[X] heißt Eisenstein-Polynom, wenn es Eisensten-Polynom bezüglich irgendeines Primelements von R ist.

2.7.12 Irreduzibilitätskriterium von Eisenstein

Sei R ein ZPE-Ring mit dem Quotientenkörper K = Q(R). Dann ist jedes Eisenstein-Polynom von R[X] irreduzibel in K[X].

Beweis. Sei

$$f(X) = a^nX^n+a_{n-1}X^{n-1}+...+a_0 \in R[X]$$

ein Eisenstein-Polynom des Grades n bezüglich des Primelements

$$p \in \mathbb{P}(R).$$

Wir können f durch den Inhalt I(f) teilen und somit annehmen, daß f den Inhalt

$$I(f) = 1$$

besitzt. Wenn f(X) über K in Faktoren eines Grades < n zerfällt, so gilt nach 2.7.8 dasselbe über R,

$$f(X) = g(X) \bullet h(X) \text{ mit } g(X), h(X) \in R[X] - K.$$

Wir schreiben

$$g(X) = b_uX^u+...+b_0, b_u \neq 0, u > 0,$$

$$g(X) = c_vX^v+...+c_0, c_v \neq 0, v > 0.$$

Sei

$$\rho: R \longrightarrow R/(p), a \mapsto a + pR$$

der natürliche Homomorphismus. Er definiert einen Homomorphismus

$$: R[X] \longrightarrow (R/(p))[X], p(X) \mapsto p^\rho(X),$$

der in jedem Polynom $p(X) \in R[X]$ alle Koeffizienten durch deren Bilder bei ρ ersetzt. Mit $f = g \bullet h$ gilt dann auch

$$f^\rho = g^\rho \bullet h^\rho \text{ in } (R/(p))[X] \qquad (\subseteq Q(R/(p))[X])$$

Man beachte, (p) ist ein Primideal von R, d.h. Q(R/(p)) ein Körper. Da f ein Eisenstein-Polynom bezüglich p ist, gilt

$$f^\rho = \rho(a_n)X^n$$

Wegen der Eindeutigkeit der Zerlegung in Primfaktoren im Ring

$$Q(R/(p))[X]$$

sind somit alle Primteiler von f^ρ assoziiert zu X. Also gilt

$$g^\rho(X) = \rho(b_u)X^u \text{ und } h^\rho = \rho(c_v)X^v,$$

also

$$b_0 \equiv 0 \pmod p \text{ und } c_0 \equiv 0 \pmod p$$

also

$$a_0 = b_0c_0 \equiv 0 \pmod{p^2}.$$

Letzteres steht aber im Widerspruch zu der Annahme, daß f ein Eisenstein-Polynom bezüglich p sein soll. Also ist f irreduzibel in K[X].

QED.

Beispiel 1

$f(X) = X^2 - 2 \in \mathbb{Z}[X]$ ist ein Eisenstein-Polynome bezüglich 2, also irreduzibel in $\mathbb{Q}[X]$.

Beispiel 2

$f(X) = X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ ist reduzibel in $\mathbb{Q}(\sqrt{2})[X]$.

2.7.13 Reduktionskriterium der Irreduzibilität

Seien R und S Integritätsbereiche mit den Quotientenkörpern

$$K = Q(R) \text{ und } L = Q(S)$$

und

$$h: R \longrightarrow S$$

ein Homomorphismus von Ringen mit 1. Weiter sei

$$f(X) \in R[X]$$

ein Polynom mit

$$f^h(X) \neq 0, \deg f^h(X) = \deg f(X), f^h(X) \text{ irreduzibel in } L[X]$$

wenn f^h das Bild von f beim Homomorphismus

$$R[X] \longrightarrow S[X], p(X) \mapsto p^h(X),$$

bezeichnet, der in jedem Polynom von R[X] die Koeffizienten durch deren Bilder bei h ersetzt.

Dann läßt sich f(X) über R nicht in ein Produkt von Polynomen kleineren Grades zerlegen.

Beweis. Aus der Existenz einer solchen Zerlegung, sagen wir

$$f(X) = g(X) \bullet h(X) \text{ in } R[X],$$

folgte

$$f^h(X) = g^h(X) \bullet h^h(X) \text{ in } L[X],$$

was nicht möglich ist, da f^h irreduzibel sein soll.

QED.

Beispiel 1

Das Polynom

$$f(X) = X^2 + X + 1 \in \mathbb{Z}[X]$$

ist irreduzibel in $\mathbb{Q}[X]$.

Beweis. Wir betrachten den natürlichen Homomorphismus

$$h: \mathbb{Z} \longrightarrow \mathbb{Z}/(2) = \mathbb{F}_2.$$

Wäre f(X) reduzibel, so würde dasselbe für

$$f^h(X) = X^2 + X + 1 \in \mathbb{F}_2[X].$$

gelten. Das Polynom wäre über $\mathbb{F}_2$ das Produkt von zwei linearen Polynomen, würde also in $\mathbb{F}_2$ eine Nullstelle besitzen. Das ist aber nicht so:

$f^h(0) = 1 \neq 0$

$f^h(1) = 1 + 1 + 1 = 1 \neq 0.$

QED.

Beispiel 2 (weglassen)

Das Polynom

$$f(X) = X^5 - 5X^4 - 6X - 1 \in \mathbb{Z}[X]$$

ist irreduzibel in $\mathbb{Q}[X]$.

Beweis. Wir betrachten den natürlichen Homomorphismus

$$h: \mathbb{Z} \longrightarrow \mathbb{Z}/(2) = \mathbb{F}_2.$$

Es gilt

$$f^h(X) = X^5 + X^4 + 1 \in \mathbb{F}_2[X].$$

Falls f^h in ein Produkt von Faktoren kleineren Grades zerfällt, so hat einer der Faktoren einen Grad ≤ 2. Der Grad 1 ist nicht möglich, denn dann hättte f^h in $\mathbb{F}_2$ ein Nullstelle. Bleibt noch der Fall, daß f in einen quadratischen Faktor und einen Faktor dritten Grades zerfälllt (über $\mathbb{Q}$, also über $\mathbb{Z}$):

$$f(X) = (X^2+aX + b)(X^3+cX^2+dX+e),\ a,b,c,d,e \in \mathbb{Z}.$$

Wegen be = -1 folgt

$$b = -e = \pm 1,$$

sagen wir

$$b = \varepsilon \text{ und } e = -\varepsilon.$$

d.h.

$$\begin{aligned} f(X) &= (X^2+aX + \varepsilon)(X^3+cX^2+dX-\varepsilon) \\ &= X^5 + X^4(c+a) + X^3(\varepsilon+ac+d) + X^2(-\varepsilon+ad+\varepsilon c) + X(-\varepsilon a+\varepsilon d) - 1. \end{aligned}$$

Damit ist

$$\begin{aligned} a + c &= -5 \\ \varepsilon+ac+d &= 0 \\ -\varepsilon+ad+\varepsilon c &= 0 \\ -\varepsilon a+\varepsilon d &= -6 \end{aligned}$$

Aus der ersten und letzten Gleichung folgt c = -5-a und d = -6ε+a, also

$$\begin{aligned} \varepsilon-5a-a^2-6\varepsilon+a &= 0 \\ -\varepsilon-6a\varepsilon+a^2-5\varepsilon-a\varepsilon &= 0 \end{aligned}$$

d.h.

$$\begin{aligned} &(I) \quad a^2+4a+5\varepsilon = 0 \\ &(II) \quad a^2-7a\varepsilon-6\varepsilon = 0 \end{aligned}$$

d.h. (Differenz):

$$(4+7\varepsilon)a + 11\varepsilon = 0$$

Der Fall ε = +1:11a + 11 = 0 liefert a = -1 (keine Lösung von (I) ist nicht möglich.
Der Fall ε = -1: -3a - 11 = 0 ist nicht möglich (3 ist kein Teiler von 11).
QED.

Bemerkung

Die nachfolgenden Ergebnisse stehen nicht unmittelbar in Zusammenhang mit ZPE-Ringen, werden jedoch später benötigt.

2.7.14 Die Ableitung eines Polynoms

Für jeden kommutativen Ring R mit 1 definieren wir die Abbildung

$$D = \partial/\partial X: R[X] \longrightarrow R[X],\ f(X) = \sum_{i=0}^{n} a_i X^i \mapsto f'(X) := \sum_{i=0}^{n} i a_i X^{i-1}.$$

Wie in der reellen Analysis heißt Df <u>Ableitung</u> von f nach X. Es gelten die üblichen Rechenregeln:

1. $D(f+g) = Df + Dg$
2. $D(fg) = (Df)\bullet g + f\bullet Dg$
3. $Df(g_1(X),...,g_n(X)) = \sum_{i=1}^{n} \frac{\partial f}{\partial Y_i}(g_1(X),...,g_n(X))\bullet\frac{\partial g}{\partial X}(X)$ für $f \in R[Y_1,...,Y_n]$

Insbesondere ist D eine R-lineare Abbildung (nach 1. und 2. mit deg f = 0).
Beweis. Zu 1: trivial.
Zu 2: beide Seiten sind additiv in f und g. Es reicht den Spezialfall

$$f(X) = rX^a, g(X) = sX^b$$

zu betrachten, in welchem die Behauptung trivial ist.
Zu 3: Beide Seiten sind R-linear in f. Es reicht den Fall

$$f = Y_1^{k_1} \bullet \ldots \bullet Y_n^{k_n}$$

zu betrachten, in welchem die Behauptung unmittelbar aus 2. folgt.
QED.

2.7.15 Ableitungen und mehrfache Nullstellen

Seien K ein Körper, $f(X) \in K[X]$ ein Polynom und $a \in K$ eine Nullstelle von f. Dann sind folgende Aussagen äquivalent.

(i) a ist eine mehrfache Nullstelle von f(X), d.h. es gilt
$f(X) = (X-a)^m g(X)$ mit $m > 1$ und $g(X) \in K[X]$.

(ii) $f'(a) = 0$.

Beweis. (i) $\Rightarrow$ (ii). Aus

$$f(X) = (X-a)^m g(X)$$

folgt

$$\frac{\partial f}{\partial X}(X) = m(X-a)^{m-1} g(X) + (X-a)^m g'(X)$$

also

$$(1) \qquad f'(a) = \frac{\partial f}{\partial X}(a) = m(a-a)^{m-1} g(a) + (a-a)^m g'(a).$$

Wegen $m > 1$ steht auf der rechten Seite Null.

(ii) $\Rightarrow$ (i). Sei $f(X) = \sum_{i=0}^{n} a_i X^i$. Wegen $f(a) = 0$ gilt

$$\begin{aligned} f(X) &= f(X) - f(a) \\ &= \sum_{i=0}^{n} a_i (X^i - a^i) = \sum_{i=0}^{n} a_i (X-a)(X^{i-1} + aX^{i-2} + a^2 X^{i-3} + \ldots + a^{i-1}) \\ &= (X-a) \bullet \text{Polynom aus } K[X]. \end{aligned}$$

Wir können also schreiben

$f(X) = (X-a)^m g(X)$ mit $m \geq 1$ und $g(X) \in K[X]$.

Wir können damit m so groß wählen, daß $g(a) \neq 0$ gilt. Es reicht zu zeigen,

$$m > 1.$$

Wie oben gezeigt, gilt (1). Nach Voraussetzung ist die linke Seite gleich Null, d.h.

$$0 = m(a-a)^{m-1} g(a) + (a-a)^m g'(a).$$

Wegen $m \geq 1$ ist der zweite Summand Null, also ist es auch der erste. Wäre $m = 1$, so würden wir erhalten

$$0 = g(a),$$

im Widerspruch zur Wahl von g.
QED.

*2.8 Ganze Erweiterungen

2.8.1 Ganze Ringhomomorphismen ("Erweiterungen")

Sei $h:R \longrightarrow S$ ein Homomorphismus von kommutativen Ringen mit 1. Ein Element $x \in S$ heißt ganz über R (bezüglich h), wenn es ein Polynom $f \in R[X]-\{0\}$ mit dem höchsten Koeffizienten 1 gibt mit

$$f^h(x) = 0.$$

Der Homomorphismus $h: R \longrightarrow S$ heißt ganz, wenn jedes Element von S ganz ist über R bezüglich h.

Bemerkung

Sei $h: R \longrightarrow S$ ein Homomorphismus von kommutativen Ring mit 1. Dann ist S ein R-Modul bezüglich der Modul-Multiplikation

$$R \times S \longrightarrow S, (r,s) \mapsto h(r) \bullet s.$$

2.8.2 Kriterium für die Ganzheit eines Elements

Seien $h:R \longrightarrow S$ ein Homomorphismus von kommutativen Ringen mit und $x \in S$ ein Element. Dann sind folgende Aussagen äquivalent.

(i) x ist ganz über R bezüglich h.

(ii) Der Ring h(R)[x] ist ein endlich erzeugter R-Teilmodul von S.

(iii) Es gibt einen endlich erzeugten Teilmodul $M \subseteq S$ mit

$$xM \subseteq M \text{ und } 1 \in M.$$

Beweis. (i) $\Rightarrow$ (ii). Nach Voraussetzung besteht eine Relation der Gestalt

(1) $$x^n + h(a_1)x^{n-1} + ... + h(a_n) = 0 \text{ mit } a_i \in R.$$

Sei

$$M := R \bullet x^0 + R \bullet x + R \bullet x^2 + ... + R \bullet x^{n-1}$$

Dann ist M ein endlich erzeugter R-Modul mit

$$h(R) \bigcup \{x\} \subseteq M \subseteq h(R)[x].$$

Es reicht zu zeigen, rechts gilt das Gleichheitszeichen. Der Ring

$$h(R)[x]$$

ist der kleinste Teilring von S, der h(R) und x enthält. Deshalb reicht es zu zeigen,

$$M \text{ ist ein Teilring von } S.$$

Offensichtlich ist M eine additive Untergruppe von S. Es reicht also zu zeigen, die Produkt von zwei Elementen aus M liegt wieder in M. Da M ein R-Modul ist, reicht es zu zeigen, das Produkt von je zwei der Erzeugenden x^i liegt wieder in M,

$$x^i \bullet y^j \in M \text{ für } i,j = 0,...,n-1.$$

Zum Beweis kann man annehmen, i = 1. Dann ist die Aussage aber für j=0,..., n-2 trivial:

$$x \bullet x^j = x^{j+1} \in M.$$

Sei also h = n-1. Wir haben zu zeigen $x^n \in M$. Das gilt aber wegen (1).

(ii) $\Rightarrow$ (iii). trivial: M = h(R)[x] ist ein solcher Modul.

(iii) $\Rightarrow$ (i). Sei

$$M = Rm_1 + ... + Rm_s$$

ein Teilmodul von S mit $xM \subseteq M$ und $1 \in M$. Wegen $xM \subseteq M$ gilt

$$xm_i = \sum_{j=1}^{s} a_{ij} m_j \text{ mit } a_{ij} \in R,$$

d.h.

$$0 = \sum_{j=1}^{s} (x\delta_{ij} - a_{ij}) m_j \text{ für } i = 1,...,s,$$

wobei δ_{ij} das Kronecker-Symbol bezeichne. Wir fixieren jetzt einen Index ℓ betrachten die s×s- Matrix $(x\delta_{ij} - a_{ij})$, multiplizieren die i-te Gleichung mit dem Minor $A_{i\ell}$ und bilden die alternierende Summe. Nach dem Entwicklungssatz für Determinanten erhalten wir

$$0 = \det(x\delta_{ij} - a_{ij}) \bullet m_\ell.$$

Diese Relation gilt für jedes m_ℓ und, da die m_ℓ den Modul M erzeugen, für jedes Element von m,

$$\det(x\delta_{ij} - a_{ij}) \bullet m = 0 \text{ für jedes } m \in M.$$

Wegen $1 \in M$ ist damit auch

$$\det(x \bullet h(\delta_{ij}) - h(a_{ij})) = 0.$$

Nun ist

$$f(x) = \det(\delta_{ij} \bullet X - a_{ij}) \in R[X]$$

ein Polynom vom Grad s mit dem höchsten Koeffizienten 1 und es gilt

$$f^h(x) = \det(x \bullet h(\delta_{ij}) - h(a_{ij})) = 0.$$

Mit anderen Worten x ist ganz über R.
QED.

2.8.3 Beispiele

(i) Der Ring der ganzen Gaußschen Zahlen ist ganz über $\mathbb{Z}$ (weil er als $\mathbb{Z}$-Modul endlich erzeugt wird).

(ii) Der Ring $\mathbb{Z}[\sqrt[3]{2}]$ von 2.1.7 ist ganz über $\mathbb{Z}$ (aus demselben Grund).

(iii) Die Ringe von 2.1.8 Beispiel 3 sind ganz über R (aus demselben Grund). Explizit: ist S ein kommutativer Ring mit 1,

$$R \subseteq S$$

ein Teilring mit 1 und $x \in S$ ein über R ganzes Element, so ist

$$R[x] \text{ ganz über } S.$$

Denn R[x] ist dann ein endlich erzeugter R-Modul der die 1 enthält und jedes Element y von R[x] hat die Eigenschaft

$$y \bullet R[x] \subseteq R[x]$$

2.8.4 Die ganze Abschließung

Sei $h: R \longrightarrow S$ ein Homomorphismus von Ringen mit 1. Dann ist die Menge

$$\overline{R} := \{ x \in S \mid x \text{ ist ganz über R bezüglich h} \}$$

ein Teilring von S. Er heißt ganze Abschließung von R in S.

Ist R ein Teilring von S und h die natürliche Einbettung $R \longrightarrow S$, so sagt man, R ist ganz abgeschlossen in S, falls $R = \overline{R}$ gilt.

Beweis. Wir können R durch $h(R) \subseteq S$ ersetzen und deshalb annehmen,

$$R \subseteq S$$

(und h ist die natürliche Einbettung). Wir haben zu zeigen, mit je zwei Elementen

$$x,y \in \overline{R}$$

liegen auch Produkt und Summe in $\overline{R}$. Weil x ganz ist über R, ist R[x] ein endlich erzeugter R-Modul,

$$R[x] = R\omega_1 + ... + R\omega_s$$

Weil das Element y ganz ist über R, ist es auch ganz über R[x], d.h.
R[x,y] ist ein endlich erzeugter R[x]-Modul,

$$R[x, y] = R[x]\eta_1 + ... + R[x]\eta_s.$$

Zusammen erhalten wir, daß R[x,y] als Modul über R von den endlich vielen Produkten

$$\omega_i.\eta_j$$

erzeugt wird. Deshalb ist jedes Element von R[x,y] ganz über R, inbesondere also auch xy und x+y.
QED.

2.8.6 Beispiel für einen ganz abgeschlossenen Teilring

Sei R ein ZPE-Ring mit dem Quotientenkörper K. Dann ist R ganz abgeschlossen in K.

Beweis. Sei $x \in K$ ganz über K. Wir haben zu zeigen,

$$x \in R.$$

Wir schreiben x in der Gestalt

$$x = a/b \text{ mit } a,b \in R \text{ und } a,b \text{ teilerfremd.}$$

Nach Voraussetzung gilt für x eine Identität der Gestalt

$$x^n + a_1 x^{n-1} + ... + a_n = 0 \text{ mit } a_i \in R.$$

Wir multiplizieren diese Identität mit b^n und erhalten

$$a^n + a_1 a^{n-1} b + a_2 a^{n-2} b^2 + ... + a_n b^n = 0.$$

Dies ist eine Identität in R. Es gilt also

$$b \text{ teilt } a^n.$$

Das ist aber nur möglich, wenn b eine Einheit ist, denn a und b sind nach Wahl teilerfremd. Also ist x = a/b ein Element von R.
QED.

3. Körper

3.1 Körper, Teilkörper, Körpererweiterunge

3.1.1 Definitionen

Ein Körper ist eine kommutativer Ring mit 1, dessen von Null verschiedene Elemente Einheiten sind. Ein Teilkörper eines Körpers K ist eine Teilmenge

$$k \subseteq K,$$

die mit den Operationen von K ein Körper ist. Man sagt in dieser Situation auch, K/k ist eine Körpererweiterung oder auch, K ist ein Erweiterungskörper von k.

Bemerkungen

(i) Ist K/k eine Körpererweiterung, so besitzt K die Struktur eines k-Vektorraums und die einer k-Algebra mit dem Struktur-Homomorphismus

$$k \longrightarrow K, x \mapsto x.$$

(ii) Besitzt ein Körper K die Struktur einer Algebra über einem Körper k, so ist der Strukturhomomorphismus

$$h: k \longrightarrow K$$

injektiv, d.h. k kann mit seinem Bild bei h identifiziert und damit als Teilkörper von K aufgefaßt werden. Mit anderen Worten, K/k ist eine Körpererweiterung. Die Injektivität von h folgt aus der Tatsache, daß Ker h ein Ideal von k ist und k als Körper nur die Ideale (0) und k besitzt. Der Fall Ker h = k ist nicht möglich, denn dann wäre h identisch Null, im Widerspruch dazu, daß $h(1) = 1 \neq 0$ ist.

(iii) Seien K/k und K'/k Körpererweiterungen. Ein k-Homorphismus $K \longrightarrow K'$ ist ein Homomorphismus von k-Algebren

$$h: K \longrightarrow K'.$$

Wegen $k \subseteq K$ und $k \subseteq K'$ bedeutet dies insbesondere, daß h jedes Element von k in sich abbildet, also nicht die Null-Abbildung ist, also injektiv ist. Wir sprechen in dieser Situation daher auch von h als von einer k-Einbettung oder einer Einbettung über k. Ist h bijektiv, so heißt h auch k-Isomorphismus oder Isomorphismus über k.

3.1.2 Beispiele: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper. $\mathbb{H}$ ist kein Körper (da das Kommutativitätsgesetz in $\mathbb{H}$ nicht gilt).

3.1.3 Beispiel: $\mathbb{F}_p$

$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ist für jede Primzahl ein Körper mit endlich vielen (nämlich p) Elementen.

3.1.4 Beispiel: Rationale Funktionenkörper

Für jeden Integrietätsbereich K und beliebige Unbestimmte $X_1,...,X_n$ ist der volle Quotientenring

$$K(X_1,...,X_n) := Q(K[X_1,...,X_n])$$

ein Körper (weil Polynomringe über Integritätbereichen nullteilerfrei sind). Insbesondere ist dies der Fall, wenn K ein Körper ist.

3.1.5 Beispiel: Durchschnitte von Teilkörpern

Seien K ein Körper und $\{K_i\}_{i \in I}$ eine Familie von Teilkörpern von K. Dann ist

$$k := \bigcap_{i \in I} K_i$$

ein Teilkörper von K: mit je zwei Elementen aus k liegt auch deren Summe, deren Produkt und - falls defniert - deren Quotient in k. Die Körperaxiome für K übertragen sich auf k.

3.1.6 Beispiel: der von einer Menge erzeugte Teilkörper

Seien K ein Körper, $k \subseteq K$ ein Teilkörper und $M \subseteq K$ eine Teilmenge. Dann ist der Durchschnitt

$$k(M) := \bigcap_{k \subseteq K' \subseteq K,\ M \subseteq K'} K'$$

aller Teilkörper K' von K, welche den Körper k und die Menge M enthalten, wieder ein Körper. Er heißt der von M über k erzeugte Teilkörper von K. Ist M endlich, sagen wir

$$M = \{m_1,...,m_r\}$$

so schreibt man auch

$$k(m_1,...,m_r) = k(M).$$

Ein Körper der Gestalt

$$k(m_1,...,m_r)$$

heißt endlich erzeugte Körpererweiterung von k und im Fall r = 1 auch einfache Körpererweiterung.

Bemerkungen

(i) Sind $m_1,...,m_r$ endlich viele Elemente aus M, $f,g \in k[X_1,...,X_r]$ Polynome mit

$$g(m_1,...,m_r) \neq 0,$$

so liegt auf Grund der Körperaxiome das Element

(1) $f(m_1,...,m_r)/g(m_1,...,m_r)$ in k(M)

(ii) Umgekehrt bilden die Elemente der Gestalt (1) einen Körper,

$$\{ f(m)/g(m) \mid m = (m_1,...,m_r),\ m_i \in M,\ f,g \in k[X_1,...,X_r],\ g(m) \neq 0\}$$

der den Körper k und die Menge M enthält. Nach Definition von k(M) liegt k(M) ganz in diesem Körper. Nach (i) ist dieser Körper aber auch ganz in k(M) enthalten, d.h. es ist

$$k(M) = \{ f(m)/g(m) \mid m = (m_1,...,m_r),\ m_i \in M,\ f,g \in k[X_1,...,X_r],\ g(m) \neq 0\}$$
$$\neq 0\}$$

(iii) Es gilt

$$k(M) = Q(k[M]).$$

Beweis von (iii). Nach Definition ist k[M] der kleinste Ring, der k und die Menge M enthält. Da k(M) ebenfalls ein solcher Ring ist, folgt

$$k[M] \subseteq k(M).$$

Da jedes Element von k[M] - {0} eine Einheit von k(M) ist, gilt auf Grund der Universalitätseigenschaft der Quotientenringe,

$$Q(k[M]) \subseteq k(M).$$

Schließlich ist Q(k[M]) ein Körper, der k und die Menge M enthält. Also gilt

$$k(M) \subseteq Q(k[M]).$$

QED.

3.1.7 Das Kompositum, ausgezeichnete Klassen

Seien K' und K" zwei Körper, welche Teilkörper eines gemeinsamen Erweiterungskörpers K sind. Dann heißt der Durchschnitt

$$K'K'' := \bigcap_{K' \cup K'' \subseteq L \subseteq K} L$$

über alle Teilkörper L von K, welche sowohl K' als auch K" enthalten, Kompositum von K' und K". Wir sagen in dieser Situation (d.h. wenn es einen gemeinsamen Erweiterungskörper von K' und K" gibt), daß K'K" definiert ist.

Eine Kette

$$\ldots \subseteq K_i \subseteq K_{i+1} \subseteq \ldots$$

von ineinanderliegenden Teilkörpern heißt auch Körperturm.
Eine Klasse $\mathcal{K}$ von Körpererweiterungen heißt ausgezeichnet, wenn sie folgende Eigenschaften besitzt.

1. Komposition. Für jeden Körperturm $k \subseteq F \subseteq K$ gilt

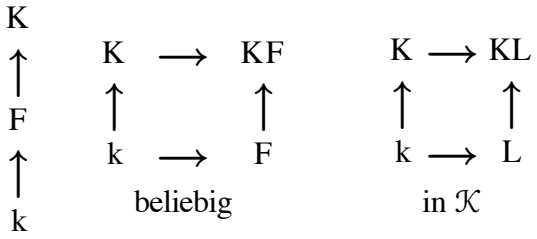
$$K/k \in \mathcal{K} \Leftrightarrow K/F \in \mathcal{K} \text{ und } F/k \in \mathcal{K}.$$

2. Basiswechsel. Für jede Körpererweiterung F/k gilt

$$K/k \in \mathcal{K} \text{ und } KF \text{ ist definiert} \Rightarrow KF/F \in \mathcal{K}.$$

3. Fasersummen. $K/k \in \mathcal{K}$ und $L/k \in \mathcal{K}$ und KL ist definiert $\Rightarrow KL/k \in \mathcal{K}$.

Die in 1., 2. und 3. beschriebenen Situationen kann man durch die folgenden Diagramme illustrieren.



Bemerkung
Falls für eine Klasse $\mathcal{K}$ von Körpererweiterungen die ersten beiden Bedingungen erfüllt sind, so ist es auch die drittte, d.h. $\mathcal{K}$ ist ausgezeichnet.
Beweis. Betrachten wir das rechte Diagramm. Nach Voraussetzung stehen der linke und der untere Pfeil für ein Element aus $\mathcal{K}$. Wegen 2 stehen dann aber auch der rechte und der obere Pfeil für solche Elemente. Dasselbe gilt dann aber auch für die Zusammensetzung zweier Pfeile dieses Diagramms (wegen 1).
QED.

3.1.8 Beispiel: Erzeugendensysteme beim Übergang zum Kompositum

Seien K/k und L/k Körpererweiterungen mit folgenden Eigenschaften.

1. KL ist definiert.
2. $K = k(\alpha_i \mid i \in I)$.

Dann gilt

$$KL = L(\alpha_i \mid i \in I).$$

Beweis. (Übungsaufgabe ?) Wir setzen

$$K' := L(\alpha_i \mid i \in I).$$

Weil L in KL liegt und alle α_i in K also in KL liegen, gilt dann

$$K' \subseteq KL.$$

Außerdem gilt

$$K = k(\alpha_i \mid i \in I) \subseteq K' \text{ und } L \subseteq K'.$$

Es reicht also zu zeigen, K' ist ein Körper. Das ist aber der Fall: nach Definition ist K' der kleinste Körper, der L und alle α_i enthält.

QED.

3.2 Endliche und algebraische Körpererweiterungen

3.2.1 Definitionen

Sei K/k eine Körpererweiterung. Ein Element

$$x \in K$$

heißt algebraisch über k, wenn es ein Polynom $f(X) \in k[X] - \{0\}$ gibt mit

$$f(x) = 0.$$

Anderfalls heißt x transzendent über k. Ist $x \in K$ algebraisch über k so heißt das Polynom

$$f_\alpha(X) \in k[X]$$

kleinsten Grades mit der Nullstelle α und dem höchsten Koeffizienten 1 Minimalpolynom von α über k.

Seien

$$x_1,...,x_n \in K$$

endlich viele Elemente. Diese Elemente heißen algebraisch abhängig über k, wenn es ein Polynom

$$f(X_1,...,X_n) \in k[X_1,...,X_n] - \{0\}$$

gibt mit

$$f(x_1,...,x_n) = 0.$$

Andernfalls heißen die Elemente algebraisch unabhängig über k.

Eine beliebige Familie

$$\{x_i\}_{i \in I} \quad , x_i \in K$$

von Elementen aus K heißt algebraisch abhängig über k, falls endlich viele der x_i algebraisch abhängig sind über k. Andernfalls heißt die Familie algebraisch unabhängig über k.

Eine Körpererweiterung K/k heißt rein transzendent, wenn es eine Familie

$$\{x_i\}_{i \in I} \quad , x_i \in K$$

von Elementen aus K gibt, die algebraisch unabhängig über k ist, mit der Eigenschaft, daß die Menge der x_i der Körper K über k erzeugt:

$$K = k(x_i \mid i \in I)$$

Eine Körpererweiterung K/k heißt algebraisch, falls jedes Element von K algebraisch ist über k. Andernfalls heißt die Körpererweiterung transzendent. Eine Körpererweiterung K/k heißt endlich, wenn K als Vektorraum über k endich-dimensional ist. Die Dimension

$$[K:k] = \dim_k K$$

heißt in dieser Situation auch Körpergrad von K über k.

3.2.2 Beispiel: Rein transzendente Körpererweiterungen

(i) Seien k ein Körper, $X_1,...,X_n$ Unbestimmte und

$$K := k(X) := k(X_1,...,X_n)\ ,\ X := (X_1,...,X_n)$$

der Körper der rationalen Funktionen in $X_1,...,X_n$ über k. Dann sind die

$$X_1,...,X_n$$

algebraisch unabhängig über k und K/k ist eine rein transzendente Körpererweiterung.

(ii) Seien K/k eine Körpererweiterung und

$$x_1,...,x_n \in K$$

Elemente, die algebraisch unabhängig über k sind. Dann ist die rein transzendente Körpererweiterung

$$k(x) := k(x_1,...,x_n),\ x := (x_1,...,x_n)$$

als k-Algebra isomorph zum rationalen Funktionenkörper

$$k(X).$$

Beweis. Zu (i). Es reicht zu zeigen, die $X_1,...,X_n$ sind algebraisch unabhängig über k.

Andernfalls gibt es ein Polynom $f \neq 0$ in n Unbestimmten mit

$$fX) = 0 \text{ in } K = Q(k[X]).$$

Weil k[X] nullteilerfrei ist, gilt dann sogar

$$f(X) = 0 \text{ in } k[X],$$

im Widerspruch dazu, daß das Polynom f ungleich Null sein soll.

Zu (ii). Betrachten wir den Homomorphismus von k-Algebren

$$\varphi: k[X] \longrightarrow K,\ f(X) \mapsto f(x).$$

Sein Bild ist gerade

$$Im(\varphi) = k[x]$$

(nach Definiton von k[x]). Ist f(X) ein Element aus dem Kern, so gilt

$$f(x) = 0,$$

was auf Grund der algebraischen Unabhängigkeit der $x_1,...,x_n$ nur möglich ist wenn gilt f = 0. Also gilt

$$Ker(\varphi) = \{0\}.$$

Wir haben gezeigt, die Abbildung

$$k[X] \longrightarrow k[x],\ f(X) \mapsto f(x),$$

ist ein Isomorphismus von k-Algebren. Wir setzen diesen Isomorphismus mit der natürlichen Abbildung der rechten Rings in dessen Quotientenkörper zusammen,

$$k[X] \longrightarrow k[x] \subseteq k(x),\ f(X) \mapsto f(x).$$

Bei dieser Abbildung geht jedes von Null verschiedene Polynom in eine Einheit über. Auf Grund der Universalitätseigenschaft der Quotientenringe, gibt es eine Abbildung

$$k(X) \longrightarrow k(x),\ \frac{f(X)}{g(X)} \mapsto g(x)^{-1} f(x).$$

Auf Grund der Beschreibung von $k(x_1,...,x_n)$ in 3.1.6 Bemerkung (ii) ist diese Abbildung surjektiv. Auf Grund der algebraischen Unabhängigkeit der x_i ist sie auch injektiv, also ein Isomorphismus.

QED.

3.2.3 Beispiel: einfache endliche Körpererweiterungen

Seien k ein Körper und $f \in k[X]$ ein über k irreduzibles Polynom. Dann ist

$$K = k[X]/(f)$$

ein Körper, und die Zusammensetzung

$$k \longrightarrow K, c \mapsto c \bmod (f),$$

der natürlichen Einbettung $k \hookrightarrow k[x]$ mit dem natürlichen Homomorphismus $k[X] \longrightarrow K$ auf den Faktorring identifiziert k mit einem Teilkörper von K.
Weiter ist die Restklasse

$$\alpha := X \bmod (f) \in K$$

der Unbestimmten X im Faktorring K eine Nullstelle von f,

$$f(\alpha) = 0,$$

und es gilt

$$K = k(\alpha).$$

Die Körpererweiterung K/k ist einfach und endlich vom Grad n := deg(f). Genauer ist

$$k(\alpha) = k \bullet 1 + k \bullet \alpha + ... + k \bullet \alpha^{n-1}.$$

Ist der höchste Koeffizient von f gleich 1, so ist f das Minimalpolynom von α. (und jedes Polynom von k[X] mit der Nullstelle α ist in k[X] ein Vielfaches von f).

Bemerkungen

(i) Jedes irreduzible Polynom über k besitzt damit eine Nullstelle in einer einfachen endlichen Erweiterung von k.

(ii) Da jedes nicht-konstante Polynom aus k[x] einenn irreduziblen Faktor besitzt, hat damit jedes nicht-konstante Polynom aus k[x] eine Nullstelle in einer einfachen endlichen Erweiterung von k.

Beweis. Wir können ohne Beschränkung der Allgemeinheit annehmen, daß der höchst Koeffizient von f gleich 1 ist,

f ist normiert.

Zum Beweis der Körpereigenschaft von K reicht es zu zeigen, das von f erzeugte Ideal

(f) ist ein maximales Ideal von k[X]. (1)

Sei $I \subseteq k[X]$ ein Ideal, welches das Ideal (f) echt enthält,

$$(f) \subset I \subseteq k[X].$$

Weil k[X] ein Hauptidealring ist, gilt

$$I = gk[X]$$

mit einem Polynom $g \in k[X]$. Wegen $f \in (f) \subseteq I = (g)$ ist f ein Vielfachen von g, also g ein Teiler von f. Weil (f) echt enthalten ist in I, ist g ein echter Teiler von f. Weil f irreduzibel ist, ist damit g eine Einheit, d.h. es gilt

$$I = (g) = k[X].$$

Damit ist (1) bewiesen, also K ein Körper. Der Ring-Homomorphismus

$$k \longrightarrow K, c \mapsto c \bmod (f),$$

bildet das Einselement von k ins Einelement von K ab, ist also nicht identisch Null. Sein Kern ist also von k verschieden und weil k ein Körper ist damit gleich {0}. Der Homomorphismus ist injektiv und identifiziert k mit einem Teilkörper von K.

Weil der natürliche Homomorphismus $\rho: k[X] \longrightarrow K$ ein Homomorphismus von k-Algebren ist, gilt

$$f(\alpha) = f(\rho(X)) = \rho(f) = f \bmod (f) = 0.$$

Wegen $k \subseteq K$ und $\alpha \in K$ gilt

$$k(\alpha) \subseteq K.$$

Für jedes Element $\beta \in K$ gibt es, weil ρ surjektiv ist, ein Polynom $g \in k[X]$ welches in β abgebildet wird, d.h. es gilt

$$\beta = \rho(g(X)) = g(\rho(X)) = g(\alpha) \in k(\alpha).$$

Wir haben gezeigt,

$$K = k(\alpha).$$

Insbesondere ist die Körpererweiterung einfach. Wir haben noch die folgenden Aussagen zu beweisen.

1. $k(\alpha) = k\bullet 1 + k\bullet\alpha + ... + k\bullet\alpha^{n-1}$.
2. f ist das Minimalpolynom von α.
3. $1, \alpha, ..., \alpha^{n-1}$ sind linear unabhängig über k.

Zu 1.

Trivialerweise gilt

$$k\bullet 1 + k\bullet\alpha + ... + k\bullet\alpha^{n-1} \subseteq k(\alpha). \qquad (2)$$

Beweisen wir die umgekehrte Inklusion. Für jedes $\beta \in k(\alpha)$ gibt es ein Polynom $g \in k[X]$ mit

$$\beta = g(\alpha).$$

Wir führen den Beweis durch Induktion nach dem Grad $d = \deg(g)$ von g. Die Identität $\beta = g(\alpha)$ bedeutet, β ist eine k-Linearkombination der Gestalt

$$\beta = c_0\bullet 1 + c_1\bullet\alpha + ... + c_d\bullet\alpha^d$$

Im Fall $d < n$ liegt β trivialerweise in der linken Seite von (2). Sei also jetzt $n \le d$. Weil f den Grad n,den höchsten Koeffizienten 1 und die Nullstelle α hat ist dann

$$\beta = \beta - c_d\bullet f(\alpha)\bullet\alpha^{d-n}$$

eine k-Linearkombination von $1, \alpha, ..., c_{d-1}\bullet\alpha^{d-1}$, d.h. β ist ein Polynom in α eines Grades $\le d$. Nach Induktionsvoraussetzung liegt β in der linken Seite von (2).

Zu 2.

Bezeichne $m = m_\alpha$ das Minimalpolynom von α. Dieses Polynom existert, weil $f(\alpha) =$ ist (d.h. es gibt ein Polynom mit der Nullstelle α). Division mit Rest liefert

$$f = q\bullet m + r \text{ mit } q, r \in k[X] \text{ und } \deg r < \deg m.$$

Einsetzen von α ergibt

$$0 = q(\alpha)\bullet 0 + r(\alpha),$$

d.h. α ist eine Nullstelle von r. Nach Definition des Minimalpolynoms muß damit r das Nullpolynom sein, d.h. es ist

$$f = q\bullet m.$$

Weil f irreduzibel ist, ist q ein Einheit, d.h. eine Konstante,

$$q = k - \{0\}.$$

Weil die höchsten Koeffizienten von f und m beide gleich 1 sind, folgt q = 1, also

$$f = m.$$

Zu 3.

Wären die angegebenen Potenzen von α k-lineare abhängig, so gäbe es ein Polynom $g \in k[X] - \{0\}$ mit

$$g(\alpha) = 0 \text{ und } \deg(g) \le n-1 < \deg f.$$

Das ist aber nicht möglich, weil f das Minimalpolynom von α ist.

QED.

Bemerkung

Um Beispiele für algebraische Körpererweiterungen angeben zu können, benötigen wir zunächst ein Kriterium für das Vorliegen solcher Erweiterungen.

3.2.4 Hinreichendes Kriterium für algebraische Körpererweiterungen

Seien k ein Körper und A eine nullteilerfreie kommutative k-Algebra, die als k-Vektorraum endlich-dimensional ist.

Dann ist A ein Körper, und die Körpererweiterung A/k ist algebraisch.
Insbesondere sind endliche Körpererweiterungen algebraisch.
Beweis.
Seien

$$n := \dim_k A$$

und

$$v \in A - \{0\}.$$

Wir haben zu zeigen, v besitzt in A ein inverses Element.
Nach Definition von n sind die (n+1) Vektoren

$$v^0 = 1, v^1 = 1, v^2, \ldots, v^n$$

linear abhängig über k, dh. es gibt Koeffizienten $a_i \in k$, die nicht sämtlich gleich Null sind, mit

(3) $$a_0+a_1v+a_2v^2+\ldots + a_nv^n = 0$$

Wir wählen r derart, daß gilt

$$0 = a_0 = \ldots = a_{r-1}, 0 \neq a_r.$$

Dann kann man auf der rechten Seite von (3) die Potenz v^r ausklammern und, da A nullteilerfrei ist, kürzen. Wir erhalten so eine Identität derselben Gestalt wie (3) mit $a_0 \neq 0$. Wir können also annehmen, in (3) gilt $a_0 \neq 0$. Durch Multiplikation mit dem Inversen von a_0 können wir weiter erreichen

$$a_0 = 1.$$

Dann gilt aber

$$1+v\bullet(a_1+a_2v+\ldots + a_nv^{n-1}) = 0$$

d.h.

$$v\bullet(-a_1-a_2v-\ldots - a_nv^{n-1}) = 1.$$

Mit anderen Worten, es gibt ein zu v inverses Element

$$-a_1-a_2v-\ldots - a_nv^{n-1}$$

in A. Wir haben gezeigt, A ist ein Körper. Außerdem zeigt die Identität (3), daß jedes von von Null verschiedene Element v von A algebraische ist über k, d.h. die Körpererweiterung A/k ist algebraisch.
QED

3.2.5 Beispiel: einfache algebraische Körpererweiterungen

Seien K/k eine Körpererweiterung, $\alpha \in K$ ein über k algebraisches Element und

$$f_\alpha(X) = c_o+c_1X+\ldots+c_{n-1}X^{n-1}+X^n \in k[X]$$

das Minimalpolynom von α über k. Dann gelten die folgenden Aussagen.

(i) $[k(\alpha):k] = \deg f_\alpha = n (< \infty)$. Insbesondere ist K/k eine endliche Körpererweiterung.

(ii) $1, \alpha, \ldots, \alpha^{n-1}$ ist eine k-Vektorraumbasis von $k(\alpha)$.

(iii) Die Abbildung

$$k[X]/(f_\alpha) \longrightarrow k(\alpha), p(X) \bmod (f_\alpha) \mapsto p(\alpha),$$

ist wohldefiniert und ist ein Isomorphismus von k-Algebren (kurz k-Isomorphismus).

Beweis. Zu (iii).
Wir betrachten den folgenden Homomorphismus von Ringen mit 1.

$$\rho: k[X] \longrightarrow k(\alpha),\ g(X) \mapsto g(\alpha).$$

Weil k[X] ein Hauptidealring ist, hat sein Kern die Gestalt

$$\mathrm{Ker}(\rho) = (f)$$

mit einem Polynom $f \in k[X] - \{0\}$. Nach dem 0-ten Isomorphiesatz gilt,

$$k[X]/(f) \cong \mathrm{Im}(\rho) \subseteq k(\alpha),\ \ g(X) \bmod (f) \mapsto g(\alpha).$$

Insbesondere ist der Faktorring links nullteilerfrei, d.h. (f) ist ein Primideal und damit f ein irreduzibles Polynom. Nach 3.2.3 ist k[X]/(f) ein Erweiterungskörper von k. Dieser enthät das Element

$$\alpha = \rho(X).$$

Nach Definition von $k(\alpha)$ folgt

$$k[X]/(f) \cong \mathrm{Im}(\rho) = k(\alpha).$$

Nach Definition liegt das Minimalpolynom f_α im Kern von ρ,

$$f_\alpha \in (f),$$

d.h.

$$f_\alpha = f \bullet h \text{ mit } h \in k[X] - \{0\}.$$

Da f_α minimalen Grad unter allen Polynomen mit der Nullstelle α hat, muß h eine Konstante sein, also eine Einheit. Es folgt

$$(f) = (f_\alpha).$$

Zu (i) und (ii).
Die Aussage ergeben sich mit dem bisher bewiesenen aus dem Beispiel 3.2.3.
QED.

3.2.6 Eigenschaften endlicher Erweiterungen und Körpergrad

(i) Die endlichen Körpererweiterungen bilden eine ausgezeichnete Klasse.
(ii) Für jeden Turm

$$k \subseteq K \subseteq L$$

von endlichen Körpererweiterungen gilt

$$[L:k] = [L:K] \bullet [K:k].$$

Insbesondere ist auch L/k endlich.
(iii) Ist K/k endlich, sagen wir

$$K = k \bullet \omega_1 + \ldots + k \bullet \omega_n\ ,$$

und ist das Kompositum KF mit dem Oberkörper F von k definiert, so gilt

$$KF = F \bullet \omega_1 + \ldots + F \bullet \omega_n\ .$$

Beweis. Zu (ii). Wir wählen Vektorraumbasen von L über K und von K über k, sagen wir

$$L = K\omega_1 + \ldots + K\omega_r \text{ mit } r = [L:K]$$

und

$$K = k\eta_1 + \ldots + k\eta_s \text{ mit } s = [K:k].$$

Dann gilt

$$L = \sum_{i=1}^{r} K\omega_i = \sum_{i=1}^{r} \sum_{j=1}^{s} k\eta_j\omega_i\ ,$$

d.h. die $\eta_j\omega_i$ bilden ein Erzeugendensystem des Vektorraums L über k. Insbesondere ist L/k eine endliche Erweiterung und es gilt

$$[L:k] \leq rs = [L:K]\bullet[K:k].$$

Zum Beweis der Behauptung reicht es zu zeigen, die $\eta_j\omega_i$ sind linear unabhängig über k. Sei also

$$\sum_{i=1}^{r}\sum_{j=1}^{s} c_{ji}\eta_j\omega_i = 0 \text{ mit } c_{ji} \in k.$$

Mit

$$d_i = \sum_{j=1}^{s} c_{ji}\eta_j \in K$$

gilt dann

$$\sum_{i=1}^{r} d_i\omega_i = 0,$$

also $d_i = 0$ für alle i, denn die ω_i sind linear unabhängig über K. Mit

$$0 = d_i = \sum_{j=1}^{s} c_{ji}\eta_j$$

gilt aber auch $c_{ji} = 0$ für alle i und alle j, denn die η_j sind linear unabhängig über k.

Zu (iii). Wir setzen

$$K' := F\bullet\omega_1+...+F\bullet\omega_n \quad (\subseteq K\bullet F).$$

Dann gilt nach Definition von KF zumindest

$$K' \subseteq KF,\ F \subseteq K'^{18} \text{ und } K \subseteq K'.$$

Es reicht also zu zeigen, K' ist ein Teilkörper von KF. Beachten wir, Addition und Multiplikation von KF definieren eine Abbildungen

$$K'\times K' \longrightarrow K'.$$

Für die Addition ist das trivial. Bei der Multiplikatioin beachten wir, das Produkt von je zwei ω_i's ist eine k-Linearkombination von ω_i's, also erst recht eine F-Linearkombination. Damit ist K' zumindest eine F-Algebra mit 1. Wegen $K' \subseteq K\bullet F$ ist die F-Algebra K' nullteilerfrei (und nach Definiton von endlicher Dimension über F). Also ist K' ein Körper (nach 3.2.4).

Zu (i). Eigenschaft 1: sei

$$k \subseteq F \subseteq K$$

ein Körperturm. Seien K/F und F/k endlich. Nach (ii) ist dann auch K/k endlich.
Sei umgekehrt K/k endlich, sagen wir

$$K = k\bullet\omega_1+...+k\bullet\omega_n. \qquad (1)$$

Als k-linearer Unterraum von K ist dann auch F von endlicher Dimension über k, d.h. F/k ist endlich. Mit (1) gilt aber auch

$$K = F\bullet\omega_1+...+F\bullet\omega_n,$$

d.h. K/F ist endlich.

Eigenschaft 2: Seien K/k endlich, L/k beliebig und sei KL definiert. Dann gibt es eine endliche Basis von K über k, sagen wir

$$K = k\bullet\omega_1+...+k\bullet\omega_n .$$

Nach (iii) folgt

---

[18] Nach Wahl der ω_i ist eine k-Linearkombination der ω_i gleich 1.

$$KL = L\bullet\omega_1+...+L\bullet\omega_n ,$$

d.h. KL/L ist endlich.
QED.

3.2.7 Endlich erzeugte algebraische Erweiterungen sind endlich

Sei K/k eine endlich erzeugte Körperweiterung, sagen wir

$$K = k(\alpha_1,...,\alpha_n).$$

Wir nehmen weiter an, jedes α_i ist algebraisch über k. Dann ist die Erweiterung K/k endlich.
Insbesondere sind endlich erzeugte algebraische Körpererweiterungen endlich.
Beweis. Wir führen den Beweis durch Induktion nach n. Im Fall n = 0 gilt

$$K = k$$

und die Aussage ist trivial. Sei jetzt $n > 0$. Wir setzen

$$k' := k(\alpha_n).$$

Dann ist jedes der α_j nicht nur algebraisch über k sondern auch über k'. Nach Induktionsvoraussetzung ist

$$K/k' \text{ endliche Körpererweiterung.}$$

Nach 3.2.6 (ii) reicht es zu zeigen,

$$k'/k \text{ ist endliche Körpererweiterung.}$$

Das ist aber der Fall nacn 3.2.5.
QED.

3.2.8 Eigenschaften algebraischer Körpererweiterungen

Die algebraischen Körpererweiterungen bilden eine ausgezeichnete Klassse.

Beweis (Aufgabe?). Eigenschaft 1.
Sei

$$k \subseteq F \subseteq K$$

ein Körperturm. Falls K/k algebraisch ist, so ist jedes Element von K algebraisch über k, also auch über F, d.h.

$$K/F \text{ ist algebraisch.}$$

Außerdem ist insbesondere jedes Element von F algebraisch über k, d.h.

$$F/k \text{ ist algebraisch.}$$

Seien jetzt umgekehrt F/k und K/F algebraisch und sei

$$\alpha\in K.$$

Wir haben zu zeigen, α ist algebraisch über k. Nach Voraussetzung ist α algebraisch über F. Seien

$$\alpha_1,...., \alpha_r \in F$$

die Koeffizienten des Minimalpolynoms von α über F. Dann ist α algebraisch über $k(\alpha_1,...., \alpha_r)$, d.h.

$$k(\alpha_1,...., \alpha_r,\alpha)/k(\alpha_1,...., \alpha_r) \text{ ist endliche Körpererweiterung.}$$

Da F/k algebraisch ist, ist jedes α_i algebraisch über k, d.h.

$$k(\alpha_1,...., \alpha_r)/k \text{ ist eine endliche Körpererweiterung}$$

(nach 3.2.7). Damit ist aber auch

$$k(\alpha_1,...., \alpha_r,\alpha)/k \text{ endliche (also algebraische) Körpererweiterung,}$$

(nach 3.2.6(ii)), d.h. α ist algebraisch über k.
Eigenschaft 2. Seien K/k und L/k Körpererweiterungen mit folgenden Eigenschaften.
1. K/k ist algebraisch.

2. KL ist definiert.
Wir haben zu zeigen, KL/L ist algebraisch. Wegen 1 können wir K in der Gestalt

$$K = k(\alpha_i \mid i \in I)$$

schreiben mit einer Familie von Elementen $\alpha_i \in K$, die algebraisch über k sind. Nach 3.1.8 gilt damit

$$KL = L(\alpha_i \mid i \in I).$$

Jedes Element

$$\alpha \in KL$$

ist somit ein rationaler Ausdruck in endlich vielen der α_i, sagen wir $\alpha_1, \ldots, \alpha_n$ mit Koeffizienten aus L, d.h.

$$\alpha \in L' := L(\alpha_1, \ldots, \alpha_n).$$

Da jedes der α_i algebraisch ist über k (also erst recht über L), ist

$$L'/L \text{ endlich}$$

(nach 3.2.7) und damit erst recht algebraisch (vgl. 3.2.8). Also ist α algebraisch über L. Wir haben gezeigt KL/L ist algebraisch.
QED.

3.2.9 Fortsetzungssatz I

Seien K/k und K'/k zwei Körpererweiterungen, F ein Körper zwischen k und K und

$$h: F \longrightarrow K'$$

ein k-Homomorphismus, d.h. das folgende Diagramm sei kommutativ.

$$\begin{array}{ccccc} k & \subseteq & F & \subseteq & K \\ \cap & & \swarrow h & & \\ K' & & & & \end{array}$$

Weiter sei

$$\alpha \in K$$

ein über F algebraisches Element mit dem Minimalpolynom

$$f_\alpha(X) = \sum_{i=0}^{n} a_i X^i \in F[X].$$

Das Polynom

$$f_\alpha^h(X) = \sum_{i=0}^{n} h(a_i) X^i \in K'[X]$$

besitze eine Nullstelle α' in K',

$$f_\alpha^h(\alpha') = 0.$$

Dann gibt es genau eine Fortsetzung

$$h': F(\alpha) \longrightarrow K'$$

von h zu einem k-Homomorphismus mit $h'(\alpha) = \alpha'$.

Beweis. Existenz von h'.Wir betrachten den Homomorphismus von k-Algebren

$$F[X] \longrightarrow K', \; p(X) \mapsto p^h(\alpha').$$

Wegen $f_\alpha^h(\alpha') = 0$ liegt f_α im Kern und nach dem Homomorphiesatz gibt es einen F-Homomorphismus

$$F[X]/(f_\alpha) \longrightarrow K', p(X) \bmod (f_\alpha) \mapsto p^h(\alpha').$$

Nach 3.2.3 ist aber der Definitionsbereich dieses Homomorphismus isomorph zu $F(\alpha)$. Genauer, es gibt einen F-Isomorphismus

$$F(\alpha) \longrightarrow F[X]/(f_\alpha), p(\alpha) \mapsto p(X) \bmod (f_\alpha).$$

Durch Zusammensetzen erhalten wir also einen F-Homomorphismus

$$h':F(\alpha) \longrightarrow K', p(\alpha) \mapsto p^h(\alpha').$$

Als F-Homomorphismus ist h' eine Fortsetzung von h. Außerdem gilt

$$h'(\alpha) = X^h(\alpha') = X(\alpha') = \alpha'.$$

Eindeutigkeit von h'. Falls h' existiert, so gilt für jedes Polynom

$$p(X) = \sum_{i=0}^{m} b_i X^i \in F(X),$$

daß das Bild von $p(\alpha)$ bei h' feststeht:

$$h'(p(\alpha)) = h'(\sum_{i=0}^{m} b_i\alpha^i) = \sum_{i=0}^{m} h'(b_i)h'(\alpha)^i = \sum_{i=0}^{m} h(b_i)\alpha'^i = p^h(\alpha).$$

Jedes Element von $F(\alpha)$ hat aber die Gestalt $p(\alpha)$, d.h. h' ist eindeutig bestimmt.
QED.

3.3 Die algebraische Abschließung

3.3.1 Definitionen

Ein Körper k heißt algebraisch abgeschlossen, wenn jedes nicht-konstante Polynom

$$f(X) \in k[X]$$

mit Koeffizienten aus k mindestens eine Nullstelle in k besitzt. Eine algebraische Abschließung des Körpers k ist ein algebraisch abgeschlossener Körper K, welcher den Körper k als Teilkörper enthält und welcher algebraisch ist über k.

Bemerkung

Ziel dieses Abschnitts ist es zu zeigen, jeder Körper k besitzt eine algebraische Abschließung und diese ist bis auf k-Isomorphie eindeutig bestimmt.

3.3.2 Zerlegung in Linearfaktoren

Sei k ein Körper. Dann sind folgende Aussage äquivalent.

(i) k ist algebraisch abgeschlossen.

(ii) Jedes nicht-konstante Polynom von k[X] ist über k Produkt linearer Polynome.

Beweis. (ii) $\Rightarrow$ (i). Trivial, da jedes lineare Polynom von k[X] in k eine Nullstelle besitzt.

(i) $\Rightarrow$ (ii). Sei

$$f(X) = \sum_{i=0}^{n} a_i X^i \in k[X], a_n \neq 0,$$

ein nicht-konstantes Polynom. Wir haben zu zeigen, f ist Produkt linearer Polynome aus k[X]. Im Fall n = 1 ist das trivial. Sei jetzt n > 0. Nach Voraussetztung hat f in k eine Nullstelle

$$a \in k.$$

Deshalb gilt

$$f(X) = f(X) - f(a) = \sum_{i=0}^{n} a_i(X^i - a^i)$$

$$= \sum_{i=0}^{n} a_i (X-a)(X^{i-1}+aX^{i-2}+a^2X^{i-3}+...+a^{i-1})$$

$$= (X-a)g(X)$$

mit $g(X)\in k[X]$. Nach Induktionsvoraussetzung ist g(X) Produkt linearer Polynome aus k[X]. Also gilt dasselbe auch für f(X).
QED.

3.3.3 Fortsetzungssatz II

Seien K/k und K'/k zwei Körpererweiterungen, F ein Körper zwischen k und K und

$$h: F \longrightarrow K'$$

ein k-Homomorphismus, d.h. das folgende Diagramm sein kommutativ.

$$\begin{array}{ccccc} k & \subseteq & F & \subseteq & K \\ & & \cap & \swarrow_{h} & \\ & & K' & & \end{array}$$

Weiter seien die beiden folgenden Bedingungen erfüllt:
(i) K/F ist eine algbraische Körpererweiterung.
(ii) K' ist algebraisch abgeschlossen.

Dann gibt es eine Fortsetzung

$$h': K \longrightarrow K'$$

von h zu einem k-Homomorphismus.

Mit anderen Worten, jeder k-Homomorphismus mit Werten in einem algebraisch abgeschlossenen Köper läßt sich auf jede algebraische Erweiterung fortsetzen.

Beweis. Wir betrachten die Menge

$$\mathcal{M} = \{ (L, \varphi_L) \mid \begin{array}{l} L \text{ ist ein Körper zwischen F und K} \\ \varphi_L : L \longrightarrow K' \text{ ist eine Fortsetzung von h} \end{array} \}$$

aller Fortsetzungen von h zu einem k-Homomorphismus auf einen Körper L zwischen F und K. Wir versehen diese Mengen mit der folgenden Halbordnung.

$$(L, \varphi_L) \leq (L', \varphi_L,) \Leftrightarrow L \subseteq L' \text{ Teilkörper und } \varphi_L,|_L = . \varphi_L$$

Man beachte, "$\leq$" ist tatsächlich reflexiv, antisymmetrisch und transitiv. Zeigen wir, die halbgeordnete Menge $\mathcal{M}$ genügt den Bedingungen des Zornschen Lemmas. Sei also

$$\{(L_i , \varphi_i L_i \longrightarrow K') \mid i\in I \}$$

eine linear geordnete Teilmenge von $\mathcal{M}$, d.h. für je zwei φ_i seien die Definitionsbereiche ineinander enthalten und das eine φ_i ist Fortsetzung des anderen. Wir setzten

$$L := \bigcup_{iPI} L_i$$

und definieren $\varphi: L \longrightarrow K'$ durch $\varphi(x) = \varphi_i(x)$ falls $x\in L_i$.

Die Definition von φ ist korrekt, da je zwei φ_i die in einem $x\in L$ definiert sind, dort denselben Wert haben. Die Menge L ist ein Körper zwischen F und K,

$$F \subseteq L \subseteq K,$$

denn für je endlich viele Elemente von L gibt es ein i, so daß L_i diese Elemente enthält. Nach Konstruktion ist (L, φ) ein Element von $\mathcal{M}$ und eine obere Schranke der gegebenen linear geordneten Teilmenge.
Wir haben gezeigt, $\mathcal{M}$ genügt den Bedinungen des Zornschen Lemmas. Also besitzt $\mathcal{M}$ ein maximales Element, sagen wir

(1) $$(L': \varphi': L' \longrightarrow K').$$

Zum Beweis der Behauptung reicht es zu zeigen, L' = K: Angenommen, das ist nicht so. Dann gibt es ein Element

$$\alpha \in K' - L'.$$

Bezeichne $f_\alpha \in L'[X]$ das Minimalpolynom von α über L' Wir haben dann eine Situation wie in 3.3.12:

$$\begin{array}{ccccc} k & \subseteq & L' & \subseteq & K \\ \cap & \swarrow & \varphi' & & \\ K' & & & & \end{array} \qquad \text{(mit } F=L', h=\varphi')$$

Weiter hat das Bild $f_\alpha^{\varphi'} \in K'[X]$ von f_α eine Nullstelle in K' (weil K' algebraisch abgeschlossen ist). Nach 3.2.13 gibt es also eine Fortsetzung von φ' zu einem k-Homomorphismus $L'(\alpha) \longrightarrow K'$. Das steht aber im Widerspruch zur Maximalität von (1). Also gilt L' = K.

QED.

3.3.4 Die Existenz eines algebraisch abgeschlossenen Erweiterungskörpers

Jeder Körper k ist Teilkörper eines algebraisch abgeschlossenen Erweiterungskörpers.

Beweis. Wir betrachten die folgende Aussage

(*) Jeder Köper K ist Teilkörper eines Körpers K' mit der Eigenschaft, daß jedes nicht-konstante Polynom von K[X] eine Nullstelle in K' hat.

1. Schritt: Reduktion auf den Beweis von Aussage (*).
Wir beweisen die Aussage des Satzes unter der Annahme, daß Aussage (*) richtig.
Dazu betrachten wir eine Folge von Körpererweiterungen

$$k = k_0 \subseteq k_1 \subseteq \ldots \subseteq k_i \subseteq k_{i+1} \subseteq \ldots$$

derart, daß jedes nicht-konstante Polynom mit Koeffizienten aus k_i ein Nullstelle in k_{i+1} besitzt. Eine solche Folge von Körpererweiterungen existiert wegen (*). Wir setzen

$$K := \bigcup_{i=0}^{\infty} k_i$$

Diese Menge K hat die Eigenschaft, daß es für je endlich viele Elemente

$$c_1, \ldots, c_r \in K$$

ein i gibt mit

$$c_1, \ldots, c_r \in k_i .$$

Insbesondere liegen dann alle Elemente, die man durch Körperoperationen aus diesen gewinnen kann, wieder in k_i, also auch in K. Das Ergebniss dieser Körperoperationen

hängt damit nicht von der speziellen Wahl von i ab, da für je zwei i der eine Körper k_i ein Teilkörper des anderen ist. Mit anderen Worten,

$$K$$

ist ein Körper, der sämtliche k_i also Teilkörper enthält. Sei jetzt

$$f(X) \in K[X]$$

ein nicht-konstantes Polynom. Dann gibt es ein i derart, daß die endlich vielen Koeffizienten von f in k_i liegen, d.h. es gilt

$$f(X) \in k_i[X].$$

Nach Konstruktion besitzt f eine Nullstelle in k_i und damit auch in K. Mit anderen Worten, K ist algebraisch abgeschlossen (und enthält k als Teilkörper).

2. Schritt: Beweis der Aussage (*).

Bezeichne F die Menge der nicht-konstanten Polynome von K. Für jedes f∈F wählen wir eine Unbestimmte X_f und betrachten den Polynomring

(1) $$K[X_f \mid f \in F]$$

in den unendlich vielen Unbestimmten. Ein Element dieses Rings ist ein Polynom mit Koeffizienten aus K in jeweils endlich vielen der Unbestimmten X_f. Je endlich viele Elemente von (1) liegen deshalb bereits in einem Polynomring in endlich vielen Unbestimmten und die Ringoperationen finden bereits in diesem Teilring statt. Betrachten wir das Ideal

(2) $$I := (f(X_f) \mid f \in F)$$

von (1), das von allen Polynomen der Gestalt $f(X_f)$ erzeugt wird. Zeigen wir, I ist ein echtes Ideal von (1). Angenommen, I ist nicht echt, Dann gilt 1∈I, d.h. es gibt Polynome $g_1,...,g_r \in K[X_f \mid f \in F]$ und Polynome $f_1,...,f_r \in F$ mit

$$1 = g_1 f_1(X_{f_1}) + ... + g_r f_r(X_{f_r}).$$

Wir schreiben im folgenden einfach X_i für X_{f_1}. In der obigen Identität kommen insgesamt nur endlich viele der Unbestimmten X_f vor. Bezeichnen wir diese mit $X_1,...,X_N$ (mit $N \geq r$). Dann bekommt die Identität die Gestalt

(3) $$1 = \sum_{i=1}^{r} g_i(X_1,...,X_N) f_i(X_i)$$

und sie läßt sich als Identität im Polynomring

$$K[X_1,...,X_N]$$

auffassen. Nach den Bemerkungen von 3.2.3 und nach 3.2.6 (i) gibt es eine endliche Körpererweiterung

$$K'/K$$

die für jedes i = 1,...,r eine Nullstelle α_i von f_i enthält. Wir setzen diese Nullstellen in (3) ein ($X_i = \alpha_i$ für i = 1,...,r und $X_i = 0$ für i > r) und erhalten

$$1 = 0 \text{ in } K'.$$

Dieser Widerspruch zeigt, daß das Ideal I ein echtes Ideal ist. Wir wählen ein maximales Ideal von (1), welches I enthält,

$$m \subseteq K[X_f \mid f \in F] \text{ maximal mit } I \subseteq m,$$

und setzten

$$K' := K[X_f \mid f \in F]/m.$$

Weil m maximal ist, ist K' ein Körper. Betrachten wir die Komposition

$$K \hookrightarrow K[X_f \mid f \in F] \xrightarrow{\rho} K',\ c \mapsto c \bmod m,$$

aus der natürlichen Einbettung von K in $K[X_f \mid f \in F]$ und dem natürlichen Homomorphismus ρ. Der Körper K' wird so zur K-Algebra und damit zu einer Körpererweiterung von K. Es reicht zu zeigen, jedes f∈F besitzt in K eine Nullstelle. Mit

$$\alpha_f := \rho(X_f) \in K'$$

gilt

$$f(\alpha_f) = f(\rho(X_f)) = \rho(f(X_f)) = 0.$$

Das letzte Gleichheitszeichen gilt dabei wegen

$$f(X_f) \in I \subseteq m = \mathrm{Ker}(\rho).$$

QED.

3.3.5 Die Existenz einer algebraischen Abschließung

Seien k ein Körper und K/k eine Körpereweiterung mit K algebraisch abgeschlossen. Wir setzten

$$\overline{k} := \{\ x \in K \mid x \text{ algebraisch über } k\ \}.$$

Dann ist $\overline{k}$ ein Teilkörper von K und eine algebraische Abschließung im Sinne von 3.3.1. Insbesondere besitzt jeder Körper eine algebraische Abschließung.

Beweis. 1. Schritt: $\overline{k}$ ist ein Teilkörper von K.

Seien $x,y \in \overline{k}$. Dann ist x algebraisch über k und y ist algebraisch über k, also auch über k(x). Dann sind

$$k(x)/k \text{ und } k(x,y)/k(x)$$

endliche algebraische Körpererweiterungen, also ist auch

$$k(x,y)/k$$

eine solche. Insbesondere sind die folgenden Elemente algebraisch über k:

$$x+y,\ x \bullet y \in k(x,y)$$

im Fall $y \neq 0$ auch

$$x/y \in k(x,y).$$

Die Köperoperationen von K führen also nicht aus $\overline{k}$ heraus und $\overline{k}$ ist mit diesen Operationen ein Körper. Nach Konstruktion gilt

$$k \subseteq \overline{k} \subseteq K$$

und $\overline{k}$ ist algebraisch über k.

2. Schritt: $\overline{k}$ ist algebraisch abgeschlossen.

Sei

$$f(X) \in \overline{k}[X]$$

ein nicht-konstantes Polynom. Dann gibt es in K eine Nullstelle von f, sagen wir

$$\alpha \in K,\ f(\alpha) = 0.$$

Es reicht zu zeigen, α liegt sogar in $\overline{k}$. Nach Konstruktion ist α algebraisch über $\overline{k}$, d.h.

$$\overline{k}\,(\alpha)/\overline{k}$$

ist eine algebraische Körpererweiterung. Da $\overline{k}/k$ algebraisch ist, ist es auch $\overline{k}$ $(\alpha)/k$ (nach 3.2.11). Also ist α algebraisch über k, d.h. es gilt $\alpha \in \overline{k}$.
QED.

3.3.6 Die Eindeutigkeit der algebraischen Abschließung

Seien k ein Körper und $\overline{k}$ eine algebraische Abschließung. Dann gilt:

(i) Die natürliche Abbildung $\varphi: k \longrightarrow \overline{k}$ ist ein k-Homomorphismus mit Werten in einem algebraisch abgeschlossenen Körper.

(ii) Für jeden k-Homomorphimus $\rho: k \longrightarrow K$ mit Werten in einem algebraisch abgeschlossenen Körper K gibt es einen (nicht notwendig eindeutig bestimmten) k-Homomorphismus $\tilde{\varphi}: \overline{k} \longrightarrow K$, für welchen das folgenden Diagramm kommutativ wird.

$$\begin{array}{ccc} k & \xrightarrow{\varphi} & K \\ \rho\downarrow & \nearrow \tilde{\varphi} & \\ \overline{k} & & \end{array}$$

(iii) Ist K algebraisch über k, so ist jeder k-Homomorphismus $\tilde{\varphi}$ wie in (ii) ein k-Isomorphismus.

Bemerkung
Je zwei algebraische Abschließungen sind also isomorph. Der Isomorphismus ist jedoch im allgemeinen nicht eindeutig bestimmt (es gibt keinen "natürlichen" Isomorphismus).

Beweis. Zu (i). Trivial.

Zu (ii). Folgt aus dem Fortsetzungssatz 3.3.3 (mit F= k und $h = \varphi: k \longrightarrow K$).

Zu (iii). Als k-Homomorphismus ist

$$\tilde{\varphi}: \overline{k} \longrightarrow K$$

injektiv. Es reicht also, die Surjektivität zu beweisen. Sei

$$\alpha \in K$$

vorgegeben. Nach Voraussetzung ist K algebraisch über k. Sei

$$f_\alpha(X) \in k[X]$$

das Minimalpolynom von α über k. Weil $\overline{k}$ algebraisch abgeschlossen ist, zerfällt das Polynom f_α über $\overline{k}$ in Linearfaktoren, d.h.

$$f_\alpha = c \bullet (X-\alpha_1) \bullet \ldots \bullet (X-\alpha_r) \text{ mit } c \in k \text{ und } \alpha_1, \ldots, \alpha_r \in \overline{k}.$$

Wir wenden $\tilde{\varphi}$ auf die Koeffizienten von f_α an und erhalten, da diese in k liegen,

$$f_\alpha(X) = f_\alpha^{\tilde{\varphi}}(X) = \tilde{\varphi}(c) \bullet (X - \tilde{\varphi}(\alpha_1)) \bullet \ldots \bullet (X - \tilde{\varphi}(\alpha_r)).$$

Wegen $f_\alpha(\alpha) = 0$ gibt es somit ein i mit $\alpha = \tilde{\varphi}(\alpha_i) \in \mathrm{Im}(\tilde{\varphi})$. Insbesondere liegt α im Bild von $\tilde{\varphi}$.
QED.

3.4 Zerfällungskörper und normale Erweiterungen

3.4.1 Definition: Zerfällungskörper

Seien K/k eine Körpererweiterung und

$$\{f_i\}_{i\in I}\ ,\ f_i \in k[X]$$

eine Familie von Polynomen aus k[X]. Jedes der f_i zerfalle in Linearfaktoren über K,

$$f_i(X) = c_i(X - \alpha_{i1})\bullet\ldots\bullet(X - \alpha_{i,n(i)}),\ c_i\in k,\ \alpha_{ij} \in K.$$

Sei

$$M = \{\alpha_{ij} \mid i \in I,\ j = 1,\ldots,n(i)\}$$

die Menge der Nullstellen aller f_i in K.

Dann zerfallen die $f_i(X)$ auch über

$$K' := k(M)$$

in Linearfaktoren, und K' ist der kleinste Körper zwischen k und K mit dieser Eigenschaft.[19] Er heißt Zerfällungskörper der f_i über k (in K).

Bemerkung
Ziel dieses Abschnitts ist es, die Eindeutigkeit des Zerfällungskörpers bis auf k-Isomorphie zu beweisen und dessen grundlegende Eigenschaften zu behandeln.

3.4.2 Charakterisierung der Zerfällungskörper

Seien k ein Körper, $\overline{k}$ eine algebraische Abschließung von k und K ein Körper zwischen k und $\overline{k}$,

$$k \subseteq K \subseteq \overline{k}.$$

Dann sind folgende Bedingungen äquivalent.

(i) K/k ist Zerfällungskörper einer Menge von Polynomen aus k[X].

(ii) Jeder k-Homomorphismus $h:K \longrightarrow \overline{k}$ ist ein k-Automorphismus $K\longrightarrow K$, d.h. es gilt h(K) = K.

(iii) Jedes irreduzible Polynom $f(X)\in k[X]$ mit einer Nullstelle in K zerfällt über K in Linearfaktoren.

Beweis. (i) $\Rightarrow$ (ii). Sei

$$M := \{\ \alpha\in\overline{k} \mid f_i(\alpha)=0 \text{ für ein } i\in I\}$$

die Menge aller Nullstellen aller f_i. Dann gilt

$$K = k(M),$$

d.h. die Elemente sind Quotienten von Polynomen über k in den Elementen von M. Es folgt

$$h(K) = h(k(M)) = k(h(M)).$$

Als k-Homomorphismus induziert h auf der Menge der Nullstellen von f_i eine Permutation.[20] Es gilt also

---

[19] d.h. jeder Körper zwischen k und K, über dem die f_i in Linearfaktoren zerfallen, enthält K' als Teilkörper.

$$h(M) = M,$$

also

$$h(K) = K.$$

(ii) $\Rightarrow$ (iii): Seien

$$f \in k[X]$$

ein irreduzibles Polynom,

$$\alpha \in K$$

eine Nullstelle von f und

$$\beta \in \overline{k}$$

eine weitere Nullstelle von f. Es reicht zu zeigen, auch β liegt in K.

Nach dem Fortsetzungssatz 3.3.3 gibt es eine k-Einbettung

$$h: k(\alpha) \longrightarrow \overline{k} \text{ mit } h(\alpha) = \beta.$$

Wir setzen diesen zu einer k-Einbettung

$$\widetilde{h}: K \longrightarrow \overline{k}.$$

fort. Nach Voraussetzung (ii) gilt dann

$$\widetilde{h}(K) = K,$$

also

$$\beta = \widetilde{h}(\alpha) \in \widetilde{h}(K) = K.$$

(iii) $\Rightarrow$ (i). Für jedes $\alpha \in K$ zerfällt das Mininmalpolynom f_α von α über k in Linearfaktoren über K, d.h. K ist Zerfällungskörper der Familie

$$\{f_\alpha\}_{\alpha \in K}$$

über k.
QED.

3.4.3 Definition: normale Körpererweiterungen

Eine algebraische Körpererweiterung K/k, die den äquivalenten Bedingungen von 3.4.2 genügt, heißt normal.

Beispiel 1

Sei $\zeta = e^{2 \pi i/n}$ eine primitive Einheitswurzel. Dann ist die Körpererweiterung

$$\mathbb{Q}(\zeta)/\mathbb{Q}$$

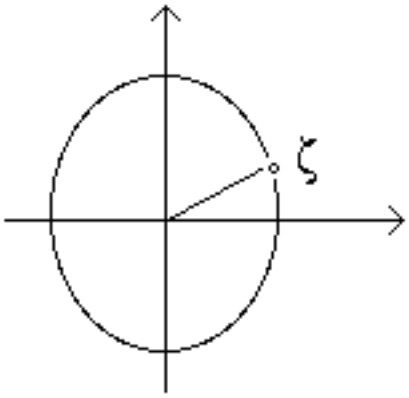
normal.

Beweis. Die ersten n Potenzen von ζ sind paarweise verschieden und Nullstellen von

$$f(X) = X^n - 1 \in \mathbb{Q}[X].$$

---

[20] Für $\alpha \in K$ gilt $f_i(h(\alpha)) = h(f_i(\alpha))$. Mit α ist also auch $h(\alpha)$ eine Nullstelle von f_i. Also induziert h auf zwischen den endlichen Nullstellen-Mengen von f_i in K und in $\overline{k}$ eine Injektion. Da beide Mengen aus derselben Zahl von Elementen bestehen, handelt es sich sogar um eine Bijektion.



Der Einheitskreis wird durch die Potenzen von ζ in n gleiche Sektoren geteilt.

Sie liegen alle im Körper $\mathbb{Q}(\zeta)$. Also ist dieser Zerfällungskörper von f über $\mathbb{Q}$.
QED.

Beispiel 2
Jede Quadratische Erweiterung, d.h. jede Erweiterung K/k des Grades 2 ist normal.

Beweis. Seien $\alpha \in K - k$ und $f_\alpha \in k[x]$ das Minimalpolynom von α. Dann gilt

$$k(\alpha) \subseteq K$$

und

$$1 <^{21} \deg f_\alpha = [k(\alpha):k] \mid [K : k] = 2$$

Es folgt

$$\deg f_\alpha = 2 \text{ und } k(\alpha) = K.$$

Als quadratisches Polynom mit einer Nullstelle $\alpha \in K$ zerfällt f_α über K in Linearfaktoren, d.h. K ist Zerfällungskörper von f_α über k.

QED.

Beispiel 2
Die Erweiterung

$$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$$

ist nicht normal.

Beweis. Wegen $\sqrt[3]{2} \in \mathbb{R}$ gilt

$$K := \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}.$$

Das Polynom

$$f(X) = X^3 - 2$$

besitzt in K die Nullstelle $\sqrt[3]{2}$. Die beiden anderen Nullstellen sind jedoch komplexe Zahlen[22] mit einem Imaginärteil $\neq 0$, liegen also nicht in K. Also ist K/k nicht normal.
QED.

---

[21] weil α nicht in k liegt.

[22] Sie entstehen aus $\sqrt[3]{2}$ durch Multiplikation mit den dritten Einheitswurzeln $-\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$.

3.4.4 Eindeutigkeit des Zerfällungskörpers

Seien K/k und K'/k zwei Körpererweiterungen und

(1) $\{f_i\}_{i\in I}$

eine Familie von Polynomen aus k[X], von denen jedes über K und über K' in Linearfaktoren zerfalle. Wir bezeichnen mit

$$L \text{ bzw. } L'$$

den Zerfällungskörper von über k in K bzw. in K'. Dann gibt es einen (nicht notwendig eindeutig bestimmten) k-Isomorphismus

$$L \longrightarrow L'.$$

Beweis. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccccc} \overline{L} & & & & \\ \cup & & & & \\ L & \nwarrow\tau & & & \\ \cup & & & & \\ k & \subset & L' & \subset & \overline{L}' \end{array}$$

Dabei seien $\overline{L}$ bzw. $\overline{L}'$ eine algebraische Abschließungen von L bzw. L' und τ eine Forsetzung der Einbettung $k \hookrightarrow L \hookrightarrow \overline{L}$ auf L'. Eine solche existiert, weil $\overline{L}$ algebraisch abgeschlossen ist (nach 3.3.3). Analog sei $\sigma: L \longrightarrow \overline{L}'$ eine Fortsetzung der Einbettung $k \hookrightarrow L' \hookrightarrow \overline{L}'$ auf L (die ebenfalls nach 3.3.3 existiert):

$$\begin{array}{ccccc} \overline{L} & & & & \\ \cup & & & & \\ L & & & & \\ \cup & \searrow\sigma & & & \\ k & \subset & L' & \subset & \overline{L}' \end{array}$$

Da σ und τ Homomorphismen über k sind, überführen sie die Nullstellen der f_i in Nullstellen der f_i. Da diese Nullstellen die Körper L bzw. L' erzeugen, folgt

$$\sigma(L) \subseteq L' \text{ und } \tau(L') \subseteq L,$$

d.h. σ und τ sind k-Homomorphismen

$$\sigma: L \longrightarrow L' \text{ bzw. } \tau: L' \longrightarrow L.$$

Die beiden Zusammensetzungen

$$\tau\circ\sigma: L \longrightarrow L \text{ und } \sigma\circ\tau: L' \longrightarrow L'$$

sind nach 3.4.2 Automorphismen über k. Insbesondere sind σ und τ surjektiv. Als k-Homomorphismen sind sie injektiv, d.h. σ und τ sind k-Isomorphismen

$$K \longrightarrow K' \text{ bzw. } K' \longrightarrow K.$$

QED.

3.4.5 Eigenschaften normaler Körpererweiterungen

Seien K/k und L/k algebraische Körpererweiterungen.

(i) Ist K/k normal und KL definiert, so ist auch

$$KL/L \text{ normal.}$$

(ii) Ist K/k normal und F ein Körper zwischen k und K,

$$k \subseteq F \subseteq K.$$

dann ist K/F normal.

(iii) Sind K' und K" Körper zwischen k und K so besteht die folgende Implikation:

$$K'/k \text{ und } K"/k \text{ normal} \Rightarrow K'K"/k \text{ normel und } K' \bigcap K"/k \text{ normal.}$$

Beweis. Zu (i) und (ii). Nach Voraussetzung gilt

$$K = k(\alpha_i \mid i \in I),$$

wobei $\{\alpha_i \mid i \in I\}$ die Menge der Nullstellen einer Familie von Polynomen $f_j \in k[x]$ ist.

In der Situation von (i) gilt

$$KL = L(\alpha_i \mid i \in I)$$

und die f_j lassen sich als Polynome aus L[x] auffassen.

In der Situation von (ii) gilt auch

$$K = F(\alpha_i \mid i \in I),$$

und die f_j lassen sich als Polynome aus F[x] auffassen.

Zu (iii). Wir können bei Bedarf den gemeinsamen Oberkörper K durch KL ersetzen und danach vergrößern. Deshalb können wir annehmen,

$$K/k \text{ ist normal.}$$

Normalität von K'K"/k:
Sei

$$h: K'K" \longrightarrow \overline{k}$$

eine k-Einbettung in eine algebraische Abschließung $\overline{k}$ von k. Nach dem Fortsetzungssatz 3.3.3 gibt es eine Fortsetzung von h zu einer k-Einbettung

$$\widetilde{h}: K \longrightarrow \overline{k}.$$

Weil K/k normal ist, kann man $\widetilde{h}$ auch als k-Automorphismus

$$\widetilde{h}: K \longrightarrow K$$

ansehen. Auf Grund der Normalität von K' und K" über k erhalten wir

$$\widetilde{h}(K') = K' \text{ und } \widetilde{h}(K") = K",$$

also

$$h(K'K") = \widetilde{h}(K'K") = \widetilde{h}(K')\widetilde{h}(K") = K'K".$$

Die mittlere Identität besteht, weil die Bildung des Kompositums mit k-Isomorphismen kommutiert (nach Defintion des Kompositums).

Normalität von $K' \bigcap K"/k$.
Sei

$$h: K' \bigcap K" \longrightarrow \overline{k}$$

eine k-Einbettung in eine algebraische Abschließung $\overline{k}$ von k. Nach dem Fortsetzungssatz 3.3.3 gibt es eine Fortsetzung von h zu einer k-Einbettung

$$\widetilde{h}: K \longrightarrow \overline{k},$$

welche auch als k-Automorphismus

$$\widetilde{h}: K \longrightarrow K$$

aufgefaßt werden kann. Auf Grund der Normalität von K' und K" über k erhalten wir

$$\widetilde{h}(K') = K' \text{ und } \widetilde{h}(K") = K",$$

also

$$h(K' \bigcap K'') = \tilde{h}(K' \bigcap K'') = \tilde{h}(K') \bigcap \tilde{h}(K'') = K' \bigcap K''.$$

QED.

3.5 Separabilität

Zum Inhalt des Abschnitts

Sei K/k eine algebraische Körpererweiterung. Ein Element $\alpha \in K$ heißt inseparabel über k, falls das Minimalpolynom f_α von α über k in irgendeiner Erweiterung mehrfache Nullstellen besitzt, und andernfalls separabel über k. Die Erweiterung K/k heißt separabel, falls jedes $\alpha \in K$ separabel über k ist, und andernfalls inseparabel.

Fakten

(i) Inseparable Erweiterungen gibt es nur in positiver Charakteristik.

(ii) Jede endliche separable Erweiterung ist einfach (Satz vom primitiven Element).

(iii) Die separablen Elemente einer algebraischen Erweiterung K/k bilden einen Teilkörper, die separable Abschließung von k in K. Erweiterungen mit trivialer separabler Abschließung heißen rein inseparabel.

(iv) Jede algebraische Erweiterung K/k ist die Zusammensetzung aus einer separablen und einer rein inseparablen Erweiterung,

$$k \subseteq k^s \subseteq K.$$

Die Grade

$$[K:k]_s := [k^s : k]$$

$$[K:k]_i := [K:k^s]$$

heißen Separabilitätgrad bzw. Inseparabilitätsgrad von K/k. Diese Verhalten sich wie der Grad, d.h. sie multiplizieren sich beim Zusammensetzen von Erweiterungen.

(v) Der Separabilitätsgrad $[K:k]_s$ von K/k ist gerade die Anzahl der k-Einbettungen

$$K \longrightarrow \overline{k}$$

in eine algebraische Abschließung von k.

(vi) Rein inseparable Erweiterungen sind gerade die Zusammensetzungen von Erweiterungen der Gestalt

$$k(\sqrt[p]{\alpha})/k \text{ mit } p = \text{char}(k).$$

3.5.1 Separabilitätsgrad

Seien

$$K/k$$

eine endliche Körpererweiterung und $\overline{k}$ eine algebraische Abschließung des Körpers k. Dann heißt die Anzahl der k-Einbettungen von K in $\overline{k}$ Separabilitätsgrad von K über k und wird mit

$$[K:k]_s := \#\{\sigma : K \longrightarrow \overline{k} \mid \sigma \text{ ist eine k-Einbettung}\}$$

bezeichnet. Die Bilder eines Elements $\alpha \in K$ bei diesen k-Einbettungen heißen die zu α über k konjugierten Elemente (von $\overline{k}$).

Bemerkungen

(i) Da je zwei algebraische Abschließungen k-isomorph sind (nach 3.3.6), ist die Definition des Separabilitätsgrads unabhängig von der speziellen Wahl von $\overline{k}$.

(ii) Der Separabilitätsgrad ist endlich. Um das einzusehen, wählen wir eine k-Vektorraumbasis von K über k, sagen wir

$$K = k\bullet\omega_1+...+k\bullet\omega_n.$$

Zum Beweis der Endlichkeit des Separabilitätsgrades reicht es zu zeigen, daß es für das Bild jedes Basiselementes ω_i bei einer k-Einbettung nur endlich viele Möglichkeiten gibt.
Jedes der Basiselemente ω_i ist nach Voraussetzung algebraisch über k. Sei

$$f_{\omega_i}(X) \in k[X]$$

das Minimalpolynom von ω_i über k. Die Bilder von ω_i bei einer k-Einbettung sind aber wieder Nullstellen von f_{ω_i}, und die Zahl dieser Nullstellen ist endlich.

3.5.2 Beispiel: $[k(\alpha):k]_s$

Seien K/k eine einfache algebraische Körpererweiterung, sagen wir

$$K = k(\alpha),$$

und bezeichne f_α das Minimalpolynom von α über k. Dann gilt gerade die Anzahl

$$\begin{aligned}[k(\alpha):k]_s &= \text{Anzahl der Nullstellen von } f_\alpha \\ &= \text{Anzahl der zu } \alpha \text{ konjugierten Elemente}\end{aligned}$$

Insbesondere gilt

$$[k(\alpha):k]_s \leq [k(\alpha):k]$$

Beweis. Für jede Nullstelle $\beta\in\overline{k}$ von f_α gibt es genau eine k-Einbettung

$$\sigma:k(\alpha) \longrightarrow \overline{k} \text{ mit } \sigma(\alpha) = \beta$$

(nach dem Fortsetzungssatz 3.3.3). Deshalb gilt die ersten Identität und, nach Definition des Begriffs „konjugiertes Elements“ (vgl. 3.5.1) auch die zweite.
QED.

3.5.3 Verhalten beim Zusammensetzen von Körpererweiterungen

Seien K/k eine endliche Körpererweiterung und F ein Körper zwischen k und K,

$$k \subseteq F \subseteq K.$$

Dann gilt

$$[K:k]_s = [K:F]_s\bullet[F:k]_s.$$

Beweis. Bezeiche

$$\overline{F}$$

eine algebraische Abschließung von F und

$$Hom_k(K', K'')$$

die Menge der k-Einbettungen des Körpers K' in den Körper K".

Wir betrachten die Abbildung

$$\psi:Hom_k(K, \overline{F}) \longrightarrow Hom_k(F, \overline{F}), \sigma \mapsto \sigma|_F.$$

Es gilt

$$\mathrm{Hom}_k(K,\overline{F}) = \bigcup_{\tau\in\mathrm{Hom}_k(F,\overline{F})} \psi^{-1}(\tau).$$

also

$$[K:k]_s = \#\,\mathrm{Hom}_k(K,\overline{F}) = \sum_{\tau\in\mathrm{Hom}_k(F;\overline{F})} \#\,\psi^{-1}(\tau).$$

Es reicht zu zeigen,

(1) Alle Mengen $\psi^{-1}(\tau)$ bestehen aus derselben Anzahl von Elementen,

denn dann gilt

$$\begin{aligned}[K:k]_s &= \#\,\mathrm{Hom}_k(F,\overline{F}) \bullet \#\,\psi^{-1}(\mathrm{Id})\\ &= [F:k]_s \bullet \#\{\sigma\in\mathrm{Hom}_k(K,\overline{F}) \mid \sigma|_F = \mathrm{Id}\}\\ &= [F:k]_s \bullet \#\,\mathrm{Hom}_F(K,\overline{F})\\ &= [F:k]_s \bullet [K:F]_s\,.\end{aligned}$$

Aussage (1) ergibt sich aber aus dem nachfolgenden Satz.
QED.

3.5.4 Forsetzungsatz III

Für jeden Körperturm

$$k \subseteq F \subseteq K$$

von algebraischen Erweiterungen besteht eine Bijektion zwischen je zwei Fasern der Abbildung

$$\psi{:}\mathrm{Hom}_k(K,\overline{F}) \longrightarrow \mathrm{Hom}_k(F,\overline{F}),\ \sigma \mapsto \sigma|_F.$$

Insbesondere ist die Abbildung surjektiv.

Beweis. Sei $\tau\in\mathrm{Hom}_k(F,\overline{F})$ vorgegeben. Es reicht eine Bijektion

(1) $$\{\sigma\in\mathrm{Hom}_k(K,\overline{F}) \mid \sigma|_F = \mathrm{Id}\} \longrightarrow \{\sigma\in\mathrm{Hom}_k(K,\overline{F}) \mid \sigma|_F = \tau\}$$

zu konstruieren.

Nach dem Fortsetzungssatz 3.3.3 gibt es eine Fortsetzung von $\tau\colon F \longrightarrow \overline{F}$ zu einer k-Einbettung

$$\widetilde{\tau} : \overline{F} \longrightarrow \overline{F}.$$

Nach dem Eindeutigkeitssatz für algebraische Abschließungen (vgl. 3.3.6(iii)) ist diese ein k-Automorphismus.

Eine Bijektion (2) kann man deshalb durch

$$\sigma \mapsto \widetilde{\tau}\circ\sigma$$

definieren (und die Umkehrung durch $\sigma \mapsto \widetilde{\tau}^{-1}\circ\sigma$.
QED.

3.5.5 Vergleich mit dem Körpergrad

Für jede endliche Körpererweiterung K/k gilt

$$[K:k]_s \le [K:k].$$

Beweis. Als endliche Körpererweiterung ist K/k endlich erzeugt, sagen wir

$$K = k(\alpha_1,...,\alpha_n)$$

Wir führen den Beweis durch Induktion nach n. Im Fall n = 1 gilt die Behauptung auf nach Beispiel 3.5.2. Sei jetzt n > 1.Wir setzen

$$F := k(\alpha_1)$$

Dann gilt

$$K = F(\alpha_2,...,\alpha_n).$$

und

$$[K:F]_s \leq [K.F].$$

$$[F:k]_s \leq [F:k].$$

(das erste nach Induktionsvoraussetzung, das zweite auf Grund des Induktionsanfangs). Durch Multiplikation der untereinander stehenden Ausdrücke erhalten wir

$$[K:k]_s \leq [K:k]$$

(nach 3.5.3 bzw. 3.2.9)
QED.

3.5.6 Separabilität: Polynome, Elemente und Erweiterungen

Sei k ein Körper. Ein nicht-konstantes Polynom $f(X) \in k[X]$ heißt <u>separabel</u> über k, wenn es in keinem Erweiterungskörper K von k eine mehrfache Nullstelle besitzt. Sei K/k eine algebraische Körpererweiterung. Ein Element $\alpha \in K$ heißt <u>separabel</u> über k, wenn das Minimalpolynom f_α von α über k separabel ist.

Eine algebraische Körpererweiterung K/k heißt <u>separabel</u>, wenn jedes Element von K separabel ist über k. Im entgegengesetzten Fall spricht man von <u>inseparabel</u>.

Bemerkungen

(i) Ist K/k eine separable algebraische Erweiterung und F ein Körper zwischen k und K, so ist (trivialerweise) auch F/k separabel.

(ii) In der Situation von (i) ist aber auch K/F separabel.

Beweis von (ii). Sei $\alpha \in K$. Seien

$$f_\alpha \in k[X] \text{ und } g_\alpha \in F[X]$$

die Minimalpolynome von α über k bzw. über F. Wegen $k \subseteq F$ ist dann das Polynom g_α ein Teiler von f_α ,

$$g_\alpha \mid f_\alpha.$$

Mit f_α ist dann aber auch g_α separabel.
QED.

3.5.7 Beispiel: eine inseparable Körpererweiterung vom Grad p

Seien p eine Primzahl k der rationale Funktionenkörper

$$k = \mathbb{F}_p(T)$$

in einer Unbestimmten T über dem Körper $\mathbb{F}_p$ aus p Elementen. Das Polynom

$$f(X) := X^p - T \in \mathbb{F}_p[T]$$

ist ein Eisenstein-Polynom bezüglich T, also irreduzibel über k. Sei

$$K/k$$

eine Körpererweiterung, die eine Nullstelle

$$x \in K$$

von f(X) enthält.Dann gilt

$$f(X) = X^p - T = X^p - x^p = (X-x)^p \text{ über } K.$$

also:

(i) $f(X) := X^p - T$ ist inseparabel über k.
(ii) Jede Nullstelle von f ist inseparabel.
(iii) Der Körper

$$F := k[X]/(X^p - T)$$

inseparabl, normal und vom Grad p über k.

Bemerkung
Der nachfolgende Satz zeigt, daß separable Erweiterung eine besonders einfache Struktur besitzen: sie sind alle vom Typ des in 3.2.3 berschriebenen Beispiels.

3.5.8 Der Satz vom primitiven Element

Sei K/k eine endliche separable Körpererweiterung. Dann besitzt K über k ein primitives Element, d.h. ein Element $\alpha \in K$ mit

$$K = k(\alpha).$$

Beweis. Wir führen den Beweis hier nur für den Fall,, daß k unendlich viele Elemente enthält,

$$\# k = \infty.$$

Den Fall endlicher Körper behandeln wir im nächsten Abschnitt (vgl. 3.6.5). Weil K/k endlich ist, gilt

$$K = k(\alpha_1,...,\alpha_r).$$

Wir führen den Beweis durch Induktion nach r. Der Fall r = 1. ist trivial. Sei jetzt

$$r > 1.$$

Nach Induktionsvoraussetzung besitzt dann

$$k(\alpha_1,...,\alpha_{r-1})/k$$

ein primitives Element, sagen wir x, d.h.

$$k(\alpha_1,...,\alpha_{r-1}) = k(x)$$

und es gilt

$$K = k(x, y)$$

mit $y = \alpha_r$. Seien

$$f := f_x \text{ und } g := f_y$$

die Minimalpolynome von x bzw. y über k. In einer algebraischen Abschließung

$$\overline{K}$$

von k, die K enthält, zerfallen f und g in Linearfaktoren, sagen wir

$f(X) = (X-x_1)\bullet...\bullet(X-x_r)$ mit $x = x_1$

$g(X) = (X-y_1)\bullet...\bullet(X-y_s)$ mit $y = y_1$

Weil K/k separabel ist, sind die x_i paarweise verschieden und dasselbe gilt für die y_j. Die Gleichungen

$$x_i + Xy_j = x + Xy \ (i=1,...,r, j = 2,...,r)$$

in der Unbestimmten X haben jede höchstens eine Lösungen. Da k unendlich ist, gibt es ein

$$c \in k - \{0\}$$

das von allen diesen Lösungen verschieden ist, d.h. es gilt

(1) $$x_i + cy_j \neq x + cy \ (i=1,...,r, j = 2,...,r).$$

Wir setzen

$$\theta := x + cy.$$

Es reicht zu zeigen, θ ist ein primitives Element, d.h.

$$K = k(\theta).$$

Nach Konstruktion gilt

$$\theta \in k(x,y) = K.$$

Es reicht zu zeigen

(2) $$x,y \in k(\theta).$$

Zu Beweis beachten wir, y ist Nullstelle der Polynome

$$f(\theta - cX) , g(X) \in k(\theta)[X].$$

Es gilt nämlich

$$f(\theta - cy) = f(x) = 0.$$

Die Polynome $f(\theta - cX)$, $g(X)$ haben also einen größten gemeinsamen Teiler positiven Grades

$$\deg ggT(f(\theta - cX) , g(X)) > 0.$$

Außer y haben die beiden Polynome keine weiteren gemeinsamen Nullstellen: für jede Nullstelle y_j von g mit $j>1$ gilt $\theta - cy_j = x + cy - cy_j \neq x_i$ (wegen (1)) also

$$f(\theta - cy_j) \neq 0.$$

Wegen der Separabilität von K/k besitzt g keine mehrfachen Nullstellen und der ggT ist ´linear,

$$ggT(f(\theta - cX) , g(X)) = X - y.$$

Nun hat der größte gemeinsame Teiler Koeffizienten im selben Körper wie die Ausgangspolynome, d.h. es gilt

$$X - y \in k(\theta)[X],$$

also

$$y \in k(\theta),$$

also

$$x = \theta - cy \in k(\theta).$$

also

$$k(x,y) \subseteq k(\theta) \subseteq k(x,y).$$

.**QED**.

3.5.9 Kriterium für die Separabilität eines Elements

Seien K/k eine Körpererweiteung und $\alpha \in K$ ein über k algebraisches Element mit dem Minimalpolynom

$$f_\alpha(X) \in k[X]$$

über k. Dann sind folgende Bedingungen äquivalent.

(i) α ist inseparabel über k.

(ii) $\frac{df_\alpha}{dX}(\alpha) = 0$ (d.h. f_α hat in $k(\alpha)$ die mehrfache Nullstelle α).

(iii) $\frac{df_\alpha}{dX}(X) = 0.$

Insbesondere ist jedes algebraische Element über einem Körper der Charakteristik 0 separabel.[23]

Bemerkung

---

[23] denn die Ableiung eines nicht-konstanten Polynoms ist in der Charakteristik 0 stets $\neq 0$.

Bedingung (iii) bedeutet, f_α ist ein Polynom der Gestalt $g(X^p)$ mit $g \in k[X]$, wobei $p > 0$ die Charakteristik von k bezeichne.

Beweis. (i) ⇒ (iii). Nach Voraussetzung hat f_α eine mehrfache Nullstelle, also eine gemeinsame Nullstelle mit seiner Ableitung (vgl. 2.7.15). Weil f_α irreduzibel ist, ist letzteres nur möglich, wenn die Ableitung von f_α identisch Null ist (vgl. auch die Übungsaufgaben).
(iii) ⇒ (ii). trivial.
(ii) ⇒ (i). α ist eine mehrfache Nullstelle von f_α.
QED.

3.5.10 Charakterisierung der separablen Erweiterungen

Sei K/k eine algebraische Körpererweiterung. Dann sind folgende Bedingungen äquivalent.
(i) K/k ist separabel.
(ii) K wird über k von separablen Elementen erzeugt, d.h.

$$K = k(\alpha_i \mid i \in I)$$

mit einer Familie $\{\alpha_i\}_{iPI}$ von Elementen $\alpha_i \in K$, die separabel über k sind.
Falls K/k endlich ist, sind diese Bedingungen auch äquivalent zur folgenden.

(iii) $[K:k]_s = [K:k]$.

Beweis. (i) ⇒ (ii). trivial.

(ii) ⇒ (iii) im Fall K/k endlich.

Weil K/k endlich ist, wird K bereits von endlich vielen der α_i erzeugt[24], sagen wir

$$K = k(\alpha_1,...,\alpha_n).$$

Wir führen den Beweis durch Induktion nach n. Im Fall n = 1 gilt nach 3.5.2

$[K:k]_s$ = Anzahl der Nullstellen des Minimalpolynoms $f_{\alpha_i} = \deg f_{\alpha_i} = [K:k]$.

Sei jetzt $n > 1$. Wir setzen

$$F := k(\alpha_n).$$

Dann gilt

$$K = F(\alpha_1,...,\alpha_{n-1}).$$

Nach Induktionsvoraussetzung gilt

$$[K:F]_s = [K:F]$$

und nach Beispiel 3.5.2 ist

$$[F:k]_s = [F:k].$$

Zusammen erhalten wir (nach 3.5.3 und 3.2.9)

$$[K:k]_s = [K:F]_s\,[F:k]_s = [K:F] \bullet [F:k] = [K:k].$$

(iii) ⇒ (i) im Fall K/k endlich.

---

[24] Wegen $\dim_k K < \infty$ ist jede aufsteigende Kette von k-linearen Unterräumen stationär.

Sei $\alpha \in K$. Wir haben zu zeigen, α ist separabel über k, d.h. wir haben zu zeigen, das Minimalpolynom

$$f_\alpha(X) \in k[X]$$

von α über k hat in keinem Erweiterungskörper von k mehrfache Nullstellen. Falls es doch irgendwo mehrfache Nullstellen hätte, so würde auf Grund von Beispiel 3.5.2

$$[k(\alpha):k]_s < \deg f_\alpha = [k(\alpha):k].$$

gelten. Es reicht also zu zeigen,

(1) $$[k(\alpha):k]_s \geq [k(\alpha):k].$$

Nach Voraussetzung (iii) gilt

$$[K:k(\alpha)]_s \bullet [k(\alpha):k]_s = [K:k]_s = [K:k] = [K:k(\alpha)] \bullet [k(\alpha):k],$$

also

$$[k(\alpha):k]_s = \frac{[K:k(\alpha)]}{[K:k(\alpha)]_s} \bullet [k(\alpha):k] \geq [k(\alpha):k],$$

wobei die Abschätzung rechts besteht wegen 3.5.4. Also gilt tatsächlich (1).

<u>(ii) $\Rightarrow$ (i)</u> im allgemeinen Fall.

Sei

$$\alpha \in K.$$

Wir haben zu zeigen, α ist separabel. Das Element α kann als rationale Funktion in endlich vielen der α_i, $i \in I$, mit Koeffizienten aus k geschrieben werden. Also liegt α in einem von endlich vielen α_i erzeugten Körper, sagen wir

$$\alpha \in k(\alpha_1,...,\alpha_n).$$

Da die α_i nach Voraussetzung (ii) separabel sind über k, genügt die Körpererweiterung

(3) $$k(\alpha_1,...,\alpha_n)/k$$

der Bedingung (ii) des zu beweisenden Satzes. Die Körpererweiterung ist endlich erzeugt und algebraisch, also endlich. Auf Grund der im endlichen Fall bereits bewiesenen Implikationen

$$\text{(ii)} \Rightarrow \text{(iii)} \Rightarrow \text{(i)}$$

ist die Körpererweiterung (3) separabel. Insbesondere ist $\alpha \in k(\alpha_1,...,\alpha_n)$ separabel über dem Körper k.

QED.

3.5.11 Eigenschaften separabler Körpererweiterungen

Die separablen Körpererweiterungen bilden eine ausgezeichnete Klasse.

Beweis. <u>Eigenschaft 1</u>. Sei

$$k \subseteq F \subseteq K$$

ein Körperturm algebraischer Erweiterungen. Wir haben die folgenden Implikationen zu beweisen.

1. K/k separabel $\Rightarrow$ F/k separabel.

2. K/k separabel $\Rightarrow$ K/F separabel.

3. K/F und F/k separabel $\Rightarrow$ K/k separabel.

Zu 1. trivial.
Zu 2. siehe Bemerkung 3.5.5 (ii).
Zu 3. Sei $\alpha \in K$. Wir haben zu zeigen,

$$\alpha \text{ ist separabel über } k.$$

Nach Voraussetzung ist α separabel über F, d.h. die Abbleitung des Minimalpolynoms

$$f_\alpha \in F[X]$$

von α über F ist nicht Null an der Stelle α,

$$f_\alpha'(\alpha) \neq 0$$

(vgl. 3.5.8). Seien

$$\alpha_1,...,\alpha_r \in F$$

die Koeffizienten von f_α. Dann ist f_α auch das Minimalpolynom von α über

$$F' := k(\alpha_1,...,\alpha_r).$$

Nach 3.5.8 ist α separabel über F' und nach 3.5.9 ist die Körpererweiterung

$$F'(\alpha)/F' \text{ separabel}$$

(da von separablen Elementen erzeugt). Ebenfalls nach 3.5.9 ist auch

$$F'/k \text{ separabel}$$

(da die $\alpha_i \in F$ separabel über k sind). Die beiden letzten Erweiterungen sind endlich (da sie von endlich vielen algebraisdchen Elementen erzeugt werden). Die Separabilität dieser Erweiterungen ist nach 3.5.9 äquivalent zu

(1) $\quad [F'(\alpha):F']_s = [F'(\alpha):F']$ und $[F':k]_s = [F':k]$.

Damit gilt

$$\begin{aligned} [F'(\alpha):k]_s &= [F'(\alpha):F']_s \bullet [F':k]_s \quad \text{(nach 5.3.5)} \\ &= [F'(\alpha):F'] \bullet [F':k] \quad \text{(wegen (1))} \\ &= [F'(\alpha):k]. \quad \text{(nach 3.2.9)} \end{aligned}$$

Nach 3.5.9 ist

$$F'(\alpha)/k \text{ separabel},$$

also

$$\alpha \text{ separabel über } k.$$

Eigenschaft 2. Seien K/k und L/k Körpererweiterungen mit

$$K/k \text{ separabel (und algebraisch).}$$

Weil K separabel ist über k, gilt

$$K = k(\alpha_i \mid i \in I)$$

mit über k separablen Elementen α_i. Dann gilt aber

$$KL = L(\alpha_i \mid i \in I)$$

und die α_i sind auch separabel über L[25]. Dann ist aber KL separabel über L (nach 3.5.9 (ii)).
QED.

3.5.12 Die separable Abschließung, rein inseparable Erweiterungen

Seien K/k eine algebraische Körpererweiterung und $\overline{k}$ eine algebraische Abschließung von k, welche K enthält[26],

---

[25] denn die Minimalpolynome über L teilen die Minimalpolynome über k.

[26] sei $\overline{k}$ zum Beispiel eine algebraische Abschließung von K

$$K \subseteq \overline{k}.$$

Dann heißt

$$k_{sep} := \{ \alpha \in \overline{k} \mid \alpha \text{ separabel über } k \}$$

separable Abschließung von k in $\overline{k}$ und

$$K \cap k_{sep} = \{ \alpha \in K \mid \alpha \text{ separabel über } k \}$$

separable Abschließung von k in K.
Eine algebraische Körpererweiterung K/k heißt rein inseparabel, wenn

$$K \cap k_{sep} = k$$

gilt, d.h. wenn jedes Element von K - k inseparabel ist über k.

Bemerkungen

(i) k_{sep} und $K \cap k_{sep}$ sind Teilkörper von $\overline{k}$ bzw. K.

(ii) k_{sep} ist bis auf k-Isomorphie ein deutig bestimmt.

(iii) Eine algebraische Körpererweiterung K/k ist genau dann rein inseparabel, wenn es für jedes Element $\alpha \in K$ ein $i \in \mathbb{N} \cup \{0\}$ gibt mit

$$\alpha^{p^i} \in k.$$

Dabei bezeichne p die Charakteristik von k (bzw. p sei gleich 1 fall die Charakteristik von k gleich Null ist).

(iv) Der Separatilitätsgrad rein inseparabler (endlicher) Erweiterungen ist 1.

(v) Ist K/k eine endliche Körpererweiterung, so gilt

$$[K:k]_s = [K \cap k_{sep}:k] \text{ und } [K:K \cap k_{sep}]_s = 1.$$

Insbesondere ist $[K:k]_s$ ein Teiler von [K:k]. Der Quotient

$$[K:k]_i := [K:k]/[K:k]_s = [K:K \cap k_s]$$

heißt Inseparabilitätsgrad. Mit anderen Worten: jede endliche Erweiterung ist die Zusammensetzung einer separablen und einer rein inseparablen Erweiterung. Der Separabilitätsgrad mißt den Grad des separablen Teils der Erweiterung und der Inseparabilitätsgrad den des rein inseparablen Teils.

Beweis. Zu (i). , Nach 3.5.9 bestehen die von k_{sep} bzw. $K \cap k_{sep}$ über k erzeugten Körper aus lauter Elementen, die separabel sind über k, d.h. es gilt

$$k(k_{sep}) \subseteq k_{sep}$$

und

$$k(K \cap k_{sep}) \subseteq K \cap k_{sep}$$

Trivialerweise gilt auch "$\supseteq$", d.h. rechts stehen Körper.

Zu (ii). Ist k'_{sep} eine weitere separable Abschließung, sagen wir in der algebraischen Abschließung $\overline{k}'$, so gibt es einen k-Isomorphismus

$$h: \overline{k} \longrightarrow \overline{k}'$$

(nach. 3.3.6). Dieser überführt separable Elemente in separable Elemente (da er deren Minimalpolynome über k nicht ändert), also gilt

$$h(k_{sep}) \subseteq k'_{sep}$$

und analog

$$h^{-1}(k'_{sep}) \subseteq k_{sep}.$$

Also induziert h einen k-Isomorphismus $k_{sep} \longrightarrow k'_{sep}$.

Zu (iii). Wir können annehmen

$$p := \mathrm{char}(k) > 0.$$

Sei K/k ist rein inseparabel. Wir betrachten ein Element

$$\alpha \in K$$

und dessen Minimalpolynom

$$f_\alpha \in k[X]$$

über k. Wir beweisen durch Induktion nach

$$d = \deg f_\alpha,$$

daß es ein i gibt mit $\alpha^{p^i} \in k$. Im Fall d = 1 liegt α selbst schon in k und die Aussage gilt mit i = 0.

Sei jetzt d > 1. Nach Voraussetzung ist f_α inseparabel. Nach 3.6.8 gilt

$$f_\alpha(X) = g_\alpha(X^p) \text{ mit } g_\alpha \in k[X].$$

Das Polynom g_α ist Minimalpolynom von α^p über k: es gilt $g_\alpha(\alpha^p) = 0$ und gäbe es ein Polynom kleineren Grades mit dieser Nullstelle, so gäbe es ein Polynom eines Grades < deg f_α mit der Nullstelle α, d.h. f_α wäre kein Minimalpolynom.

Wegen

$$\deg g_\alpha < \deg f_\alpha$$

gibt es nach Induktionsvoraussetzung ein i mit $(\alpha^p)^{p^i} \in k$.

Wir nehmen umgekehrt an, für jedes $\alpha \in K$ existiert ein $i \in \mathbb{N} \cup \{0\}$ mit

$$\alpha^{p^i} \in k.$$

Wir haben zu zeigen, jedes

$$\alpha \in K\text{-}k$$

ist inseparabel über k. Wegen

$$a := \alpha^{p^i} \in k \text{ für ein } i \in \mathbb{N} \cup \{0\}$$

ist α Nullstelle des Polynoms

$$f(X) := X^{p^i} - a \in k[X].$$

Das Minimalpolynom f_α von α über k ist deshalb ein Teiler von f,

$$f_\alpha \mid f \text{ in } k[X].$$

Nun gilt

$$f(X) = X^{p^i} - \alpha^{p^i} = (X-\alpha)^{p^i},$$

also

$$f_\alpha(X) = (X-\alpha)^n \text{ mit } 0 \le n \le p^i.$$

Wegen $\alpha \notin k$ gilt n = deg $f_\alpha > 1$, d.h. α ist inseparabel über k. Wir haben gezeigt, jedes Element von K-k ist inseparabel, d.h. K/k ist rein inseparabel.

Zu (iv). Sei K/k eine rein inseparable endliche Erweiterung. Dann hat K die Gestalt

$$K = k(\alpha_1,\ldots,\alpha_r),$$

Wir setzen

$$K_i := k(\alpha_1,...,\alpha_i).$$

Es reicht zu z eigen, für jedes i gilt

$$[K_{i+1}:K_i]_s = 1.$$

Es gilt

$$K_{i+1} = K_i(\alpha_{i+1}).$$

Nach (iii) ist $\alpha = \alpha_{i+1}$ Nullstelle eine Polynoms der Gestalt

$$X^{p^i} - a \in k[X]$$

mit $a = \alpha^{p^i}$. Dieses Polynom hat außer α keine weiteren Nullstellen. Das Minimalpolynom f_α von α über K_i teilt dieses Polynom, d.h. auch f_α hat nur eine Nullstelle. Damit gilt aber

$$[K_{i+1}:K_i]_s = 1$$

(nach 3.5.2).

Zu (v). Nach Definition von $K \cap k_{sep}$ ist

$$K \cap k_{sep}/k \text{ separabel}$$

und

$$K/ K \cap k_{sep} \text{ rein inseparabel}$$

(jedes über $K \cap k_{sep}$ separable Element $x \in K$ ist nach 3.5.10 separabel über k also in $K \cap k_{sep}$). Damit gilt

$$[K \cap k_{sep}:k]_s = [K \cap k_{sep}:k]$$

(nach 3.5 .9) und

$$[K: K \cap k_{sep}]_s = 1$$

(nach (iv)). Wir gehen zu den Produkten über und erhalten

$$[K:k]_s = [K \cap k_{sep}:k].$$

QED.

3.6 Endliche Körper

Zum Inhalt des Abschnitts

(i) Körper der Charakteristik 0 sind unendlich

(ii) Endliche Körper K der Charakteristik p sind endlich-dimensionale Vektorräume über ihrem Primkörper $\mathbb{F}_p$, bestehen also aus

$$\# K = p^n$$

Elementen mit $n := \dim_{\mathbb{F}_p} K$.

(iii) Für jede Potenz $q = p^n$ einer Primzahl p gibt es bis auf Isomorphie genau einen Körper mit q Elementen. Dieser heißt Galoisfeld der Ordnung q und wird mit

$$\mathbb{F}_q = GF(q)$$

bezeichnet.

(iv) GF(q) ist der Zerfällungskörper von $X^q - X$[27] über $\mathbb{F}_p$ mit p := char GF(q) und besteht gerade aus 0 und den (q-1)-Einheitswurzeln[28]:

$$GF(q) = \{\alpha \in K \mid \alpha^q = \alpha\}$$

wenn $K := \overline{GF(q)} = \overline{GF(p)}$ eine algebraische Abschließung von GF(q) bezeichnet.

(v) GF(q) besitzt genau dann einen zu GF(q') isomorphen Teilkörper, wenn gilt

$$q'-1 | q-1.$$

In diesem Fall bestitzt GF(q) genau einen solchen Teilkörper. Genauer:

$$GF(q') = \{\alpha \in GF(q) \mid \alpha^{q'} = \alpha\}.$$

Man beachte, jede (q'-1)-te Einheitswurzel ist auch eine (q-1)-te Einheitswurzel.

(vi) Jede Erweiterung von endlichen Körpern ist separabel.

(vii) Die multiplikative Gruppen eines endlichen Körpers ist zyklisch. Insbesondere gibt es für jedes $q = p^n$ in der algebraischen Abschließung von GF(p) eine (q-1)-te primitive Einheitswurzel.

(viii) Abbildung

$$F: GF(q) \longrightarrow GF(q), \alpha \mapsto \alpha^p,$$

ist (für $q = p^n$, p = char GF(q)) ein $\mathbb{F}_p$-Automorphismus. Diese heißt <u>Frobenius-Automorphismus</u> oder auch einfach nur <u>Frobenius</u>.

(ix) Die Automorphismengruppe von GF(q) besteht aus den Potenzen von F, d.h.

$$GF(q) = < F >$$

ist zyklisch mit dem Erzeuger F.

(ix) Im Fall $GF(q') \subseteq GF(q)$ und $q' = p^{n'}$ ist GF(q') der Fixkörper von $F^{n'}$,

$$GF(q') = \{\alpha \in GF(q) \mid F^{n'}(\alpha) = \alpha\}$$

Man beachte, es gilt $F^{n'}(\alpha) = \alpha^{p^{n'}} = \alpha^{q'}$.

3.6.1 Charakteristik, Primkörper, Körpergrad und Ordnung endlicher Körper

Sei F ein endlicher Körper. Dann gilt

(i) Die Charakteristik[29] von F ist eine Primzahl

$$p = \text{char}(F)$$

(ii) Der <u>Primkörper</u>[30] von F ist bis auf Isomorphie gleich

$$\mathbb{F}_p = \mathbb{Z}/(p).$$

(iii) Der Körper F ist eine endliche Körpererweiterung von $\mathbb{F}_p$, d.h. der <u>Körpergrad</u>

$$n = \dim_{\mathbb{F}_p} F = [F: \mathbb{F}_p] < \infty$$

von F ist endlich.

(iv) Der Körper F besteht aus

---

[27] und wegen $X^q - X = X \bullet (X^{q-1} - 1)$ auch der Zerfällungskörper von $X^{q-1} - 1$.

[28] die Zahl der Nullstellen von $X^{q-1} - 1$ ist q-1, weil $X^{q-1} - 1$ separabel ist.

[29] Die Charakteristik ist die kleinste natürliche Zahl p mit $p \bullet 1_F = 0$, falls es eine solche natürliche Zahl gilbt. Andernfalls ist die Charakteristik gleich 0.

[30] d.h. der Durchschnitt aller Teilkörper von F

$$\# F = p^n$$

Elementen.

Bemerkung

Die Ordnung eines endlichen Körpers ist also eine Primzahlpotenz.

Beweis. Zu (i). Weil F endlich ist, gibt es zwei natürliche Zahlen m und n mit

$$m \bullet 1_F = n \bullet 1_F,$$

also eine natürliche Zahl p mit

$$p \bullet 1_F = 0.$$

Sei p die kleinste dieser natürlichen Zahlen. Wäre p keine Primzahl, sagen wir

$$p = a \bullet b$$

mit natürlichen Zahle $\neq 1$, so würde

$$a \bullet 1_F = 0 \text{ oder } b \bullet 1_F = 0$$

gelten im Widerspruch zur Minimalität von p.

Zu (ii). Der Homomorphismus

$$\varphi: \mathbb{Z} \longrightarrow F, g \mapsto g \bullet 1_F .$$

induziert eine Injektion

(1) $$\mathbb{Z}/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi) \subseteq F.$$

(nach dem 0-ten Isomorphiesatz) mit

$$\mathrm{Ker}(\varphi) = m\mathbb{Z}.$$

(weil $\mathbb{Z}$ ein Hauptidealring ist). Weil F nullteilerfrei ist, ist $m\mathbb{Z}$ ein Primideal, also

$$m = p$$

eine Primzahl. Also ist

$$\mathbb{F}_p = \mathbb{Z}/(p) \cong \mathrm{Im}(\varphi) \subseteq F$$

ein Teilkörper von F ist als0 der Primkörper von F.[31]

Zu (iii). Da F endlich ist, wird F als $\mathbb{F}_p$-Vektorraum endlich erzeugt, hat also eine endliche Dimension

$$n = \dim_{\mathbb{F}_p} F.$$

Zu (iv). Als n-dimensionaler $\mathbb{F}_p$-Vektorraum ist F isomorph zu

$$F \cong (\mathbb{F}_p)^n.$$

Also gilt

$$\# F = (\#\mathbb{F}_p)^n = p^n$$

(Ein Element von F ist durch n Koordinaten festgelegt, und für jede Koordinate gibt es p Möglichkeiten).

QED.

3.6.2 Existenz und Eindeutigkeit der endlichen Körper

Seien p eine Primzahl, n eine natürliche Zahl und

$$q = p^n.$$

Dann gelten folgende Aussagen.

(i) Es gibt bis auf $\mathbb{F}_p$-Isomorphie genau einen Körper der Ordnung q. Dieser wird mit

---

[31] Jeder Teilkörper von F enthält 1_F also auch $\mathbb{F}_p$.

$$\mathbb{F}_q$$

bezeichnet und heißt Galois-Feld der Ordnung q.

(ii) In jedem Körper K der Charakteristik p gibt es höchstens einen Teilkörper der Ordnung q und mindestens einen, falls K algebraisch abgeschlossen ist (und jeder Körper, der einen Körper der Ordnung q enthält, hat trivialerweise die Charakteristik p).

(iii) Der Körper $\mathbb{F}_q$ ist der Zerfällungskörper des separablen Polynoms

$$f(X) = X^q - X$$

über dem Körper $\mathbb{F}_p$. Ist $\overline{\mathbb{F}}_p$ eine algebraische Abschließung von $\mathbb{F}_p$, die den Körper $\mathbb{F}_q$ enthält, so gilt

$$\mathbb{F}_q = \{ x \in \overline{\mathbb{F}}_p \mid f(x) = 0 \} = \mathbb{F}_q^* \bigcup \{0\}$$

$$\mathbb{F}_q^* = \{x \in \overline{\mathbb{F}}_p \mid x^{q-1} = 1 \}.$$

Der Körper $\mathbb{F}_q$ ist normal und separabel über $\mathbb{F}_p$.

Beweis. Existenz von $\mathbb{F}_q$. Sei

$$K := \overline{\mathbb{F}}_p$$

eine algebraische Abschließung des Körpers $\mathbb{F}_p = \mathbb{Z}/(p)$ und

$$F := \{x \in K \mid x^q = x\}.$$

Das Polynom

$$f(X) = X^q - X \in K[X]$$

hat höchstens q Nullstellen in K und zerfällt über K in Linearfaktoren (weil K algebraisch abgeschlossen ist). Wegen

$$f'(X) = q \cdot X^{q-1} - 1 = -1 \neq 0$$

hat f in K keine mehrfachen Nullstellen. Die Anzahl der Nullstellen ist also gleich q. Damit besteht die Menge F aus q Elementen,

$$q = \#F.$$

Es reicht also zu zeigen, daß F ein Körper ist. Sind $x,y \in F$ so gilt

$$(xy)^q = x^q \cdot y^q = xy$$

also $xy \in F$. Außerdem gilt, weil K die Charakteristik p hat[32]

$$(x-y)^p = x^p - y^p$$

also auch

$$(x-y)^q = (x-y)^{p^n} = x^q - y^q,$$

also $x-y \in F$. Die Ring-Operationen des Körpers K definieren also Operationen

$$F \times F \longrightarrow F.$$

und F ist, wie gerade gezeigt, eine Untergruppe der Additiven Gruppe des Körpers K. Die übrigen Ringaxiome für F gelten auf Grund der Ringaxiome für K. Wir haben noch zu zeigen, jedes Element

$$x \in F - \{0\}$$

ist in F eine Einheit. Wegen $x^q = x$ gilt aber auch

---

[32] Das Minuszeichen rechts ist für ungerade Primzahlen p offensichtlich. Für p = 2 gilt in K aber -1 = +1.

$$(x^{-1})^q = \frac{1}{x^q} = \frac{1}{x} = x^{-1}$$

also $x^{-1} \in F$.
Bezeichnung

$$F = \mathbb{F}_q.$$

Abschluß des Beweises.
Wir haben bisher gesehen:

1. Die Formeln von (iii) definieren tatsächlich einen Körper $\mathbb{F}_q$ mit q Elementen.
2. Nach Konstruktion ist $\mathbb{F}_q$ der Zerfällungskörper des Polynoms $f(X) = X^q - X$, also insbesondere ist $\mathbb{F}_q$ normal.
3. Weil $f(X) = X^q - X$ keine mehrfachen Nullstellen besitzt ist die Körpererweiterung
$$\mathbb{F}_q / \mathbb{F}_p$$
separabel.

Es reicht deshalb die Eindeutigkeitsaussagen von (i) und (ii) zu beweisen.
Eindeutigkeitsaussage von (i). Sei F ein Körper mit q Elementen. Dann hat die multiplikative Gruppe F* die Ordnung q-1, d.h. es gilt

$$x^{q-1} = 1 \text{ für jedes } x \in F^*,$$

d.h.

$$x^q = x \text{ für jedes } x \in F.$$

Also ist F der Zerfällungskörper von des Polynoms $X^q - X$ (über $\mathbb{F}_p$) und als solcher bis auf Isomorphie eindeutig bestimmt.
Eindeutigkeitsaussage von (ii). Seien K ein Körper und $F \subseteq K$ ein Körper von der Ordnung q. Wie gerade gezeigt, gilt dann

$$F \subseteq \{x \in K \mid x^q - x = 0\}.$$

Da beide Mengen dieselbe Anzahl q von Elementen besitzten (denn $X^q - X$ hat höchsten q Nullstellen in K), gilt sogar das Gleichheitszeichen,

$$F = \{x \in K \mid x^q - x = 0\},$$

d.h. F ist eindeutig bestimmt.
QED.

3.6.3 Einheitswurzeln

Sei K ein Körper und n ein natürliche Zahl. Ein Element

$$x \in K$$

heißt n-te Einheitswurzel von K, wenn gilt

$$x^n = 1.$$

Es heißt primitive n-te Einheitswurzel, wenn außerdem gilt

$$x^m \neq 1 \text{ für } m = 1, 2, \ldots, m-1.$$

Beispiel 1

Die komplexe Zahl $e^{2\pi i/n}$ ist eine primitive n-te Einheitswurzel von $\mathbb{C}$.
Beispiel 2
Die von Null verschiedenen Elemente des endlichen Körpers $\mathbb{F}_q$ sind (q-1)-te Einheitswurzeln:

$$x^{q-1} = 1 \text{ für jedes } x \in \mathbb{F}_q^*$$

(da $\mathbb{F}_q^*$ eine multiplikative Gruppe der Ordnung q-1 ist): Auf Grund des nachfolgenden Satzes gibt es unter diesen auch eine primitive.

Bemerkungen

(i) Die n-ten Einheitswurzeln bilden eine Untergruppe

$$\mu_{K,n} \subset K^*$$

der multiplikativen Gruppe des Körpers K.

(ii) Ist ζ eine primitive n-te Einheitswurzel, so sind deren Potenzen

$$\zeta, \zeta^2, \zeta^3, \ldots, \zeta^n$$

paarweise verschieden und ebenfalls n-te Einheitswurzeln. Diese Potenzen sind damit aber alle n-ten Einheitswurzeln in dem gegebenen Körper.

(iii) Eine n-te Einheitswurzel ζ von K ist genau dann primitiv, wenn gilt

$$\mu_{K,n} = <\zeta> \text{ und } \# \mu_{K,n} = n.$$

(iv) Ist ζ primitive n-te Einheitszwurzel, so sind die Potenzen mit zu n teilerfremden Exponenten,

$$\zeta^i \text{ mit } ggT(i, n) = 1, i = 1,\ldots,n-1,$$

gerade die übrigen primitiven n-ten Einheitswurzeln.

(v) Falls eine primitive n-te Einheitswurzel in K existiert, so ist die Anzahl dieser primitiven n-ten Einheitswurzeln gleich der Anzahl

$$\varphi(n) = \#(\mathbb{Z}/(n))^*$$

der primen Restklassen modulo n.

Beweis. Zu (i). der Quotient zweier n-ten Einheitswurzeln ist eine n-te Einheitswurzel.

Zu (ii). Die ζ^i sind trivialerweise wieder n-te Einheitswurzeln. Wären zwei von ihnen gleich, so würde ein Quotient von ihnen eine zu niedrige Potenz von ζ liefern, die gleich 1 ist. Es kann keine weiteren n-ten Einheitswurzeln in K geben, da X^n-1 höchstens n Nullstellen hat.

Zu (iii). Ist ζ eine n-te primitive Einheitswurzel, so gilt wegen (ii)

$$\mu_{K,n} = <\zeta> \text{ und } \# \mu_{K,n} = n.$$

Sind umgekehrt diese Bedingungen erfüllt, so hat das erzeugende Element ζ von $\mu_{K,n}$ die Ordnung n, d.h. die n-te Potenz von ζ ist 1 und keine frühere Potenz hat diese Eigenschaft.

Zu (iv). Sei i teilerfremd zu n. Dann gibt es ganze Zahlen i' und n' mit

$$i \bullet i' + n \bullet n' = 1.$$

Damit gilt

$$(\zeta^i)^{i'} = \zeta^{i \bullet i + n \bullet n'} = \zeta$$

Damit gilt

$$<\zeta^i> = <\zeta> = \mu_K \text{ (und } \# \mu_{K,n} = n).$$

Also ist ζ^i primitive n-te Einheitswurzel.

Hat i einen gemeinsamen Teiler > 1 mit n, sagen wir

$$d \mid i, d \mid n, d > 1$$

so gilt $i = d \bullet j$, also

$$(\zeta^i)^{n/d} = (\zeta^n)^{i/d} = 1,$$

d.h. ζ^i ist nicht primitiv.

Zu (v). Da ζ^j nur von der Restklasse von j in $\mathbb{Z}/(n)$ abhängt, folgt die Behauptung aus (iv).

QED.

3.6.4 Existenz primitiver Einheitswurzeln

Seien K ein algebraisch abgeschlossener Körper und n eine natürliche Zahl. Wir nehmen an, eine der beiden folgenden Bedingungen ist erfüllt.

1. Die Charakteristik von K ist Null.
2. Die Charakteristik von K ist p>0 und p ist kein Teiler von n.

Dann gibt es in K eine primitive n-te Einheitswurzel.

Bemerkung:
Auf Grund der Voraussetzungen ist $n \cdot 1_K$ ist in K eine Einheit.

Beweis. Es reicht zu zeigen, die Gruppe der n-ten Einheitswurzeln ist zyklisch von der Ordnung n,

(1) $\mu_{K,n}$ ist zyklisch von der Ordnung n.

Die n-ten Einheitswurzeln sind die Nullstellen des Polynoms

$$f(X) = X^n - 1$$

(welches nach 3.5.9 separabel ist), d.h. f hat im algebraisch abgeschlosseen Körper K genau n paarweise verschiedene Nullstellen, d.h.

$$\# \mu_{K,n} = n.$$

Es reicht zu zeigen

(2) $\mu_{K,n}$ ist zyklisch.

Wir schreiben n als Produkt teilerfremder Primzahlpotenzen,

$$n = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$$

mit paarweise verschiedenen Primzahlen p_i und natürlichen Zahlen n_i.

Fall 1: r = 1.
Es gilt

$$n = p'^{,m}$$

mit einer Primzahl p' und einer natürlichen Zahl m
Im Fall m = 1 hat die Gruppe $\mu_{K,n}$ Primzahlordnung, ist also zyklisch. Sei jetzt m > 1.
Wir setzen

$$n' := p'^{,m-1}$$

Wäre $\mu_{K,n}$ nicht zyklisch, so hätte jedes Element $x \in \mu_{K,n}$ eine Ordnung, die ein echter Teiler von n ist, d.h. es wäre $x^{n'} = 1$, also $x \in \mu_{K,n'}$, Damit wäre

$\mu_{K,n} \subseteq \mu_{K,n'}$, , also

$$p'^{,m} = n = \# \mu_{K,n} \leq \# \mu_{K,n'} = n' = p'^{,m-1}$$

Dieser Widerspruch zeigt, daß $\mu_{K,n}$ zyklisch ist.

Fall 2: r beliebig.
Auf Grund des ersten Falls ist

$$\mu_i = \mu_{K,p_i^{n_i}}.$$

für jedes i zyklisch von der Ordnung $p_i^{n_i}$. Wir betrachten die Abbildung

$$\varphi : \mu_1 \times \mu_2 \times \ldots \times \mu_r \longrightarrow \mu := \mu_{K,n}, (\zeta_1, \ldots, \zeta_r) \mapsto \zeta_1 \cdot \ldots \cdot \zeta_r .$$

Da jedes $\zeta_i \in \mu_i$ eine n-te Einheitswurzel ist, ist auch das Produkt solcher ζ_i ein solche, d.h. die Abbildung ist wohldefiniert. Nach Definiton ist es ein Gruppen-Homomorphismus. Es reicht zu zeigen, φ ist ein Isomorphismus, denn auf der linken Seite steht ein direktes Produkt zyklischer Gruppen mit teilerfremden Ordnungen, also eine zyklische Gruppe.
Zeigen wir also, φ ist ein Isomorphismus. Die Gruppen auf beiden Seiten haben dieselben Ordnung

$$p_1^{n_1} \bullet ... \bullet p_r^{n_r} = n.$$

Es reicht also zu zeigen, φ ist injektiv. Sei also

$$\varphi(\zeta_1,...,\zeta_r) = 1,$$

d.h.

$$\zeta_1 \bullet ... \bullet \zeta_r = 1.$$

Es reicht zu zeigen,

$$\zeta_i = 1 \text{ für } i = 1,...,r.$$

Sei $u = n/p_i^{n_i}$. Dann ist u für jedes $j \neq i$ ein Vielfaches von $p_j^{n_j}$, d.h. es ist $(\zeta_j)^u = 1$ für jedes soche j. Dann ist aber

$$(\zeta_i)^u = 1.$$

Weil u teilerfremd ist zu $v := p_i^{n_i}$ gibt es ganze Zahlen u', v' mit uu'+vv' = 1, also

$$\zeta_i = (\zeta_i)^{uu+vv'} = ((\zeta_i)^u)^{u'} \bullet ((\zeta_i)^v)^{v'} = 1^{u'} \bullet 1^{v'} = 1.$$

QED.

3.6.5 Die multiplikative Gruppe eines endlichen Körpers

Sei F ein endlicher Körper. Dann ist die multiplikative Gruppe F* von F zyklisch,

$$F^* = \langle \zeta \rangle.$$

Bemerkung
Insbesondere gilt

$$F = k(\zeta)$$

für jeden Teilkörper k von F, d.h. für Erweiterungen endlicher Körper gilt der Satz vom primitiven Element.
Beweis. Seien

$$q := p^s = \#F$$

die Ordnung von F, $\overline{F}$ eine algebraische Abschließung von F und

(1) $$n := \#F^* = p^s - 1.$$

Dann ist n teilerfremd zur Charakteristik p von $\overline{F}$. Also gibt es nach 3.6.4 in $\overline{F}$ eine primitive n-te Einheitswurzel

$$\zeta \in \overline{F}.$$

Die davon erzeugte multiplikative Gruppe

$$\langle \zeta \rangle = \mu_{\overline{F},n}$$

hat die Ordnung n und besteht gerade aus allen n-ten Einheitwurzeln von $\overline{F}$. Wegen (1) sind die Elemente von F* lauter n-te Einheitswurzeln, d.h. es gilt

$$F^* \subseteq \mu_{\overline{F},n}.$$

Da beide Gruppen aus derselben Anzahl n von Elementen bestehen, gilt sogar

$$F^* = \mu_{\overline{F},n} = <\zeta>.$$

QED.

3.6.6 Die Automorphismengruppe eines endlichen Körpers

Seien p eine Primzahl und $q = p^n$ eine Potenz von p. Dann gelten die folgenden Aussagen.

(i) Die Gruppe der Automorphismen von $\mathbb{F}_q$ besteht aus lauter $\mathbb{F}_p$-Automorphismen,

$$\mathrm{Aut}(\mathbb{F}_q) = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q),$$

(ii) Die Ordnung dieser Gruppe ist

$$\#\,\mathrm{Aut}(\mathbb{F}_q) = n.$$

(iii) Die Gruppe wird vom Frobenius-Automorphismus

$$F: \mathbb{F}_q \longrightarrow \mathbb{F}_q,\ x \mapsto x^p,$$

erzeugt,

$$\mathrm{Aut}(\mathbb{F}_q) = <F>.$$

Sie ist also zyklisch, abelsch, auflösbar.

Beweis. Zu (i). Sei $f: \mathbb{F}_q \longrightarrow \mathbb{F}_q$ ein Automorphismus. Dann gilt

$f(1) = 1$
$f(2) = f(1+1) = f(1) + f(1) = 1 + 1 = 2$
...

also

$f(x) = x$ für jedes $x \in \mathbb{F}_p$.

Zu (ii). Sei K ein algebraische Abschließung von $\mathbb{F}_q$,

$$\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq K.$$

Dann ist K auch eine algebraische Abschließung von $\mathbb{F}_p$ und die Zahl der $\mathbb{F}_p$-Einbettungen

$$\mathbb{F}_q \hookrightarrow K$$

ist gleich dem Separabilitätsgrad

$$[\mathbb{F}_q:\mathbb{F}_p]_s = [\mathbb{F}_q:\mathbb{F}_p] = n.$$

Nun ist $\mathbb{F}_q/\mathbb{F}_p$ ist nach 3.6.2 eine normale separable Körpererweiterung (nach 3.6.2), d.h. jede dieser Einbettungen läßt sich also $\mathbb{F}_p$-Automorphismus

$$\mathbb{F}_q \longrightarrow \mathbb{F}_q$$

auffassen. Es folgt

$$\#\,\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) = n.$$

Zusammen mit (i) folgt die Behauptung.

Zu (iii). Weil $\mathbb{F}_q$ die Charakteristik p hat, gilt

$$(x+y)^p = x^p+y^p \text{ und } (xy)^p = x^p y^p \text{ für } x,y \in \mathbb{F}_q,$$

d.h.

$$F: \mathbb{F}_q \longrightarrow \mathbb{F}_q$$

ist ein Automorphismus.

$$F \in \mathrm{Aut}(\mathbb{F}_q).$$

Man beachte $F(0) = 0 \neq 1 = F(1)$, d.h. F ist nicht die Nullabbildung. Sei $\zeta \in \mathbb{F}_q$ eine primitive (q-1)-Einheitswurzel. Eine solche existiert nach 3.6.5. Dann gilt

$$\zeta = F^{\ell}(\zeta) = \zeta^{p^{\ell}}$$
$$\Leftrightarrow \zeta^{p^{\ell}-1} = 1$$
$$\Leftrightarrow p^n - 1 \mid p^{\ell} - 1$$

Insbesondere ist

$$F^{\ell}(\zeta) \neq \zeta \text{ für } \ell = 1,...,n-1,$$

d.h.

$$F^{\ell} \neq \mathrm{Id} \text{ für } \ell = 1,...,n-1.$$

Die von F erzeugte zyklische Untergruppe

$$\langle F \rangle \subseteq \mathrm{Aut}(\mathbb{F}_q)$$

hat eine Ordnung $\geq n$. Zusammen mit (ii) ergibt sich, daß die Ordnung gleich n sein muß und

$$\langle F \rangle = \mathrm{Aut}(\mathbb{F}_q)$$

gilt.
QED.

3.7 Hauptsatz der Galois-Theorie

3.7.1 Galois-Erweiterungen

Eine Körper-Erweiterung K/k heißt Galois-Erweiterung, wenn sie algebraisch, separabel und normal ist. Die Gruppe der k-Automorphismen von K heißt in dieser Situation auch Galois-Gruppe von K über k und wird mit

$$\mathrm{Gal}(K/k) = G(K/k) := \mathrm{Aut}_k(K).$$

bezeichnet. Seien K ein Körper und

$$G \subseteq \mathrm{Aut}(K)$$

eine Gruppe von Automorphismen von K. Dann heißt die Menge

$$K^G := \{ x \in K \mid \sigma(x) = x \text{ für alle } \sigma \in G \}$$

der Elemente von K, die bei den Automorphismen von G in sich abgebildet werden, Fixkörper von G in K.

Bemerkungen

(i) K^G ist ein Teilkörper von K.

(ii) Seien K/k eine Galois-Erweiterung und $\overline{k} = \overline{K}$ eine algebraische Abschließung von k, welche den Körper K enthält. Dann gilt,

$$\mathrm{Gal}(K/k) = \text{Menge der k-Einbettungen } K \longrightarrow \overline{k}.$$

Beweis. Zu (i). Für je zwei Elemente $x,y \in K^G$ und jedes $\sigma \in G$ gilt

$$\sigma(x-y) = \sigma(x) - \sigma(y) = x-y \text{ d.h. } x-y \in K^G$$

und

$$\sigma(xy) = \sigma(x)\sigma(y) = xy \text{ , d.h. } xy \in K^G,$$

d.h. K^G ist ein Teilring von K (mit 1).

Für $x \in K^G - \{0\}$ und $\sigma \in G$ gilt weiter

$$\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1},$$

d.h. K^G ist ein Teilkörper von K.

Zu (ii). Galois-Erweiterungen sind normal.

QED.

3.7.2 Hauptsatz der Galois-Theorie (für endliche Erweiterungen)

Sei K/k eine endliche Galois-Erweiterung mit der Galois-Gruppe

$$G = \mathrm{Gal}(K/k)$$

Dann sind die folgenden beiden Abbildungen zueinaner inverse Bijektionen

$$\{\text{Untergruppen von G}\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \{\text{Körper zwischen k und K}\}$$

$$\mathrm{Gal}(K/F) \mapsfrom F$$
$$U \mapsto K^U$$

mit folgenden Eigenschaften.

(i) $[K:F] = \#\,\mathrm{Gal}(K/F)$ für jeden Körper F zwischen k und K.

(ii) $\#\,U = [K:K^U]$ für jede Untergruppe U von G.

(iii) Für jede Untergruppe U von G und jedes Element $\sigma \in G$ gilt

$$K^{(\sigma U \sigma^{-1})} = \sigma(K^U)$$

(iv) Für jeden Körper F zwischen k und K gilt:

$$F/k \text{ normal} \Leftrightarrow \mathrm{Gal}(K/F) \text{ Normalteiler in G}$$

(v) Für je zwei Körper F' und F'' zwischen k und K gilt:

$$\mathrm{Gal}(K/F'F'') = \mathrm{Gal}(K/F') \bigcap \mathrm{Gal}(K/F'').$$

(vi) Für je zwei Körper F' und F'' zwischen k und K gilt:

$$\mathrm{Gal}(K/F' \bigcap F'') = \langle \mathrm{Gal}(K/F'), \mathrm{Gal}(K/F'') \rangle.$$

Dabei steht rechts die von den beiden Galois-Gruppen erzeugte Untergruppe.

(vii) Für je zwei Untergruppen U' und U'' von G gilt

$$K^{U' \bigcap U''} = K^{U'} \cdot K^{U''}$$

(viii) Für je zwei Untergruppen U' und U'' von G gilt

$$K^{\langle U', U'' \rangle} = K^{U'} \bigcap K^{U''}$$

Dabei bezeichnet $\langle U', U'' \rangle$ die von U' und U'' erzeugte Untergruppen.

Bemerkung

Als direkte Folge der Existenz der Bijektion ergibt sich, daß die Menge

$$\{ F \mid F \text{ Körper zwischen } k \text{ und } K \}$$

der Körper zwischen k und K endlich ist. Im Fall unendlicher Körper ergibt sich daraus eine Erklärung für die Gültigkeit des Satzes vom primitiven Element: jedes Element von K, welches in keinem der endlich vielen echten k-linearen Unterräume von K liegt, welche Teilkörper von K sind, erzeugt die Körpererweiterung K/k.

Beweis des Hauptsatzes. Wir fixieren eine algebraische Abschließung $\overline{k}$ von k, die K enthält,

$$k \subseteq K \subseteq \overline{k}.$$

und beginnen mit drei (trivialen) Bemerkungen.

1. Für jeden Körper F zwischen k und K ist auch K/F eine Galois-Erweiterung.
2. $\#\mathrm{Gal}(K/k) = \#\{k\text{-Einbettungen } K \longrightarrow \overline{k} \} = [K:k]_s = [K:k]$
3. Beim Anwenden von φ und ψ kehren sich alle Inklusionen um, d.h. große Untergruppen haben kleine Fixkörper und die Galois-Gruppen großer Zwischenkörper sind klein.

Zu (i). Dies gilt nach Bemerkung 2 im Fall F = k. Und im allgemeinen Fall nach Bemerkung 1.

Zu (ii). Mit $F = K^U$ gilt

$$U \subseteq G(K/F)$$

also

$$\# U \leq \#G(K/F) \overset{(i)}{=} [K:F] . \tag{1}$$

Wir haben noch die umgekehrte Ungleichung zu beweisen, d.h.

$$[K:F] \leq \# U. \tag{2}$$

Nach Bemerkung 1 ist K/F eine Galois-Erweiterung. Nach dem Satz vom primitiven Element gilt

$$K = F(\alpha)$$

für ein α. Wir betrachten die größte natürliche Zahl r mit der Eigenschaft, daß es Elemente

$$\sigma_1,...,\sigma_r \in U$$

gibt mit

$$\sigma_1(\alpha),...,\sigma_r(\alpha) \text{ paarweise verschieden}$$

Dann gilt

$$r \leq \#U.$$

Für die wie oben gewählten $\sigma_1,...,\sigma_r$ und beliebige $\tau \in U$ sind dann die Elemente

$$\tau\sigma_1(\alpha),...,\tau\sigma_r(\alpha)$$

nur eine Permutation der $\sigma_1(\alpha),...,\sigma_r(\alpha)$, denn andernfalls könnte man die Zahl r vergrößern. Mit anderen Worten, das Polynom

$$f(X) = (X- \sigma_1(\alpha))\bullet...\bullet(X - \sigma_r(\alpha))$$

ist invariant bei jedem $\tau \in U$,

$$f^{\tau} = f \text{ für jedes } \tau \in U$$

und hat (tirivialerweise) die Nullstelle α. Es folgt

$$f(X) \in K^U[X] = F[X]$$

und wegen $f(\alpha) = 0$ ist f ein Teiler des Minimalpolynoms f_α von α über f. Wir erhalten

$$[K:F] = [F(\alpha):F] = \deg f_\alpha \leq \deg f = r \leq \#U,$$

d.h. es gilt (2).

Beweis von $\varphi \circ \psi = Id$.

Mit (2) gilt in der Abschätzung (1) das Gleichheitszeichen, d.h. es ist

$$U = G(K/K^U) = \varphi(K^U) = \varphi(\psi(U))$$

für jede Untergruppe U von G.

Beweis von $\psi \circ \varphi = Id$.

Wir haben zu zeigen, für jeden Körper F zwischen k und K gilt

$$K^{G(K/F)} = F.$$

Da die Abbildungen von G(K/F) die Elemente von F fest lassen, gilt jedenfalls

$$F' := K^{G(K/F)} \supseteq F. \tag{3}$$

Angenommen, die Inklusion ist echt. Dann gilt

$$[F':F] > 1,$$

und da F'/F als Teilerweiterung der Galois-Erweiterung K/F separabel ist, auch

$$[F':F]_s > 1.$$

Es gibt also eine F-Einbettung

$$\sigma: F' \longrightarrow \overline{k}$$

die von der identischen Abbildung verschieden ist:

$$\sigma(x) \neq x \text{ für ein } x \in F'. \tag{4}$$

Wir setzen σ fort zu einer F-Einbettung

$$\sigma: K \longrightarrow \overline{k}.$$

Weil K normal ist, gilt $\sigma(K) = K$, d.h. $\sigma \in G(K/F)$. Wegen (4) liegt x nicht im Fixkörper von G(K/F), d.h.

$$x \notin K^{G(K/F)} = F'.$$

das steht aber im Widerspruch zur Wahl von x. Deshalb gilt in (3) das Gleichheitszeichen.

Zu (iii). Es gilt

$$\begin{aligned} K^{(\sigma U \sigma^{-1})} &= \{x \in K \mid \sigma g \sigma^{-1}(x) = x \text{ für } g \in U\} \\ &= \{x \in K \mid g\sigma^{-1}(x) = \sigma^{-1}x \text{ für } g \in U\} \\ &= \sigma\{\sigma^{-1}x \in K \mid g\sigma^{-1}(x) = \sigma^{-1}x \text{ für } g \in U\} \\ &= \sigma\{x \in K \mid g(x) = x \text{ für } g \in U\} \\ &= \sigma(K^U). \end{aligned}$$

Zu (iv). Es gilt (weil φ und ψ invers zueinander sind)

$$F = K^U \text{ mit } U = Gal(K/F),$$

also

$$\begin{aligned} F/k \text{ normal} &\Leftrightarrow \sigma(K^U) = K^U \text{ für } \sigma \in G \\ &\overset{(iii)}{\Leftrightarrow} K^{(\sigma U \sigma^{-1})} = K^U \text{ für } \sigma \in G \\ &\Leftrightarrow \sigma U \sigma^{-1} = U \text{ für } \sigma \in G \qquad (\psi \text{ ist injektiv}) \\ &\Leftrightarrow U \text{ ist normal in } G. \end{aligned}$$

Zu (v). φ kehrt Inklusionen um, d.h.

$$\mathrm{Gal}(K/F'F'') \subseteq \mathrm{Gal}(K/F') \bigcap \mathrm{Gal}(K/F'').$$

Beweis von "$\supseteq$":

Jedes $\sigma \in \mathrm{Gal}(K/F') \bigcap \mathrm{Gal}(K/F')$ läßt F' und F" elementweise fest, also auch F'F".

Zu (vi).s.u.
Zu (vii). Mit

$$F' := K^{U'} \text{ und } F'' := K^{U''}.$$

gilt (nach (v)):

$$U' \bigcap U'' = \mathrm{Gal}(K/F') \bigcap \mathrm{Gal}(K/F'') = \mathrm{Gal}(K/F'F''),$$

also

$$K^{U' \bigcap U''} = K^{\mathrm{Gal}(K/F'F'')} = F'F'' = K^{U'} \bullet K^{U''}.$$

Zu (viii). ψ kehrt Inklusionen um, d.h.

$$K^{<U',U''>} \subseteq K^{U'} \bigcap K^{U''}.$$

Beweis von "$\supseteq$":

Jedes $x \in K^{U'} \bigcap K^{U''}$ bleibt x bei den Elementen von U' und U" fest, also auch bei den Elementen von $< U', U'' >$.

Zu (vi). Mit

$$U' ;= \mathrm{Gal}(K/F') \text{ und } U'' := \mathrm{Gal}(K/F'').$$

gilt (nach (viii)):

$$K^{<U',U''>} = K^{U'} \bigcap K^{U''} = F' \bigcap F'' = K^{\mathrm{Gal}(K/F' \bigcap F'')},$$

also

$$<U', U''> = \mathrm{Gal}(K/F' \bigcap F'').$$

QED.

3.8. Symmetrische Polynome

3.8.1 Die elementarsymmetrischen Funktionen

Ein Polynom heißt symmetrisch, wenn es sich bei beliebigen Permutationen der Unbestimmten nicht ändert.

Seien $X_1,...,X_n$ Unbestimmte. Weiter sei

$$f(T) := (T-X_1) \bullet ... \bullet (T-X_n).$$

Wir betrachten f als Polynom mit Koeffizienten aus

$$\mathbb{Z}[X_1,...,X_n],$$

d.h.

$$f(T) = \sum_{i=0}^{n} (-1)^{n-i} \sigma_{n-i}(X_1,...,X_n) \bullet T^i$$

mit

$$\sigma_i(X_1,...,X_n) := \sum_{1\le j_1<...<j_i\le n} X_{j_1}\bullet...\bullet X_{j_i}.$$

Das Polynom

$$\sigma_i \in \mathbb{Z}[X_1,...,X_n]$$

heißt i-tes elementarsymmetrisches Polynom von $X_1,...,X_n$. Zum Beispiel ist

$$\sigma_1(X) = X_1+...+ X_n$$

$$\sigma_n(X) = X_1\bullet...\bullet X_n$$

Bemerkungen

(i) Für jeden kommutativen Ring R mit 1 können wir den natürlichen Homomorphismus

$$h: \mathbb{Z} \longrightarrow R, g \mapsto g\bullet 1_R ,$$

fortsetzen zu einem Homomorphismus

$$\mathbb{Z}[X_1,...,X_n] \longrightarrow R[X_1,...,X_n], g(X_1,...,X_n) \mapsto g^h(X_1,...,X_n).$$

Wir werden im folgenden statt σ_i^h oft auch einfach σ_i schreiben und auch in diesem Kontext vom i-ten elementarsymmetrischen Polynom sprechen.

(ii) Sei k ein algebraisch abgeschlossener Körper. Dann ist die Abbildung

$$k^n \longrightarrow k^n, x = (x_1,...,x_n) \mapsto (\sigma_1(x),...,\sigma_n(x)),$$

surjektiv.

(iii) Seien k ein Körper und $X_1,...,X_n$. Dann sind die elementarsymmetrischen Funktionen

$$\sigma_i(X_1,...,X_n)\in k[X_1,...,X_n] , i = 1,...,n$$

algebraisch unabhängig über k.

Beweis von (ii). Sei $(a_1,...,a_n)\in k^n$ vorgegeben. Das Polynom

$$f(X) = X^n-a_1X^{n-1}+a_2X^{n-2}-+...+(-1)^na_n$$

zerfällt über dem algebraisch abgeschlossenen Körper k in Linearfaktoren,

$$f(X) = (X-x\bullet_1)\bullet...\bullet(X-x_n) \text{ mit } x_i\in k.$$

Dann gilt aber

$$\sigma_i(x_1,...,x_n) = a_i \text{ für jedes i,}$$

d.h. $(a_1,...,a_n)$ liegt im Bild der Abbildung von (ii).

QED.

Beweis (iii). Angenommen, die σ_i sind algebraisch abhängig. Dann gibt es ein Polynom

$$g(Y_1,...,Y_n) \in k[Y_1,...,Y_n] - \{0\}$$

derart, daß $g(\sigma_1,...,\sigma_n)\in k[X_1,...,X_n]$ das Nullpolynom ist,

(1) $$g(\sigma_1,...,\sigma_n) = 0.$$

Bezeichne

$$\overline{k}$$

eine algebraische Abschließung von k. Da g nicht identisch Null ist und $\overline{k}$ unendlich viele Elemente besitzt, gibt es ein n-Tupel

$$(a_1,...,a_n) \in \overline{k}^n$$

mit

(2) $$g(a_1,...,a_n) \neq 0.$$

Wegen (ii) gibt es ein n-Tupel

$$(x_1,...,x_n) \in \overline{k}^n$$

mit

$$\sigma_i(x_1,...,x_n) = a_i \text{ für jedes } i,$$

Das steht aber im Widerspruch zu (1) und (2).
QED.

3.8.2 Die Operation der symmetrischen Gruppe S_n auf $k(X_1,...,X_n)$

Seien k ein Körper und $X_1,...,X_n$ Unbestimmte. Für jedes $\sigma \in S_n$ und jedes

$$r(X_1,...,X_n) \in k(X_1,...,X_n)$$

setzen wir

$$(\sigma \bullet r)(X_1,...,X_n) := r(X_{\sigma^{-1}(1)},...,X_{\sigma^{-1}(n)}).$$

Dann ist auf diese Weise eine Opertion

$$S_n \times k(X_1,...,X_n) \longrightarrow k(X_1,...,X_n), (\sigma, r) \mapsto \sigma \bullet r ,$$

von S_n auf $k(X_1,...,X_n)$ definiert.[33] Es ist eine Opertion durch k-Automorphismen.[34] Sei

$$F := k(X_1,...,X_n)^{S_n} := \{ r \in k(X_1,...,X_n) \mid \sigma \bullet r = r \text{ für jedes } \sigma \in S_n \}$$

der Fixköper dieser Operation. Dann gilt:

(i) $F = k(\sigma_1,...,\sigma_n)$,
wobei die σ_i die elementarsymmetrischen Polynome in $X_1,...,X_n$ seien.

(ii) K/F ist eine Galois-Erweiterung vom Grad n! und der Galois-Gruppe
$$Gal(K/F) = S_n.$$

(iii) $f(T) := (T-X_1)\bullet...\bullet(T-X_n)$ ist Minimalpolynom der X_i über F.

*(iv) Ein Polynom $p \in k[X_1,...,X_n]$ ist genau dann <u>symmetrisch</u>, d.h. es gilt

$$\sigma \bullet p = p \text{ für jedes } \sigma \in S_n ,$$

---

[33] Man beachte, für $\sigma,\tau \in S_n$ gilt

$$\begin{aligned} ((\sigma\bullet\tau)\bullet r)(X_1,...,X_n) &= r(X_{\tau^{-1}\sigma^{-1}(1)},...,X_{\tau^{-1}\sigma^{-1}(n)}) \\ &= (\tau\bullet r)(X_{\sigma^{-1}(1)},...,X_{\sigma^{-1}(n)}) \\ &= (\sigma\bullet(\tau\bullet r))(X_1,...,X_n). \end{aligned}$$

[34] d.h. für jedes $\sigma \in S_n$ ist die Abbildung $k(X_1,...,X_n) \longrightarrow k(X_1,...,X_n), r \mapsto \sigma\bullet r$, ein k-Isomorphismus.

wenn es als Polynom in den elementarsymmetrischen Funktionen geschrieben werden kann,

$$p(X_1,...,X_n) = q(\sigma_1,...,\sigma_n) \text{ mit } q \in k[X_1,...,X_n].$$

Das Polynom q ist durch p eindeutig bestimmt.

Beweis.

Zu (i) und (ii). Die elementarsymmetrischen Funktionen sind invariant bei den Elementen von S_n , d.h. es gilt

$$F' := k(\sigma_1,...,\sigma_n) \subseteq F \subseteq L := k(X_1,...,X_n).$$

Jedes X_i ist Nullstelle von

$$f = (T-X_1)\bullet...\bullet(T-X_n) \in F'[T],$$

also algebraisch über F'. Damit ist

$$L/F' \text{ endliche Körpererweiterung.}$$

Das Minimalpolynom von X_1 über F' ist ein Teiler von f, also vom Grad $\leq n$,

$$[F'(X_1):F'] \leq n.$$

Das Minimalpolynom von X_2 über $F'(X_1)$ ist ein Teiler von $f/(T-X_1)$, also vom Grad $\leq$ n-1. Indem wir auf diese Weise fortfahren, erhalten wir

$$[F'(X_1,...,X_{i+1}):F'(X_1,...,X_i)] \leq n-i, \qquad (1)$$

d.h.

$$[L:F'] \leq n! .$$

Die X_i sind sämtlich separabel über F', denn f hat den Grad n und die paarweise verschiedenene Nullstellen $X_1,...,X_n$, d.h. X_i ist keine mehrfache Nullstelle von f (vgl. 3.5.9(ii)).[35] Außerdem ist L der Zerfällungskörper von f, also normal über F'. Wir haben gezeigt,

$$L/F' \text{ ist eine Galois-Erweiterung vom Grad} \leq n!.$$

Wegen $F' \subseteq F$ (nach Definition) gilt

$$S_n \subseteq Gal(L/F) \subseteq Gal(L/F')$$

also

$$n! = \#S_n \leq \#Gal(L/F) \leq \#Gal(L/F') = [L:F'] \leq n! \qquad (2)$$

In der letzten Abschätzung gilt überall das Gleicheitszeichen. Insbesondere gilt

$$Gal(L/F') = Gal(L/F)$$

also

$$F = F' = k(\sigma_1,...,\sigma_n).$$

Damit sind (i) und (ii) bewiesen.

Zu (iii). Da in (2) überall das Gleichheitszeichen gilt, ist dies auch der Fall für die Abschätzungen (1). Insbesondere gilt

$$[F(X_i) : F] = n,$$

d.h. das Minimalpolynom von X_i über F hat den Grad n = deg f. Wegen $f(X_i) = 0$ ist damit f das Minimalpolynom, d.h. es gilt (iii).

---

[35] d.h. der irreduzible Faktor von f mit der Nullstelle X_i hat X_i auch nur als einfache Nullstelle.

*Zu (iv). Ein Polynom in den elementarsymmetrischen Polynomen ist trivialerweise symmetrisch. Nehmen wir umgekehrt an, p ist symmetrisch

$$\sigma \bullet p = p \text{ für jedes } \sigma \in S_n$$

Dann gilt nach (ii)

$$p \in k(X_1,...,X_n)^{S_n} \cap k[X_1,...,X_n] = k(\sigma_1,...,\sigma_n) \cap k[X_1,...,X_n].$$

Es reicht also zu zeigen,

$$k(\sigma_1,...,\sigma_n) \cap k[X_1,...,X_n] \subseteq k[\sigma_1,...,\sigma_n]. \quad (2)$$

Jedes X_i ist Nullstelle des normierten Polynoms

$$f(T) := (T-X_1)\bullet...\bullet(T-X_n) = \sum_{i=0}^{n} (-1)^{n-i}\sigma_{n-i}(X_1,...,X_n)\bullet T^i \in k[\sigma_1,...,\sigma_n][T]$$

also ganz über $k[\sigma_1,...,\sigma_n]$. Also liegen die X_i und damit alle Elemente von $k[X_1,...,X_n]$ in der ganzen Abschließung von $k[\sigma_1,...,\sigma_n]$ in $k(X_1,...,X_n)$.

Damit sind aber alle Elemente von

$$k(\sigma_1,...,\sigma_n) \cap k[X_1,...,X_n] \quad (3)$$

ganz über $k[\sigma_1,...,\sigma_n]$. Da die σ_i algebraisch unabhängig sind, ist $k[\sigma_1,...,\sigma_n]$ ein ZPE-Ring und damit ganz-abgeschlossen in $k(\sigma_1,...,\sigma_n)$. Die Elemente von (3) liegen daher sämtlich in $k[\sigma_1,...,\sigma_n]$, d.h. es besteht die Inklusion (2).

QED.

3.9 Lineare Unabhängigkeit der Charaktere

3.9.1 Definitionen

Seien G eine Gruppe und K ein Körper. Ein Charakter von G in K ist ein Gruppenhomomorphismus

$$\chi: G \longrightarrow K^*.$$

Insbesondere ist

$$G \longrightarrow K^*, g \mapsto 1,$$

ein Charakter, welcher trivialer Charakter heißt.

Eine Familie von Funktionen

$$f_i: G \longrightarrow K \text{ , } i = 1,...,n$$

heißt linear unabhängig über K, wenn eine Relation der Gestalt

$$a_1f_1+...+a_nf_n = 0 \text{ mit } a_1,...,a_n \in K$$

nur im Fall $a_1=...=a_n = 0$ besteht, d.h. nur die triviale Linearkombination ist die "identisch verschwindende" Funktion.

Beispiel

Die Elemente der Galois-Gruppe Gal(K/k) definieren Charaktere

$$K^* \longrightarrow K^*$$

der multiplikativen Gruppe K* mit Werten in K.

3.9.2 Satz von Artin

Seien G eine Gruppe, K ein Körper und

$$\chi_1,...,\chi_n: G \longrightarrow K^*$$

paarweise verschiedene Charaktere von G in K. Dann sind $\chi_1,...,\chi_n$ linear unabhängig über K.

Beweis. Wir führen den Beweis durch Induktion nach n. Der Fall n = 1 ist trivial. Sei jetzt n > 1. Angenommen, es gibt eine endliche Familie von n linear abhängigen paarweise verschiedenen Charakteren, d.h. die Linearkombination

(1) $$a_1\chi_1+...+a_n\chi_n = 0 \text{ (mit } a_1,...,a_n \in K, \text{ nicht alle } a_i = 0)$$

ist auf ganz G Null. Der Fall, daß ein a_i gleich Null ist, ist nach Induktionsvoraussetzung nicht möglich, d.h. es gilt

$$a_1,...,a_n \in K - \{0\}.$$

Da χ_1 und χ_2 verschieden sind, gibt es ein $g \in G$ mit

$$\chi_1(g) \neq \chi_2(g).$$

Für jedes $x \in G$ erhalten wir aus (1), indem wir als Argument gx einsetzen:

$$a_1 \chi_1(g) \chi_1(x)+...+a_n \chi_n(g) \chi_n(x) = 0,$$

d.h. es ist

(2) $$a_1 \chi_1(g) \chi_1+...+a_n \chi_n(g) \chi_n = 0.$$

Andererseits erhalten wir aus (1) durch Multiplikation mit $\chi_1(g)$:

(3) $$a_1 \chi_1(g) \chi_1+...+a_n \chi_1(g) \chi_n = 0.$$

Wir bilden die Differenz aus (2) und (3) und erhalten

$$a_2 (\chi_2 (g)- \chi_1(g)) \chi_2+...+a_n(\chi_n (g)-\chi_1(g)) \chi_n = 0.$$

Dies ist eine nicht-triviale Relation zwischen n-1 Charakteren, die nach Induktionsvoraussetzung nicht möglich ist.

QED.

3.10 Spur und Norm

3.10.1 Definitionen (separabler Fall)

Seien K/k eine endliche separable Körpererweiterung und $\alpha \in K$ ein Element. Wir setzen

$$N_{K/k}(\alpha) = \prod_{\sigma: K \hookrightarrow \overline{k}} \sigma(\alpha)$$

$$Tr_{K/k}(\alpha) = \sum_{\sigma: K \hookrightarrow \overline{k}} \sigma(\alpha)$$

Dabei werden Summe bzw Produkt über alle k-Einbettungen $\sigma: K \hookrightarrow \overline{k}$ erstreckt. Auf diese Weise sind Abbildungen

$$N_{K/k}: K \longrightarrow k$$

$$Tr_{K/k}: K \longrightarrow k$$

definiert, welche Norm bzw. Spur von K über k heißen.

Beweis. Zunächst nehmen diese Abbildungen nur Werte in $\overline{k}$ an. Wir müssen zeigen, die Bilder dieser Abbildungen liegen in k. Dazu wählen wir eine Galois-Erweiterung

$$L/k$$

mit $K \subseteq L$ und der Galois-Gruppe

$$G := Gal(L/k).$$

Wir betrachten die Untergruppe

$$U := Gal(L/K)$$

und zerlegen G in Nebenklassen modulo U,

$$(*) \qquad G = g_1 U \bigcup \ldots \bigcup g_r U.$$

<u>1. Schritt</u>: Für jedes $\alpha \in K$ gilt

$$(1) \qquad N_{K/k}(\alpha) = \prod_{i=1}^{r} g_i(\alpha) \in L$$

$$(2) \qquad Tr_{K/k}(\alpha) = \sum_{i=1}^{r} g_i(\alpha) \in L$$

Es reicht zu zeigen, die Einschränkungen

$$g_1|_K , \ldots , g_r|_K$$

sind gerade die k-Einbettungen von K in $\overline{k}$.

Für jedes $\sigma \in G(L/k)$ ist

$$\sigma|_K : K \longrightarrow L \subset \overline{k},$$

eine k-Einbettung von K in $\overline{k}$, und man erhält nach dem Fortsetzungssatz I auf diese Weise jede k-Einbettung von K in $\overline{k}$. Wir haben noch zu zeigen, zwei σ liefern genau dann dieselbe k-Einbettung von K, wenn sie in derselben Nebenklasse modulo U liegen.

Für $\sigma, \tau \in G(L/k)$ gilt

$$\sigma|_K = \tau|_K \Leftrightarrow \sigma^{-1}\tau|_K = Id \Leftrightarrow \sigma^{-1}\tau \in U \Leftrightarrow \sigma U = \tau U,$$

<u>2. Schritt</u>: Norm und Spur nehmen ihre Wert in k an.

Nach Definition von G gilt $L^G = k$. Es reicht also zu zeigen, die rechten Seiten von (1) und (2) sind invariant bei den Elementen von G.Sei $g \in G$. Dann gilt wegen (*)

$$gg_i = g_{\sigma(i)} u_i \text{ mit } u_i \in U$$

und einer Permutation $\sigma \in S_r$.

Es folgt

$$g(N_{K/k}(\alpha)) = \prod_{i=1}^{r} gg_i(\alpha)$$

$$= \prod_{i=1}^{r} g_{\sigma(i)} u_i (\alpha)$$

$$= \prod_{i=1}^{r} g_{\sigma(i)}(\alpha) \qquad \text{(wegen } u_i \in U = Gal(L/K) \text{ und } \alpha \in K)$$

$$= \prod_{i=1}^{r} g_i(\alpha) \qquad \text{(weil L kommutativ ist)}$$
$$= N_{K/k}(\alpha)$$

Dieselbe Rechnung kann man auch mit der Summe anstelle des Produkts durchführen. Wir haben gezeigt, $N_{K/k}(\alpha)$ und $Tr_{K/k}(\alpha)$ sind invariant bei den Elementen von G, liegen also in k.

QED.

Bemerkung

Der obige Beweis zeigt, für jede endliche Galois-Erweiterung L/k, jede Teilerweiterung K/k und jedes Element $\alpha \in K$ gilt

$$N_{K/k}(\alpha) = \prod_{[g] \in Gal(L/k)/Gal(L/K)} g(\alpha).$$

$$Tr_{K/k}(\alpha) = \sum_{[g] \in Gal(L/k)/Gal(L/K)} g(\alpha).$$

Dabei bezeichne [g] die (Links-) Nebenklasse von $g \in Gal(L/k)$ modulo Gal(K/k).

3.10.2 Eigenschaften der Norm

Sei K/k eine separable Körpererweiterung vom Grad $n = [K:k] < \infty$. Dann gilt

(i) $N_{K/k}(\alpha \cdot \beta) = N_{K/k}(\alpha)\, N_{K/k}(\beta)$ für $\alpha, \beta \in K$.

(ii) $N_{K/k}(\alpha) = \alpha^n$ für $\alpha \in k$.

(iii) $N_{K/k} = N_{F/k} \circ N_{K/F}$ für jeden Körper F zwischen k und K.

(iv) $N_{K/k}(\alpha) = (-1)^n f_\alpha(0)$ falls $K = k(\alpha)$.

(v) $N_{K/k}(\alpha) = \det(mult_\alpha)$.

Dabei bezeichne f_α das Minimalpolynom von α über k und $mult_\alpha$ die k-lineare Abbildung

$$mult_\alpha : K \longrightarrow K,\ x \mapsto \alpha x.$$

Beweis. Zu (i). Für jede k-Einbettung $\sigma: K \hookrightarrow \overline{k}$ gilt $\sigma(\alpha\beta) = \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$.

Zu (ii). Für jede k-Einbettung $\sigma: K \hookrightarrow \overline{k}$ gilt $\sigma(\alpha) = \alpha$ (wegen $\alpha \in k$).

Zu (iii). Wir wählen eine endliche Galois-Erweiterung L/k mit $K \subseteq L$ und setzen

$G := Gal(L/k)$ $\qquad k \subseteq F \subseteq K \subseteq L$

$U := Gal(L/F)$ $\qquad V \subseteq U \subseteq G$

$V := Gal(L/K)$.

Nach der Bemerkung von 3.12.2 gilt dann für jedes $\alpha \in K$:

$$\beta := N_{K/F}(\alpha) = \prod_{[g] \in U/V} g(\alpha)$$

und

$$N_{F/k}(N_{K/F}(\alpha)) = N_{F/k}(\beta) = \prod_{[h]\in G/U} h(\beta)$$

$$= \prod_{[h]\in G/U} h\Big(\prod_{[g]\in U/V} g(\alpha)\Big)$$

$$= \prod_{[h]\in G/U}\prod_{[g]\in U/V} hg(\alpha)$$

Durchlaufe jetzt h ein Repräsentantensystem von G/U,

$$G = \bigcup_{i=1}^{r} h_i U$$

und g ein Repräsentantensystem vom U/V,

$$U = \bigcup_{j=1}^{s} g_j V.$$

Dann durchlaufen die hg ein Repräsentantensystem von G/V:

$$G = \bigcup_{i=1}^{r}\bigcup_{j=1}^{s} h_i g_j V.$$

Das obige Doppelprodukt läßt sich damit wie folgt schreiben.

$$N_{F/k}(N_{K/F}(\alpha)) = \prod_{[g]\in G/V} g(\alpha) = N_{K/k}(\alpha).$$

Zu (iv). Die Nullstellen des Minimalpolynoms sind gerade die Konjugierten von α, d.h. es gilt

$$f_\alpha(X) = \prod_{\sigma:K\hookrightarrow\overline{k}} (X-\sigma(\alpha)),$$

also

$$f_\alpha(0) = \prod_{\sigma:K\hookrightarrow\overline{k}} (-\sigma(\alpha)) = (-1)^n \prod_{\sigma:K\hookrightarrow\overline{k}} \sigma(\alpha) = (-1)^n N_{K/k}(\alpha)$$

Zu (v). Seien $\alpha\in K$,

$$f_\alpha(X) = c_0+c_1X + ... + c_{n-1}X^{n-1} + X^n \in k[X]$$

das Minimalpolynom von α über k und

$$F = k(\alpha).$$

Dann gilt

$$\begin{aligned} N_{K/k}(\alpha) &= N_{F/k}(N_{K/F}(\alpha)) && \text{(nach (iii))}\\ &= N_{F/k}(\alpha^{[K:F]}) && \text{(nach (ii) wegen } \alpha\in F = k(\alpha))\\ &= N_{F/k}(\alpha)^{[K:F]} && \text{(nach (i))}\\ &= ((-1)^{[F:k]}c_0)^{[K:F]} && \text{(nach (iv))} \end{aligned}$$

d.h.

$$(1)\qquad N_{K/k}(\alpha) = (-1)^{[K:k]}c_0^{[K:F]}$$

Es reicht zu zeigen, der Ausdruck auf der rechten Seite ist die Determinante der Multiplikationsabbildung mult_α bezüglich einer geeignet gewählten Basis von K/k. Sei irgendeine Basis von K über F gegeben, sagen wir

$$K = F\omega_1 + ... + F\omega_r \text{ mit } r = [K:F].$$

Wegen

$$F = k\bullet 1 + k\bullet\alpha + ... + k\bullet\alpha^{s-1} \text{ mit } s = \deg f_\alpha = [F:k].$$

erhalten wir damit die folgenden k-Vektorraum-Basis von K.

$$\begin{array}{ll} & \omega_1, \alpha\,\omega_1, ..., \alpha^{s-1}\,\omega_1, \\ (2) & \omega_2, \alpha\,\omega_2, ..., \alpha^{s-1}\,\omega_2, \\ & ... \\ & \omega_r, \alpha\,\omega_r, ..., \alpha^{s-1}\,\omega_r \end{array}$$

Bei Multiplikation mit α gehen die Basisvektoren jeder Zeile in eine Linearkombination der Basisvektoren dieser Zeile über. Zum Beispiel erhält man für den letzten Basisvektor jeder Zeile

$$\alpha^s\omega_j = (-c_0 - c_1\alpha + ... - c_{s-1}\alpha^{s-1})\omega_j.$$

Deshalb zerfällt die Matrix vom mult_α bezüglich der Basis (2) in r Blöcke,

$$M(\text{mult}_\alpha) = \begin{pmatrix} B & 0 & ... & 0 \\ 0 & B & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & B \end{pmatrix} \text{ (r Blöcke)}$$

wobei jeder Block die Gestalt

$$B = \begin{pmatrix} 0 & 0 & 0 & ... & 0 & -c_0 \\ 1 & 0 & 0 & ... & 0 & -c_1 \\ 0 & 1 & 0 & ... & 0 & -c_2 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 0 & -c_{s-1} \end{pmatrix}$$

hat. Durch (s-1) Nachbartausche kann man die erste Zeile von B in die letzte überführen. Deshalb gilt

$$\det B = (-1)^{s-1}(-c_0) = (-1)^s c_0$$

also

$$\det(\text{mult}_\alpha) = (\det B)^r = (-1)^{rs} c_0^r.$$

Wegen r = [K:F] , s = [F:k], also rs = [K:k], erhalten wir durch Vergleich mit (1) die Behauptung.
QED.

3.10.3 Eigenschaften der Spur

Sei K/k eine separable Körpererweiterung vom Grad $n = [K:k] < \infty$. Dann gilt

(i) $\text{Tr}_{K/k}(\alpha+\beta) = \text{Tr}_{K/k}(\alpha) + \text{Tr}_{K/k}(\beta)$ für $\alpha,\beta \in K$.

(ii) $\text{Tr}_{K/k}(\alpha) = n$ für $\alpha \in k$.

(iii) $\text{Tr}_{K/k} = \text{Tr}_{F/k} \circ \text{Tr}_{K/F}$ für jeden Körper F zwischen k und K.

(iv) $Tr_{K/k}(\alpha) = - a_{n-1}$ falls $K = k(\alpha)$ ist und a_{n-1} den Koeffizienten von X^{n-1} im Minimalpolynom f_α von α über k bezeichnet.

(v) $Tr_{K/k}(\alpha) = Tr(mult_\alpha)$:= Summe der Elemente auf der Hauptdiagonalen einer Matrix von $mult_\alpha$.

Dabei bezeichne $mult_\alpha$ die k-lineare Abbildung

$$mult_\alpha: K \longrightarrow K, x \mapsto \alpha x.$$

Beweis. Ist analog zum Beweis von 3.12.2.
QED.

3.11 Zyklische Erweiterungen

3.11.1 Definition

Eine endliche Galois-Erweiterung K/k heißt abelsch bzw. zyklisch, wenn die Galois-Gruppe

$$Gal(K/k)$$

abelsch bzw. zyklisch ist.

Beispiel 1

Seien k ein Körper der eine n-te primitive Einheitswurzel

$$\zeta \in k$$

enthält und

$$K = k(\alpha) \text{ mit } a := \alpha^n \in k,$$

d.h. α ist eine n-te Wurzel aus einem Element von k. Es gelte

$$n \cdot 1_k \neq 0$$

(d.h. n sei teilerfremd zur Charakteristik). Dann ist

$$k(\alpha)/k$$

eine zyklische Galois-Erweiterung.

Beweis. Wir können annehmen , α ist nicht Null .Das Element α ist Nullstelle des Polynoms

$$f(X) = X^n - a,$$

Die n Nullstellen des Polynoms f sind gerade die folgenden:

$$\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{n-1}\alpha .$$

Diese sind paarweise verschieden (weil ζ primitiv ist) und liegen in $k(\alpha)$ (wegen $\zeta \in k$). Also ist $k(\alpha)$ Zerfällungskörper des separablen Polynoms f, d.h.

$$K/k \text{ eine Galois-Erweiterung.}$$

Sei

$$G = G(K/k)$$

die Galois-Gruppe. Für jedes $\sigma \in G$ ist $\sigma(\alpha)$ eine Nullstelle von f, also von der Gestalt

$$\sigma(\alpha) = \omega_\sigma \alpha$$

mit einer n-ten Einheitswurzel $\omega_\sigma \in k$. Wir betrachten die Abbildung

$$\varphi: G \longrightarrow \langle\zeta\rangle \subseteq k^*, \sigma \mapsto \omega_\sigma.$$

Es reicht zu zeigen,
1. φ ist ein Gruppen-Homomorphismus.
2. φ ist injektiv.

Denn dann kann man G als Untergruppe der zyklischen Gruppe $<\zeta>$ auffassen, d.h. G ist selbst zyklisch.

Zu 1 Für $\sigma, \tau \in G$ gilt

$$\omega_{\sigma\tau}\alpha = \sigma\tau(\alpha) = \sigma(\omega_\tau \alpha) = \omega_\tau \sigma(\alpha) = \omega_\tau\, \omega_\sigma \alpha,$$

Zu 2. Weil K von α erzeugt wird, ist σ durch das Bild

$$\sigma(\alpha) = \omega_\sigma \alpha$$

bereits vollständig festgelegt, d.h. durch $\varphi(\sigma) = \omega_\sigma$.

QED.

Beispiel 2

Sei K/k eine Körpererweiterung und $\zeta \in K$ eine primitive n-te Einheitswurzel mit

n teilerfremd zur Charakteristik von k.

Dann ist

$$k(\zeta)/k$$

eine abelsche Galois-Erweiterung.

Beweis. $k(\zeta)$ ist der Zerfällungskörper des Polynoms

$$f(X) = X^n - 1,$$

also normal und separabel über k, d.h. $k(\zeta)/k$ ist endliche Galois-Erweiterung. Sei

$$G = G(k(\zeta)/k)$$

die Galois-Gruppen. Jedes $\sigma \in G$ bildet ζ in eine primitive n-te Einheitswurzel ab, d.h.

$$\sigma(\zeta) = \zeta^i \text{ mit } ggT(i,n) = 1.$$

Der Exponent $i = i(\sigma)$ ist dabei modulo n eindeutig festgelegt. Auf diese Weise ist also eine Abbildung

$$h: G \longrightarrow (\mathbb{Z}/(n))^*, \sigma \mapsto i(\sigma) \bmod n,$$

definiert. Es reicht zu zeigen,
1. h ist ein Gruppen-Homomorphismus.
2. h ist injektiv.
Denn dann ist G als Untergruppe einer abelschen Gruppe abelsch.

Zu 1. Für $\sigma, \tau \in G$ gilt

$$\zeta^{i(\sigma\tau)} = (\sigma\tau)(\zeta) = \sigma(\zeta^{i(\tau)}) = (\sigma(\zeta))^{i(\tau)} = \zeta^{i(\sigma)i(\tau)}$$

Zu 2. Weil $k(\zeta)$ von ζ erzeugt wird, ist jedes $\sigma \in G$ durch das Bild von ζ bereits eindeutig festgelegt, also durch

$$\sigma(\zeta) = \zeta^{i(\sigma)},$$

also durch $i(\sigma) \bmod n$.

QED.

Bemerkung

Im Fall $k = \mathbb{Q}$ und $n = 12$ kann man zeigen, daß die obige Erweiterung nicht zyklisch ist. Es ist dann G eine Untergruppe von

$$(\mathbb{Z}/(12))^* = \{\pm\overline{1}, \pm\overline{5}\}$$

Jedes Element dieser Gruppe hat das Quadrat $\overline{1}$, d.h. es handelt sich um die Kleinsche Vierergruppe, d.h. um eine Gruppe, die nicht zyklisch ist. Es reicht also zu zeigen,

$$G = (\mathbb{Z}/(12))^*.$$

Angenommen, es gilt nicht das Gleichheitszeichen. Dann hat G die Ordnung

$$\# G = 2,$$

also $\mathbb{Q}(\zeta)$ den Grad

$$[\mathbb{Q}(\zeta):\mathbb{Q}] = \# G = 2,$$

d.h. ζ würde einer Gleichung zweiten Grades über $\mathbb{Q}$ genügen. Nun ist aber ζ^3 eine 4 .te primitive Einheitswurzel[36], d.h. $\zeta^3 = \pm i$, also gilt $i \in \mathbb{Q}(\zeta)$, also aus Gradgründen

(1) $$\mathbb{Q}(\zeta) = \mathbb{Q}(i) = \mathbb{Q} + i \bullet \mathbb{Q}.$$

Weiter ist ζ^4 eine 3-te primitive Einheitswurzel[37], also $\zeta^4 = -\frac{1}{2} \pm \frac{i}{2}\sqrt{3}$, also gilt

$$\sqrt{3} \in \mathbb{Q}(\zeta),$$

also aus Gradgründen

(2) $$\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{3}) = \mathbb{Q} + \sqrt{3} \bullet \mathbb{Q}.$$

Die Identitäten (1) und (2) sind aber unvereinbar: nach (2) liegt $\mathbb{Q}(\zeta)$ ganz in den reellen Zahlen.

3.11.2 Hilberts Satz 90

Seien K/k eine (endliche) zyklische Erweiterung mit der Galois-Gruppe G, σ ein erzeugendes Element von G,

$$G = <\sigma>$$

und $\alpha \in K$. Dann sind folgende Bedingungen äquivalent.

(i) $N_{K/k}(\alpha) = 1$.

(ii) Es gibt ein Element $\beta \in K - \{0\}$ mit $\alpha = \beta/\sigma(\beta)$.

Beweis. Wir schreiben $N := N_{K/k}$ für die Normabbildung $K \longrightarrow k$.

(ii) $\Rightarrow$ (i). Es gilt

$$N(\alpha) = N(\beta)/N(\sigma(\beta)) = 1,$$

denn β und $\sigma(\beta)$ haben dieselben Konjugierten.

(i) $\Rightarrow$ (ii). Wir setzen

$$n := \# G = [K:k]$$

Nach Voraussetzung gilt $N_{K/k}(\alpha) = 1$, also

$$\alpha \neq 0.$$

Die Abbildungen

$$\sigma^i : K^* \longrightarrow K^*, \; i = 0,1,...,n$$

sind paarweise verschiedene Charaktere von K^* in K, also K-linear unabhängig (nach dem Satz von Artin, 3.9.2). Insbesondere ist die folgende Abbildung $K \longrightarrow K$ nicht identisch Null:

$$\sum_{i=0}^{n-1} c_i \sigma^i \text{ mit } c_i :=^{38} \alpha \bullet \sigma(\alpha) \bullet ... \bullet \sigma^{i-1}(\alpha)$$

Es gibt also ein Element $\theta \in K$ für welches der Wert β dieser Abbildung an der Stelle θ ungleich Null ist:

$$0 \neq \beta := \sum_{i=0}^{n-1} c_i \sigma^i(\theta) = \sum_{r=0}^{n-1} \beta_r \text{ mit } \beta_i :=^{39} c_i \bullet \sigma^i(\theta)$$

---

[36] Wäre ζ^3 nicht primitiv, so wäre $\zeta^3 = \pm 1$, also $\zeta^6 = 1$, d.h. ζ wäre nicht primitiv.

[37] Wäre ζ^4 nicht primitiv, so wäre $\zeta^4 = 1$, d.h. ζ wäre nicht primitiv.

[38] Rechts stehen i Faktoren. Im Fall i = 0 sei $c_0 := 1$.

Es gilt

$$\sigma(\beta_i) = \sigma(\alpha)\bullet\ldots\bullet\sigma^i(\alpha)\sigma^{i+1}(\theta) = \frac{\beta_{i+1}}{\alpha} \text{ für } i = 0, \ldots, n\text{-}2$$

$$\sigma(\beta_{n-1}) = \sigma(\alpha)\bullet\ldots\bullet\sigma^{n-1}(\alpha)\sigma^n(\theta)$$

$$= \sigma(\alpha)\bullet\ldots\bullet\sigma^{n-1}(\alpha)\bullet\theta$$

$$= \frac{N(\alpha)\bullet\theta}{\alpha}$$

$$= \theta/\alpha \qquad \text{(wegen } N(\alpha) = 1\text{)}$$

Einsetzen in die Definition von β liefert

$$\sigma(\beta) = \sum_{r=0}^{n-1} .\sigma(\beta_r)$$

$$= \sum_{r=0}^{n-2} \beta_{r+1}/\alpha + \theta/\alpha$$

$$= \sum_{r=0}^{n-2} \beta_{r+1}/\alpha + \beta_0/\alpha$$

$$= \beta/\alpha$$

also

$$\alpha = \beta/\sigma(\beta)$$

QED.

3.11.3 Satz von den zyklischen Erweiterungen

Seien k ein Körper und n eine natürliche Zahl, die im Fall char $k \neq 0$ teilerfremd zu Charakteristik von k ist. Der Körper k enthalte eine primitive n-te Einheitswurzel. Dann gelten folgende Aussagen.

(i) Jede zyklische Erweiterung K von k des Grades n hat die Gestalt

$$K = k(\alpha),$$

wobei α ein Element mit dem Minimalpolynom

$$f_\alpha(X) = X^n - a \in k[X]$$

ist.

(ii) Sei α aus einer Körpererweiterung von k und Nullstelle eines Polynoms der Gestalt

$$f(X) = X^n - a \in k[X]$$

Dann ist $k(\alpha)/k$ eine zyklische Körpererweiterung, deren Grad d ein Teiler von n ist. Außerdem gilt $\alpha^d \in k$.

Beweis. Zu (i). Seien K/k eine zyklische Erweiterung des Grades n mit der Gruppe

$$G = \langle\sigma\rangle$$

und

$$\zeta \in k$$

eine n-te Einheitswurzel. Es gilt

$$N_{K/k}(\zeta^{-1}) = (\zeta^{-1})^n \qquad \text{(wegen } \zeta\in k \text{ und 3.10.2)}$$

$$= 1.$$

Nach Hilberts Satz 90 gibt es ein $\alpha \in K$ mit $\zeta^{-1} = \alpha/\sigma(\alpha)$, d.h.

---

[39] Insbesondere sei $\beta_0 := \theta$.

$$\sigma(\alpha) = \zeta\alpha.$$

Wegen $\zeta \in k$ folgt

$$\sigma^i(\alpha) = \zeta^i\alpha \text{ für } i = 1,...,n.$$

Die Elemente $\zeta^i a$ sind die (paarweise verschiedenen) zu α über k konjugierten Elemente. Es folgt

$$[k(\alpha):k] = [k(\alpha):k]_s \quad \text{(weil K/k galoisch, also separabel ist)}$$
$$= n \quad \text{(nach 3.5.2).}$$

Damit ist

$$K = k(\alpha)$$

und

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = (\zeta)^n(\alpha)^n = \alpha^n,$$

d.h.

$$a := \alpha^n \in K^G = k,$$

d.h. α ist Nullstelle von $X^n - a \in k[X]$ (und hat dieses Polynom als Minimalpolynom).

Zu (ii). Sei $\overline{k}$ eine algebraische Abschließung von k und $\alpha \in \overline{k}$ Nullstelle von

$$f(X) = X^n - a \in k[X].$$

Dann hat f die n paarweise verschiedenen Nullstellen

$$\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{n-1}\alpha,$$

die wegen $\zeta \in k$ in $k(\alpha)$ liegen. Also ist $k(\alpha)$ Zerfällungskörper des separablen Polynoms f, d.h.

$k(\alpha)/k$ ist eine Galois-Erweiterung.

Sei

$$G := G(k(\alpha)/k)$$

deren Galois-Gruppe. Für jedes $\sigma \in G$ ist $\sigma(\alpha)$ eine Nullstelle von f(X), d.h.

$$\sigma(\alpha) = \omega_\sigma \bullet \alpha, \text{ mit } \omega_\sigma \text{ n-te Einheitswurzel } (\in k).$$

Nach Beispiel 1 von 3.1.11 ist die Abbildung

$$\varphi: G \longrightarrow <\zeta> = \mu_{k,n}, \ \alpha \mapsto \omega_\sigma,$$

ein injektiver Gruppen-Homomorphismus. Wir können G als Untergruppe der zyklischen Gruppe

$$\mu_{k,n} = <\zeta>$$

der Ordnung n auffassen. Insbesondere ist

G zyklisch von der Ordnung $d = \#\,\mathrm{Im}(\varphi)$ mit $d \mid n$.

Sei σ jetzt ein erzeugendes Element von G,

$$G = <\sigma>.$$

Dann ist ω_σ eine primitive d-te Einheitswurzel und es gilt

$$\sigma(\alpha^d) = (\sigma(\alpha))^d = (\omega_\sigma\alpha)^d = \alpha^d,$$

d.h.

$$\alpha^d \in k(\alpha)^G = k.$$

QED.

3.12 Auflösbare Erweiterungen (in der Charakteristik 0)

3.12.1 Definitionen

Eine endliche separable Körper-Erweiterung.

$$K/k$$

heißt auflösbar, wenn sie ganz in einer Galois-Erweiterung L/k mit auflösbarer Galois-Gruppe liegt, deren Ordnung teilerfremd zur Charakteristik von k ist[40].

Die Erweiterung K/k heißt auflösbar durch Radikale, wenn es einen Körperturm

$$k = K_0 \subset K_1 \subset ... \subset E_r = E$$

gibt mit $K \subseteq E$ und

$$K_{i+1} = K_i(\alpha_i),$$

wobei eine Potenz von α_i in K_i liegen soll,

$$(\alpha_i)^{n_i} \in K_i ,$$

wobei der Exponent n_i teilerfremd zur Charakteristik des Grundkörpers sein soll.

3.12.2 Eigenschaften auflösbarer Erweiterungen

Die Auflösbaren Körpererweiterungen bilden eine ausgezeichnete Klasse.
Beweis. Übungsaufgabe.
QED.

3.12.3 Auflösbarkeit und Auflösbarkeit durch Radikale

Sei

$$K/k$$

eine endliche separable Körpererweiterung. Dann sind folgende Aussagen äquivalent.
(i) K/k ist auflösbar.
(ii) K/k ist auflösbar durch Radikale.

Beweis. (ii) $\Rightarrow$ (i). Wir müssen die Existenz einer Galois-Erweiterung

$$L/k$$

mit

$$K \subseteq L \text{ und } G(L/k) \text{ auflösbar}$$

beweisen. Dazu können wir K bei Bedarf vergrößern.
1. Schritt. Reduktion auf den Fall, daß K/k eine Galois-Erweiterung ist.
Nach Voraussetzung entsteht K aus k durch wiederholte Adjunktion von n-ten Wurzeln. Indem wir mit jeder Wurzel auch alle adjungierten Wurzeln zum Körper hinzunehmen, d.h. wir adjungieren zusätzlich n-te Einheitswurzeln, bleibt die betrachtete Erweiterung E/k nach wie vor auflösbar durch Radikale wird aber zusätzlich normal und dadurch eine Galois-Erweiterung.

Nach Voraussetzung entsteht K durch Adjunktion von endlich vielen Nullstellen von Polynomen der Gestalt

$$X^n - a.$$

Wir bezeichnen mit

$$N$$

eine natürliche Zahl, die von allen dabei auftretenden Graden n geteilt wird (und teilerfremd zur Charakteristik des Grundkörpers sein soll).

2. Schritt: Reduktion auf den Fall, daß k eine primitive N-te Einheitswurzel enthält.

---

[40] Die Bedingung an die Ordnung kann man fallen lassen, wenn man zu den durch Radikale auflösbaren Erweiterungen die Artin-Schreier-Erweiterungen hinzunimmt (die in der Charakteristik 0 nicht auftreten). Man muß dann zusätzlich den Satz von Artin-Schreier beweisen.

Bezeichne

$$\zeta$$

eine primitive N-te Einheitswurzel. Wir setzen

$$F = k(\zeta).$$

Wir wollen die Auflösbarkeit der Gruppe G(K/k) beweisen. Auf Grund der Surjektion

$$f: G(KF/k) \longrightarrow G(F/k), \sigma \mapsto \sigma|_F ,$$

reicht es, die Auflösbarkeit von G(KF/k) zu beweisen:

Betrachten wir nämlich die exakte Sequenz

$$1 \longrightarrow G(KF/F) \xrightarrow{g} G(KF/k) \xrightarrow{f} G(F/k) \longrightarrow 1$$

Die Gruppe rechts ist abelsch[41], also auflösbar. Deshalb ist die Gruppe in der Mitte auflösbar, wenn es die Gruppe links ist. Es reicht also die Auflösbarkeit von

$$G(KF/F),$$

zu beweisen, d.h. wir können annehmen, der Grundkörper enthält eine N-te primitive Einheitswurzel.

3. Schritt. Abschluß des Beweises.

Nach Voraussetzung gibt es einen Körperturm

$$k = K_0 \subset K_1 \subset ... \subset E_r = K$$

mit

$$K_{i+1} = K_i(\alpha_i) , (\alpha_i)^{n_i} \in K_i , n_i \mid N.$$

Nach Voraussetzung enthält k eine primitive N-te Einheitswurzel. Also enthält K_i eine primitive n_i-te Einheitswurzel. Nach 3.11.1 Beispiel 1 ist

$$K_{i+1}/ K_i \text{ zyklische Galois-Erweiterung}$$

(also auflösbar). Aus der kurzen exakten Sequenz

$$1 \longrightarrow G(K_{i+1}/K_i) \longrightarrow G(K_{i+1}/k) \longrightarrow G(K_i/k) \longrightarrow 1$$

sehen wir, mit $G(K_i/k)$ ist auch $G(K_{i+1}/k)$ auflösbar. Also ist G(K/k) auflösbar.

(i) $\Rightarrow$ (ii). Wird so ähnlich bewiesen: man reduziert die Aussage auf den Fall, daß K/k Galois-Erweiterung ist und k eine primitive n-te Einheitswurzel enthält mit n = [K:k] und benutzt dann die Beschreibung der zyklischen Erweiterungen von 3.11.3(i).

Genauer, sei K/k auflösbar. Wir haben die Auflösbarkeit durch Radikale nachzuweisen. Sei

$$L/k$$

eine endliche Galois-Erweiterung mit $K \subseteq$ und auflösbarer Gruppe, deren Ordnung teilerfremd zur Charakteristik des Grundkörpers k ist, und bezeichne

$$N$$

das Produkt aller Primzahlpotenzen, welche den Körpergrad

$$[L:k]$$

teilen. Wir fixieren in der algebraischen Abschließung von L eine primtive N-te Einheitswurzel ζ, und setzen

$$F := k(\zeta), \zeta \text{ primitive N-te Einheitswurzel.}$$

Betrachten wir das folgende kommutative Diagramm von Körpererweiterungen.

---

[41] nach Beispiel 2 von 3.11.1.

$$\begin{array}{ccc} L & \subset & LF =: K \\ \cup & & \cup \\ k & \subset & F \end{array}$$

Nach Wahl von L ist L/k auflösbar und nach Wahl von F = k(ζ) auch F/k (nach 3.11.1 Beispiel 2). Also ist LF/k auflösbar (nach 3.12.2).

Als Galoiserweiterung ist L Zerfällungskörper einer Familie von Polynomen über k. Fügen wir zu dieser Familie das Polynom X^N hinzu, so erhalten wir eine Beschreibung von LF als Zerfällungskörper über k. Mit anderen Wort,

LF/k ist eine Galois-Erweiterung.

Nach Konstruktion ist die Galois-Gruppe G dieser Erweiterung auflösbar, d.h. es gibt eine Normalreihe

$$\{0\} = G_0 \subset G_1 \subset ... \subset G_r = G,$$

deren Faktoren G_{i+1}/G_i zyklisch von Primzahlpotenzordnung sind. Wir betrachten den zugehörigen Körperturm

$$K = K^{G_0} \supset K^{G_1} \supset ... \supset K^{G_r} = k$$

und setzen

$$K_i := K^{G_i}.$$

Dann gilt

$$K^{G(K/K_i)} = K_i = K^{G_i}$$

also

$$G_i = G(K/K_i).$$

Nach Wahl der obigen Normalreihe ist die Untergruppe

$$G_{i-1} = G(K/K_{i-1}) \text{ Normalteiler in } G_i = G(K/K_i),$$

d.h. $K^{G_{i-1}} = K_{i-1}$ ist normale Körpererweiterung von K_i, also eine Galois-Erweiterung. Berechnen wir deren Galois-Gruppe. Die Einschränkungsabbildung

$$\varphi_\iota : G(K/K_i) \longrightarrow G(K_{i-1}/K_i),\ \sigma \mapsto \sigma|_{K_{i-1}},$$

als Kern die Gruppe $G(K/K_{i-1}) = G_{i-1}$, d.h. es gilt

$$G(K_{i-1}/K_i) \cong G_i/G_{i-1},$$

d.h. K_{i-1}/K_i ist zyklische Galois-Erweiterung. Nach 3.11.3 hat K_{i-1}/K_i die Gestalt

$$K_{i-1} = K_i(\alpha_i) \text{ mit } (\alpha_i)^{n_i} \in K_i.$$

Damit ist $K_0/k = K/k$ auflösbar durch Radikale.

QED.

3.13 Die Galois-Gruppe eines Polynoms

3.13.1 Definition

Seien k ein Körper und

$$f(X) \in k[X]$$

ein separables Polynom. Weiter sei K der Zerfällungskörper von f über k. Dann heißt

$$G(f) := G(f/k) := G(K/k)$$

Galois-Gruppe von f über k.

3.13.2 Beispiel

Seien $\sigma_1,...,\sigma_n$, T Unbestimmte und

$$f(X) = X^n - \sigma_1 X^{n-1} + - \ldots + (-1)^n \sigma_n \in K := k(\sigma_1,...,\sigma_n)$$

das "allgemeine" Polynom n-ten Grades. Dann hat f die Galois-Gruppe S_n. Insbesondere ist die Galois-Gruppe im Fall $n \geq 5$ nicht auflösbar und die Nullstellen von f lassen sich nicht als Radikale in den Koeffizienten $\sigma_1,...,\sigma_n$ von f ausdrücken.

Mit anderen Worten, es gibt keine Formeln für die Nullstellen eines Polynoms des Grades $n \geq 5$ die für alle Polynomes dieses Grades gleichermaßen gelten und in denen außer den vier Grundrechenarten nur noch Wurzel-Ausdrücken auftreten.

Unser nächstes Ziel besteht darin zu zeigen, daß es solche Formeln nicht einmal für die Nullstellen des Polynoms

$$f(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$$

gibt. Zu diesem Zweck benutzen wir das folgende Kriterium.

3.13.3 Ein Kriterium für Polynome f mit G(f) = S_n

Sei $f \in \mathbb{Q}[X]$ ein Polynom von Primzahlgrad p mit genau zwei nicht-reellen Nullstellen in $\mathbb{C}$. Dann ist die Galois-Gruppe von f über $\mathbb{Q}$ gleich der symmetrischen Gruppe S_p.

(vgl. Karpfinger & Meyberg, Lemma 27.5, S. 295)

Beweis. Seien

$$\alpha_1, \alpha_2 \in \mathbb{C} - \mathbb{Q} \text{ und } \alpha_3, \ldots, \alpha_p \in \mathbb{C}$$

die Nullstellen von f und

$$G = G(f) = G(K/\mathbb{Q})$$

die Galoisgruppe des Zerfällungskörpers $K = \mathbb{Q}(\alpha_1,...,\alpha_p)$ von f über $\mathbb{Q}$. Für jedes

$$\sigma \in G$$

schreiben wir

$$\sigma(\alpha_i) = \alpha_{\tilde{\sigma}(i)}.$$

Dann ist $\tilde{\sigma}$ ein Permutation von S_p und für $\sigma, \tau \in G$ gilt

$$\tau(\sigma(\alpha_i)) = \tau(\alpha_{\tilde{\sigma}(i)}) = \alpha_{\tilde{\tau}(\tilde{\sigma}(i))},$$

d.h. $(\tau\sigma)^{\sim} = \tilde{\tau}\tilde{\sigma}$. Mit anderen Worten,

$$G \longrightarrow S_p, \sigma \mapsto \tilde{\sigma}, \qquad (1).$$

ist ein injektiver Homomorphismus (injektiv, weil jeder Automorphismus von $K/\mathbb{Q}$ durch seine Werte auf den Erzeugern der Körpererweiterung festgelegt ist). Es reicht zu zeigen, dieser Homomorphismus ist surjektiv.

Die Einschränkung der komplexen Konjugation

$$\mathbb{C} \longrightarrow \mathbb{C}, z \mapsto \overline{z},$$

auf K definiert eine $\mathbb{Q}$-Einbettung $K \longrightarrow \mathbb{C}$ und, weil K normal über $\mathbb{Q}$ ist, einen $\mathbb{Q}$-Automorphismus von K,

$$\varepsilon: K \longrightarrow K, z \mapsto \overline{z}\ , (\in G = G(K/\mathbb{Q})).$$

Weil die Koeffizienten von f reel sind, sind die beiden nicht-reellen Nullstellen konjugiert zueinander, d.h. ε permutiert α_1 und α_2, und es ist

$$\tilde{\varepsilon} = (1,2).$$

Weiter gilt

$$G = [K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha_1)]\bullet[\mathbb{Q}(\alpha_1):\mathbb{Q}] = [K:\mathbb{Q}(\alpha_1)]\bullet p.$$

Die p-Sylow-Untergruppe von G ist somit nicht-trivial. Insbesondere enthält G ein Element von p-Potenz-Ordnung und damit auch ein Element δ der Ordnung p. Weil p eine Primzahl ist, ist $\tilde{\delta}$ ein p-Zyklus.[42] Es gilt also

$$\tilde{\delta} = (1, n_2, \ldots, n_p).$$

Zum Beweis der Behauptung reicht es zu zeigen, die Injektion (1) ist surjektiv. Dazu wiederum reicht es zu zeigen,

$$\tilde{\varepsilon} = (1,2) \text{ und } \tilde{\delta} = (1, n_2, \ldots, n_p) \text{ erzeugen } S_p. \qquad (2)$$

Die nicht-trivialen Potenzen von $\tilde{\delta}$ sind wieder p-Zyklen. Wir können deshalb δ durch eine geeignete Potenz ersetzung und annehmen,

$$\tilde{\delta} = (1, 2, n_3, \ldots, n_p).$$

Es gilt

$$\tilde{\delta}^j\bullet(1,2)\bullet(\tilde{\delta}^j)^{-1} = (\tilde{\delta}^j(1), \tilde{\delta}^j(2)) = (n_{j+1}, n_{j+2}),$$

also

$$(n_j, n_{j+1}) \in < \tilde{\varepsilon}, \tilde{\delta} > \text{ für } j = 1, 2, \ldots, p-1$$

Weiter ist

$$(n_j, n_{j+1})\bullet(n_i, n_j)\bullet(n_j, n_{j+1}) = (n_i, n_{j+1}) \text{ für } i < j \leq p-1,$$

also

$$(n_i, n_j) \in < \tilde{\varepsilon}, \tilde{\delta} > \text{ für alle i und j mit } i < j.$$

Mit anderen Worten, alle Transpositionen liegen in der von $\tilde{\varepsilon}$ und $\tilde{\delta}$ erzeugten Untergruppe, d.h. es gilt (2).

QED.

---

[42] Man zerlege $\tilde{\delta}$ ein Produkt von elementfremden Zyklen. Jeder Faktor ist dann ein Zyklus, dessen Ordnung die Primzahl p teilt.

3.13.4 Beispiel: $X^5 - 4X + 2$

Das Polynom $f(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist irreduzibel und besitzt die Galois-Gruppe

$$G(f) = S_5$$

Insbesondere lassen sich die Nullstellen von f nicht als Radikale schreiben (vgl. Karpfinger & Meyberg, Beipiel 29.5, S. 320).

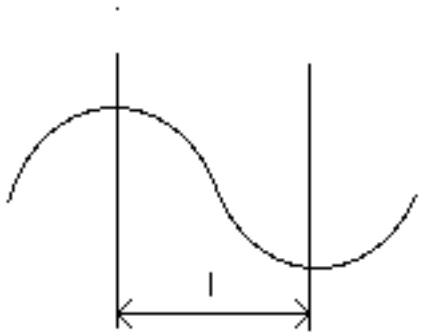
Beweis. Das Polynom f ist ein Eisenstein-Polynom zur Primzahl 2, also irreduzibel. Es reicht deshalb zu zeigen, f besitzt genau drei reelle Nullstellen. Die Ableitung

$$f' = 5X^4 - 4$$

ist positiv außerhalb des Intervalls

$$I = [-\sqrt[4]{4/5}, +\sqrt[4]{4/5}]$$

und negativ im Innern dieses Intervalls. Also ist f streng monoton steigend außerhalb und streng monoton fallend im Innern des Intervalls.



In jedem der Intervalle, in denen f streng monoton ist, kann das Polynom höchstens eine Nullstelle besitzen. Insgesamt hat f also höchstens drei reelle Nullstellen.
Außerdem ist

$f(-2) = -32 + 8 + 2 < 0$
$f(-1) = -1 + 4 + 2 > 0$
$f(1) = 1 - 4 + 2 < 0$
$f(2) = 32 - 8 + 2 > 0$

Es gibt also in den Intervallen $(-2, -1), (-1, +1), (+1, +2)$ je eine Nullstelle. Damit hat f genau drei reelle Nullstellen.

QED.

Bemerkungen

(i) Der obige Beweis benutzt wesentlich die algebraische Abgeschlossenheit des Körper $\mathbb{C}$ der komplexen Zahlen (die wir hier nicht bewiesen haben). Das nachfolgende Beispiel (aus dem Algebra-Buch von van der Waerden) hat diesen Mangel nicht, ist allerdings aufwendiger.

(ii) Man kann die Hauptsatz der Galois-Theorie verwenden, um die algebraische Abgeschlossenheit von $\mathbb{C}$ zu beweisen.

3.13.5 Beispiel: X^5-X-1

Der Zerfällungkörper von

$$f(X) := X^5\text{-}X\text{-}1$$

hat über $\mathbb{Q}$ die Galois-Gruppe

$$G = S_5.$$

Insbesondere lassen sich die Nullstellen dieses Polynoms nicht durch Radikale ausdrücken.

Zum Beweis dieser Aussage brauchen wir einige allgemeine Sätze zur Berechnung der Galois-Gruppe eines Polynoms.

3.13.6 Konstruktion

Seien

$$f(X) \in k[X]$$

ein Polynom ohne mehrfachen Nullstellen,

$$\alpha_1,...,\alpha_n \in \overline{k}$$

dessen Nullstellen in einer algebraischen Abschließung $\overline{k}$ von k. Wir führen Unbestimmte

$$u_1,...,u_n$$

ein und setzen

$$\theta := u_1\alpha_1 + ...u_n\alpha_n$$

und

$$F(z, u) :=^{43} \prod_{s \in S_n} (z - s \bullet \theta) \in k[u, z]$$

Dabei operiere $s \in S_n$ auf den Polynomen in den u_i durch Permutation der Unbestimmten u_i. Wir zerlegen F in irreduzible Faktoren

$$F(z,u) = F_1(z, u) \bullet ... \bullet F_r(z,u) \text{ in } k[u,z].$$

Die Permutationen von S_n, die F_1 in sich abbilden, bilden eine Untergruppe von S_n,

$$G' = \{s \in S_n \mid sF_1 = F_1\}$$

Bemerkungen

(i) Die Elemente der Galois-Gruppe G := G(f) von f permutieren die Nullstellen

$$\alpha_1,...,\alpha_n$$

von f. Wir haben also einen wohldefinierten Gruppen-Homomorphismus

$$G \longrightarrow S_n, \sigma \mapsto \sigma|\{\alpha_1,...,\alpha_n\}$$

wenn wir S_n als Gruppe der Permutation von $\{\alpha_1,...,\alpha_n\}$ auffassen. Diese Abbildung ist injektiv, weil die α_i den Zerfällungskörper von f erzeugen. Wir können also G als Untergruppe der S_n auffassen.

(ii) Der nachfolgende Satz besagt, daß man die beiden eben beschriebenen Untergruppen der S_n identifizieren kann.

3.13.7 Eine alternative Beschreibung der Galois-Gruppe eines Polynoms

Mit den Bezeichnungen von 3.13.6 gilt

$$G(f) = \{s \in S_n \mid sF_1 = F_1\}.$$

---

[43] Wir schreiben hier abkürzend u für $u_1,...,u_n$.

Beweis. Sei K der Zerfällungskörper von f über k,

$$K = k(\alpha_1,...,\alpha_n).$$

Über K[u] zerfällt F in die Linearfaktoren

$$z - s\theta = z - u_1\alpha_{s^{-1}(1)} +...u_n\alpha_{s^{-1}(n)} \qquad (s\in S_n).$$

Wir wählen die Bezeichnungen so, daß F_1 den Faktor

$$z - \theta$$

enthält. Wie schon angemerkt können wir die $s\in S_n$ zum Permutieren der u_i benutzen, aber auch zum Permutieren der α_i. Je nachdem, welcher Fall vorliegt, wollen wir $s = s_u$ oder $s = s_\alpha$ schreiben. Es gilt

(1) $$F_1(z, u) \mid \sum_{s\in G(f)} (z - s_\alpha\theta) \text{ in } k[z, u]$$

denn rechts steht ein Polynom mit Koeffizienten aus K, welches bei den Elementen von G(f) unverändert bleibt, d.h. die Koeffizienten liegen in $K^{G(f)} = k$. Die Teilbarkeitsrelation besteht, weil F_1 irreduzibel ist und mit dem Polynom rechts die Nulstelle $z - \theta$ gemeinsam hat.[44]

1.Schritt: $s_\alpha\theta = s_u^{-1}\theta$

Das Produkt

$$s_u s_\alpha$$

permutiert die Summanden des Ausdrucks

$$\theta := u_1\alpha_1 +...u_n\alpha_n ,$$

laßt ihn also unverändert, d.h. es gilt

$$s_u s_\alpha\theta = \theta,$$

d.h.

$$s_\alpha\theta = s_u^{-1}\theta.$$

2. Schritt: $G' := \{s\in S_n \mid s_u F_1 = F_1\}$ ist gleich $\{ s\in S_n \mid s_u(z-\theta) \mid F_1\}$

Beweis von "$\supseteq$". Sei

$$\sigma\in \{ s\in S_n \mid s_u(z-\theta) \mid F_1\}$$

Nach Definition von F(z,u) bleibt dieses Polynom unverändert bei σ_u. Jeder Linearfaktor L von F_1 wird von σ_u in einen Linearfaktor $\sigma_u L$ von $\sigma_u F_1$ überführt. Speziel für $L = z-\theta$ sehen, daß

$$\sigma_u L$$

ein Linearfaktor von $\sigma_u F_1$ und (nach Wahl von σ auch) von F_1 ist. Also haben $\sigma_u F_1$ und F_1 einen nicht-trivialen gemeinsamen Faktor. Da beide Polynome irreduzibel sind[45], müssen sie gleich sein, d.h. es gilt

---

[44] Zunächst besteht die Teilbarkeitsbeziehung in k(u)[z]. Nun ist aber k[u] ein ZPE-Ring und beide Polynome haben den höchsten Koeffizienten 1, also den Inhalt 1.

[45] und den Inhalt 1 haben (als Teiler von F(z,u)).

$$\sigma_u F_1 = F_1,$$

also $\sigma \in G'$.

Beweis von "$\subseteq$".

Sei $\sigma \in G'$. Dann überführt σ_u jeden Linearfaktor von F_1 in einen Linearfaktor von F_1. Dies gilt insbesondere für $z - \theta$.

3.Schritt. $G' = G(f)$.

Die Permutationen $s_\alpha \in G(f)$ überführen

$$\theta := u_1\alpha_1 + ...u_n\alpha_n$$

in die Konjugierten von θ, d.h. sie überführen den Linearfaktor $z-\theta$ von F_1 in einen Linearfaktor von F_1. Wegen $s_\alpha\theta = s_u^{-1}\theta$ gilt dasselbe auch für die s_u, d.h. es gilt $s \in G'$. Wir haben gezeigt:

$$G(f) \subseteq G'.$$

Ist umgekehrt $s \in G'$, so überführt s_u nach dem zweiten Schritt $z - \theta$ in einen Linearfaktor von F_1. Wegen $s_\alpha\theta = s_u^{-1}\theta$ überführt s_α das Element θ in ein zu θ konjugiertes Element. Die zu θ konjugierten Elemente erhält man aber, indem man auf die α_i ein Element $\sigma \in G(f)$ anwendet (wegen (1)), d.h. es gilt

$$s_\alpha = \sigma \in G(f).$$

QED

3.13.8 Einige Untergruppen der Galois-Gruppe

Sei R ein ZPE-Ring mit dem Primideal P und

$$f(X) = X^n + ... \in R[X]$$

ein Polynom. Bezeichne

$$h: R \longrightarrow R/P$$

den natürlichen Homomorphismus. Es gelte:

f und f^h haben keine mehrfachen Nullstellen.

Bezeichne

$$G$$

die Galois-Gruppe des Zerfällungskörpers von f über $\mathbb{Q}(R)$ und

$$\overline{G}$$

die Galois-Gruppe des Zerfällungskörpers von f^h über $\mathbb{Q}(R/P)$.

Dann kann man $\overline{G}$ als Untergruppe von G auffassen,

$$\overline{G} \subseteq G.$$

Beweis. Wir verwenden die Bezeichnungen des Beweises von 3.13.7.Sei

$$F(z,u) = F_1(z,u) \bullet ... \bullet F_r(z,u)$$

die Zerlegung von F in irreduzible Faktoren über Q(R). Weil R ein ZPE-Ring ist, können wir annehmen,

$$F_i(z,u) \in R[z,u]$$

für alle i, und wir erhalten eine Zerlegung

$$F^h(z,u) = F_1^h(z,u)\bullet...\bullet F_r^h(z,u)$$

über Q(R/P). Die Elemente von $G \subseteq S_n$ sind nach 3.13.7 gerade die Permuationen die F_1 in sich überführen:

$$G = \{s \in S_n \mid s_u F_1 = F_1\}$$

Sie überführen jedes der F_i in sich[46] und damit auch jedes der F_i^h in sich.[47]

Die Elemente der Galois-Gruppe (des Zerfällungskörpers) von F^h überführen jeden irreduziblen Faktor von F_1^h in sich und damit auch F_1^h in sich. Als Elemente von S_n liegen sie also in der Untergruppe $G(f) \subseteq S_n$.

QED.

3.13.9 Zur Berechnung der Galois-Gruppe von $f(X) = X^5-X-1$

Bezeichne

$$G$$

die Galois-Gruppe von f über $\mathbb{Q}$. Jedes Element von G permutiert die fünf Nullstellen von f und ist durch seine Werte auf diesen Nullstellen bestimmt. Wir können also G wie bisher als Untergruppe der S_5 auffassen,

$$G \subseteq S_5$$

1. Schritt: G enthält einen Zweierzyklus

Modulo 2 ist f zerlegbar in

$$f(X) = (X^2+X+1)(X^3+X^2+1)$$

Die Galois-Gruppe des ersten Faktors (modulo 2) ist von der Ordnung 2, und permutiert die beiden Nullstellen dieses Faktors[48]. Nach 3.13.6 enthält also die Galois-

---

[46] Jeder der irreduziblen Faktoren F_i von F ist gleichberechtigt.

[47] Es ist egal, ob man erst die Nullstellen permutiert und dann h auf die Koeffizienten anwendet, oder ob man dies in umgekehrter Reihenfolge tun.

[48] Die Galois-Gruppe des zweiten Faktors ist von der Ordnung 6: Die Diskriminante von $f = X^3+X^2+1$ ist nämlich kein Quadrat:

$$\Delta(f) = \mathrm{Res}(f, f') = \det\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 3 & 2 & 0 & 0 & 0 \\ 0 & 3 & 2 & 0 & 0 \\ 0 & 0 & 3 & 2 & 0 \end{pmatrix}$$

$$= -\det\begin{pmatrix} 1 & 1 & 0 & 1 \\ 3 & 2 & 0 & 0 \\ 0 & 3 & 2 & 0 \\ 0 & 0 & 3 & 2 \end{pmatrix} = -\det\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & -1 & 0 & -3 \\ 0 & 3 & 2 & 0 \\ 0 & 0 & 3 & 2 \end{pmatrix}$$

$$= -\det\begin{pmatrix} -1 & 0 & -3 \\ 3 & 2 & 0 \\ 0 & 3 & 2 \end{pmatrix} = -\det\begin{pmatrix} -1 & 0 & -3 \\ 0 & 2 & -9 \\ 0 & 3 & 2 \end{pmatrix}$$

Gruppe von f einen Zweier-Zyklus. Bei geeigneter Nummerierung der Nullstellen von f können wir annehmen

$$(12) \in G.$$

2. Schritt: Modulo 3 ist f irreduzibel:

Hätte f modulo 3 einen linearen oder quadratischen Faktor, so hätte f eine Nullstelle in einer quadratischen Erweiterung von $\mathbb{F}_3$, d.h. in $\mathbb{F}_9$. Die Elemente von $\mathbb{F}_9$ sind aber Nullstellen von X^9-X, d.h. f hätte mit X^9-X einen Faktor gemeinsam, also auch mit

$$X^{10}-X^2 = (X^5-X)(X^5+X),$$

also mit

$$X^5-X \text{ oder } X^5+X,$$

was offensichtlich nicht der Fall ist. Damit definiert f eine Erweiterung des Grades 5 von $\mathbb{F}_3$. Die Galois-Gruppe dieser Erweiterung ist $\mathbb{Z}/5\mathbb{Z}$. Jedes Erzeugende Element dieser Gruppe bewirkt eine zyklische Vertauschung der Nullstellen von f. Nach 3.13.6 ergibt sich:

$$G \subseteq S_5 \text{ enthält einen Fünfer-Zyklus.}$$

Wir können O.B.d.A. annehmen[49],

$$(12345) \in G.$$

Wiederholte Konjugation von (12) mit (12345) liefert weitere Zweier-Zyklen, die in G liegen:

$$(12), (23), (34), (45), (51) \in G$$

Konjugation von (12) mit (23) liefert

$$(13) \in G.$$

Konjugation von (13) mit (34) liefert

$$(14) \in G.$$

Damit gilt

$$(12), (13), (14), (15) \in G.$$

Da (12), (13), (14), (15) die S_5 erzeugen, folgt

$$G = S_5.$$

QED.

Literatur

1) Lang, S.: Algebra, Addison-Wesley, Reading, Mass., 1965
2) van der Waerden, B.L.: Algebra, Springer, Berlin 1966

$$= \det \begin{pmatrix} 2 & -9 \\ 3 & 2 \end{pmatrix}$$
$$= 4 + 27$$
$$= 31,$$

d.h. die Galois-Gruppe von f ist die S_3

[49] Zumindest ein Fünfer-Zyklus, in welchem die Elemente 1 und 2 benachbart auftreten, läßt sich durch Umbenennen der übrigen Elemente in die angegebene Gestalt bringen. Andernfalls kann man zumindest erreichen daß zwischen 1 und 2 nur ein Element steht. Dann sind aber 1 und 2 im Quadrat dieses Fünferzyklus (welches auch ein Fünferzyklus ist) benachbart.

3) Scheja, G., Storch, U.: Lehrbuch der Algebra, 2 Bände, Teubner, Stuttgard 1980, 1988.
4) Bourbaki, N. Algébre, Hermann, Paris (englische Übersetzung bei Springer)
5) Artin, M.: Algebra, Prentice Hall, Englewood Cliffs, NJ.

6) Karpfinger, C., Meyberg, K.: Algebra, Gruppe - Ringe - Körper, Spektrum Akademischer Verlag, Heidelberg 2009.

Index

—F—

—G—

—H—

—I—

—K—

—L—

—M—

—N—

—O—

—P—

—Q—

—R—

—S—

—T—

—U—

—V—

—W—

—Z—

Inhalt