

Algebra I



Prof. Dr. Jürg Kramer

Ursprüngliche Abschrift im Wintersemester 2002/2003 von Claudia Hein

Erweiterungen von Jana Bielagk, Leonard Kern, Michael Kreikenbaum und Yves Radunz

Version vom 23. Oktober 2007

Inhaltsverzeichnis

1	Gruppentheorie	5
1.1	Allgemeines	5
1.2	Grundlagen	5
1.3	Die beiden Isomorphiesätze	8
1.4	Die Sylow-Sätze	10
1.5	Klassifikation endlicher und endlich erzeugter abelscher Gruppen	16
1.6	Normalreihen, Kompositionsreihen, Auflösbarkeit	23
2	Körpertheorie	29
2.1	Wiederholung/Einführung	29
2.2	Algebraische und transzendente Erweiterungen	34
2.3	Separabilität und Normalität	39
3	Galois-Theorie	44
3.1	Hauptsatz	44
4	Auflösbare Polynome	48
4.1	Einführung	48
4.2	Auflösbare Gruppen (Wiederholung)	49
4.3	Satz von Abel	50

Literatur zur Vorlesung "Algebra I"

Michael Artin, Algebra. Birkhäuser Verlag (1998; Zbl 0922.00001)

Jörg Bewersdorff, Algebra für Einsteiger. Von der Gleichungsaufösung zur Galois-Theorie. Vieweg-Verlag (2002; Zbl 0995.12001)

Siegfried Bosch, Algebra. Springer-Lehrbuch (2004; Zbl 1037.00002)

Bernhard Hornfeck, Algebra. 3. verbess. Aufl., de Gruyter-Lehrbuch (1976; Zbl 0324.00005)

Nathan Jacobson, Basic Algebra I. 2nd ed. (English), W. H. Freeman and Company (1989; Zbl 0557.16001)

George R. Kempf, Algebraic Structures. Vieweg Verlag (1995; Zbl 0831.00002)

Serge Lang, Algebra. 3rd revised ed. (English), Graduate Texts in Mathematics 211. Springer-Verlag (2002; Zbl 0984.00001).

John Stillwell, Elements of algebra: geometry, numbers, equations. (English), Undergraduate Texts in Mathematics. Springer-Verlag (1994; Zbl 0832.00001)

Bartel L. van der Waerden, Algebra I. Unter Benutzung von Vorlesungen von E. Artin und E. Noether. 9. Aufl., Springer Verlag (1993; Zbl 0781.12002)

Gisbert Wüstholz, Algebra. Vieweg Studium: Aufbaukurs Mathematik (2004; Zbl 1050.00003)

1 Gruppentheorie

1.1 Allgemeines

Die Vorlesung Algebra I wird sich mit 3 Themenkomplexen befassen:

1. Gruppentheorie
2. Ring- und Körpertheorie
3. Galois-Theorie

Als Motivation hierfür sei zunächst der Satz von Abel genannt.

Satz 1.1.1 (Satz von Abel).

Polynome $f(x) \in \mathbb{Q}(X)$ mit Grad $\deg f \geq 5$ haben in der Regel Nullstellen, die sich nicht durch Radikale ausdrücken lassen.

Für kleine Grade $n = \deg f$ des Polynoms f gilt:

- $n = 1$: $f(X) = aX + b$
 $x_0 = -\frac{b}{a} \in \mathbb{Q}$
- $n = 2$: $f(X) = aX^2 + bX + c$
 $x_{1/2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- $n = 3$: $f(X) = aX^3 + bX^2 + cX + d$
Die Nullstellen $x_{1/2/3}$ sind durch die *Cardano-Formeln* gegeben.
- $n = 4$: $f(X) = aX^4 + bX^3 + cX^2 + dX + e$
Die Nullstellen $x_{1/2/3/4}$ lassen sich durch die *Formeln von Ferrari* bestimmen.

Für größere Grade gibt es jedoch keine derartige Darstellung.

1.2 Grundlagen

sind größtenteils eine Wiederholung des ersten Semesters. Für Details und Beweise schaut bitte auf der Vorlesungshomepage in das Skript für das erste Semester der Linearen Algebra-Vorlesung. Ihr könnt es auch unter http://www.informatik.hu-berlin.de/~kreikenb/abschrift_laag.pdf finden.

- Eine *Halbgruppe* (H, \circ) ist eine nichtleere Menge H mit einer assoziativen Verknüpfung $\circ : H \times H \rightarrow H$.

- Ein *Monoid* (M, \circ) ist eine Halbgruppe, welche über ein eindeutiges neutrales Element $e \in M$ verfügt. Dieses Element hat die Eigenschaft, dass $\forall m \in M : e \circ m = m = m \circ e$ gilt.
- Eine *Gruppe* (G, \circ) ist ein Monoid mit der zusätzlichen Eigenschaft $\forall g \in G : \exists g' \in G : g' \circ g = e$ für ein neutrales Element $e \in G$. Dies bedeutet, dass für jedes Element aus G ein (links)inverses Element existiert. Man kann zeigen, dass dieses inverse Element eindeutig bestimmt und sowohl links- als auch rechtsinvers ist. Wir werden im folgenden die Verknüpfung \circ nur angeben, wenn es nicht offensichtlich ist, welche Verknüpfung zu der Gruppe gehört.
- Eine Gruppe G heißt *abelsch* oder *kommutativ*, wenn $\forall g_1, g_2 \in G : g_1 \circ g_2 = g_2 \circ g_1$ gilt.
- Die Kardinalität (Mächtigkeit) der Menge G heißt die *Ordnung von G* und wird mit $|G|$ oder $\#G$ bezeichnet
- Die Teilmenge $H \subseteq G$ der Elemente einer Gruppe G heißt *Untergruppe von G* (in Zeichen $H \leq G$), wenn H mit der von G induzierten Verknüpfung (eingeschränkt auf H) wieder eine Gruppe bildet.
- Wenn $H \leq G$ eine Untergruppe ist, so heißt $g \circ H = \{g' \in G \mid \exists h \in H : g' = g \circ h\}$ die zu $g \in G$ gehörige *Linksnebenklasse bezüglich H* .
Es gilt: $g_1 \circ H = g_2 \circ H \Leftrightarrow g_1^{-1} \circ g_2 \in H \Leftrightarrow \exists h \in H : g_2 = g_1 \circ h$
Die Linksnebenklassen bilden eine disjunkte Zerlegung von G .
- Für $H \leq G$ und $g \in G$ gilt $|g \circ H| = |H|$. Hieraus folgt der

Satz 1.2.1 (Satz von Lagrange).

Die Gruppenordnung wird von der Ordnung der Untergruppe geteilt: $|H| \mid |G|$

- Als G/H bezeichnen wir die Menge der Linksnebenklassen der Gruppe G bezüglich der Untergruppe H .
- Analog wird mit $H \circ g$ eine *Rechtsnebenklasse* bezeichnet. $G \setminus H$ ist die Menge der Rechtsnebenklassen.
Im allgemeinen gilt $G \setminus H \neq G/H$, aber $|G \setminus H| = |G/H|$.
- Der *Index von H in G* ist definiert als $(G : H) := |G/H|$.
- Eine Untergruppe $N \leq G$ heißt *Normalteiler*, wenn für die Nebenklassen bezüglich N die Gleichung $g \circ N = N \circ g$ gilt. In diesem Fall schreibt man $N \trianglelefteq G$.
- Wenn $N \trianglelefteq G$ ein Normalteiler ist, so kann man auf der Menge G/N eine Gruppenstruktur durch $(g_1 \circ N) \bullet (g_2 \circ N) = (g_1 \circ g_2) \circ N$ definieren. G/N wird dann *Faktorgruppe* genannt.
- Seien G eine Gruppe und $S \subseteq G$ eine Teilmenge. Wir sagen, G ist erzeugt durch S , falls jedes $g \in G$ ein endliches Produkt von Elementen aus S und deren Inversen ist. Wir schreiben: $G = \langle S \rangle$. S wird *Erzeugendensystem* genannt.

Ein Beispiel hierfür ist die Diedergruppe D_n . Sie stellt die Menge der Symmetrien eines regelmäßigen n -Ecks dar.

Es gilt $D_n = \{r^0, \dots, r^n, s_1, \dots, s_n\}$, wobei r eine Drehung um $\frac{2\pi}{n}$ ist und s_k ($k = 1, \dots, n$) Spiegelungen. D_n wird nun durch die Menge $S = \{r, s_1\} \subseteq D_n$ erzeugt.

- Die *Ordnung* $\text{ord}_G(g)$ eines Elements g einer Gruppe G ist die kleinste natürliche Zahl $n \in \mathbb{N}, n > 0$, für welche $g^n = e$ gilt. Wenn keine derartige Zahl existiert, so ist $\text{ord}_G(g) = \infty$. Weil $\langle g \rangle$ eine Untergruppe von G ist und $\text{ord}(g) = |\langle g \rangle|$ gilt, teilt die Ordnung von g nach dem Satz von Lagrange die Ordnung der Gruppe G .
- Gegeben seien zwei Gruppen (G, \circ_G) und (H, \circ_H) . Eine Abbildung $f : G \rightarrow H$ heißt *Homomorphismus*, wenn gilt:

$$\forall g_1, g_2 \in G : f(g_1 \circ_G g_2) = f(g_1) \circ_H f(g_2)$$

- Ein bijektiver Homomorphismus heißt *Isomorphismus*.
- Der *Kern* $\ker(f)$ eines Homomorphismus $f : G \rightarrow H$ ist die Menge aller Elemente aus G , die auf das neutrale Element von H abgebildet werden. Der Kern ist ein Normalteiler von G .
Das *Bild* $\text{im}(f)$ ist die Menge aller Elemente $h \in H$, für die ein Element $g \in G$ existiert, so dass $h = f(g)$ gilt. $\text{im}(f)$ ist eine Untergruppe von H .
- Sei $G = (G, \circ)$ eine Gruppe und $N \trianglelefteq G$ ein Normalteiler in G . Dann wird durch die Zuordnung $\pi : G \rightarrow G/N$ mit $\pi(g) := g \circ N \quad \forall g \in G$ ein surjektiver Homomorphismus definiert. π heißt *natürliche* oder *kanonische Projektion*.

Satz 1.2.2 (Homomorphiesatz). Gegeben seien zwei Gruppen G und H und ein Homomorphismus $f : G \rightarrow H$.

Es gibt nun genau einen injektiven Homomorphismus $\bar{f} : G/\ker(f) \rightarrow H$, für welchen $f(g) = \bar{f}(\pi(g))$ gilt.

Wenn f zudem surjektiv ist, so ist \bar{f} ein Isomorphismus.

Definition 1.2.3 (Direktes Produkt, direkte Summe). Sei I eine Indexmenge und für $i \in I$ sei G_i eine Gruppe. Das direkte Produkt $\prod_{i \in I} G_i$ ist gegeben durch das entsprechende kartesische

Produkt mit komponentenweiser Gruppenstruktur

$$g = (g_i)_{i \in I} \in \prod_{i \in I} G_i, \quad g_i \in G_i$$

$$g \circ h = (g_i \circ h_i)_{i \in I}$$

(ist $|I| < \infty$, z.B. $I = \{1, \dots, n\}$, so schreiben wir anstelle $\prod_{i \in I} G_i : G_1 \times \dots \times G_n$)

Die direkte Summe $\bigoplus_{i \in I} G_i$ ist gegeben durch das entsprechende kartesische Produkt, wobei an fast allen Stellen das neutrale Element steht, mit komponentenweiser Gruppenstruktur.

Offensichtlich ist das direkte Produkt gleich der direkten Summe, wenn die Indexmenge endlich ist: $G_1 \times \dots \times G_n = G_1 \oplus \dots \oplus G_n$

Als Beispiel sei hier $I = \{1, \dots, n\}$ mit $G_i = \mathbb{R}$ angegeben. Dann gilt $\prod_{i \in I} G_i = \mathbb{R}^n = \bigoplus_{i \in I} G_i$.

Definition 1.2.4 (Zentrum). Das Zentrum $Z(G)$ einer Gruppe ist die Menge aller Elemente aus G , die mit allen Elementen aus G kommutieren, d.h.

$$Z(G) = \{g \in G \mid \forall h \in G : g \circ h = h \circ g\}$$

Das Zentrum einer Gruppe ist ein Normalteiler.

Definition 1.2.5 (Normalisator). Es sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann ist der Normalisator von H in der Gruppe G definiert durch

$$N_G(H) = \{g \in G \mid g \circ H \circ g^{-1} = H\}$$

$N_G(H)$ ist wieder eine Untergruppe von G und H ist ein Normalteiler von $N_G(H)$.

1.3 Die beiden Isomorphiesätze

Satz 1.3.1 (1. Isomorphiesatz).

Es sei G eine Gruppe. $H, K \leq G$ seien Untergruppen mit $H \leq N_G(K)$. Dann gilt

1. $H \cap K \trianglelefteq H$
2. $K \trianglelefteq HK = \{h \circ k \mid h \in H, k \in K\}$
3. $HK/K \cong H/H \cap K$

Beweis

Wir beginnen mit der Vorüberlegung, dass $HK \leq G$ gilt. Weiterhin gilt:

$$(*) \quad H \leq N_G(K) \Rightarrow \forall h \in H : hKh^{-1} = K$$

Nun benutzen wir das Untergruppenkriterium:

- $HK \neq \emptyset$, da $e \in HK$
- zu zeigen: $ab^{-1} \in HK, \forall a, b \in HK$

Seien $a, b \in HK$, d.h. $a = hk, b = h'k'$ mit $h, h' \in H$ und $k, k' \in K$.

$$\Rightarrow ab^{-1} = (hk)(h'k')^{-1} = h(kk'^{-1})h'^{-1} = hk''h'^{-1} \text{ mit } k'' = kk'^{-1}$$

Es ist mit (*): $h'k''h'^{-1} \in K$, d.h. $\exists k''' \in K : h'k''h'^{-1} = k''' \Leftrightarrow k''h'^{-1} = h'^{-1}k'''$

$$\Rightarrow ab^{-1} = hk''h'^{-1} = h(h'^{-1}k''') = (hh'^{-1})k''' \in HK$$

Somit gilt $HK \leq G$.

1. Wir zeigen: $H \cap K \trianglelefteq H \Leftrightarrow h(H \cap K)h^{-1} = H \cap K, \forall h \in H$

Dazu sei $h \in H, k \in H \cap K$.

Nun ist zu zeigen, dass $hkh^{-1} \in H \cap K$ gilt.

Hierfür beachten wir, das

$$k \in H \cap K \Rightarrow k \in H \Rightarrow hkh^{-1} \in H \text{ und}$$

$$k \in H \cap K \Rightarrow k \in K \Rightarrow hkh^{-1} \in K \text{ (letzteres wegen (*)) gilt.}$$

Hieraus folgt sofort $\forall k \in H \cap K : \forall h \in H : hkh^{-1} \in H \cap K$. Somit ist $H \cap K$ ein Normalteiler von H .

2. Wir zeigen: $K \trianglelefteq HK$, d.h. $(hk)K(hk)^{-1} = K, \forall hk \in HK$.

$$\text{Dies ist einfach, denn: } (hk)K(hk)^{-1} = h(kKk^{-1})h^{-1} = hKh^{-1} \stackrel{(*)}{=} K$$

$$\Rightarrow K \trianglelefteq HK.$$

3. Mit 1. und 2. sind die Faktorgruppen HK/K und $H/H \cap K$ wohldefiniert. Nun definieren wir $\varphi : HK \rightarrow H/H \cap K$ durch $\varphi(hk) = h(H \cap K)$ ($h \in H, k \in K$).

Zunächst müssen wir uns überlegen, dass φ wohldefiniert ist. Dazu ist zu zeigen:

Gilt $h'k' = hk$ (in $HK, h, h' \in H, k, k' \in K$) so folgt $h'(H \cap K) = h(H \cap K)$.

Seien also $h, h' \in H$ und $k, k' \in K$ mit $h'k' = hk$ gegeben.

Dann gilt auch $h'^{-1}h = k'k^{-1} \in H \cap K$.

Somit folgt: $h'(H \cap K) = h'((h'^{-1}h)(H \cap K))$.

Wegen der Assoziativität gilt: $h'(H \cap K) = (h'h'^{-1})h(H \cap K) = h(H \cap K)$. φ ist also wohldefiniert.

Im nächsten Schritt zeigen wir, dass φ ein Homomorphismus ist:

$$\varphi(hk \cdot h'k') = \varphi(hk) \cdot \varphi(h'k')$$

Wir haben für $hk, h'k' \in HK$:

$$\varphi((hk)(h'k')) = \varphi(h(h'h'^{-1})kh'k') = \varphi(hh'(h'^{-1}kh')k') = (hh')(H \cap K), \text{ weil } h'^{-1}kh' \in K \text{ und somit } (h'^{-1}kh')k' \in K \text{ gilt.}$$

Damit erhalten wir $\varphi((hk) \cdot (h'k')) = (hh')(H \cap K) = h(H \cap K) \cdot h'(H \cap K)$, wobei die letzte Gleichheit wegen Punkt 1 dieses Satzes ($H \cap K \trianglelefteq H$) gilt.

Schließlich ergibt sich $\varphi((hk) \cdot (h'k')) = \varphi(hk) \cdot \varphi(h'k')$. $\Rightarrow \varphi$ ist ein Homomorphismus.

φ ist offensichtlich surjektiv, denn: $\forall h(H \cap K) \in H/H \cap K : \exists he \in HK : \varphi(he) = h(H \cap K)$.

Der Zusatz zum Homomorphiesatz besagt, dass aus der Surjektivität von φ die Isomorphie $HK/\ker(\varphi) \cong H/H \cap K$ folgt.

Es bleibt also $\ker(\varphi) = K$ zu zeigen:

Offensichtlich gilt schon $K \subseteq \ker(\varphi)$ wegen $\forall ek \in HK : \varphi(ek) = e(H \cap K) = H \cap K$. Es bleibt damit lediglich $\ker(\varphi) \subseteq K$ zu zeigen.

Es gilt $\ker(\varphi) = \{hk \in HK \mid \varphi(hk) = H \cap K\} = \{hk \in HK \mid h(H \cap K) = H \cap K\}$ und somit auch $\ker(\varphi) = \{hk \in HK \mid h \in H \cap K\} \subseteq K$.

Damit ist $\ker(\varphi) = K$ gezeigt, wodurch die gewünschte Isomorphie folgt.

□

Satz 1.3.2 (2. Isomorphiesatz).

Seien G eine Gruppe und $H, K \trianglelefteq G$ mit der Eigenschaft, dass $K \leq H$ gilt. Man kann dann selbstverständlich sogar sagen, dass $K \trianglelefteq H$ gilt.

Dann ist H/K Normalteiler in G/K und es besteht die Isomorphie $(G/K)/(H/K) \cong G/H$.

Beweis

Wir definieren $\varphi : G/K \rightarrow G/H$ durch $\varphi(gK) = gH$ ($g \in G$). Zunächst müssen wir uns überlegen, dass φ wohldefiniert ist. Hierfür sei $g' \in gK$ ein weiterer Repräsentant.

Dann gilt $g' = gk, k \in K \leq H \Rightarrow g' \in gH \Rightarrow g'H = gH$. Somit ist φ wohldefiniert.

Wir zeigen im nächsten Schritt, dass φ ein Homomorphismus ist:

Seien $gK, g'K \in G/K$.

$$\Rightarrow \varphi((gK) \cdot (g'K)) = \varphi((gg')K) = (gg')H = (gH) \cdot (g'H) = \varphi(gK) \cdot \varphi(g'K).$$

Offensichtlich ist φ auch surjektiv und auch hier zeigt der Zusatz zum Homomorphiesatz, dass $(G/K)/\ker(\varphi) \cong G/H$ gilt, wenn φ ein surjektiver Homomorphismus ist.

Es bleibt daher lediglich $\ker(\varphi) = H/K$ zu zeigen.

$$\text{Wir haben } \ker(\varphi) = \{gK \mid \varphi(gK) = H\} = \{gK \mid gH = H\} = \{gK \mid g \in H\} = H/K.$$

Hieraus folgt in der Tat die Behauptung des 2. Isomorphiesatzes und überdies haben wir wegen $\ker(\varphi) \trianglelefteq G/K$ auch die Normalteilerbeziehung $H/K \trianglelefteq G/K$. \square

1.4 Die Sylow-Sätze

Wiederholung

Die Operation einer Gruppe auf einer Menge ist folgendermaßen definiert:

Es sei (G, \circ) eine Gruppe und M eine Menge. Dann operiert G auf M , falls eine Verknüpfung

$\bullet : G \times M \rightarrow M$ existiert, welche die folgenden Eigenschaften erfüllt:

1. $\forall g_1, g_2 \in G, m \in M : (g_1 \circ g_2) \bullet m = g_1 \bullet (g_2 \bullet m)$
2. $\forall m \in M : e \bullet m = m$, wobei $e \in G$ das neutrale Element ist.

Die Operation heißt *transitiv*, falls zu $m, m' \in M$ jeweils ein $g \in G$ mit $m' = g \bullet m$ existiert.

Die Operation heißt *einfach transitiv*, falls obiges g eindeutig bestimmt ist.

Definition 1.4.1 (Bahn, Orbit).

G operiere auf M und es sei $m \in M$. Dann heißt die Menge $G \bullet m = \{g \bullet m \mid g \in G\}$ die Bahn oder der Orbit von m unter G .

Definition 1.4.2 (Stabilisator).

$G_m = \{g \in G \mid g \bullet m = m\}$ heißt Stabilisator von m in G .

Bemerkungen

1. Die Gruppe G operiert auf einer Bahn transitiv.
2. Der Stabilisator G_m ist eine Untergruppe in G . Man spricht auch von der Stabilisatoruntergruppe oder Fixgruppe.

Die Stabilisatoruntergruppen zu verschiedenen Elementen einer Bahn sind zueinander konjugiert:

Es sei $m \in M : G \bullet m \ni m, g \bullet m$ für $g \in G$. Dann ist die Stabilisatorgruppe von m die Gruppe G_m . Der Stabilisator von $g \bullet m$ ist $g \circ G_m \circ g^{-1}$, weil:

$$\forall h \in G_m : (g \circ h \circ g^{-1}) \bullet (g \bullet m) = (g \circ h) \bullet (e \bullet m) = g \bullet (h \bullet m) = g \bullet m$$

3. Betrachte die Abbildung $\psi : G \rightarrow G \bullet m$ mit einem fest gewählten $m \in M$.

ψ ist surjektiv auf Grund der Definition einer Bahn. Damit gilt:

$$\psi(g) = \psi(g') \Leftrightarrow g \bullet m = g' \bullet m \Leftrightarrow (g^{-1} \circ g') \bullet m = m \Leftrightarrow g^{-1} \circ g' \in G_m \Leftrightarrow g' \in g \circ G_m$$

Durch den Homomorphiesatz existiert also ein Isomorphismus von G/G_m nach $G \bullet m$.

Im Fall $|G| < \infty$ gilt nun $(G : G_m) = |G \circ m|$. $|G \circ m|$ wird auch als *Länge der Bahn* bezeichnet.

4. G wirke auf M .

Wir definieren auf M die Relation \sim durch $m \sim m' \Leftrightarrow \exists g \in G : m' = g \circ m$. Zwei Elemente m und m' stehen daher in Relation zueinander, wenn sie in derselben Bahn liegen.

Dies ist eine Äquivalenzrelation, bei welcher die Bahnen die Äquivalenzklassen darstellen. Daher existiert eine Partition von M in Bahnen:

$$M = \bigcup_{j \in I} G \bullet m_j, \text{ wobei } I \text{ eine geeignete Indexmenge ist.}$$

Seien nun $|M|, |G| < \infty$.

$$\text{Dann gilt die Bahnformel: } |M| = \sum_{j \in I} |G \bullet m_j| = \sum_{j \in I} (G : G_{m_j}).$$

Beispiel

Wir möchten uns an dieser Stelle mit einem Beispiel für die Verwendung der Bahnformel befassen.

Sei $G = (G, \circ)$ eine Gruppe und $M = G$ die G zugrunde liegende Menge. Die Wirkung \bullet von G auf sich selbst (d.h. auf $M = G$) wird durch Konjugation definiert: $g \bullet m = g \circ m \circ g^{-1}$.

Für $m \in G$ ist $G \bullet m = \{g \bullet m = g \circ m \circ g^{-1} \mid g \in G\}$ die Konjugationsklasse von m .

$G_m = \{g \in G \mid g \circ m \circ g^{-1} = m\} = N_G(m)$ ist der Normalisator des Elements $m \in G$ in G .

Bemerkung

Wenn $m \in Z(G)$ gilt, so gilt $G \bullet m = \{m\}$, d.h. die Bahn, bzw. die Konjugationsklasse, von m besteht nur aus einem Element: aus m selbst.

Nun folgt aus der Bahnformel

$$\begin{aligned} |M| &= |G| = \sum_{j \in I} |G \bullet m_j| = \sum_{j \in I, m_j \in Z(G)} |G \bullet m_j| + \sum_{j \in I, m_j \notin Z(G)} |G \bullet m_j| \\ &= |Z(G)| + \sum_{j \in I, m_j \notin Z(G)} (G : N_G(m_j)) \end{aligned}$$

Definition 1.4.3 (p -Untergruppen, p -Sylowuntergruppen).

Sei G eine endliche Gruppe der Ordnung $n = p^r m$, wobei $p \in \mathbb{P}$ und $p \nmid m$ gelte. \mathbb{P} bezeichne hierbei die Menge der Primzahlen.

Eine Untergruppe $H \leq G$ mit $|H| = p^s$, $s \in \mathbb{N}, 0 \leq s \leq r$ heißt eine p -Untergruppe von G .

Eine Untergruppe $H \leq G$ mit $|H| = p^r$ (d.h. $s = r$) heißt eine p -Sylowuntergruppe von G .

Lemma 1.4.4.

Sei $n = p^r m$ mit einer Primzahl p und einer zu p teilerfremden Zahl $0 < m \in \mathbb{N}$. Weiterhin sei s eine natürliche Zahl mit $0 \leq s \leq r$.

Dann gilt $\binom{n}{p^s} = p^{r-s} m l$ mit $l \equiv 1 \pmod{p}$ (d.h. $p \nmid (l-1)$).

Beweis

Gemäß der Definition gilt

$$\binom{n}{p^s} = \frac{n \cdot (n-1) \cdot \dots \cdot (n-p^s+1)}{1 \cdot \dots \cdot (p^s-1) \cdot p^s} = \frac{p^r m}{p^s} \cdot \frac{(n-1) \cdot \dots \cdot (n-p^s+1)}{1 \cdot \dots \cdot (p^s-1)} = p^{r-s} m \binom{n-1}{p^s-1} = p^{r-s} m l \text{ mit } l = \binom{n-1}{p^s-1}.$$

Nun bleibt $l \equiv 1 \pmod{p}$ zu zeigen:

$$l = \prod_{j=1}^{p^s-1} \frac{p^r m - j}{p^s - j} = \prod_{j=1}^{p^s-1} \frac{p^r m - p^{r_j} t_j}{p^s - p^{r_j} t_j} = \prod_{j=1}^{p^s-1} \frac{p^{r-r_j} m - t_j}{p^{s-r_j} - t_j}$$

Die mittlere Gleichheit erhält man, indem man $j = p^{r_j} t_j$ mit $p \nmid t_j$ und $0 \leq r_j \leq s$ schreibt.

$\Rightarrow l = \frac{pA+a}{pB+a}$ mit $A, B, a \in \mathbb{Z}$ und $a = \prod_{j=1}^{p^s-1} (-t_j)$. Auf Grund der verwendeten Konstruktion gilt $p \nmid a$.

$$\Rightarrow l(pB+a) = pA+a \Rightarrow (l-1)a = p(A-lB) \Rightarrow p|(l-1)a$$

Wegen $p \nmid a$ erhält man $p|(l-1)$. Hieraus folgt $l \equiv 1 \pmod{p}$, womit wir die Aussage des Lemmas bewiesen haben. \square

Satz 1.4.5 (1.Sylow-Satz).

Sei G eine Gruppe der Ordnung $n = p^r m$ mit $p \in \mathbb{P}$ und $p \nmid m$.

Dann gilt: $\forall s \in \mathbb{N}, 0 \leq s \leq r : \exists H \leq G : |H| = p^s$.

Insbesondere existiert hierdurch eine p -Sylowuntergruppe, weil die Behauptung auch für $r = s$ gilt.

Beweis

Zunächst betrachten wir die Menge $M = \{S \subseteq G \mid |S| = p^s\}$, welche die Menge der Teilmengen von G mit der Ordnung p^s darstellt. Um den Satz zu beweisen, reicht es nun aus, für jedes s eine Untergruppe $S_0 \in M$ zu finden, welche die Ordnung p^s hat.

Aus kombinatorischen Gründen gilt $|M| = \binom{n}{p^s} = p^{r-s} m l$ mit $l \equiv 1 \pmod{p}$, wobei die zweite Gleichheit bereits im Lemma 1.4.4 bewiesen wurde.

Wir lassen jetzt G auf M durch Linkstranslation wirken, d.h. wir verwenden die Abbildung $(g, S) \mapsto g \circ S = \{g \circ h \mid h \in S\}$. Mit Hilfe der Gruppeneigenschaften von G erkennt man, dass damit eine Wirkung von G auf M definiert wird.

Durch die Bahnformel erhält man:

$$p^{r-s} m l = |M| = \sum_{S \in \mathfrak{S}} |G \circ S| = \sum_{S \in \mathfrak{S}} (G : G_S), \text{ wobei } \mathfrak{S} \text{ ein Vertretersystem der Bahnen ist.}$$

Nun wissen wir wegen $|M| = p^{r-s} m l$, dass p^{r-s} die Ordnung von M teilt, dies aber nicht für p^{r-s+1} gilt. Somit ist p^{r-s} mit dieser Teilbarkeitseigenschaft maximal.

Aus der Bahnformel folgt nun: $\exists S_0 \in M : p^{r-s+1} \nmid |G \circ S_0|$, weil p^{r-s+1} nicht die Kardinalität von M teilt. Daher muss jedoch ein Summand in der Summe aus der Bahnformel existieren, der nicht durch p^{r-s+1} teilbar ist. Dieser sei gerade $|G \circ S_0|$.

Mit anderen Worten: $p^\lambda \mid |G \circ S_0|$ mit $0 \leq \lambda \leq r-s$.

Weiterhin haben wir die Äquivalenz $|G \circ S_0| \mid |G| \Leftrightarrow |G \circ S_0| \mid p^r m$, welche direkt aus den Voraussetzungen des Satzes ($|G| = n = p^r m$) folgt.

$\Rightarrow |G \circ S_0| \leq p^{r-s} m$ (*), weil die höchste Potenz von p , die in $|G \circ S_0|$ vorkommen kann, gerade $r-s$ ist.

Betrachten wir nun den Stabilisator G_{S_0} zu $S_0 \in M$. Wir wissen bereits, dass dieser eine Untergruppe in G ist. Daher bleibt nur noch zu zeigen, dass $|G_{S_0}| = p^s$ gilt.

1. Abschätzung nach unten

$$\frac{|G|}{|G_{S_0}|} = (G : G_{S_0}) = |G \circ S_0| \leq p^{r-s}m \text{ wegen } (*).$$

Somit erhalten wir $|G| = p^r m \leq p^{r-s} m |G_{S_0}|$, woraus $|G_{S_0}| \geq p^s$ folgt.

2. Abschätzung nach oben

Für jedes $h \in G_{S_0}$ gilt $h \circ S_0 = S_0$.

Somit erhalten wir $G_{S_0} \circ S_0 \subseteq S_0 \Rightarrow \forall t \in S_0 : G_{S_0} \circ t \subseteq S_0$

$$\Rightarrow |G_{S_0}| = |G_{S_0} \circ t| \leq |S_0| = p^s.$$

Somit hat die Stabilisatoruntergruppe G_{S_0} wirklich die Ordnung p^s . Damit existiert in G eine Untergruppe mit der Ordnung p^s , womit wir den Satz bewiesen haben. \square

Satz 1.4.6 (2. Sylow-Satz).

Sei G eine Gruppe der Ordnung $n = p^r m$ mit $p \in \mathbb{P}$ und $p \nmid m$. Weiter seien $H \leq G$ eine p -Untergruppe der Ordnung $|H| = p^s$ ($s \in \mathbb{N}, 0 \leq s \leq r$) und $V \leq G$ eine p -Sylowuntergruppe.

Dann existiert eine zu V konjugierte Untergruppe $V' \leq G$, d.h. $\exists g \in G : V' = g \circ V \circ g^{-1}$ mit $H \leq V'$. (Nebenbei gilt damit auch $|V'| = |V| = p^r$, womit V' auch eine p -Sylowuntergruppe ist.)

Außerdem gilt $H \leq V$.

Insbesondere sind alle p -Sylowuntergruppen zueinander konjugiert.

Bemerkung

Weiß man, dass eine derartige Gruppe G genau eine p -Sylowuntergruppe V enthält, so gilt $\forall g \in G : V = g \circ V \circ g^{-1}$, d.h. $V \trianglelefteq G$.

Beweis: 2. Sylow-Satz

Zunächst betrachten wir die Menge $M = \{U \subseteq G \mid \exists g \in G : U = g \circ V\}$, also die Menge aller Linksnebenklassen der p -Sylowuntergruppe V .

Dann gibt es die beiden folgenden Wirkungen von G bzw. H auf M :

1. $G \times M \rightarrow M : (g, U) \mapsto (g \circ U)$

2. $H \times M \rightarrow M : (h, U) \mapsto (h \circ U)$

Ziehen wir zunächst die 1. Wirkung heran:

Offensichtlich ist diese Wirkung transitiv. Damit folgt aus der Bahnformel:

$$|M| = |G \circ V| = (G : G_V) = \frac{|G|}{|G_V|} = \frac{p^r m}{p^r} = m$$

Aus der Bahnformel in Verbindung mit der zweiten Wirkung folgt:

$$|M| = \sum_{U \in \mathfrak{U}} |H \circ U|, \text{ wobei } \mathfrak{U} \text{ ein Repräsentantensystem der } H\text{-Bahnen ist.}$$

Aus $p \nmid m$ folgt, dass p nicht alle Summanden $|H \circ U|$ teilen kann.

Somit existiert ein $U_0 = g_0 \circ V \in M$, so dass $p \nmid |H \circ U_0|$ gilt.

Andererseits haben wir wegen $|H| = p^s$ die Äquivalenz $|H \circ U_0| \mid |H| \Leftrightarrow |H \circ U_0| \mid p^s$.

$$\Rightarrow |H \circ U_0| = 1$$

$$\Rightarrow H \circ U_0 = U_0.$$

Hiermit erhalten wir nun folgende Äquivalenzen:

$$\begin{aligned} H \circ U_0 = U_0 &\Leftrightarrow H \circ (g_0 \circ V) = g_0 \circ V \\ &\Leftrightarrow (h \circ g_0) \circ V = g_0 \circ V (\forall h \in H) \\ &\Leftrightarrow h \circ g_0 \in g_0 \circ V (\forall h \in H) \\ &\Leftrightarrow h \in g_0 \circ V \circ g_0^{-1} (\forall h \in H) \\ &\Leftrightarrow H \leq V' = g_0 \circ V \circ g_0^{-1} \end{aligned}$$

□

Satz 1.4.7 (3. Sylow-Satz).

Sei G eine Gruppe der Ordnung $n = p^r m$ mit $p \in \mathbb{P}$ und $p \nmid m$.

Für jedes $s \in \mathbb{N}$, $0 \leq s \leq r$ bezeichne k die Anzahl der Untergruppen $H \leq G$ mit $|H| = p^s$.

Dann gilt $k \equiv 1 \pmod{p}$.

Falls $s = r$ gilt (d.h. wenn k die Anzahl der p -Sylowuntergruppen ist), so gilt überdies: $k \mid m$.

Beweis

Wie im Beweis des 1. Sylow-Satz gilt für $M = \{S \subseteq G \mid |S| = p^s\}$ die Gleichung

$$|M| = \binom{n}{p^s} = \binom{p^r m}{p^s} = p^{r-s} m l \text{ mit } l \equiv 1 \pmod{p}$$

Jetzt zerlegen wir M in zwei disjunkte Teilmengen:

$$1. M_1 = \{S \in M \mid p^{r-s+1} \nmid |G \circ S|\}$$

Wie im Beweis des ersten Sylow-Satzes gilt auch hier die Bahnformel. Damit erhalten wir $|M| = \sum_{S \in \mathcal{G}} |G \circ S|$. Wenn jede Menge S die Eigenschaft $p^{r-s+1} \mid |G \circ S|$ hat, müsste auch $|M|$ durch p^{r-s+1} teilbar sein. Es gilt jedoch $|M| = p^{r-s} m l$ mit $p \nmid m l$. Daher ist M_1 nicht leer.

$$2. M_2 = \{S \in M \mid p^{r-s+1} \mid |G \circ S|\} = M \setminus M_1$$

Als Zwischenziel möchten wir $|M_1|$ und $|M_2|$ bestimmen. Hierfür reicht es aus, $|M_1|$ abzuzählen.

Dafür beweisen wir: $S \in M_1$, d.h. $S \in M$ mit $p^{r-s+1} \nmid |G \circ S| \Leftrightarrow \begin{cases} \exists H \leq G, |H| = p^s \text{ und} \\ \exists a \in G : S = H \circ a \end{cases}$

1. Hinrichtung " \Rightarrow "

Erinnern wir uns an dieser Stelle an folgenden Sachverhalt aus dem Beweis des ersten Sylow-Satzes:

Die Stabilisatoruntergruppe von $S \in M_1$ hat die Eigenschaft $|G_S| = p^s$.

Dann haben wir $G_S \circ t \leq S$ für $t \in S$. Somit gilt wegen $|G_S \circ t| = p^s = |S|$ auch $G_S \circ t = S$.

Indem wir $H = G_S$ und $a = t \in G$ setzen, erhalten wir $S = H \circ a$.

2. Rückrichtung " \Leftarrow "

Hier gehen wir von der Voraussetzung $S = H \circ a$ mit $H \leq G$, $|H| = p^s$, $a \in G$ aus. Offensichtlich gilt nun $S \in M$. Daher bleibt noch zu zeigen, dass $S \in M_1$ gilt.

Berechnen wir nun die Stabilisatoruntergruppe G_S von S . Wie wir gleich sehen werden, ist diese gerade die Gruppe H .

Sei $g \in H$. Dann gilt $g \circ S = g \circ (H \circ a) = (g \circ H) \circ a = H \circ a = S$

$$\Rightarrow g \in G_S \Rightarrow H \leq G_S$$

Umgekehrt haben wir $g \in G_S \Rightarrow g \circ (H \circ a) = H \circ a$. Hieraus folgt direkt $g \circ H = H$, also $g \in H$. Damit erhalten wir $G_S \leq H$, woraus $G_S = H$ folgt.

$\Rightarrow |G \circ S| = (G : G_S) = (G : H) = \frac{|G|}{|H|} = \frac{p^r m}{p^s} = p^{r-s} m \Rightarrow p^{r-s+1} \nmid |G \circ S|$, weil p und m teilerfremd sind. Wir erhalten daher $S \in M_1$.

Somit ist $M_1 = \{H \circ a \mid H \leq G, |H| = p^s, a \in G\}$.

Betrachten wir nun die offensichtlich surjektive Mengenabbildung

$$\varphi : M_1 \rightarrow \{H \mid H \leq G \text{ wobei } |H| = p^s\} = N \text{ mit } |N| = k \text{ und } H \circ a \mapsto H.$$

Dann ist $\varphi^{-1}(H)$ die Menge der Urbilder von $H \in N$ in M_1 . Diese Menge wird auch als Faser über $H \in N$ bezeichnet.

Jetzt ist $|\varphi^{-1}(H)|$ die Anzahl der Rechtsnebenklassen von $H \in N$ und damit gleich

$$(G : H) = \frac{|G|}{|H|} = \frac{p^r m}{p^s} = p^{r-s} m.$$

Seien nun $H_1, H_2 \in N$ mit $H_1 \neq H_2$. Dann gilt $\varphi^{-1}(H_1) \cap \varphi^{-1}(H_2) = \emptyset$.

Dies beweisen wir indirekt. Dazu nehmen wir an, dass $\varphi^{-1}(H_1) \cap \varphi^{-1}(H_2) \neq \emptyset$ gilt.

$\Rightarrow \exists H_1 \circ a \in \varphi^{-1}(H_1), H_2 \circ b \in \varphi^{-1}(H_2)$ mit $H_1 \circ a = H_2 \circ b$.

Dann erhält man $a \in H_1 \circ a = H_2 \circ b$.

$$\Rightarrow H_2 \circ a = H_2 \circ b = H_1 \circ a$$

$$\Rightarrow H_2 = H_1$$

Dies stellt jedoch einen Widerspruch zu unserer Voraussetzung dar.

$\Rightarrow |M_1| = p^{r-s} m k$ wegen der Zerlegung in k Nebenklassen.

$$|M_2| = |M| - |M_1| = p^{r-s} m l - p^{r-s} m k = p^{r-s} m (l - k)$$

Somit erhalten wir zusammenfassend:

1. $|M_1| = p^{r-s} m k$ (wobei $M_1 = \{S \subseteq G \text{ mit } p^{r-s+1} \nmid |G \circ S|\}$)
2. $|M_2| = p^{r-s} m (l - k)$ (wobei $M_2 = \{S \subseteq G \text{ mit } p^{r-s+1} \mid |G \circ S|\}$)

Beachte: G operiert auf M und lässt dabei die Teilmengen M_1 und M_2 invariant, d.h. G operiert insbesondere auf M_2 durch $(g, S) \mapsto g \circ S$

Mit der Bahnformel erhalten wir $|M_2|$ als Summe der Bahnlängen.

$$\Rightarrow p^{r-s+1} \mid |M_2| = p^{r-s} m (l - k)$$

Weil p und m teilerfremd sind, gilt $p \mid l - k$.

$\Rightarrow k \equiv 1 \pmod{p}$, weil $l \equiv 1 \pmod{p}$ nach Voraussetzung gilt.

Damit ist der Satz (bis auf den Zusatz) bewiesen.

Daher müssen wir nur noch den Zusatz $k \mid m$ beweisen.

Betrachten wir also $M = \{H \leq G \mid |H| = p^r\}$, d.h. die Menge aller p -Sylowuntergruppen. Nun lassen wir G auf M durch Konjugation operieren: $(g, V) \mapsto g \circ V \circ g^{-1}$. Nach dem zweiten Sylow-Satz ist diese Wirkung transitiv.

Sei $H_0 \in M$. Dann gilt $M = G \bullet H_0$ wegen der Transitivität der Wirkung. Aus der Bahnformel folgt, dass $k = |M| = |G \bullet H_0|$ die Gruppenordnung $|G|$ teilt.

$$\Rightarrow k \mid p^r m$$

Da $k \equiv 1 \pmod{p}$ gilt, ist $\text{ggT}(p, k) = 1$.

$$\Rightarrow k \mid m \quad \square$$

1.5 Klassifikation endlicher und endlich erzeugter abelscher Gruppen

Wir möchten uns nun mit der Klassifikation endlicher und endlich erzeugter abelscher Gruppen beschäftigen. Dabei werden wir uns zuerst den endlichen Gruppen zuwenden.

Beispielsweise hatten wir die abelschen Gruppen der Ordnung 4 bereits durch

1. $G \cong \mathbb{Z}/4\mathbb{Z}$ (zyklisch)
2. $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (kleinsche Vierergruppe)

klassifiziert.

Bevor wir uns nun der eigentlichen Behandlung der endlichen abelschen Gruppen widmen, führen wir die folgenden Schreibweisen ein:

Weil die Struktur der Gruppen, die wir hier betrachten, additiv ist, schreiben wir statt (G, \circ) auch $(A, +)$. Als neutrales Element verwenden wir dann 0 statt e .

Des weiteren schreiben wir na statt a^n , wobei $na = \overbrace{a + a + \dots + a}^{n\text{-mal}}$ gilt.

Definition 1.5.1 (p -primärer Bestandteil).

Seien A eine endliche abelsche Gruppe und p eine Primzahl.

Dann setzen wir

$$A(p) = \{a \in A \mid \exists v \in \mathbb{N} : \text{ord}(a) = p^v\}$$

Offensichtlich gilt $A(p) \leq A$. Man nennt $A(p)$ auch den p -primären Bestandteil von A .

Bemerkung

Wenn p die Gruppenordnung nicht teilt, so ist $A(p)$ offensichtlich die triviale Gruppe, d.h. $p \nmid |A| \Rightarrow A(p) = \{0\}$.

Lemma 1.5.2.

Seien A eine endliche abelsche Gruppe und $p \in \mathbb{P}$.

Dann ist $A(p)$ eine p -Sylowuntergruppe von A . Dies ist die einzige p -Sylowuntergruppe von A .

Beweis

Wir zeigen zunächst, dass $A(p)$ eine p -Untergruppe in A ist.

Den Beweis hierfür führen wir indirekt. Daher nehmen wir an, dass $A(p)$ keine p -Untergruppe ist.

$$\Rightarrow \exists q \in \mathbb{P}, q \neq p \text{ mit } q \mid |A(p)|$$

$$\Rightarrow |A(p)| = q^r m \text{ mit } \text{ggT}(q, m) = 1 \text{ und } r \geq 1$$

$$\Rightarrow \exists H \leq A(p) \text{ mit } |H| = q \text{ (1. Sylow-Satz) und es gilt } H \cong \mathbb{Z}/q\mathbb{Z}.$$

$$\Rightarrow \exists a \in A(p) \text{ mit } \text{ord}(a) = q$$

Dies stellt jedoch einen Widerspruch zur Definition von $A(p)$ dar.

Die Definition von $A(p)$ zeigt, dass $A(p)$ sogar eine maximale p -Untergruppe ist. Somit ist $A(p)$ eine p -Sylowuntergruppe.

Das $A(p)$ die einzige p -Sylowuntergruppe in A ist, folgt mit Hilfe des 2. Sylow-Satzes: Alle p -Sylowuntergruppen sind zueinander konjugiert, also im abelschen Falle gleich. \square

Satz 1.5.3 (1. Klassifikationssatz).

Sei A eine endliche abelsche Gruppe und es bestehe für die Ordnung $|A|$ die Primfaktorzerlegung $|A| = \prod_{j=1}^k p_j^{r_j}$ mit $p_1, \dots, p_k \in \mathbb{P}$ und $r_1, \dots, r_k \in \mathbb{N}_{>0}$.
Dann gilt

$$A \cong \bigoplus_{i=1}^k A(p_i)$$

mit $|A(p_i)| = p_i^{r_i}$.

Beweis

Nach dem Lemma gilt $|A(p_i)| = p_i^{r_i} = n_i$ mit $i = 1, \dots, k$

Definieren wir nun $N_i = \frac{|A|}{n_i}$ und betrachten (den Homomorphismus)

$f: A \rightarrow \bigoplus_{i=1}^k A(p_i) = A(p_1) \oplus \dots \oplus A(p_k)$ mit $a \mapsto (N_1 a, \dots, N_k a)$.

Nun zeigen wir die Injektivität von f .

Daraus folgt dann wegen $|A| = \prod_{j=1}^k p_j^{r_j} = \prod_{j=1}^k |A(p_j)| = |\bigoplus_{i=1}^k A(p_i)|$ auch die Bijektivität von f .

Zum Beweis der Injektivität von f stellen wir zunächst fest, dass N_1, \dots, N_k teilerfremd sind, d.h. es gilt $\text{ggT}(N_1, \dots, N_k) = 1$. Durch den euklidischen Algorithmus erhalten wir natürliche Zahlen $x_1, \dots, x_k \in \mathbb{Z}$ mit $x_1 N_1 + \dots + x_k N_k = 1$.

Sei nun $a \in \ker f$. Dann gilt $a \in A$ und $f(a) = 0$, d.h. $(N_1 a, \dots, N_k a) = (0, \dots, 0)$.

$\Rightarrow \forall i \in \{1, \dots, k\} : N_i a = 0$.

$\Rightarrow a = 1 \cdot a = (x_1 N_1 + \dots + x_k N_k) \cdot a = x_1 (N_1 a) + \dots + x_k (N_k a) = 0$, wegen $a \in \ker f$.

Daher ist $\ker(f) = \{0\}$.

$\Rightarrow f$ ist injektiv und somit letztendlich auch ein Isomorphismus. □

Satz 1.5.4 (2. Klassifikationssatz).

Sei B eine endliche abelsche Gruppe der Ordnung p^r mit $p \in \mathbb{P}$ und $r \in \mathbb{N}$.

Dann existiert eine Partition $r = s_1 + \dots + s_l$ mit $s_1 \geq s_2 \geq \dots \geq s_l > 0$ sodass $B \cong \bigoplus_{j=1}^l \mathbb{Z}/p^{s_j} \mathbb{Z}$ gilt. Überdies ist diese Partition von r eindeutig bestimmt.

Man nennt (s_1, \dots, s_l) den Typ der abelschen p -Gruppe B .

Beispiel: $|A| = 4 = 2^2$

In diesem Fall gilt

1. $2 = 2(+0) \Rightarrow A \cong \mathbb{Z}/4\mathbb{Z}$

2. $2 = 1 + 1 \Rightarrow A \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Corollar 1.5.5 (Klassifikationssätze 1 & 2).

Sei A eine endliche abelsche Gruppe der Ordnung $n = p_1^{r_1} \cdot \dots \cdot p_k^{r_k}$.

Dann existieren eindeutig bestimmte Partitionen $r_i = s_{i,1} + \dots + s_{i,l_i}$, mit

$s_{i,j} \in \mathbb{N}, s_{i,1} \geq \dots \geq s_{i,l_i} > 0, i = 1, \dots, k$, sodass $A \cong \bigoplus_{i=1}^k A(p_i) \cong \bigoplus_{i=1}^k \bigoplus_{j=1}^{l_i} \mathbb{Z}/p_i^{s_{i,j}} \mathbb{Z}$ gilt.

Jede endliche abelsche Gruppe ist daher eine direkte Summe zyklischer Gruppen.

Bevor wir mit dem Beweis des zweiten Klassifikationssatzes für endliche Gruppen beginnen, machen wir die folgende

Vorüberlegung:

Sei $b_1 \in B$ ein Element mit maximaler Ordnung $\text{ord}_B(b_1) = p^{s_1}$.

Weiterhin seien $B_1 = \langle b_1 \rangle$, $\pi : B \rightarrow B/B_1$ die kanonische Projektion und $\bar{b} = (b + B_1)$ mit Ordnung $\text{ord}_{B/B_1}(\bar{b}) = p^s$.

Dann gilt: $\exists c \in B : \text{ord}_B(c) = p^s$ und $\pi(c) = \bar{b}$.

Beweis: Vorüberlegung

Es gilt $\text{ord}_{B/B_1}(\bar{b}) = p^s \Rightarrow p^s(b + B_1) = B_1 \Rightarrow p^s b \in B_1$. Damit erhalten wir $s \leq s_1$: Wäre $s > s_1$, dann würde schon für s_1 die Gleichung $p^{s_1} b = 0$ und damit $p^{s_1}(b + B_1) = (p^{s_1}) + B_1 = B_1$ gelten. Dann wäre jedoch $\text{ord}_{B/B_1}(\bar{b}) < p^s$. Widerspruch.

Mit $p^s b \in B_1$ folgt $p^s b = y b_1$ mit $y \in \mathbb{Z}$.

$$\Rightarrow p^{s_1} b_1 = 0 = p^{s_1} b = p^{s_1-s}(p^s b) = p^{s_1-s}(y b_1) = (p^{s_1-s} y) b_1 \Rightarrow p^{s_1} | p^{s_1-s} y$$

$$\Rightarrow \exists u \in \mathbb{Z} : p^{s_1-s} y = u p^{s_1} \Rightarrow y = u p^s$$

$$\Rightarrow p^s b = p^s u b_1 \Rightarrow p^s(b - u b_1) = 0 \text{ mit } u b_1 \in B_1$$

Setze nun $c = b - u b_1$.

Konstruktionsgemäß erhalten wir $\pi(c) = c + B_1 = (b - u b_1) + B_1 = b + (-u b_1 + B_1) = b + B_1 = \pi(b) = \bar{b}$.

Wir haben nun $p^s c = p^s(b - u b_1) = 0$. Daher gilt auf jeden Fall $\text{ord}_B(c) \leq p^s$.

Nun bleibt nun noch zu zeigen, dass $\text{ord}_B(c) = p^s$ gilt. Hierfür reicht es aus, $\text{ord}_B(c) \geq p^s$ nachzuweisen.

Nehmen wir an, dies sei nicht der Fall, d.h. $\text{ord}_B(c) = p^{s'}$ mit $s' < s$.

$$\Rightarrow p^{s'} c = 0 \Rightarrow p^{s'}(b - u b_1) = 0 \Rightarrow p^{s'}(b + B_1) = B_1$$

$$\Rightarrow \text{ord}_{B/B_1}(\bar{b}) = \text{ord}_{B/B_1}(b + B_1) \leq p^{s'} < p^s.$$

Dies stellt einen Widerspruch zur Voraussetzung dar.

Damit folgt $\text{ord}_B(c) = p^s$. □

Beweis: Zweiter Klassifikationssatz

Wir führen den Beweis mittels vollständiger Induktion über die Ordnung von B .

1. Induktionsanfang: $r < 2$

Im Fall $r = 0$ gilt $B \cong \mathbb{Z}/1\mathbb{Z}$ Damit ist die Existenzaussage in diesem Fall korrekt.

Im Fall $r = 1$ gilt $B \cong \mathbb{Z}/p\mathbb{Z}$ Damit ist die Aussage auch hier korrekt.

2. Induktionsvoraussetzung:

Die Existenzaussage sei für alle abelschen Gruppen B' mit $|B'| = p^{r'}$ und $r' < r$ bewiesen.

3. Induktionsschritt: abelsche Gruppe B mit $|B| = p^r$.

Wir wählen ein $b \in B$ mit maximaler Ordnung $\text{ord}_B(b) = p^{s_1}$, bilden $B_1 = \langle b \rangle \cong \mathbb{Z}/p^{s_1}\mathbb{Z}$ und setzen $B' = B/B_1$. Wegen $b \neq 0$ gilt $\text{ord}_B(b) \neq 1$ und damit $s_1 \neq 0$. Daher erhalten wir $|B'| = \frac{|B|}{|B_1|} = p^{r-s_1}$ und $r - s_1 < r$.

Wenden wir nun die Induktionsvoraussetzung auf B' an.

$$\Rightarrow B' \cong \bigoplus_{j=2}^l \langle \bar{b}_j \rangle \cong \bigoplus_{j=2}^l \mathbb{Z}/p^{s_j}\mathbb{Z}, \text{ wobei } (s_2, \dots, s_l) \text{ eine Partition von } r - s_1 \text{ ist,}$$

d.h. $r - s_1 = s_2 + \dots + s_l$ mit $s_2, \dots, s_l \in \mathbb{N}$.

Durch die Projektion π haben wir nun $B \rightarrow B' = B/B_1 = \bigoplus_{j=2}^l \langle \bar{b}_j \rangle$.

Um eine Aussage über B statt B' treffen zu können, verwenden wir die Vorüberlegung. Mit dieser existieren $c_2, \dots, c_l \in B$ mit $\text{ord}_B(c_j) = \text{ord}_{B'}(\bar{b}_j) = p^{s_j}$, $\pi(c_j) = \bar{b}_j$ und $j = 2, \dots, l$.

Wegen $B/B_1 = \langle \bar{b}_2 \rangle \oplus \dots \oplus \langle \bar{b}_l \rangle = \langle \bar{c}_2 \rangle \oplus \dots \oplus \langle \bar{c}_l \rangle$ folgt $B = B_1 + \langle c_2 \rangle + \dots + \langle c_l \rangle$, also auch $B = \langle b_1 \rangle + \langle c_2 \rangle + \dots + \langle c_l \rangle$.

Damit ist B erzeugt durch b_1, c_2, \dots, c_l . Es bleibt also zu zeigen, dass die obige Summe direkt ist, d.h. aus $m_1 b_1 + m_2 c_2 + \dots + m_l c_l = 0 \in B$ mit $m_1, \dots, m_l \in \mathbb{Z}$ folgt $m_1 = \dots = m_l = 0$.

Betrachten wir nun $\pi(m_1 b_1 + m_2 c_2 + \dots + m_l c_l)$.

$$\Rightarrow m_2 \bar{c}_2 + \dots + m_l \bar{c}_l = 0 = B_1$$

Mit der Induktionsvoraussetzung folgt nun $m_2 = \dots = m_l = 0$.

Damit erhalten wir durch $0 = m_1 b_1 + m_2 c_2 + \dots + m_l c_l = m_1 b_1$ auch $m_1 = 0$.

Es gilt daher $B = \langle b_1 \rangle \oplus \langle c_2 \rangle \oplus \dots \oplus \langle c_l \rangle$.

Da der Beweis der Eindeutigkeit dieser Partition als Übungsaufgabe gestellt wurde, wird dieser Beweis hier nicht angeführt. \square

Damit schließen wir den Abschnitt über die Klassifikation endlicher abelscher Gruppen ab und wenden uns den endlich erzeugten abelschen Gruppen zu.

Definition 1.5.6 (endlich erzeugt, Erzeugendensystem, frei, Basis).

Eine abelsche Gruppe A heißt endlich erzeugt, wenn $a_1, \dots, a_r \in A$ existieren, sodass sich jedes $a \in A$ in der Form $a = \sum_{j=1}^r x_j a_j$ mit $x_1, \dots, x_r \in \mathbb{Z}$ schreiben lässt.

Die Elemente a_1, \dots, a_r heißen Erzeugendensystem von A .

Eine endlich erzeugte abelsche Gruppe A mit Erzeugendensystem a_1, \dots, a_r heißt freie abelsche Gruppe von Rang r , falls die Darstellung $a = \sum_{j=1}^r x_j a_j$ eindeutig ist. Man sagt in diesem Fall auch, dass $\{a_1, \dots, a_r\}$ eine Basis von A ist.

Bemerkung

Sei A eine freie abelsche Gruppe von Rang r .

Dann gilt $A \cong \mathbb{Z}^r = \bigoplus_{k=1}^r \mathbb{Z}$.

Beweis

Sei $\{a_1, \dots, a_r\}$ eine Basis von A .

Dann existiert ein Isomorphismus von A nach \mathbb{Z}^r , welcher durch $a_j \mapsto e_j = (0, \dots, 0, 1, 0, \dots, 0)^t$

und $a = \sum x_j a_j \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}$ definiert ist. \square

Lemma 1.5.7.

Sei $0 \rightarrow B \rightarrow A \rightarrow C \rightarrow 0$ eine kurze exakte Sequenz abelscher Gruppen, wobei C frei vom Rang r , $g: B \rightarrow A$ injektiv und $f: A \rightarrow C$ surjektiv ist.

Dann existiert eine zu C isomorphe Untergruppe $C' \leq A$ mit $A \cong B \oplus C'$.

Beweis

Sei $\{c_1, \dots, c_t\}$ eine Basis von C . Seien weiterhin $c'_1, \dots, c'_t \in A$ Urbilder von c_1, \dots, c_t bezüglich f und $C' = \langle c'_1, \dots, c'_t \rangle \leq A$.

Nun bleibt zu zeigen, dass C' frei vom Rang t ist.

Per constructionem gilt $\langle c'_1, \dots, c'_t \rangle = C'$.

Es bleibt also zu zeigen, dass aus $m_1 c'_1 + \dots + m_t c'_t = 0 \in A$ und $m_1, \dots, m_t \in \mathbb{Z}$ die Gleichung $m_1 = \dots = m_t = 0$ folgt.

Wenden wir also die Funktion f auf $m_1 c'_1 + \dots + m_t c'_t = 0$ an und erhalten

$$m_1 f(c'_1) + \dots + m_t f(c'_t) = f(m_1 c'_1 + \dots + m_t c'_t) = f(0) = 0$$

Somit erhalten wir $m_1 = \dots = m_t = 0$, da c_1, \dots, c_t eine Basis von C ist.

Damit ist C' frei vom Rang t und es gilt $C' \cong C$.

Beachte nun, dass B auch als Untergruppe von A betrachtet werden kann. Man identifiziert lediglich ein Element $b \in B$ mit $g(b) \in A$. Dies ist möglich, weil g injektiv und das Bild von g eine Untergruppe in A ist.

Wir zeigen nun $A = B \oplus C'$.

Hierfür müssen wir Folgendes beweisen:

1. Jedes Element aus A ist Summe von Elementen von B, C' .

Hierfür sei $a \in A$. Betrachten wir nun $C \ni f(a) = \sum_{j=1}^t x_j c_j$ mit eindeutig bestimmten $x_j \in \mathbb{Z}$.

Nun bilden wir die Differenz $a - \sum_{j=1}^t x_j c'_j$ und erhalten

$$f(a - \sum_{j=1}^t x_j c'_j) = f(a) - \sum_{j=1}^t x_j f(c'_j) = f(a) - \sum_{j=1}^t x_j c_j = f(a) - f(a) = 0.$$

$$\Rightarrow a - \sum_{j=1}^t x_j c'_j \in \ker f = \text{im } g = B$$

$$\Rightarrow \exists b \in B : a = b + \sum_{j=1}^t x_j c'_j \in B + C'$$

2. Die Summe ist direkt, d.h. $B \cap C' = \{0\}$.

Es sei $c' \in B \cap C'$.

$$\Rightarrow c' \in B = \ker f$$

$$\Rightarrow f(c') = 0$$

Umgekehrt gilt $c' \in C' : c' = \sum_{j=1}^t x_j c'_j$, also $0 = f(c') = \sum_{j=1}^t x_j c_j$.

$$\Rightarrow x_1, \dots, x_t = 0 \Rightarrow c' = 0$$

□

Satz 1.5.8.

Seien A eine freie abelsche Gruppe vom Rang r , d.h. $A \cong \mathbb{Z}^r$ und $B \leq A$.

Dann ist auch B frei vom Rang $\leq r$.

Beweis

Den Beweis führen wir durch vollständige Induktion nach dem Rang r von A .

1. Induktionsanfang: $r = 0, 1$

Im Fall $r = 0$ haben wir $A = \{0\}$ und somit $B = \{0\}$. Damit ist die Behauptung trivialerweise korrekt.

Im Fall $r = 1$ haben wir entweder $B = \{0\} \cong \mathbb{Z}/1\mathbb{Z}$ oder $B = A$. Beide Fälle ergeben sofort, dass B frei ist.

2. Induktionsvoraussetzung: Der Satz sei für alle freien Gruppen A' mit Rang $r' < r$ bewiesen.3. Induktionsschritt ($r > 1$):

Sei $\{a_1, \dots, a_r\}$ eine Basis von A .

Betrachten wir nun die Abbildung $f : A \rightarrow \mathbb{Z}a_1$, welche durch $\sum_{j=1}^r x_j a_j \mapsto x_1 a_1$ definiert ist. Diese ist ein surjektiver Homomorphismus.

Betrachten wir nun die Einschränkung g des Homomorphismus f auf B , d.h. $g = f|_B$. Nun sei $B' = \ker g \leq B$ und $B'' = \text{im } g \leq \mathbb{Z}a_1$.

Wir erhalten die kurze exakte Sequenz $0 \rightarrow B' \rightarrow B \rightarrow B'' \rightarrow 0$.

Nun ist $B'' \leq \mathbb{Z}a_1$ eine Untergruppe der freien abelschen Gruppe $\mathbb{Z}a_1$ vom Rang 1.

Mit der Induktionsvoraussetzung ist B'' frei von Rang 0 oder 1. Durch das Lemma folgt nun $B \cong B' \oplus B''$.

Beachte, dass $\ker f$ den maximalen Rang $r - 1$ hat. Damit hat auch B' den maximalen Rang $r - 1$.

$\Rightarrow B' \leq \ker f$ ist frei nach der Induktionsvoraussetzung.

$\Rightarrow B$ ist frei.

□

Definition 1.5.9 (Torsionsbestandteil).

Sei A eine abelsche Gruppe. Dann ist $A_{\text{tor}} = \{a \in A \mid \text{ord } a < \infty\}$ der Torsionsbestandteil von A . Gilt $A_{\text{tor}} = \{0\}$, so heißt A torsionsfrei.

Lemma 1.5.10 (Serie 5, Aufgabe 2).

Sei A eine endlich erzeugte abelsche Gruppe. Dann gilt:

1. A_{tor} ist eine endliche abelsche Untergruppe von A .
2. A/A_{tor} ist torsionsfrei.

Beweis

Weil die Beweise Bestandteil der Übungsaufgabe 2 (Serie 5) war, werden wir hier nur eine kurze Beweisskizze angeben.

1. Sei $A = \langle a_1, \dots, a_r \rangle$ und e_j mit $j = 1, \dots, r$ der j -te Standardbasisvektor der freien abelschen Gruppe \mathbb{Z}^r . Betrachte den durch die Zuordnung $e_j \mapsto a_j$ mit $j = 1, \dots, r$ induzierten surjektiven Homomorphismus $\varphi : \mathbb{Z}^r \rightarrow A$ mit $\varphi(\sum_{j=1}^r \lambda_j e_j) = \sum_{j=1}^r \lambda_j a_j$.

Das A_{tor} eine Untergruppe ist, werden wir hier nicht weiter beweisen.

Betrachte nun $B = \varphi^{-1}(A_{tor})$. Dann ist $B \leq \mathbb{Z}^r$.

Mit Satz 1.5.8 erhalten wir, dass B frei ist. Sei also b_1, \dots, b_s eine Basis von B .

$$\Rightarrow A_{tor} = \langle \varphi(b_1), \dots, \varphi(b_s) \rangle$$

Hierbei haben jedoch $\varphi(b_1), \dots, \varphi(b_s)$ endliche Ordnung. Damit gilt für jedes Element in A_{tor} die Gleichung $a = \sum_{j=1}^s \lambda_j \varphi(b_j)$, wobei $\lambda_j \in \mathbb{Z}$ und $0 \leq \lambda_j < \text{ord } \varphi(b_j)$ mit $j = 1, \dots, s$ gilt.

Es folgt also sofort $|A_{tor}| < \infty$.

2. Sei $\bar{a} \in A/A_{tor}$ mit $a \in A$ als Repräsentant von \bar{a} , d.h. $\bar{a} = a + A_{tor}$.

Es ist nun zu zeigen, dass aus der Existenz eines Elements $m \in \mathbb{N}_{>0}$ mit $m \cdot \bar{a} = \bar{0}$ die Gleichung $\bar{a} = \bar{0}$ folgt.

Aus $m \cdot \bar{a} = \bar{0}$ folgt nun $ma \in A_{tor}$.

$$\Rightarrow \exists n \in \mathbb{N}_{>0} : (nm)a = n(ma) = 0.$$

$$\Rightarrow a \in A_{tor} \Rightarrow \bar{a} = \bar{0}.$$

□

Satz 1.5.11.

Sei A eine endlich erzeugte abelsche Gruppe. Dann ist A/A_{tor} frei und es gilt $A \cong \mathbb{Z}^r \oplus A_{tor}$, wobei r der Rang von A/A_{tor} ist.

Beweis

Es sei $A' = A/A_{tor}$. Es ist nun zu zeigen, dass A' frei ist. Weil die endliche Erzeugtheit von A' bereits klar ist, muss nur noch gezeigt werden, dass A' eine Basis besitzt.

Zunächst zum trivialen Fall:

Falls $A' = \{0\}$, so folgt $A = A_{tor}$. Damit gilt $r = 0$ und wir sind fertig.

Nun zum interessanten Fall $A' \neq \{0\}$. Sei $S = \{a'_1, \dots, a'_n\}$ ein Erzeugendensystem von A' .

O.B.d.A. sei $\{a'_1, \dots, a'_r\} \subseteq S$ eine maximale Teilmenge mit der Eigenschaft (*), dass aus

$$\sum_{j=1}^r \lambda_j a'_j = 0 \in A' \text{ mit } \lambda_1, \dots, \lambda_r \in \mathbb{Z} \text{ die Relation } \lambda_1 = \dots = \lambda_r = 0 \text{ folgt.}$$

Hierfür sei $B' = \langle a'_1, \dots, a'_r \rangle = \mathbb{Z}a'_1 \oplus \dots \oplus \mathbb{Z}a'_r \leq A'$. Wegen (*) ist B' eine freie abelsche Untergruppe von A' .

Sei $a' \in A'$ beliebig. Aufgrund der Wahl von $\{a'_1, \dots, a'_r\}$, gibt es von Null verschiedene ganze Zahlen $\lambda_1, \dots, \lambda_r$ mit $\lambda a' + \lambda_1 a'_1 + \dots + \lambda_r a'_r = 0$. Dabei darf λ nicht null sein, da sonst $\lambda = 0, \lambda_1 = \dots = \lambda_r = 0$ folgte.

$$\Rightarrow \lambda a' = -\sum_{j=1}^r \lambda_j a'_j \in B'$$

Ist $a' \in A'$ beliebig, so existiert $\lambda = \lambda(a') \in \mathbb{Z}$ mit $\lambda(a') \cdot a' \in B'$. Insbesondere ist $\lambda(a'_j) \in \mathbb{Z}$, also $\lambda(a'_j) a'_j \in B'$ für $j = 1, \dots, n$.

Definieren wir nun $\mathbb{Z} \ni \Lambda = \lambda(a'_1) \cdot \dots \cdot \lambda(a'_n)$.

$$\Rightarrow \Lambda \cdot a'_j \in B' \text{ mit } j = 1, \dots, n$$

$$\Rightarrow \forall a' \in A' : \Lambda \cdot a' \in B'$$

$$\Rightarrow \Lambda \cdot A' \leq B'.$$

Mit Satz 1.5.8 erhalten wir nun, dass $\Lambda \cdot A'$ frei mit einem Rang von höchstens r ist.

Wie erkennen wir nun, dass A' frei ist?

Betrachten wir hierfür den Gruppenhomomorphismus $f : A' \rightarrow \Lambda \cdot A'$ mit $a' \mapsto \Lambda \cdot a'$. Da A' nach dem Lemma torsionsfrei ist, ist f injektiv, denn: $f(a') = 0 \Leftrightarrow \Lambda \cdot a' = 0 \Leftrightarrow a' = 0$.

$$\Rightarrow A' \cong f(A') \leq \Lambda \cdot A' \leq B'$$

Damit ist A' frei.

Somit bleibt nur noch die Isomorphie $A \cong \mathbb{Z}^r \oplus A_{tor}$ mit $r = \text{rg } A/A_{tor}$ zu zeigen.

Betrachten wir nun die kurze exakte Sequenz $0 \rightarrow A_{tor} \rightarrow A \rightarrow A/A_{tor} \rightarrow 0$. Wir wissen, dass A/A_{tor} frei ist. Durch das Lemma 1.5.3 folgt nun $A' \cong \mathbb{Z}^r \oplus A_{tor} \cong A_{tor} \oplus \mathbb{Z}^r$. \square

Zusammenfassung

Sei A eine endlich erzeugte abelsche Gruppe. Dann existiert $r \in \mathbb{N} : A \cong \mathbb{Z}^r \oplus A_{tor}$.

Sei nun $|A_{tor}| = n = p_1^{n_1} \cdot \dots \cdot p_k^{n_k}$. Dann gilt weiterhin $A_{tor} = \bigoplus_{j=1}^k A(p_j)$. Schließlich bestimmen wir den Typ von $A(p_j)$ mittels einer Partition von n_j , wobei $|A(p_j)| = p_j^{n_j}$ gilt.

$$\Rightarrow A(p_j) \cong \bigoplus_{k=1}^l \mathbb{Z}/p_j^{s_{jk}} \mathbb{Z}.$$

Damit ist jede endlich erzeugte abelsche Gruppe als direkte Summe von Gruppen der Form $\mathbb{Z}/p_i^{n_i} \mathbb{Z}$ mit $p \in \mathbb{P}$ darstellbar.

1.6 Normalreihen, Kompositionsreihen, Auflösbarkeit

In diesem Abschnitt sei $G = (G, \circ)$ eine beliebige Gruppe, also nicht notwendigerweise abelsch. Wie gewohnt bezeichnen wir das neutrale Element mit e .

Definition 1.6.1 (einfache Gruppe).

Eine Gruppe G heißt einfach, falls G und $\{e\}$ die einzigen Normalteiler in G sind.

Definition 1.6.2 (Normalreihe, Länge, Faktoren).

Eine endliche Reihe von Untergruppen von G mit

$$(1) G = G_1 \geq G_2 \geq \dots \geq G_r = \{e\},$$

so dass G_{i+1} Normalteiler in G_i mit $i = 1, \dots, r-1$ ist, heißt Normalreihe von G .¹ Die Zahl r heißt die Länge der Normalreihe (1). Die sukzessiven Faktorgruppen G_i/G_{i+1} mit $i = 1, \dots, r-1$ heißen die Faktoren der Normalreihe (1).

Definition 1.6.3 (Verfeinerung, isomorph).

Die Normalreihe (1) sei vorgelegt. Eine weitere Normalreihe

$$(2) G = H_1 \geq H_2 \geq \dots \geq H_s = \{e\}$$

heißt Verfeinerung der Normalreihe (1), falls alle Untergruppen G_i mit $i = 1, \dots, r$ von (1) unter den Untergruppen H_j mit $j = 1, \dots, s$ von (2) auftreten. Damit gilt offensichtlich $s \geq r$.

¹Oft soll G_j echte Untergruppe von G_{j+1} sein.

Zwei Normalreihen (1) und (2) heißen isomorph, falls eine Bijektion zwischen den Indexmengen $\{1, \dots, r\}$ und $\{1, \dots, s\}$ besteht, so dass die entsprechenden Faktorgruppen $G_i/G_{i+1} \cong H_{i'}/H_{i'+1}$ erfüllen. Insbesondere gilt dann $r = s$.

Definition 1.6.4 (Kompositionsreihe).

Die Normalreihe (1) von G heißt Kompositionsreihe von G , falls alle Faktoren von G_i/G_{i+1} einfach sind, wobei $i = 1, \dots, r - 1$ gilt.

Bemerkungen

Es stellen sich hierbei die folgenden Fragen:

1. Wann existieren Kompositionsreihen?
2. Sind die Kompositionsreihen eindeutig?

Diese Frage werden wir später mit dem Satz von Jordan-Hölder beantworten.

Satz 1.6.5 (Schreier).

Seien

(1) $G = G_1 \geq \dots \geq G_r = \{e\}$ und

(2) $G = H_1 \geq \dots \geq H_s = \{e\}$

zwei Normalreihen von G .

Dann existieren Verfeinerungen (1') von (1) und (2') von (2), die zueinander isomorph sind.

Bevor wir diesen Satz beweisen, formulieren wir das folgende Lemma.

Lemma 1.6.6 (Butterfly Lemma).

Seien U, V Untergruppen von G und $u \trianglelefteq U, v \trianglelefteq V$ Normalteiler in U bzw. V .

Dann gilt:

1. $u \cdot (U \cap v) \trianglelefteq u \cdot (U \cap V)$
2. $(u \cap V) \cdot v \trianglelefteq (U \cap V) \cdot v$
3. $u \cdot (U \cap V) / u \cdot (U \cap v) \cong (U \cap V) \cdot v / (u \cap V) \cdot v$

Beweis

Wir setzen $H = U \cap V$ und $K = u \cdot (U \cap v)$.

Damit erhalten wir die Gleichungen

$$H \cap K = (U \cap V) \cap u \cdot (U \cap v) = (u \cap V) \cdot (U \cap v)$$

$$\text{und } H \cdot K = (U \cap V) \cdot u \cdot (U \cap v) = u \cdot (U \cap V) \cdot (U \cap v) = u \cdot (U \cap V).$$

Wir überprüfen nun $H \leq N_G(K)$, d.h. $\forall g \in U \cap V : g \cdot K \cdot g^{-1} = K$.

Dies ist äquivalent zu $\forall g \in U \cap V : g \cdot (u \cdot (U \cap v)) \cdot g^{-1} = u \cdot (U \cap v)$.

Durch eine weitere äquivalente Umformung erhält man $(g \cdot u \cdot g^{-1})(g \cdot U \cdot g^{-1} \cap g \cdot v \cdot g^{-1}) = u \cdot (U \cap v)$.

Diese Gleichung lässt sich nun leicht nachweisen:

$$(g \cdot u \cdot g^{-1})(g \cdot U \cdot g^{-1} \cap g \cdot v \cdot g^{-1}) = (u \cdot g \cdot g^{-1})(U \cap v \cdot g \cdot g^{-1}) = u \cdot (U \cap v)$$

Somit sind die Voraussetzungen für den ersten Isomorphiesatz erfüllt. Dieser sagt nun folgendes aus:

Wenn $K \trianglelefteq HK$, also $u(U \cap v) \trianglelefteq u(U \cap V)$ gilt, dann folgt $HK/K \cong H/H \cap K$, also $u(U \cap V)/u(U \cap v) \cong U \cap V/(u \cap V)(U \cap v)$.

Analog erhält man die Isomorphie $(U \cap V)v/(u \cap V)v \cong U \cap V/(u \cap V)(U \cap v)$. \square

Beweis: Satz von Schreier

Als Beweisidee betrachten wir Folgendes:

Wir wählen $G_{i,j} = G_{i+1} \cdot (G_i \cap H_j)$ und $H_{j,i} = (G_i \cap H_j) \cdot H_{j+1}$ als Verfeinerungen der Normalreihen

$$(1) G = G_1 \triangleright \dots \triangleright G_r = \{e\} \text{ und}$$

$$(2) G = H_1 \triangleright \dots \triangleright H_s = \{e\}.$$

Nun zeigen wir:

1. G_{ij} bilden eine Verfeinerung von (1).

Es gilt offensichtlich

$$G = G_1 \geq G_{1,1} \geq G_{1,2} \geq \dots \geq G_{1,s-1},$$

$$G_2 \geq G_{2,1} \geq G_{2,2} \geq \dots \geq G_{2,s-1},$$

\vdots

$$G_{r-1} \geq G_{r-1,1} \geq G_{r-1,2} \geq \dots \geq G_{r-1,s-1} \geq \{e\}.$$

Mit einer kleinen Überlegung sieht man auch $G_{1,s-1} \trianglelefteq G_2, \dots, G_{r-2,s-1} \trianglelefteq G_{r-1}$. Durch Punkt 1 des Butterfly-Lemmas erhalten wir mit $u = G_{i+1} \trianglelefteq G_i = U$ und $v = \{e\} \trianglelefteq H_{s-1} = V$ die Normalteilerbeziehung $u \cdot (U \cap v) \trianglelefteq u \cdot (U \cap V)$, also $G_{i+1} = G_{i+1} \cdot (G_i \cap \{e\}) \trianglelefteq G_{i+1} \cdot (G_i \cap H_{s-1})$.

Ebenfalls aus der ersten Aussage dieses Lemmas erhalten wir die Normalteilerbeziehungen in den einzelnen Zeilen: $G_{i+1} \cdot (G_i \cap H_{j+1}) = u \cdot (U \cap v) \trianglelefteq u \cdot (U \cap V) = G_{i+1} \cdot (G_i \cap H_j)$.

Analog erhalten wir mit Hilfe der zweiten Aussage des Lemmas, dass $H_1 = H_{11} \geq \dots \geq H_{ji} \geq \dots \{e\}$ eine Verfeinerung von (2) ist.

2. Isomorphie zwischen den Verfeinerungen

Mit Hilfe des dritten Punktes des Butterfly-Lemmas folgern wir sofort die gewünschte Isomorphie der Faktorgruppen:

$$G_{ij}/G_{i(j+1)} = G_{i+1} \cdot (G_i \cap H_j)/G_{i+1} \cdot (G_i \cap H_{j+1}) \cong (G_i \cap H_j) \cdot H_{j+1}/(G_{i+1} \cap H_j) \cdot H_{j+1} = H_{ji}/H_{j(i+1)}.$$

Damit bilden G_{ij} und H_{ji} Normalreihen mit jeweils $(r-1)(s-1)+1$ Elementen und isomorphen Faktoren. Daher sind die Normalreihen zueinander isomorph. \square

Satz 1.6.7 (Satz von Jordan-Hölder).

Es sei $G = G_1 \geq \dots \geq G_r = \{e\}$ eine Kompositionsreihe von G .

Dann ist sie bis auf Isomorphie eindeutig bestimmt.

Beweis

Sei eine weitere Kompositionsreihe gegeben. Nach dem Satz von Schreier folgt nun, dass isomorphe Verfeinerungen dieser Kompositionsreihen existieren. Diese sind dann jedoch isomorph zu den Kompositionsreihen selbst, weil alle Faktorgruppen einer Kompositionsreihe bereits einfach sind. Damit sind auch die Kompositionsreihen zueinander isomorph. \square

Proposition 1.6.8.

Sei G eine endliche Gruppe.

Dann besitzt G eine Kompositionsreihe.

Der Beweis wurde uns als Übungsaufgabe überlassen und wird daher an dieser Stelle nicht aufgeführt.

Bemerkung

Mit dieser Proposition kann die Klassifikation endlicher Gruppen auf die Kompositionsreihen und Klassifikation einfacher endlicher Gruppen zurückgeführt werden. Weiterhin existiert eine Liste einfacher endlicher Gruppen.

Dazu gehören:

1. $\mathbb{Z}/p\mathbb{Z}$ mit $p \in \mathbb{P}$
2. A_n mit $n \geq 5$
3. $PSL_n(\mathbb{F}_q) = SL_n(\mathbb{F}_q)/Z(SL_n(\mathbb{F}_q))$ mit $n \geq 2$ und (im Fall $n = 2$ mit $q > 3$)

Außer diesen Gruppen existieren nur noch endlich viele weitere einfache Gruppen. Zu diesen gehört auch die sogenannte Monstergruppe.

Im Folgenden untersuchen wir Gruppen, deren Faktoren in der Kompositionsreihe zyklisch sind.

Definition 1.6.9 (auflösbar).

Eine Gruppe G heißt auflösbar, wenn sie eine Normalreihe mit abelschen Faktoren besitzt.

Lemma 1.6.10.

Sei $f : G \rightarrow H$ ein Homomorphismus. Weiterhin sei $H = H_1 \supseteq \dots \supseteq H_l = \{e\}$ eine Normalreihe mit zyklischen Faktoren. Dann ist $G = f^{-1}(H_1) \supseteq f^{-1}(H_2) \supseteq \dots \supseteq f^{-1}(H_l) = \ker f \supseteq \{e\}$ eine Normalreihe mit zyklischen Faktoren $f^{-1}(H_j)/f^{-1}(H_{j+1})$, wobei $j \leq l - 1$.

Beweis

Wir führen den Beweis in zwei Schritten:

1. Zunächst stellen wir fest, dass $f^{-1}(H_{j+1}) \trianglelefteq f^{-1}(H_j)$ gilt.

Hierfür sei $h \in H_j$ beliebig gewählt. Dann gilt $f(h \circ f^{-1}(H_{j+1}) \circ h^{-1}) = f(h) \circ H_{j+1} \circ f(h)^{-1} = H_{j+1}$, wegen $f(h) \in H_j$ und $H_{j+1} \trianglelefteq H_j$. Hieraus erhalten wir sofort $h \circ f^{-1}(H_{j+1}) \circ h^{-1} \in f^{-1}(H_{j+1})$ und damit auch die gewünschte Normalteilereigenschaft von H_{j+1} in H_j .

2. Nun zeigen wir, dass die Faktoren zyklisch sind.

Wir zeigen zunächst, dass in dem folgenden kommutativen Diagramm mit exakten Zeilen die Funktion \bar{f} injektiv ist.

$$\begin{array}{ccccccc} 0 & \longrightarrow & f^{-1}(H_{j+1}) & \longrightarrow & f^{-1}(H_j) & \xrightarrow{p_1} & f^{-1}(H_j)/f^{-1}(H_{j+1}) & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow f & & \downarrow \bar{f} & & \\ 0 & \longrightarrow & H_{j+1} & \longrightarrow & H_j & \xrightarrow{p_2} & H_j/H_{j+1} & \longrightarrow & 0 \end{array}$$

Um zu zeigen, dass \bar{f} injektiv ist, sei $\bar{g} = p_1(g) \in \ker \bar{f}$, also $\bar{f}(\bar{g}) = e \circ H_{j+1}$. Damit gilt auch $H_{j+1} = \bar{f}(p_1(g)) = p_2(f(g))$. Jetzt ergibt sich sofort $f(g) \in \ker p_2 = H_{j+1}$.

Wegen $f(f^{-1}(H_{j+1})) \subseteq H_{j+1}$ gilt nun $g \in f^{-1}(H_{j+1})$ und somit auch $\bar{g} = p_1(g) = f^{-1}(H_{j+1})$.

Somit ist \bar{f} injektiv.

Durch die Definition von \bar{f} ist dieser Homomorphismus auch surjektiv und damit ein Isomorphismus.

Schließlich ist $f^{-1}(H_j)/f^{-1}(H_{j+1})$ isomorph zu einer Untergruppe einer zyklischen Gruppe und damit auch zyklisch.

□

Proposition 1.6.11.

Es sei G eine endliche, auflösbare Gruppe. Dann besitzt G eine Normalreihe mit zyklischen Faktoren.

Beweis

Wir führen eine Induktion über die Anzahl der Elemente $|G|$ der Gruppe durch.

1. Induktionsanfang: $G = \{e\}$

Hier gilt die Aussage trivialerweise.

2. Induktionsvoraussetzung:

Die Aussage gelte für alle Gruppen deren Ordnung kleiner als $|G|$ ist.

3. Induktionsschritt:

Es sei $G = G_1 \supseteq \dots \supseteq G_r = \{e\}$ eine Normalreihe von G . O.B.d.A. sei $G_2 \leq G_1$ eine echte Untergruppe, welche in der Normalreihe von G enthalten ist, also mit der Eigenschaft $1 < |G_2| < |G_1|$. Dann ist auch $G_2 \supseteq \dots \supseteq G_r = \{e\}$ eine Normalreihe mit abelschen Faktoren. Nach der Induktionsvoraussetzung ist G_2 wegen $|G_2| < |G_1|$ sogar eine Normalreihe mit zyklischen Faktoren.

Weiterhin wissen wir, dass G_1/G_2 abelsch ist, also $G_1/G_2 \cong B_1 \times \dots \times B_s$ mit zyklischen Gruppen B_1, \dots, B_s . Diese Zerlegung folgt aus dem Klassifikationssatz von endlichen abelschen Gruppen.

Nun müssen wir diese Zerlegung noch auf G übertragen.

Dafür wenden wir das obige Lemma auf

$\pi : G = G_1 \rightarrow G_1/G_2 = B_1 \times \dots \times B_s \supseteq \{e\} \times B_2 \times \dots \times B_s \supseteq \dots \supseteq \{e\}^{s-1} \times B_s \supseteq \{e\}^s$ an.
 Laut der Induktionsvoraussetzung sind die Faktoren der Normalreihe von G_1/G_2 zyklisch.
 Damit erhalten wir $G = \pi^{-1}(B_1 \times \dots \times B_s) \supseteq \dots \supseteq \pi^{-1}(\{e\}^s) = G_2$, wobei G_2 eine Normalreihe mit zyklischen Faktoren besitzt. Durch das Lemma hat auch der erste Teil dieser Normalreihe zyklische Faktoren.

□

Corollar 1.6.12.

Sei G eine endliche, auflösbare Gruppe. Dann sind die Faktoren einer Kompositionsreihe von G zyklische Gruppen von Primzahlordnung.

Bemerkungen zu endlichen Untergruppen der $SO_3(\mathbb{R})$

Die Menge $SO_3(\mathbb{R}) = \{A \in M_3(\mathbb{R}) \mid A^t = A^{-1}, \det A = 1\}$ ist gerade die Menge der Drehungen im Raum \mathbb{R}^3 .

Satz 1.6.13.

Es sei $G \leq SO_3$ eine endliche Untergruppe. Dann ist G isomorph zu

1. $\mathbb{Z}/n\mathbb{Z}$

Zum Beispiel ist $\begin{pmatrix} \cos \frac{2k\pi}{n} & \sin \frac{2k\pi}{n} & 0 \\ -\sin \frac{2k\pi}{n} & \cos \frac{2k\pi}{n} & 0 \\ 0 & 0 & 1 \end{pmatrix}$ mit $k = 0, \dots, n-1$ eine Drehung mit endlicher Ordnung.

2. D_{2n}

Dies entspricht der ebenen Diedergruppe.

3. Tetraedergruppe (die Drehungen, die ein Tetraeder in sich selbst überführen)

4. Hexaedergruppe \cong Oktaedergruppe

5. Dodekaedergruppe \cong Ikosaedergruppe

Beweis

Wir betrachten die Wirkung von G auf $S_2 = \{v \in \mathbb{R}^3 \mid \|v\| = 1\}$.

Wegen $|G| = N < \infty$ existieren endlich viele Pole, d.h. Punkte, wo die Drehachsen der Elemente aus G die S_2 schneiden.

Nun sei r_p die Anzahl der Elemente von G , für die P ein Pol ist.

Nun zählen wir: $\sum (r_p - 1) = 2N - 2$, weil für jedes Element außer dem neutralen Element eine Drehachse und somit zwei Pole existieren.

Jetzt verfeinern wir die Summe als Summe über die Bahnen der Pole.

Damit erhalten wir $\sum n_j(r_j - 1) = 2N - 2 \Leftrightarrow 2 > 2 - \frac{2}{N} = \sum_j (1 - \frac{1}{r_j}) \geq \frac{1}{2}$. Es existieren also höchstens 3 Bahnen. Nun müssen wir diese lediglich durchdiskutieren. □

2 Körpertheorie

2.1 Wiederholung/Einführung

Ringe und Unterringe

Definition 2.1.1 (Ring).

Ein Ring R ist eine Menge mit einer additiven Verknüpfung $+$ und einer multiplikativen Verknüpfung \cdot , welche die folgenden Eigenschaften erfüllt:

1. $(R, +)$ ist eine kommutative Gruppe.
2. (R, \cdot) ist eine Halbgruppe.
3. Für alle $a, b, c \in R$ gelten die Distributivgesetze $a \cdot (b+c) = a \cdot b + a \cdot c$ und $(b+c) \cdot a = b \cdot a + c \cdot a$.

Bemerkung

Falls $\forall a, b \in R : a \cdot b = b \cdot a$ gilt, so heißt R *kommutativ* oder *abelsch*. Das neutrale Element bzgl. $+$ heißt *Nullelement* und wird mit 0 bezeichnet. Falls ein neutrales Element bzgl. \cdot existiert, so heißt es *Einselement* und wird mit 1 bezeichnet.

Bemerkung: Rechenregeln

Für einen Ring R und alle $a, b, c \in R$ gilt:

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$
5. $(b - c) \cdot a = b \cdot a - c \cdot a$

Definition 2.1.2 (Nullteiler, Integritätsbereich).

Ein Element $a \in R \setminus \{0\}$ heißt linker (bzw. rechter) Nullteiler, falls ein $b \in R \setminus \{0\}$ mit $a \cdot b = 0$ (bzw. $b \cdot a = 0$) existiert. R heißt nullteilerfrei, falls keine Nullteiler in R existieren. Ein abelscher, nullteilerfreier Ring heißt Integritätsbereich.

Definition 2.1.3 (Charakteristik).

Sei $(R, +, \cdot)$ ein nullteilerfreier Ring mit Einselement 1, und es existiere eine minimale positive Zahl p mit

$$p \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{p\text{-mal}} = 0$$

Dann heißt p die Charakteristik des Rings R , geschrieben $p = \text{char}(R)$.

Bemerkung

1. Man kann zeigen, dass p eine Primzahl ist.
2. Falls keine minimale positive natürliche Zahl p existiert mit $p \cdot 1 = 0$, so sagt man, R habe die Charakteristik 0. ($\text{char}(\mathbb{Z}) = 0 = \text{char}(\mathbb{R})$)

Definition 2.1.4 (Inverse, Einheiten).

Sei R Ring mit 1. Dann heißt $b \in R$ Rechtsinverses (bzw. Linksinverses) zu $a \in R$, falls $a \cdot b = 1$ (bzw. $b \cdot a = 1$) gilt. Ist beides erfüllt, so heißt b Inverses zu a .

Ein Element $a \in R$, das ein Inverses besitzt, heißt Einheit von R . Die Menge der Einheiten wird mit R^\times bezeichnet. (R^\times, \cdot) ist die multiplikative Gruppe von R .

Beispiel

Die Einheiten von $(\mathbb{Z}, +, \cdot)$ sind ± 1 ; die Einheiten von $M_n(\mathbb{Z})$ sind in $\text{GL}_n(\mathbb{Z})$.

Definition 2.1.5 (Unterring).

Eine Teilmenge $U \subseteq R$ eines Rings R heißt Unterring, falls U mit den von R geerbten Verknüpfungen ein Ring ist.

Man beachte, dass $\{0\}$ und R immer Unterringe von R sind.

Bemerkung: Unterringkriterium

Seien $(R, +, \cdot)$ ein Ring und $S \subseteq R$ seine nicht-leere Teilmenge. Dann besteht folgende Äquivalenz:

$$S \leq R \iff \begin{aligned} &a - b \in S \quad \forall a, b \in S \\ &\text{und } a \cdot b \in S \quad \forall a, b \in S \end{aligned}$$

Ringhomomorphismen, Ideale, Faktorringer**Definition 2.1.6** (Ideal).

Eine Teilmenge $\mathfrak{a} \subseteq R$ eines Rings R heißt Ideal in R , wenn \mathfrak{a} bezüglich der Addition $+$ und bezüglich der Multiplikation \cdot mit Ringelementen abgeschlossen ist, d.h. wenn für alle $a, b \in \mathfrak{a}$ und $r \in R$ auch $a + b, a \cdot r, r \cdot a \in \mathfrak{a}$ gilt. Jedes Ideal ist somit auch ein Unterring von R .

Weiterhin sind R und $\{0\}$ immer Ideale in R . Das Nullideal $\{0\}$ wird auch mit (0) bezeichnet.

Definition 2.1.7 (Ringhomomorphismus).

Seien R, S Ringe. Eine Abbildung $f : R \rightarrow S$ heißt Ringhomomorphismus, falls für alle $a, b \in R$ die Gleichungen $f(a + b) = f(a) + f(b)$ und $f(a \cdot b) = f(a) \cdot f(b)$ gelten. Ist f zudem bijektiv, so heißt f Ringisomorphismus.

Definition 2.1.8 (Kern, Bild).

Seien R und S Ringe und $f : R \rightarrow S$ ein Ringhomomorphismus. Dann heißt die Menge $\ker(f) = \{a \in R \mid f(a) = 0\}$ der Kern von f . Man sieht leicht ein, dass $\ker(f)$ ein Ideal in R ist.

Weiterhin nennen wir $\operatorname{im}(f) = \{b \in S \mid \exists a \in R : f(a) = b\}$ das Bild von f . $\operatorname{im}(f)$ ist ein Unterring in S .

Bemerkung

1. Wenn ein Ring R abelsch ist, so ist für jedes $a \in R$ die Menge $(a) := a \cdot R := \{a \cdot r \mid r \in R\}$ ein Ideal. Es wird als das von a erzeugte Hauptideal bezeichnet.
2. Wenn $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale in R sind, so sind auch $\mathfrak{a} \cap \mathfrak{b}$ und $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ Ideale in R .

Definition 2.1.9 (Faktorring).

Sei $\mathfrak{a} \subseteq R$ Ideal in einem Ring R . Offensichtlich ist dann $(R/\mathfrak{a}, \oplus)$ eine abelsche Gruppe. Durch $(r + \mathfrak{a}) \odot (s + \mathfrak{a}) = (r \cdot s) + \mathfrak{a}$ können wir nun eine Multiplikation einführen. Man rechnet leicht nach, dass dann $(R/\mathfrak{a}, \oplus, \odot)$ ein Ring ist. Er heißt der Faktorring von R .

Satz 2.1.10 (Homomorphiesatz für Ringe).

Sei $f : R \rightarrow S$ Ringhomomorphismus. Dann induziert f einen injektiven Ringhomomorphismus $\bar{f} : R/\ker(f) \rightarrow S$.

Wenn f zudem surjektiv ist, so ist \bar{f} ebenfalls surjektiv und damit ein Isomorphismus.

Körper und Schiefkörper**Definition 2.1.11** (Schiefkörper, Körper).

Ein Ring R heißt Schiefkörper, falls $R^\times = R \setminus \{0\}$ gilt.

Ein Körper ist ein kommutativer Schiefkörper.

Bemerkung: Rechenregeln

Es sei K ein Körper. Dann gilt für alle $a, b, c, d \in K$:

1. Wenn $b, c \neq 0$ gilt, so gilt $\frac{a}{b} = \frac{a \cdot c}{b \cdot c}$.
2. Für $b, d \neq 0$ gilt $\frac{a}{b} \pm \frac{c}{d} = \frac{a \cdot d \pm b \cdot c}{b \cdot d}$.
3. Für $b, d \neq 0$ gilt $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$.

Teilbarkeit, Euklidische, Faktorielle und Hauptidealring

Definition 2.1.12 (teilt, größter gemeinsamer Teiler, irreduzibel).

Sei R ein abelscher Ring mit 1 und $a, b \in R$.

1. b teilt a (man schreibt $b|a$), falls ein $c \in R$ mit $b \cdot c = a$ existiert.
2. Falls $d|a, d|b$ und $\forall d'$ mit $(d'|a \wedge d'|b) \Rightarrow d'|d$ gilt, so heißt d größter gemeinsamer Teiler von a und b . Man schreibt dann $d = \text{ggT}(a, b) = (a, b)$.
3. $0 \neq p \in R \setminus R^*$ heißt unzerlegbar oder irreduzibel, falls gilt:
 $p = b \cdot c \Rightarrow b$ oder c ist Einheit

Bemerkung

Im Gegensatz zu \mathbb{Z} muss die Darstellung als Produkt irreduzibler Faktoren in beliebigen Ringen nicht eindeutig sein.

Definition 2.1.13 (Teilbarkeit von Idealen).

Es sei R ein Ring und $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale in R . Das Ideal \mathfrak{a} teilt \mathfrak{b} genau dann, wenn $\mathfrak{b} \subseteq \mathfrak{a}$ gilt.

Definition 2.1.14 (Primideal, Maximalideal).

Es sei R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal in R . Dann heißt \mathfrak{a}

1. Primideal, wenn für alle $a \cdot b \in \mathfrak{a}$ auch $a \in \mathfrak{a}$ oder $b \in \mathfrak{a}$ gilt.
2. Maximalideal, falls $\mathfrak{a} \neq R$ gilt und es kein Ideal $\mathfrak{b} \subseteq R$ gibt, für welches $\mathfrak{a} \subset \mathfrak{b} \subset R$ gilt.

Bemerkung

Es seien R ein Ring, $a, b \in R$ und $\mathfrak{p}, \mathfrak{m} \subseteq R$ Ideale in R . Dann gilt:

1. $b|a \Leftrightarrow (b)|(a)$
2. \mathfrak{p} ist ein Primideal genau dann, wenn R/\mathfrak{p} ein Integritätsbereich ist.
3. \mathfrak{m} ist genau dann ein Maximalideal, wenn R/\mathfrak{m} ein Körper ist.

Definition 2.1.15 (faktorieller, Hauptideal-, euklidischer Ring).

Ein Integritätsbereich R mit 1 heißt

1. faktoriell (oder ZPE-Ring, d.h. Ring mit eindeutiger Zerlegung in Primelemente), falls sich jedes von 0 verschiedene $a \in R \setminus R^\times$ eindeutig (bis auf die Reihenfolge und Multiplikation mit Einheiten) in unzerlegbare Elemente zerlegen lässt.
2. Hauptidealring (HIR), falls jedes Ideal in R ein Hauptideal ist.

3. euklidisch, falls eine Abbildung $w : R \setminus \{0\} \rightarrow \mathbb{Q}_{>0}$ mit den folgenden Eigenschaften existiert:

- a) Sind $a, b \in R$ und gilt $b \neq 0$, dann existieren $q, r \in R$ mit $a = b \cdot q + r$ und $w(r) < w(b)$ oder es gilt $r = 0$. Dies entspricht dem Euklidischen Algorithmus.
- b) Zu gegebenem $s \in \mathbb{Q}$ ist die Wertemenge

$$W(s) = \{w(a) \mid a \in R \setminus \{0\}, w(a) < s\}$$

endlich.

Satz 2.1.16.

Es gilt: R euklidisch $\Rightarrow R$ Hauptidealring $\Rightarrow R$ faktoriell

Beweis

Dass ein Hauptidealring ein ZPE-Ring ist, bewies Prof. Kramer nicht in der Vorlesung, Bernhard Hornfecks soll es in "Algebra" bewiesen haben.

Sei nun $\mathfrak{a} \subseteq R$ ein Ideal. Zu zeigen ist, dass es ein $a \in R$ gibt, so dass $(a) = \mathfrak{a}$.

Falls $\mathfrak{a} = (0)$ ist, sind wir fertig. Sei also $\mathfrak{a} \neq (0)$, es gebe also ein $a_0 \in \mathfrak{a}, a_0 \neq 0$. Sei $w_0 := w(a_0) \in \mathbb{Q}$. Nach 3b) ist $\{w(a) \mid a \in \mathfrak{a} \setminus \{0\}, w(a) < w_0\}$ endlich, es gibt also ein $a \in \mathfrak{a}$ mit minimalem Wert.

Sei nun $b \in \mathfrak{a}$ beliebig. Nach 3a) gibt es $q, r \in R$, so dass $b = qa + r$, wobei $r = 0$ oder $w(r) < w(a)$. Da a minimal ist, kann nur $r = 0$ sein.¹ Also ist $b = qa$, somit $\mathfrak{a} \subseteq (a)$.

Andererseits ist wegen der Idealeigenschaft $(a) \subseteq \mathfrak{a}$, also zusammen $\mathfrak{a} = (a)$. □

Satz 2.1.17.

R faktoriell $\Rightarrow R[x]$ faktoriell

Konstruktion des Quotientenkörpers

Satz 2.1.18.

Es sei R ein Integritätsbereich mit 1. Dann existiert ein kleinster R umfassender Körper.

Bemerkung

$M := R \times (R \setminus \{0\}) = \{(a, b) \mid a, b \in R, b \neq 0\}$

Äquivalenzrelation $(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c$

$K := M / \sim$

Äquivalenzklasse zu (a, b) wird mit $[a, b]$ bezeichnet

Schreibe anstelle $[a, b]$ den Bruch $\frac{a}{b}$

$\text{Quot}(R) = K$ ist Quotientenkörper von R .

¹Da b und qa im Ideal sind, ist auch $b - qa = r$ im Ideal

2.2 Algebraische und transzendente Erweiterungen

Sei $K = (K, +, \cdot)$ ein beliebiger Körper und $K[X]$ der Polynomring über X . (Das ist ein euklidischer Ring, also Hauptidealring, also ZPE-Ring.)

Lemma 2.2.1.

Die Einheiten von $K[X]$ sind durch die multiplikative Gruppe K^\times von K gegeben.

Beweis

Sei $f \in K[X]^\times$ Polynom von Grad ≥ 0 . Damit ist auch $f^{-1} \in K[X]^\times$.

Wäre nun $\deg(f) > 0$, so wäre $f^{-1} \notin K[X]$. also ist $\deg(f) = 0$ und f eine Konstante, d.h. $f \in K$. Damit f^{-1} existiert, muß $f \neq 0$ sein. Also ist $f \in K^\times$, woraus $K^\times = K[X]^\times$ folgt. \square

Definition 2.2.2 (Erweiterungskörper).

K sei fixierter Körper. Ein Körper E , der den Körper K umfaßt, heißt Erweiterungskörper oder Erweiterung von K ,

Schreibweise: E/K .

Definition 2.2.3 (algebraisch, transzendent).

Seien $E \supseteq K$ eine Erweiterung und $\alpha \in E$. Falls ein $f \in K[X]$, $f \neq 0$, $f(\alpha) = 0$ existiert, so heißt α algebraisch über K . Falls kein derartiges f existiert, so heißt α transzendent über K .

Beispiel

Es sei K ein Körper und $E \supseteq K$ ein Oberkörper von K , z.B. $K = \mathbb{Q}$ und $E = \mathbb{Q}(\sqrt{2})$. Dann ist $\sqrt{2}$ algebraisch über \mathbb{Q} , z.B. $f(X) = X^2 - 2$.

Mit $K = \mathbb{Q}$ und $E = \mathbb{C}$ erhalten wir zum Beispiel die transzendente Zahl $e = 2.71828\dots$

Proposition 2.2.4.

Sei α algebraisch über K . Dann existiert ein Polynom $p \in K[X]$ mit den folgenden Eigenschaften:

1. p ist normiert, d.h. der höchste Koeffizient ist 1.
2. $p(\alpha) = 0$
3. Ist $f \in K[X]$ mit $\deg f < \deg p$, so gilt $f(\alpha) \neq 0$.
4. Erfüllt $\tilde{p} \in K[X]$ die Eigenschaften 1 bis 3, so gilt $\tilde{p} = p$.

Beweis

Wir betrachten die Menge $M = \{g \in K[X] \mid g(\alpha) = 0\}$, welche sich mit Hilfe des Grades eines Polynoms (partiell) anordnen lässt.

Da $M \neq \emptyset$ und geordnet ist, findet sich ein Polynom $h(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in M$ kleinsten positiven Grades, welches die Eigenschaft $\forall g \in K[X], \deg g < \deg h : g(\alpha) \neq 0$ erfüllt. Nun setzen wir $p(x) = \frac{1}{a_n} h(X) = X^n + \frac{a_{n-1}}{a_n} X^{n-1} + \dots + \frac{a_0}{a_n} \in K[X]$. Dann gilt:

1. p ist normiert und in $K[X]$.
2. Wegen $h \in M$ gilt $p(\alpha) = 0$.
3. Ist $g \in K[X]$ mit $\deg g < \deg p$, dann gilt $g(\alpha) \neq 0$.
4. Sei $\tilde{p} \in K[X]$, sodass 1. bis 3. erfüllt sind. Betrachte nun $\tilde{p} - p \in K[X]$ mit $\deg(\tilde{p} - p) < \deg p$ (wegen der Normiertheit von p und \tilde{p}) und $(\tilde{p} - p)(\alpha) = 0$. Mit 3. gilt dann $\tilde{p} - p = 0$.

□

Bemerkung: Alternativer Beweis

Die Menge $\mathfrak{M} = M$ (definiert wie oben) ist ein Ideal in $K[X]$. Weil $K[X]$ ein Hauptidealring ist, gilt $\mathfrak{M} = (F)$ mit $F \in K[X]$, $F(\alpha) = 0$. F hat minimalen positiven Grad. Durch Normierung von F erhalten wir p .

Definition 2.2.5 (Minimalpolynom).

Sei α algebraisch über K . Dann heißt das nach der Proposition 2.2.4 eindeutig bestimmte Polynom $p \in K[X]$ mit den Eigenschaften 1-3 das Minimalpolynom von α über K .

Proposition 2.2.6.

Seien α algebraisch über K und $p \in K[X]$ das Minimalpolynom von α über K . Dann ist p irreduzibel über K in $K[X]$.

Beweis

Annahme: Wäre p nicht irreduzibel, das heißt reduzibel über K , so existierten Polynome $a, b \in K[X]$ mit $0 < \deg a, \deg b < \deg p$ und $p = a \cdot b$. Wegen $p(\alpha) = 0$ folgt $a(\alpha) \cdot b(\alpha) = 0$, d.h. $a(\alpha) = 0$ oder $b(\alpha) = 0$. Dies widerspricht der Eigenschaft 3. Also muss p irreduzibel sein. □

Bemerkung: Bezeichnung des Minimalpolynoms

Wegen Proposition 2.2.6 schreibt man für das Minimalpolynom von α über K auch $\text{Irr}(\alpha, K) \in K[X]$. Man sagt, α sei algebraisch vom Grad $\deg(\text{Irr}(\alpha, K))$ über K .

Beispiel

Sei $K = \mathbb{Q}$, $R = \mathbb{R} \ni \sqrt{2}$. Dann gilt $\text{Irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$ und $\sqrt{2}$ ist algebraisch vom Grad 2 über \mathbb{Q} .

Proposition 2.2.7.

Seien α algebraisch über K und $p = \text{Irr}(\alpha, K) \in K[X]$ das Minimalpolynom von α über K . Weiter sei $f \in K[X]$ ein Polynom mit $f(\alpha) = 0$, d.h. f erfüllt 2. Dann folgt $p|f$.

Beweis

Wir dividieren f mit Rest durch p , d.h. wir erhalten $f = q \cdot p + r$ mit $q, r \in K[X]$ und $r = 0$ oder $\deg r < \deg p$. Nehmen wir an, es wäre $r \neq 0$, also $\deg r < \deg p$.

Damit erhalten wir $0 = f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha)$, also $r(\alpha) = 0$, wegen $p(\alpha) = 0$. Dies ist jedoch ein Widerspruch zu 3.

Daher gilt $r = 0$, also $f = pq$. Somit folgt $p|f$. \square

Bemerkung

Erfüllt $f \in K[X]$ sowohl 1 also auch 2 in der Proposition 2.2.4 und ist f zudem irreduzibel über K , so zeigt Proposition 2.2.7 die Gleichheit $f = p$.

Satz 2.2.8.

Seien α algebraisch über K und $p = \text{Irr}(\alpha, K)$ das Minimalpolynom von α über K . Dann ist der Ring $K[\alpha]$ ein Körper. Hierbei bezeichnet $K[\alpha]$ den Polynomring $K[X]$, wobei α in X eingesetzt wird.

Beweis

Wir betrachten die Einsetzungsabbildung $\varphi : K[X] \rightarrow K[\alpha]$ mit $f(X) \mapsto f(\alpha)$. Offensichtlich ist φ ein surjektiver Ringhomomorphismus. Es gilt $\ker \varphi = \{g \in K[X] \mid g(\alpha) = 0\} = (p)$.

Der Homomorphiesatz für Ringe liefert die Ringisomorphie $K[X]/(p) \cong K[\alpha]$. Weil p irreduzibel ist, ist (p) ein Primideal im Hauptidealring $K[X]$. Dann ist (p) sogar ein Maximalideal in $K[X]$.

Damit ist $K[X]/(p)$ ein Körper.

$\Rightarrow K[\alpha]$ ist auch ein Körper. \square

Bemerkung

1. Sei $p \in K[X]$ ein irreduzibles, normiertes Polynom.

Dann ist (p) ein Maximalideal und $K[X]/(p) = E$ ist ein Körper.

Jetzt hat p eine Nullstelle in E . Wir wählen einfach $\alpha = X + (p) \in E$.

2. Um $K[\alpha]$ als Körper zu erkennen, ist zu zeigen, dass jedes $0 \neq f(\alpha) \in K[\alpha]$ ein multiplikativ Inverses besitzt. Da $f(\alpha) \neq 0$ gilt, ist f teilerfremd zu p (anderenfalls folgte $p|f$). Da $K[X]$ ein euklidischer Ring ist, existieren $\lambda, \mu \in K[X]$ mit $\lambda f + \mu p = 1 = (f, p)$.

Also gilt $\lambda(\alpha) \cdot f(\alpha) = 1$ durch einsetzen von α . Somit erhalten wir $\lambda(\alpha) = f(\alpha)^{-1}$.

Definition 2.2.9 (einfach algebraische Erweiterung).

Ist α algebraisch über K , so schreiben wir $K[\alpha] = K(\alpha)$ und nennen $K(\alpha)$ eine einfach algebraische Erweiterung von K (erzeugt durch das Element α).

Beispiel

Sei $K \subseteq E \ni \alpha$ algebraisch über K . Dann gilt $K \subseteq K(\alpha) = K[\alpha] \subseteq E$. $K(\alpha)$ ist also der kleinste K umfassende Körper, der α enthält.

Bemerkung

Sei α algebraisch vom Grad n über K . Der Körper $K(\alpha)$ kann als K -Vektorraum betrachtet werden und es gilt $\dim_K K(\alpha) = n$. Als Basis verwenden wir z.B. $\{1, \alpha, \dots, \alpha^{n-1}\}$.

Endliche Erweiterungen

Definition 2.2.10 (endliche Erweiterung, Körpergrad).

Eine Erweiterung E über K heißt endlich über K , falls $\dim_K E < \infty$ gilt.

Wir setzen $[E : K] = \dim_K E$ und nennen dies den (Körper-)Grad von E über K .

Beispiel

Sei α algebraisch über K .

Dann ist $K(\alpha)$ eine endliche Erweiterung über K mit $[K(\alpha) : K] = \deg(\text{Irr}(\alpha, K))$.

Proposition 2.2.11.

Sei E endlich über L und L endlich über K .

Dann ist E endlich über K mit $[E : K] = [E : L] \cdot [L : K]$.

Beweis

Wir wissen, dass E endlich über L ist. Damit ist $\{\alpha_1, \dots, \alpha_n\}$ eine L -Basis von E .

Es gilt also $[E : L] = n < \infty$. Weiterhin sei $\{\beta_1, \dots, \beta_m\}$ eine Basis von L über K , also $[L : K] = m < \infty$.

Nun wollen wir zeigen, dass $\{\alpha_j \cdot \beta_k\}$ mit $j = 1, \dots, n$ und $k = 1, \dots, m$ eine Basis von E über K ist.

1. Erzeugtheit:

Sei $\alpha \in E$ beliebig. Wir zeigen nun, dass α eine K -Linearkombination von $\{\alpha_j \beta_k\}$ ist. Aus $\alpha \in E$ und der Endlichkeit von E/L mit der Basis $\{\alpha_1, \dots, \alpha_n\}$ folgt $\exists a_1, \dots, a_n \in L : \alpha = \sum_{j=1}^n a_j \alpha_j$. Aus $a_j \in L$ folgt analog $\exists b_{j,1}, \dots, b_{j,m} \in K : a_j = \sum_{k=1}^m b_{j,k} \beta_k$.

Durch Einsetzen erhalten wir $\alpha = \sum_{j=1}^n a_j \alpha_j = \sum_{j=1}^n (\sum_{k=1}^m b_{j,k} \beta_k) \alpha_j = \sum_{j=1}^n \sum_{k=1}^m b_{j,k} \alpha_j \beta_k$.

2. Lineare Unabhängigkeit:

Sei $\sum_{j=1}^n \sum_{k=1}^m b_{j,k} (\alpha_j \beta_k) = 0$.

$\Rightarrow \sum_{j=1}^n (\sum_{k=1}^m b_{j,k} \beta_k) \alpha_j = 0$.

$\Rightarrow \sum_{k=1}^m b_{j,k} \beta_k = 0$ für $j = 1, \dots, n$.

$\Rightarrow \beta_{j,k} = 0$ für $k = 1, \dots, m, j = 1, \dots, n$.

□

Definition 2.2.12 (algebraische Erweiterung).

Eine Erweiterung E über K heißt algebraisch über K , falls jedes $\alpha \in E$ algebraisch über K ist.

Proposition 2.2.13.

E/K endlich $\Rightarrow E/K$ ist algebraisch. Die Umkehrung gilt im Allgemeinen nicht.

Beweis

Weil E/K endlich ist, gilt $[E : K] = n < \infty$.

Für beliebiges $\alpha \in E$ ist nun zu zeigen, dass α algebraisch über K ist.

Betrachten wir nun die Elemente $1, \alpha, \alpha^2, \dots, \alpha^n$. Dies sind $n + 1$ Elemente (Vektoren) von E .

Nun ist $\dim_K E = [E : K] = n < n + 1$, wodurch $\{1, \dots, \alpha^n\}$ linear abhängig über K ist.

\Rightarrow Es existieren $a_0, a_1, \dots, a_n \in K$, welche nicht alle 0 sind und $\sum_{k=1}^n a_k \alpha^k = 0$ erfüllen.

$\Rightarrow \exists m \in \mathbb{N}, m \leq n : a_m \neq 0$ und m ist maximal.

$\Rightarrow f(X) = \sum_{k=1}^m a_k \alpha^k \in K[X]$ ist nicht-trivial mit $f(\alpha) = 0$.

Somit ist α algebraisch über K . □

Beispiel

Sei α/K algebraisch. Damit ist $E = K(\alpha)/K$ endlich.

$\Rightarrow E = K(\alpha)/K$ ist algebraisch.

Damit impliziert "einfach algebraisch" auch "algebraisch".

Bemerkung: Bezeichnungsweise

Seien E und K Körper, $E \supseteq K$ und $\alpha_1 \in E$ algebraisch über K .

Dann ist $K(\alpha_1)/K$ einfach algebraisch.

Sei nun $\alpha_2 \in E$ algebraisch über $K(\alpha_1)$. Dann ist $K(\alpha_1)(\alpha_2)$ einfach algebraisch über $K(\alpha_1)$.

Hierfür schreiben wir auch $K(\alpha_1, \alpha_2)$.

Dies kann man natürlich iterieren:

Sei $\alpha_n \in E$ algebraisch über $K(\alpha_1, \dots, \alpha_{n-1})$. Dann ist $K(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)$ algebraisch über $K(\alpha_1, \dots, \alpha_{n-1})$.

Proposition 2.2.14.

Seien E, K Körper mit $E \supseteq K$. Dann gilt:

E/K endlich $\Leftrightarrow \exists \alpha_1, \dots, \alpha_n \in E$ algebraisch über $K : E = K(\alpha_1, \dots, \alpha_n)$.

Beweis

1. " \Leftarrow ":

Seien also $\alpha_1, \dots, \alpha_n \in E$ algebraisch über K und $E = K(\alpha_1, \dots, \alpha_n)$.

Es ist zu zeigen, dass E/K endlich ist.

Weil α_1 algebraisch über K ist, ist $K(\alpha_1)/K$ endlich.

Weiterhin ist α_2 algebraisch über K , also auch über $K(\alpha_1)$. Damit ist auch $K(\alpha_1, \alpha_2)$ endlich über $K(\alpha_1)$.

Somit ist $K(\alpha_1, \alpha_2)/K(\alpha_1)$ endlich und $K(\alpha_1)/K$ endlich. Damit ist auch $K(\alpha_1, \alpha_2)/K$ endlich.

Induktiv folgt nun die Endlichkeit von $E = K(\alpha_1, \dots, \alpha_n)/K$.

2. " \Rightarrow ":

Sei E/K endlich, also $[E : K] = n$. Damit existiert eine Basis $\{\alpha_1, \dots, \alpha_n\} \subseteq E$. Nun sind $\alpha_1, \dots, \alpha_n$ algebraisch über K .

Weiterhin gilt $E = K \cdot \alpha_1 + \dots + K \cdot \alpha_n \subseteq K[\alpha_1, \dots, \alpha_n] = K(\alpha_1, \dots, \alpha_n)$.

Umgekehrt haben wir $\alpha_1, \dots, \alpha_n \in E \Rightarrow K[\alpha_1, \dots, \alpha_n] \subseteq E \Rightarrow K(\alpha_1, \dots, \alpha_n) \subseteq E$.
 $\Rightarrow E = K(\alpha_1, \dots, \alpha_n)$.

□

2.3 Separabilität und Normalität

Sei K als Körper fixiert.

Definition 2.3.1 (Separabilität).

Sei E/K eine endliche Erweiterung.

Dann heißt $\alpha \in E$ separabel über K , falls $\text{Irr}(\alpha, K) \in K[X]$ keine mehrfachen Nullstellen besitzt.

Die endliche Erweiterung E/K heißt separabel über K , falls alle $\alpha \in E$ separabel über K sind.

Falls E/K nicht separabel ist, so heißt E/K inseparabel über K .

Beispiel

$K = \mathbb{Q}(\sqrt{2})$ ist über \mathbb{Q} separabel, denn $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ hat keine mehrfachen Nullstellen.

Satz 2.3.2 (Satz vom primitiven Element).

Sei $\#K = \infty$ und E/K eine endliche Erweiterung.

Falls E/K überdies separabel ist, so existiert ein $\theta \in E$ mit $E = K(\theta)$.

Beweis

Da E/K endlich ist, existieren $\alpha_1, \dots, \alpha_n \in E$ mit $E = K(\alpha_1, \dots, \alpha_n)$. Es genügt, den Fall $n = 2$ mit $\alpha = \alpha_1$ und $\beta = \alpha_2$ zu behandeln, da der Fall $n > 2$ induktiv folgt.

Wir zeigen nun $\exists \theta \in E : K(\alpha, \beta) = K(\theta)$. Man beachte dabei, dass $\alpha, \beta \in E$ separabel über K sind. Seien nun $f(X) = \text{Irr}(\alpha, K) \in K[X]$ und $g(X) = \text{Irr}(\beta, K) \in K[X]$ die Minimalpolynome von α bzw. β . Weiterhin seien $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$ und $\beta_1 = \beta, \beta_2, \dots, \beta_n$ die jeweils paarweise verschiedenen Nullstellen von f bzw. g .

Für $j = 1, \dots, m$ und $k = 2, \dots, n$ betrachte man die linearen Gleichungen der Form

$$\alpha_j + X \cdot \beta_k = \alpha + X \cdot \beta$$

Für jedes $j \in \{1, \dots, m\}$ und $k \in \{2, \dots, n\}$ findet man höchstens endlich viele Lösungen dieser Gleichung.

Weil $\#K = \infty$ gilt, existiert ein $c \in K$ mit $\alpha_j + c\beta_k \neq \alpha + c\beta$ für alle $j = 1, \dots, m$ und $k = 2, \dots, n$. Setzen wir nun $\theta = \alpha + c\beta$. Offensichtlich gilt $K(\theta) \subseteq K(\alpha, \beta)$.

Betrachten wir nun $f(\theta - cX) \in K(\theta)[X]$ und $g(X) \in K[X] \subseteq K(\theta)[X]$. Für diese Polynome gilt $f(\theta - c\beta) = f(\alpha) = 0$ und $g(\beta) = 0$. Damit haben sie β als gemeinsame Nullstelle.

Weiterhin ist β die einzige gemeinsame Nullstelle, denn:

$\alpha_1, \dots, \alpha_n$ sind die einzigen Nullstellen von $f(X)$. Weiterhin gilt (auf Grund der Wahl von c) $\theta - c\beta_k \neq \alpha_j$ für alle $k = 2, \dots, n$ und $j = 1, \dots, m$. Damit kann kein β_k eine Nullstelle von $f(\theta - cX)$ sein.

Daraus folgt $\text{ggT}(f(\theta - cX), g(X)) = X - \beta$. Auf Grund der Existenz des Euklidischen Algorithmus in $K(\theta)[X]$ folgt jedoch hieraus $X - \beta \in K(\theta)[X]$, also $\beta \in K(\theta)$.

Damit erhalten wir $\beta \in K(\theta)$ und schließlich $\alpha = \theta - c\beta \in K(\theta)$ wegen $\theta, \beta \in K(\theta)$. Somit haben wir auch $K(\alpha, \beta) \subseteq K(\theta)$.

$\Rightarrow K(\theta) = K(\alpha, \beta)$. □

Lemma 2.3.3 (Separabilität bei Charakteristik 0).

Besitzt K die Charakteristik 0, so ist jede endliche Erweiterung E/K separabel.

Beweis

Sei $\alpha \in E/K$ mit Minimalpolynom $p(X) = \text{Irr}(\alpha, K) \in K[X]$. Dann ist zu zeigen, dass $p(X)$ nur einfache Nullstellen hat.

Nehmen wir also an, p hätte mindestens eine mehrfache Nullstelle.

$\Rightarrow p(X)$ und $p'(X)$ (die formale Ableitung von p) haben eine gemeinsame Nullstelle.

$\Rightarrow \text{ggT}(p, p') \neq 1$, d.h. $(p, p') \in K[X]$ ist ein Polynom vom Grad größer oder gleich 1. Weiterhin ist (p, p') ein Produkt von irreduziblen Polynomen in $K[X]$.

Weil $(p, p') \neq 1$ gilt, folgt $(p, p') = p$ auf Grund der Irreduzibilität von p . Somit gilt auch $p = (p, p')|p'$, also $p|p'$.

Wenn $p' \neq 0$ gilt, erhalten wir $\deg p \leq \deg p'$ auf Grund der Teilbarkeitsbeziehung und $\deg p' = \deg p - 1 < \deg p$ wegen der Ableitungsregeln. Widerspruch.

Somit erhalten wir $0 = p'(X) = \sum_{j=1}^n (j \cdot a_j) X^{j-1}$ und damit $j \cdot a_j = 0$. Dann folgt jedoch $p(X) = 0$, wegen $\text{char } K = 0$. Auch hier erhalten wir einen Widerspruch. □

Corollar 2.3.4.

Sei E/K endliche Erweiterung und $\text{char } K = 0$.

Dann existiert $\theta \in E : E = K(\theta)$.

Beweis

Kombiniere das vorhergehende Lemma mit dem Satz vom primitiven Element. □

Bemerkung

1. Sei E/K endlich. Dann existieren $\alpha_1, \dots, \alpha_n \in E$ (algebraisch über K) mit $E = K(\alpha_1, \dots, \alpha_n)$.
2. Wenn weiterhin $\text{char } K = 0$ gilt, dann existiert ein $\theta \in E$ mit $E = K(\theta)$ und $[E : K] = n = \deg \text{Irr}(\theta, K)$. Als Basis haben wir $\{1, \theta, \dots, \theta^{n-1}\}$.

Vereinbarung (für diese Vorlesung)

Ab jetzt besitze der Grundkörper K immer die Charakteristik 0, d.h. jede endliche Erweiterung E/K ist jeweils einfach algebraisch, also $E = K(\theta)$.

Definition 2.3.5 (K -Isomorphismus).

Seien E_1/K und E_2/K endliche Erweiterungen. Wir nennen eine Abbildung $\varphi : E_1 \rightarrow E_2$ einen K -Isomorphismus, falls gilt:

1. $\varphi : E_1 \rightarrow E_2$ ist ein Körperisomorphismus.
2. φ lässt K elementweise fest. Wir schreiben $E_1 \xrightarrow{\cong} E_2$.

Bemerkung

Im Folgenden wollen wir versuchen, die folgenden drei Fragen zu beantworten.

1. Seien endliche Erweiterungen E_1/K und E_2/K gegeben. Gibt es dann ein $\varphi : E_1 \xrightarrow{\cong} E_2$?
2. Wenn ja, wie konstruiere ich ein solches φ ?
3. Wie viele solche φ s gibt es überhaupt?

Wir können uns auf Grund von $\text{char}(K) = 0$ auf einfach algebraische Erweiterungen beschränken.

Proposition 2.3.6.

Seien α, β algebraisch über K . Dann sind die einfach algebraischen Erweiterungen $K(\alpha)$ und $K(\beta)$ genau dann K -isomorph, wenn α und β Nullstellen desselben irreduziblen Polynoms sind:

$$K(\alpha) \xrightarrow{\cong} K(\beta) \Leftrightarrow \text{Irr}(\alpha, K) = \text{Irr}(\beta, K)$$

Beweis

1. “ \Leftarrow “

α, β seien Nullstellen ein und desselben irreduziblen Polynoms, d.h. $\text{Irr}(\alpha, K) = \text{Irr}(\beta, K)$.

Dann ist zu zeigen, dass ein $\varphi : K(\alpha) \xrightarrow{\cong} K(\beta)$ existiert.

Erinnerung:

Für $K(\alpha)$ gilt $K(\alpha) = K[\alpha] = \{f(\alpha) \mid f \in K[X]\}$. Analog gilt dies für $K(\beta)$.

Nun definieren wir $\varphi : K[\alpha] \rightarrow K[\beta]$ durch $\sum_{j=0}^n b_j \alpha^j \mapsto \sum_{j=0}^n b_j \beta^j$. Beachte, dass dabei K unter φ elementweise fix bleibt. φ ist auf Grund der offensichtlichen Existenz einer Umkehrabbildung bijektiv. Weiterhin rechnet man leicht nach, dass φ strukturtreu ist.

Damit gilt $K(\alpha) \xrightarrow[\cong]{K} K(\beta)$.

2. “ \Rightarrow “

Annahme:

Es existiert ein $\varphi : K(\alpha) \xrightarrow{\cong} K(\beta)$.

Es ist zu zeigen, dass α und β Nullstellen des selben irreduziblen Polynoms sind.

Wir wissen bereits, dass $K(\alpha) = K[\alpha] \cong K[X]/(\text{Irr}(\alpha, K))$ gilt.

Nach der Annahme gilt $\exists \psi : K[X]/(\text{Irr}(\alpha, K)) \xrightarrow[\cong]{K} K[X]/(\text{Irr}(\beta, K))$.

Aufgrund der Bijektivität von ψ folgt $(\text{Irr}(\alpha, K)) = (\text{Irr}(\beta, K))$. Weil beide Ideale Hauptideale sind, existiert ein $c \in K^\times$ mit $\text{Irr}(\alpha, K) = c \text{Irr}(\beta, K)$. Da $\text{Irr}(\alpha, K)$ und $\text{Irr}(\beta, K)$ normiert sind, folgt $c = 1$ und damit die Gleichheit der Minimalpolynome.

□

Corollar 2.3.7.

Sei E/K eine endliche Erweiterung über dem Körper K der Charakteristik 0. Dann ist die Anzahl von K -Isomorphismen von E gleich dem Körpergrad $[E : K]$.

Beweis

Nach dem Satz vom primitiven Element existiert ein $\theta \in E$ mit $E = K(\theta)$. Nach der vorhergehenden Proposition werden die K -Isomorphismen von $E = K(\theta)$ durch die paarweise verschiedenen Nullstellen von $\text{Irr}(\theta, K)$ parametrisiert. Wir betrachten nun die Zerlegung von $\text{Irr}(\theta, K)$ in Linearfaktoren: $\text{Irr}(\theta, K) = (X - \theta_1)(X - \theta_2) \cdots (X - \theta_n)$ mit $\theta_1 = \theta$.

$$\Rightarrow \varphi_j : E = K(\theta) \xrightarrow[\cong]{K} K(\theta_j) \text{ mit } j = 1, \dots, n.$$

$$\Rightarrow |\{\varphi_j\}| = n = \deg(\text{Irr}(\theta, K)) = [E : K].$$

□

Definition 2.3.8 (normal, zueinander konjugierte Nullstellen).

Sei E/K eine endliche Erweiterung über dem Körper K mit der Charakteristik 0. Nach dem Satz vom primitiven Element kann $E = K(\theta)$ mit $\theta \in E$ angenommen werden. Die endliche Erweiterung $E = K(\theta)$ heißt normal über K , falls alle Nullstellen von $\text{Irr}(\theta, K)$ ebenfalls in E liegen. Die Nullstellen von $\text{Irr}(\theta, K)$ heißen zueinander konjugiert über K .

Beispiel

Es sei $\text{Irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta\sqrt[3]{2})(X - \zeta^2\sqrt[3]{2})$, mit $\zeta = e^{\frac{2\pi i}{3}} \notin \mathbb{Q}(\sqrt[3]{2})$.
 $\Rightarrow \mathbb{Q}(\sqrt[3]{2})$ ist nicht normal.

Bemerkung

Sei $f \in K[X]$ ein beliebiges Polynom und E/K die minimale (und somit endliche) Erweiterung von K , welche alle Nullstellen von f enthält. Wenn $\alpha_1, \dots, \alpha_n$ die Nullstellen von f sind, dann gilt offensichtlich $E = K(\alpha_1, \dots, \alpha_n)$.

Definition 2.3.9 (Zerfällungskörper).

E heißt der Zerfällungskörper von $\text{Irr}(\theta, K)$, falls $E = K(\theta)$ normal über K ist. E heißt auch der Zerfällungskörper von f über K .

Man beachte, dass f in $E[X]$ in Linearfaktoren zerfällt: $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$.

Corollar 2.3.10.

Sei E/K eine normale Erweiterung über einem Körper K der Charakteristik 0, d.h. $E = K(\theta)$.
Dann sind alle K -Isomorphismen auch K -Automorphismen.

Überdies ist die Menge $G = \{\sigma : E \rightarrow E \mid K\text{-Automorphismen}\}$ eine endliche Gruppe mit $[E : K]$ Elementen.

3 Galois-Theorie

3.1 Hauptsatz

Sei K ein Körper der Charakteristik 0 und E/K endlich, d.h. $[E : K] = n < \infty$. Dann ist E/K separabel und nach dem Satz vom primitiven Element existiert ein θ mit $E = K(\theta)$. Es gilt $\deg \text{Irr}(\theta, K) = n$.

Definition 3.1.1 (Galois-Erweiterung).

Sei E/K normal, so ist E eine Galois-Erweiterung von K . Kurz: E ist galois'sch über K .

Weil E/K separabel ist, hat $\text{Irr}(\theta, K)$ paarweise verschiedene Nullstellen $\theta = \theta_1, \theta_2, \dots, \theta_n$. Damit gilt $\text{Irr}(\theta, K) = (X - \theta_1) \cdot \dots \cdot (X - \theta_n)$.

Mit $G = \text{Aut}_K(E)$ gilt $\text{Irr}(\theta, K) = \prod_{\sigma \in G} (X - \sigma(\theta))$.

Die Gruppe G heißt Galois-Gruppe der Galois-Erweiterungen E/K und wird durch $\text{Gal}(E/K)$ bezeichnet.

Bemerkung

Es gilt $|\text{Aut}_K(E)| = \deg \text{Irr}(\theta, K) = [E : K]$.

Alle K -Isomorphismen von E sind automatisch K -Automorphismen.

Lemma 3.1.2 (1).

Sei $E = K(\theta)$ eine Galois-Erweiterung mit Galois-Gruppe $G = \text{Gal}(E/K)$ und $\alpha \in E$.

Dann folgt aus $\forall \sigma \in G : \sigma(\alpha) = \alpha$, dass α ein Element von K ist.

Beweis

Sei $[E : K] = n < \infty$, also $\deg \text{Irr}(\theta, K) = n$ und $\text{Irr}(\theta, K) = (X - \theta_1) \cdot \dots \cdot (X - \theta_n)$.

Wir wissen, dass $1, \theta, \theta^2, \dots, \theta^{n-1}$ eine K -Basis von E ist.

$\Rightarrow \exists a_0, \dots, a_{n-1} \in K : a_0 \cdot 1 + a_1 \cdot \theta_1 + \dots + a_{n-1} \theta_1^{n-1} = \alpha$

Analog existieren derartige Gleichungen für $\theta_2, \dots, \theta_n$ mit den selben Koeffizienten a_0 bis a_{n-1} .

Diese Gleichungen entstehen durch die Anwendung der $\sigma \in \text{Gal}(E/K)$ auf die erste Gleichung.

Damit ergibt sich ein Gleichungssystem mit a_0, \dots, a_{n-1} als Unbekannten.

Die Determinante des Gleichungssystems ist eine Vandermonde-Determinante. Da die θ_j paarweise verschieden sind, ist diese Determinante nicht 0. Die Cramersche Regel gibt uns $a_1 = \dots = a_{n-1} = 0$.

$\Rightarrow \alpha = a_0 \in K$. □

Lemma 3.1.3 (2).

Sei $E = K(\theta)$ eine Galois-Erweiterung von K mit Galois-Gruppe $G = \text{Gal}(E/K)$. Weiter sei $K \subseteq L \subseteq E$ ein Zwischenkörper.

Dann ist E auch eine Galois-Erweiterung von L . Die Galois-Gruppe dieser Erweiterung ist die Gruppe $\text{Gal}(E/L) = \{\sigma \in G = \text{Gal}(E/K) \mid \forall \alpha \in L : \sigma(\alpha) = \alpha\}$. Dies ist eine Untergruppe von G .

Beweis

Man hat $E = K(\theta)$ nach dem Satz vom primitiven Element.

Dann gilt auch $E = K(\theta) \subseteq L(\theta) \subseteq E(\theta) = E$ und damit $E = L(\theta)$.

Da $\text{Irr}(\theta, L)$ ein Teiler von $\text{Irr}(\theta, K)$ ist, E/L normal.

$\Rightarrow E/L$ ist galois'sch, d.h. es existiert $\text{Gal}(E/L)$.

Behauptung: Es gilt $\text{Gal}(E/L) = \{\sigma \in G \mid \forall \alpha \in L : \sigma(\alpha) = \alpha\}$.

Beweis:

1. " \supseteq " $\{\sigma \in G \mid \forall \alpha \in L : \sigma(\alpha) = \alpha\} \subseteq \text{Aut}_L(E) = \text{Gal}(E/L)$.
2. " \subseteq " Sei $\sigma \in \text{Aut}_L(E)$. Dann ist σ eine Abbildung $\sigma : E \rightarrow E$ mit $\forall \alpha \in L : \sigma(\alpha) = \alpha$.
 $\Rightarrow \sigma \in G$ mit $\forall \alpha \in L : \sigma(\alpha) = \alpha$.

□

Satz 3.1.4 (Hauptsatz).

Sei $E = K(\theta)$ eine Galois-Erweiterung von K mit der Galois-Gruppe $G = \text{Gal}(E/K)$. Wir betrachten die Mengen $\mathcal{G} = \{H \mid H \leq G \text{ (Untergruppe)}\}$ und $\mathcal{K} = \{L \mid K \subseteq L \subseteq E \text{ (Zwischenkörper)}\}$. Dann besteht eine Bijektion $\varphi : \mathcal{K} \rightarrow \mathcal{G}$, welche durch $L \mapsto \text{Gal}(E/L) = \{\sigma \in G \mid \forall \alpha \in L : \sigma(\alpha) = \alpha\}$ gegeben ist. (Die letzte Gleichheit gilt durch das Lemma 2).

Beweis

Wir bezeichnen $G^L = \{\sigma \in G \mid \forall \alpha \in L : \sigma(\alpha) = \alpha\}$.

$\Rightarrow \varphi(L) = G^L$

1. Injektivität von φ .

Seien $L_1, L_2 \in \mathcal{K}$ mit $\varphi(L_1) = \varphi(L_2)$. Wir müssen nun $L_1 = L_2$ zeigen.

Beachte zunächst, dass $\varphi(L_1) = \varphi(L_2) \Leftrightarrow G^{L_1} = G^{L_2}$ gilt. Wir zeigen nur $L_2 \subseteq L_1$. Die andere Inklusion folgt dann analog, wodurch wir die Gleichheit erhalten.

Sei jetzt $\alpha \in L_2$. Definitionsgemäß gilt $\forall \sigma \in G^{L_2} = \text{Gal}(E/L_2) : \sigma(\alpha) = \alpha$.

Nun gilt $G^{L_2} = G^{L_1} = \text{Gal}(E/L_1)$.

$\Rightarrow \forall \sigma \in \text{Gal}(E/L_1) : \sigma(\alpha) = \alpha$

Durch Lemma 1 folgt daraus $\alpha \in L_1$ und somit $L_2 \subseteq L_1$. Nach der obigen Überlegung folgt somit $L_1 = L_2$.

2. Surjektivität von φ .

Sei $H \in \mathcal{G}$, d.h. $H \leq G$. Wir suchen nun ein $L \in \mathcal{K}$ mit $\varphi(L) = H$.

Als Kandidat für L wählen wir $L = \{\alpha \in E \mid \forall \sigma \in H : \sigma(\alpha) = \alpha\}$.

Wir überlegen zunächst, dass L wirklich ein Zwischenkörper $K \subseteq L \subseteq E$ ist. Offensichtlich gilt $L \subseteq E$. Weil weiterhin $\forall \sigma \in G, a \in K : \sigma(a) = a$ gilt, folgt $\forall \sigma \in H, a \in K : \sigma(a) = a$, d.h. $K \subseteq L$.

Körpereigenschaft: Seien $\alpha, \beta \in L$, d.h. $\forall \sigma \in H : \sigma(\alpha) = \alpha, \sigma(\beta) = \beta$.

$$\Rightarrow \forall \sigma \in H : \sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta$$

Entsprechendes gilt für die Differenzen, Produkte und Quotienten. Damit ist L ein Körper.

Es bleibt nun noch zu zeigen, dass $H = G^L$ gilt.

Wir erinnern uns zunächst an die Gleichheit $G^L = \text{Gal}(E/L) = \{\sigma \in G \mid \forall \alpha \in L : \sigma(\alpha) = \alpha\}$.

Sei $\sigma \in H$. Nach Konstruktion von L gilt $\forall \alpha \in L : \sigma(\alpha) = \alpha$.

$$\Rightarrow \sigma \in \text{Gal}(E/L) = G^L \Rightarrow H \subseteq G^L.$$

Wir führen nun die Annahme $H \subset G^L$ zu einem Widerspruch. Es gelte $H \subset G^L$, also $|H| < |G^L|$.

Betrachten wir nun $f(X) = \prod_{\sigma \in H} (X - \sigma(\theta)) \in L[X]$ mit $\deg f = |H|$. Insbesondere ist θ eine Nullstelle von f und es gilt $E = L(\theta)$.

Aus den Eigenschaften des Minimalpolynoms folgt $\text{Irr}(\theta, L) \mid f(X)$.

Weiterhin haben wir $\deg(\text{Irr}(\theta, L)) = [E : L] = |\text{Aut}_L(E)| = |\text{Gal}(E/L)| = |G^L|$. $\Rightarrow \deg \text{Irr}(\theta, L) \leq \deg f \Leftrightarrow |G^L| \leq |H|$ Damit erhalten wir einen Widerspruch zu unserer Annahmen und schließlich die Surjektivität von φ

$\Rightarrow \varphi$ ist bijektiv. □

Bemerkung: Ergänzung/Zusatz

Wie immer sei K ein Körper der Charakteristik 0.

Sei E eine endliche Galois-Erweiterung von K mit Galois-Gruppe $G = \text{Gal}(E/K)$.

Weiter sei L mit $K \subseteq L \subseteq E$ ein Zwischenkörper mit der Galois-Gruppe $H = \text{Gal}(E/L)$, d.h. $\varphi(L)$.

Dann besteht die folgende Äquivalenz:

L ist Galois-Erweiterung über K , d.h. L ist normal über K .

\Updownarrow

H ist Normalteiler in G , d.h. $H \trianglelefteq G$.

Außerdem gilt in diesem Fall $\text{Gal}(L/K) = \text{Gal}(E/K) / \text{Gal}(E/L)$.

Beweis

Wie zuvor sei $E = K(\theta)$ und $[E : L] = m < \infty$.

1. " \Rightarrow "

Sei also L/K galois'sch. Wir betrachten die Abbildung $\varphi : \text{Gal}(E/K) \rightarrow \text{Gal}(E/L)$ mit $\varphi(\sigma) = \sigma|_L$. Weil L/K galois'sch ist, ist der K -Isomorphismus $\sigma|_L$ von L auch ein K -Automorphismus von L . Damit ist φ wohldefiniert.

Außerdem ist φ ein Homomorphismus.

$$\text{Es gilt } \ker \varphi = \{\sigma \in G \mid \varphi(\sigma) = \sigma|_L = id_L\} = \text{Gal}(E/L).$$

$$\Rightarrow \text{Gal}(E/L) \trianglelefteq \text{Gal}(E/K)$$

Außerdem ist φ surjektiv:

Sei $\tau \in \text{Gal}(L/K)$: Gesucht ist dann ein $\sigma \in G$ mit $\varphi(\sigma) = \sigma|_L = \tau$.

Dazu sei $\alpha \in E$. Da $E = L(\theta)$ mit $[E : L] = m$ gilt, folgt $\alpha = \sum_{k=0}^{m-1} a_k \theta^k$ mit $a_0, \dots, a_{m-1} \in L$.

Wir definieren nun $\sigma(\alpha) = \sum_{k=0}^{m-1} \tau(a_k) \theta^k \in E$. Man verifiziert, dass das so definierte σ ein K -Automorphismus von E ist. Überdies erhalten wir $\sigma|_L = \tau$. Damit ist φ surjektiv.

Durch den Homomorphiesatz von Gruppen erhält man:

$$\text{Gal}(L/K) \cong \text{Gal}(E/K) / \ker \varphi \cong \text{Gal}(E/K) / \text{Gal}(E/L).$$

2. “ \Leftarrow “

Sei also $H = \text{Gal}(E/K)$ Normalteiler in $G = \text{Gal}(E/K)$. Zu zeigen ist nun, dass L/K galois'sch ist, d.h. L/K ist normal, d.h. jeder K -Isomorphismus von L ist ein K -Automorphismus von L .

Sei σ ein K -Automorphismus von E , also $\sigma \in G = \text{Gal}(E/K)$. Betrachten wir nun den K -Isomorphismus $\sigma|_L : L \rightarrow L' \subseteq E$ (mit $L' \supseteq K$) von L .

Nach dem Hauptsatz der Galois-Theorie entspricht L' der Untergruppe $H' \leq G = \text{Gal}(E/K)$ mit $H' = \text{Gal}(E/L') = \text{Aut}_{L'}(E)$.

Man verifiziert (beachte $L' = \sigma(L) \subseteq E$), dass $H' = \sigma \circ H \circ \sigma^{-1} = H$ aufgrund der Normalteilereigenschaft von H in G gilt.

Also haben wir $H' = H \Rightarrow \text{Aut}_{L'}(E) = \text{Aut}_L(E)$.

Mit dem Lemma 1 erhalten wir $L' \subseteq L$ und umgekehrt $L \subseteq L'$, also $L = L'$.

Fazit: Wenn $\sigma \in \text{Gal}(E/K)$ ist, so ist $\sigma|_L \in \text{Aut}_K(L)$.

Als Letztes überlegen wir uns, dass jeder K -Isomorphismus von L von der Form $\sigma|_L$ mit $\sigma \in G$ ist, d.h. jeder K -Isomorphismus von L ist automatisch auch ein K -Automorphismus. Sei also τ ein K -Isomorphismus von L . Mit $\alpha = \sum_{k=0}^{m-1} a_k \theta^k \mapsto \sigma(\alpha) = \sum_{k=0}^{m-1} \tau(a_k) \theta^k$ zu einem K -Isomorphismus von E fortgesetzt werden, wobei $\sigma|_L = \tau$ gilt.

Weil E/K galois'sch ist, ist $\sigma \in \text{Aut}_K(E) = G = \text{Gal}(E/K)$.

□

4 Auflösbare Polynome

4.1 Einführung

Wir fixieren einen Körper K der Charakteristik 0.

Definition 4.1.1 (Radikal).

Die Nullstellen eines Polynoms $f(X) = X^n - a \in K[X]$ bezeichnen wir mit dem Symbol $\sqrt[n]{a}$ und nennen es ein Radikal.

Bemerkung

Unter dem Symbol $\sqrt[n]{a}$ verstehen wir im Folgenden keine spezifizierte Nullstelle von f .

Definition 4.1.2 (auflösbar).

Ein Polynom $f \in K[X]$ habe in seinem Zerfällungskörper die (nicht notwendigerweise verschiedenen) Nullstellen $\alpha_1, \dots, \alpha_n$. Das Polynom heißt auflösbar über K , falls jedes α_j Element eines Körpers L der Gestalt $L = K(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})$ ist, der durch sukzessive Adjunktion von Radikalen wie folgt entsteht:

$$a_1 \in K, a_2 \in K(\sqrt[n_1]{a_1}), a_3 \in K(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}), \dots, a_r \in K(\sqrt[n_1]{a_1}, \dots, \sqrt[n_{r-1}]{a_{r-1}}).$$

Beispiel

1. Grad 1

$$f(X) = X - a \in K[X]$$

$$\Rightarrow \alpha_1 = a \in K.$$

2. Grad 2

$$f(X) = X^2 + pX + q \in K[X]$$

$$\Rightarrow \alpha_{1/2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \text{ mit } K \subseteq K\left(\sqrt{\frac{p^2}{4} - q}\right) \ni \alpha_{1/2}$$

3. Grad 3

$$f(X) = X^3 + aX^2 + bX + c \in K[X]$$

\leadsto Cardanosche Lösungsformeln.

Auch diese Polynome dritten Grades sind auflösbar:

$$\text{Es sei } f(X) = aX^3 + bX^2 + cX + d \in K[X] \quad (a \neq 0)$$

$$\text{Ist } \alpha \text{ Nullstelle von } f, \text{ so gilt } \alpha^3 + \frac{b}{a}\alpha^2 + \frac{c}{a}\alpha + \frac{d}{a} = 0$$

Mit $\beta = \alpha + \frac{b}{3a} \Leftrightarrow \alpha = \beta - \frac{b}{3a}$ folgt

$$\beta^3 + p\beta + q = 0, \quad (*)$$

wobei $p = -\frac{b^2}{3a^2} + \frac{c}{a}$, $q = \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}$

Ist γ Nullstelle von $X^2 - \beta X - \frac{p}{3}$, d.h. $\gamma^2 - \beta\gamma - \frac{p}{3} = 0 \Leftrightarrow \beta = \gamma - \frac{p}{3\gamma}$, so folgt nach

Einsetzen in (*): $\gamma^3 - \frac{p^3}{27} \cdot \frac{1}{\gamma^3} + q = 0 \Leftrightarrow (\gamma^3)^2 + q(\gamma^3) - \frac{p^3}{27}$

$$\Rightarrow \gamma^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$\Rightarrow \gamma = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad (\text{Cardanosche Lösungsformeln})$$

$$\Rightarrow \alpha \in K \left(\sqrt[2]{\frac{q^2}{4} + \frac{p^3}{27}}, \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \right)$$

4. Grad 4

Wie im Fall 3 existieren hier Lösungsformeln, welche als die Formeln von Cardano bzw. Ferrari bekannt sind.

4.2 Auflösbare Gruppen (Wiederholung)

Erinnerung

Sei G eine endliche Gruppe.

Dann heißt G auflösbar genau dann, wenn eine Normalreihe $G = G_1 \trianglerighteq G_2 \trianglerighteq \dots \trianglerighteq G_r = \{e\}$ mit abelschen Faktoren G_k/G_{k+1} existiert.

Lemma 4.2.1 (1).

Jede Gruppe G der Ordnung p^s mit $s \in \mathbb{N}$ und $p \in \mathbb{P}$ ist auflösbar.

Beweis

Für $s = 0$ ist die Aussage trivial. Daher betrachten wir ab sofort $s > 0$.

Indem wir G via Konjugation auf sich selbst operieren lassen, erkennen wir mit Hilfe der Bahnformel, dass $Z(G) \neq \{e\}$ gilt.

$$\Rightarrow G \trianglerighteq Z(G) = Z_1 \triangleright \{e\}.$$

Betrachten wir nun $G^* = G/Z(G)$. Dies ist auch wieder eine p -Gruppe.

Sei $G^* \neq \{e\}$ und damit $Z(G^*) \neq \{e\}$.

Dann definieren wir die Abbildung $\pi : G \rightarrow G^*$ mit $Z_2 = \pi^{-1}(Z(G^*))$ und $Z(G^*) \trianglelefteq G^* = G/Z_1$.

Man stellt fest, dass $Z_2 \trianglelefteq G$ und $Z_1 \triangleleft Z_2$ gilt. Damit erhält man die Normalreihe $G \trianglerighteq Z_2 \triangleright Z_1 \triangleright \{e\}$.

Diese kann man aufgrund der Endlichkeit von G induktiv erweitern, bis $G = Z_k$ gilt. \square

Lemma 4.2.2 (2).

Das homomorphe Bild einer auflösbaren Gruppe ist auflösbar.

Beweis

Übungsaufgabe (Bonusserie - Aufgabe 3)

\square

Lemma 4.2.3 (3).

Die symmetrische Gruppe S_n ist für $n \geq 5$ nicht auflösbar.

Beweis

In Serie 11, Aufgabe 3c wurde gezeigt, dass die alternatierende Gruppe A_n für $n \geq 5$ einfach ist, d.h. es existiert kein nicht-trivialer Normalteiler in A_n ($n \geq 5$). Wäre S_n auflösbar, so wäre A_n (als einziger Normalteiler von S_n) ebenfalls auflösbar. Wegen der Einfachheit von A_n müsste A_n dann abelsch sein, was jedoch nicht der Fall ist. \square

4.3 Satz von Abel**Definition 4.3.1.**

Sei K ein Körper der Charakteristik 0 und $f \in K[X]$ ein separables Polynom. Dann verstehen wir unter der Galois-Gruppe von f die Galois-Gruppe $G = \text{Gal}(E/K)$ des Zerfällungskörpers E von f .

Konstruktion

Sei $\overline{\mathbb{Q}}$ ein algebraischer Abschluss von \mathbb{Q} . (Dann ist nebenbei $\overline{\mathbb{Q}}$ abzählbar und $\mathbb{C} \setminus \overline{\mathbb{Q}}$ überabzählbar.)

Wir wählen nun $x_1 \in \mathbb{C} \setminus \overline{\mathbb{Q}}$ und betrachten $\overline{\mathbb{Q}}(x_1)$. Dann wählen wir $x_2 \in \mathbb{C} \setminus \overline{\mathbb{Q}}(x_1)$ und betrachten $\overline{\mathbb{Q}}(x_1, x_2)$. Dies setzen wir fort, bis wir x_1, \dots, x_n unabhängige, transzendente Elemente gefunden haben und $E = \overline{\mathbb{Q}}(x_1, \dots, x_n)$ erhalten.

Weiterhin betrachten wir die elementar-symmetrischen Funktionen $\sigma_1 = x_1 + \dots + x_n$ bis $\sigma_n = x_1 \cdot \dots \cdot x_n$ und bilden $K = \overline{\mathbb{Q}}(\sigma_1, \dots, \sigma_n) \subset E$.

Satz 4.3.2 (Hauptsatz).

Das Polynom $f(X) = X^n - \sigma_1 X^{n-1} \pm \dots + (-1)^n \sigma_n \in K[X]$ besitzt den Zerfällungskörper $E = \overline{\mathbb{Q}}(x_1, \dots, x_n)$. Die Galois-Gruppe von f , d.h. $\text{Gal}(E/K)$, ist isomorph zu S_n .

Beweis

Siehe Serie 14, Aufgabe 3. \square

Satz 4.3.3 (2).

Sei $K \subseteq L_1 \subseteq \mathbb{C}$ ein Zwischenkörper, $p \in \mathbb{P}$ und $g(X) = X^p - a \in L_1[X]$.

Dann ist g irreduzibel oder besitzt mindestens eine Nullstelle in L_1 .

Beweis

Beachte zunächst $g(x) = \prod_{j=0}^{p-1} (X - \alpha \xi^j)$ mit $\alpha = \sqrt[p]{a}$ (eine feste p -te Wurzel) und $\xi = e^{\frac{2\pi i}{p}}$.

Entweder ist g irreduzibel über L_1 oder nicht. Sei also g reduzibel über L_1 , d.h. es existiert ein $h \in L_1[X]$ mit $h|g$ und $1 \leq \deg h = m < p$.

$$\Rightarrow h(0) = \pm \alpha^m \xi^k = \pm c \in L_1.$$

$$\Rightarrow c^p = (\alpha^m \xi^k)^p = (\alpha^p)^m (\xi^p)^k = a^m.$$

Man beachte nun $(m, p) = 1 \Rightarrow \exists \lambda, \mu \in \mathbb{Z} : \lambda m + \mu p = 1$.

$$\text{Wir berechnen nun } (c^\lambda a^\mu)^p = (c^p)^\lambda a^{\mu p} = (a^m)^\lambda \cdot a^{\mu p} = a^{\lambda m + \mu p} = a^1 = a.$$

$\Rightarrow L_1 \ni c^\lambda a^\mu$ ist eine Nullstelle von g . □

Satz 4.3.4 (3).

Sei $K = \overline{\mathbb{Q}}(\sigma_1, \dots, \sigma_n)$ und $L = K(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \dots, \sqrt[n_r]{a_r})$ eine normale (!) Körpererweiterung. Dann ist $\text{Gal}(L/K)$ auflösbar.

Beweis

Beachte, dass K alle Einheitswurzeln enthält, da diese bereits in $\overline{\mathbb{Q}}$ liegen.

Als Vorbereitung betrachten wir die Situation $K \subseteq L_1 \subseteq \mathbb{C}$, mit $p \in \mathbb{P}$ und $L_2 = L_1(\sqrt[p]{a})$. Dann ist $\text{Gal}(L_2/L_1)$ zyklisch.

Beweis dieser Behauptung: $\sqrt[p]{a}$ ist eine Nullstelle von $g(X) = X^p - a \in L_1[X]$ (wie im Satz 4.3.3). Mit Hilfe dieses Satzes folgt dann auch, dass $\sqrt[p]{a} \in L_1$ gilt (und damit auch alle anderen Wurzeln in L_1 liegen), oder dass g irreduzibel über L_1 ist. Im ersten Fall erhalten wir $L_2 = L_1$. Dann ist L_2/L_1 galoisch und $\text{Gal}(L_2/L_1)$ trivial, also insbesondere zyklisch. Im zweiten Fall erhalten wir $[L_2 : L_1] = p$ und L_2 enthält alle Nullstellen von g . Damit ist L_2/L_1 normal und es gilt $\text{Gal}(L_2/L_1) \cong \mathbb{Z}/p\mathbb{Z}$. Somit ist $\text{Gal}(L_2/L_1)$ zyklisch.

Nun zum eigentlichen Beweis des Satzes:

O.B.d.A. sei $n_1 = p_1, \dots, n_r = p_r \in \mathbb{P}$, da wir zum Beispiel $\sqrt[p_1]{a} = \sqrt[p_1]{\sqrt[p_1]{a}}$ haben.

Wir definieren $L_0 = K, L_j = L_{j-1}(\sqrt[p_j]{a_j})$ mit $j = 1, \dots, r$ und erhalten $K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_r = L$. Mit der Galoistheorie ergibt sich $\text{Gal}(L/K) = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_r = \{e\}$, wobei $G_j = \text{Gal}(L/L_j)$ mit $j = 1, \dots, r$ gilt.

Betrachten wir nun $L_{j-1} \subseteq L_j \subseteq L$ für $j = 1, \dots, r$.

Die Vorbereitung impliziert, dass L_j/L_{j-1} galoisch ist, wobei $\text{Gal}(L_j/L_{j-1})$ zyklisch ist.

Die Ergänzung zum Hauptsatz der Galoistheorie gibt uns $\text{Gal}(L/L_j) = G_j \trianglelefteq G_{j-1} = G(L/L_{j-1})$ und $\text{Gal}(L_j/L_{j-1}) \cong G_{j-1}/G_j$, wobei beide Faktorgruppen zyklisch, also abelsch sind.

Damit folgt $\text{Gal}(L/K) = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_r = \{e\}$ mit abelschen Faktoren. □

Satz 4.3.5 (4).

Sei $K = \overline{\mathbb{Q}}(\sigma_1, \dots, \sigma_n)$ (wie zuvor), $g \in K[X]$ auflösbar und $\deg g \geq 1$.

Dann ist $\text{Gal}(g)$ auflösbar.

Beweis

Sei F der Zerfällungskörper von g . Zu zeigen ist nun, dass $\text{Gal}(g) = \text{Gal}(F/K)$ auflösbar ist.

Sei L eine Radikalerweiterung von K , welche die Nullstellen von g enthält: $K \subseteq F \subseteq L$. Das Problem dabei ist jedoch, dass L/K im Allgemeinen nicht normal ist. Daher müssen wir nun eine normale Radikalerweiterung M/K mit $K \subseteq F \subseteq L \subseteq M$ konstruieren.

Wir haben $L = K(\sqrt[p_1]{a_1}, \sqrt[p_2]{a_2}, \dots, \sqrt[p_r]{a_r})$.

1. Schritt

Wir wählen eine Interpretation von $\sqrt[p_1]{a_1}$ und bilden $K(\sqrt[p_1]{a_1})$. Bei einer anderen Interpretation erhalten wir $\sqrt[p_1]{a_1^*} = \sqrt[p_1]{s_1} \xi^j$ und damit $K(\sqrt[p_1]{a_1}) = K(\sqrt[p_1]{a_1^*})$.

2. Schritt

Wir wählen $a_2 \in K(\sqrt[p_1]{a_1})$, z.B. $a_2 = \frac{1 - \sqrt[p_1]{a_1}}{1 + \sqrt[p_1]{a_1}} \rightsquigarrow K(\sqrt[p_1]{a_1}, \sqrt[p_2]{a_2})$. Wichtig ist hierbei, dass wir bei einer anderen Interpretation auch eine andere Erweiterung erhalten können.

Daher bilden wir anstelle von $K(\sqrt[p_1]{a_1}, \sqrt[p_2]{a_2})$ die Radikalerweiterung $K(\sqrt[p_1]{a_1}, \sqrt[p_2]{a_2}, \sqrt[p_2]{a_2^*}, \dots)$ mit allen Interpretationen der Wurzeln.

Nun fahren wir so fort und erhalten die Radikalerweiterung M/K mit folgenden Eigenschaften:

- a) $K \subseteq F \subseteq L \subseteq M$
- b) $\alpha \in M \Rightarrow \alpha^* \in M$, wobei α^* aus α durch eine andere Interpretation der auftretenden Radikale hervorgeht.

Zu zeigen ist noch, dass M/K normal ist. Wir schreiben nun $M = K(\sqrt[q_1]{c_1}, \dots, \sqrt[q_s]{c_s})$. Sei weiterhin $P_j(X) = \text{Irr}(\sqrt[q_j]{c_j}, K) \in K[X]$ mit $j = 1, \dots, s$, $h(X) = P_1(X) \cdot \dots \cdot P_s(X) \in K[X]$ und M' der Zerfällungskörper von h über k . Dann ist M'/K per Definition normal.

Wir wollen nun zeigen, dass $M' = M$ gilt.

Die Inklusion $M \subseteq M'$ ist dabei offensichtlich gegeben.

Somit bleibt noch $M \supseteq M'$ zu zeigen. Sei $\alpha \in M'$. Ohne Einschränkung sei α eine Nullstelle eines $P_j(X)$.

$$\Rightarrow \exists \sigma \in \text{Gal}(M'/K) : \alpha = \sigma(\sqrt[q_j]{c_j}) = \sqrt[q_j]{\sigma(c_j)}$$

Somit ist dies lediglich eine andere Interpretation des Radikals $\sqrt[q_j]{c_j}$, also auch in der Erweiterung M enthalten. Also ist die Erweiterung normal.

Jetzt wissen wir durch Satz 4.3.4, dass $\text{Gal}(M/K)$ auflösbar ist. Die Ergänzung zur Galoistheorie ergibt $\text{Gal}(F/K) \cong \text{Gal}(M/F) / \text{Gal}(M/K)$. Mit Lemma 4.2.2 ist auch das homomorphe Bild $\text{Gal}(F/K)$ von $\text{Gal}(M/K)$ auflösbar. Damit haben wir den Satz bewiesen. \square

Satz 4.3.6 (Satz von Abel).

Sei $K = \overline{\mathbb{Q}}(\sigma_1, \dots, \sigma_n)$.

Dann gibt es für $n \geq 5$ Polynome in $K[X]$, die nicht auflösbar sind.

Beweis

Wähle f gemäß Satz 4.3.2, d.h. $f(X) = X^n - \sigma_1 X^{n-1} \pm \dots + (-1)^n \sigma_n = (X - x_1) \cdot \dots \cdot (X - x_n) \in K[X]$ mit Zerfällungskörper $E = \overline{\mathbb{Q}}(x_1, \dots, x_n)$.

Wir haben $\text{Gal}(f) = \text{Gal}(E/K) \cong S_n$. Lemma 4.2.3 zeigt jedoch, dass S_n für $n \geq 5$ nicht auflösbar ist. Durch Satz 4.3.5 folgt nun auch, dass f nicht auflösbar ist. \square

Index

- K -Isomorphismus, 40
- algebraisch, 34
- Bahn, 10
- Bild
 - Ringhomomorphismus, 31
- Charakteristik, 30
- Einheit, 30
- Erweiterung, 34
 - algebraisch, 37
 - einfach algebraisch, 36
 - endlich, 37
 - Grad einer, 37
 - normal, 42
 - separabel, 39
- Erzeugendensystem, 19
- Faktorring, 31
- Faser, 15
- Galois-Theorie, 44
- größter gemeinsamer Teiler, ggT, 32
- Gruppe
 - abelsch
 - p -primärer Bestandteil, 16
 - Basis, 19
 - frei, 19
 - auflösbar, 26
 - einfach, 23
 - endlich erzeugt, 19
 - Fixgruppe, 10
 - Stabilisatoruntergruppe, 10
- Hauptideal, 31
- Homomorphiesatz
 - Ring, 31
- Homomorphismus
 - Ring-, 31
- Ideal, 30
 - Haupt-, 31
 - Maximal-, 32
 - Prim-, 32
- inseparabel, 39
- Integritätsbereich, 29
- Inverses, 30
- irreduzibel, 32
- Isomorphie
 - Normalreihen, 23
- Isomorphiesatz, 8
- Isomorphismus
 - K -Isomorphismus, 40
 - Ring-, 31
- Körper, 31
 - Erweiterungs-, 34
 - Quotienten-, 33
 - Schief-, 31
 - Zerfallungs-, 42
- Kern
 - Ringhomomorphismus, 31
- Kompositionsreihe, 24
- Linksinverses, 30
- Minimalpolynom, 35
- normal, 42
- Normalisator, 8
- Normalreihe, 23
 - Faktor, 23
 - Isomorphie, 23
 - Kompositionsreihe, 24
 - Länge, 23
 - Verfeinerung, 23
- Nullstellen
 - zueinander konjugiert, 42

Nullteiler, 29
nullteilerfrei, 29
Orbit, 10
Produkt
 direkt, 7
Quotientenkorper, 33
Radikal, 48
Rechtsinverses, 30
Ring, 29
 abelsch, kommutativ, 29
 Charakteristik, 30
 Einselement, 29
 euklidisch, 32, 33
 faktoriell, 32
 faktoriell,ZPE-, 32
 Faktoring, 31
 Hauptideal-, 32
 Integritätsbereich, 29
 Nullelement, 29
 Unter-, 30
Ringhomomorphismus, 31
 Bild, 31
 Kern, 31
Ringisomorphismus, 31
Schiefkörper, 31
separabel, 39
Stabilisator, 10
Summe
 direkt, 7
Teilbarkeit, 32
Teiler
 größter gemeinsamer, 32
teilt
 Element, 32
 Ring, 32
Torsionsbestandteil, 21
torsionsfrei, 21
transzendent, 34
unzerlegbar, 32
Verfeinerung, 23
Zentrum, 7