

Algebra I
Vorlesung Wintersemester 97/98

Gisbert Wüstholtz (§1- §3) Oliver Baues (§4-§12)

29. Juni 1998

Inhaltsverzeichnis

I	Einführung	3
1	Die Entstehung der Algebra	3
2	Transformationen und Symmetrien	4
2.1	Affine und euklidische Räume	5
2.2	Die Bewegungsgruppe in der Euklidischen Ebene	7
2.3	Symmetrien	7
II	Gruppentheorie	10
3	Gruppen	10
3.1	Untergruppen	12
3.2	Homomorphismen, Nebenklassen, Aktionen	13
3.3	Normalteiler und Faktorgruppen	17
3.4	Zyklische Gruppen	19
4	Die Sätze von Sylow	20
4.1	Die Klassengleichung einer endlichen Gruppe	20
4.2	Exponenten	21
4.3	p-Sylow Untergruppen	22
5	Normalreihen und der Satz von Jordan-Hölder	23
5.1	Auflösbare und einfache Gruppen	24
5.2	Verfeinerung von Normalreihen	25

6	Endliche erzeugte abelsche Gruppen	27
6.1	Freie abelsche Gruppen	27
6.2	Torsion in endlich erzeugten abelschen Gruppen	28
6.3	Der Hauptsatz	30
III	Ringtheorie	32
7	Ringe	32
7.1	Strukturerhaltende Abbildungen, Unterringe	34
7.2	Ideale und Quotientenringe	34
7.3	Operationen mit Idealen	36
7.4	Ideale in kommutativen Ringen	36
7.5	Der chinesische Restsatz	38
8	Lokalisierung	40
8.1	Abbildungsverhalten von Idealen unter Lokalisierung	42
9	Hauptidealringe und faktorielle Ringe	43
9.1	Faktorielle Ringe	43
9.2	Der grösste gemeinsame Teiler	44
10	Euklidische Ringe	46
10.1	Der euklidische Algorithmus	46
10.2	Polynome in einer Variablen	47
11	Ganze Zahlen in quadratischen Zahlkörpern	50
11.1	Primelemente im Ring der ganzen Gaußschen Zahlen	51
12	Polynomringe	52
12.1	Monome	52
12.2	Elementare Eigenschaften von Polynomen	53

Teil I

Einführung

1 Die Entstehung der Algebra

Das Erbe der Griechen¹

Während mit dem Zerfall des Römischen Reiches in der abendländischen Welt viele der kulturellen Leistungen der Antike in Vergessenheit gerieten, erlebte der islamische Kulturkreis eine zivilisatorische Blüte.

Eine hervorragende Rolle spielte dabei die vom Kalifen al-Ma'mūn (reg. 813-833) gegründete Akademie von Bagdad. Führer der dortigen "Griechischen Schule" war al-Ḥajjāj, der die Elemente des Euklid ins Arabische übersetzte.

Im Gegensatz zu ihm stand al-Kwārizmī, der sich auf indisch-persische Quellen abstützte. Sein Hauptwerk über die Lösung von Gleichungen durch *al-jabr*² und *al-muqabala* war denn auch für ein größeres, nicht rein wissenschaftliches Publikum bestimmt. Während der erste Teil Lösungsmethoden für lineare und quadratische Gleichungen enthielt, ging es im zweiten um die Berechnung von Flächen und Volumen. Der dritte Teil behandelte ausschließlich Erbschaftsfragen. Immerhin gab Kwārizmī die sehr gute Approximation

$$\pi \sim \frac{62832}{20000} = 3.1416$$

an, wobei er sich als Quelle auf einen hinduistischen Astronomen berief.

Kwārizmīs Nachfolger Tabit ben Qurra (836-901) zeigte sich wieder als Anhänger der Griechischen Schule und benutzte die geometrische Anschauung zur Lösung algebraischer Probleme.

Die Renaissance in Italien

Vom 13. Jh. an bildete sich in Europa eine neue Schicht "international" tätiger Händler und Financiers heran. Für ihren Geschäftsverkehr und ihre Buchhaltung waren die althergebrachten römischen Ziffern nicht geeignet. Das arabisch-hinduistische Zahlssystem erwies sich als sehr viel effizienter.

Die Werke Kwārizmī waren in Italien in lateinischer Uebersetzung bekannt. Die Technik des *al-jabr* und *al-muqabala* wurde von einer Reihe italienischer Mathematiker weitergeführt und verfeinert. Zu nennen sind Leonardo da Pisa, genannt Fibonacci und Luca Pacioli, der in seinem 1494 erschienenen Hauptwerk "Summa de arithmetica, geometria, proportioni e proportionalità" das

¹für diesen Abschnitt cf. B.L. van der Waerden: A History of Algebra, Springer oder Science: Dossier Les mathématiciens, janvier 1994.

²*al-jabr* ist der ethymologische Ursprung des Begriffs *Algebra* ! Seine Bedeutung war, zu beiden Seiten einer Gleichung denselben Term hinzuzufügen, um so negative Terme zu eliminieren.

Problem der kubischen und biquadratischen Gleichungen aufwarf.

Auf dem Weg zur modernen Algebra

Von da an zog sich das Problem der Lösung algebraischer Gleichungen wie ein roter Faden durch die Entstehungsgeschichte der Algebra, bis hin zum Beginn der modernen Algebra mit Evariste Galois.

Die kubischen und biquadratischen Fälle wurden noch im 16. Jh. von Nicolò Tartaglia, Gerolamo Cardano und Lodovico Ferrari gelöst.

An dieser Stelle muß auch auf die Leistungen René Descartes (1596-1650) hingewiesen werden, den Erfinder der analytischen Geometrie. In seinem Werk "Discours de la méthode" führte er die noch heute gebräuchliche Schreibweise algebraischer Probleme ein. Seine Vorgänger benutzten zwar schon Bezeichnungen wie a, b, \dots oder x, y, \dots für bekannte oder unbekannte Größen, kamen aber bei der Beschreibung mathematischer Operationen noch nicht ohne Worte aus. So schrieb François Viète (1540-1603) anstelle von $bx^2 + dx = z$ immer noch B in A Quadratum, plus D plano in A , aequari Z solido.

Carl Friedrich Gauss (1777-1855) schließlich zeigte die Lösbarkeit der zyklotomischen Gleichung

$$x^n - 1 = 0$$

durch Radikale. Gauss war es auch, der den sogenannten *Fundamentalsatz der Algebra* fand: Jede algebraische Gleichung hat Lösungen in der Form komplexer Zahlen $a + ib$.

Den ganz großen Schritt nach vorn schaffte aber erst Evariste Galois (1811-1832). Er erkannte, daß die Lösungen algebraischer Gleichungen durch die Symmetrien der Gleichung bestimmt werden können: Heute studiert man die zugehörige *Galoisgruppe*.

Aus den Arbeiten Galois entwickelte sich der abstrakte Gruppenbegriff heraus, dem der erste Teil des vorliegenden Skriptums gewidmet ist.

2 Transformationen und Symmetrien

Der Gruppenbegriff entwickelte sich aus dem Begriff der "Transformationsgruppe". In dieser Form tauchen auch die meisten Gruppen in der Mathematik, Physik, Chemie, Kristallographie, Kunst, Architektur und Musik auf.

Definition 1 Eine Transformation auf einer Menge X ist eine bijektive Abbildung $T : X \rightarrow X$.

Zwei Transformationen S und T können hintereinander ausgeführt werden:

$$\begin{aligned} S \circ T : X &\longrightarrow X \\ x &\longmapsto (S \circ T)(x) = S(T(x)). \end{aligned}$$

Die Identität $I : X \rightarrow X, x \mapsto I(x) = x$ ist eine Transformation. Transformationen können invertiert werden, d.h. zu jeder Transformation T gibt es eine Transformation $T' : X \rightarrow X$ mit $T \circ T' = T' \circ T = I$. Man schreibt T^{-1} für T' .

Definition 2 Eine Menge G von Transformationen auf einer Menge X heißt Transformationsgruppe, falls $I \in G$ und mit T, T_1, T_2 auch T^{-1} sowie $T_1 \circ T_2$ in G liegen.

Beispiele:

- i.) $X = \{1, \dots, n\}, G = \gamma_n$, die Permutationsgruppe von einer Menge mit n Elementen, also die Menge der Bijektionen $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$.
- ii.) $X = \text{Vektorraum } V \text{ über einem Körper } K,$
 $G = GL(V) = \{\phi : V \rightarrow V; \phi \text{ linear und bijektiv}\}.$
- iii.) $X = \mathbb{E} = (V, \langle \cdot, \cdot \rangle) = \text{euklidischer Vektorraum}, G = O(V) = \{\phi : V \rightarrow V; \phi \text{ orthogonal}\}.$ Dabei heißt eine lineare Abbildung $\phi \in GL(V)$ orthogonal, falls für alle $v, w \in V$ gilt $\langle \phi(v), \phi(w) \rangle = \langle v, w \rangle.$

2.1 Affine und euklidische Räume

Sehr häufig treten Transformationsgruppen als Bewegungsgruppen in affinen oder euklidischen Räumen auf. Wir wollen den Begriff eines affinen bzw. euklidischen Raumes kurz präzisieren.

Definition 3 Ein affiner Raum \mathbb{A} besteht aus einem n -dimensionalen reellen Vektorraum V , einer Menge \mathcal{P} und einer Abbildung $v : \mathcal{P} \times \mathcal{P} \rightarrow V$, die je zwei Elementen P, Q aus \mathcal{P} einen Vektor $v(P, Q) \in V$ zuordnet und folgende Eigenschaften besitzt:

- i.) Für alle $P \in \mathcal{P}$ und alle $v \in V$ existiert genau ein $Q \in \mathcal{P}$ mit $v(P, Q) = v$.
- ii.) Für alle $P, Q, R \in \mathcal{P}$ gilt $v(P, R) = v(P, Q) + v(Q, R).$

Für $v(P, Q)$ schreiben wir auch \vec{PQ} . Elemente aus \mathcal{P} nennt man Punkte. Aus ii.) mit $R = Q$ folgt $v(P, Q) = v(P, Q) + v(Q, Q)$ und somit $v(Q, Q) = 0$. Setzt man $R = P$, so erhält man $v(P, Q) = -v(Q, P).$

Beispiel:

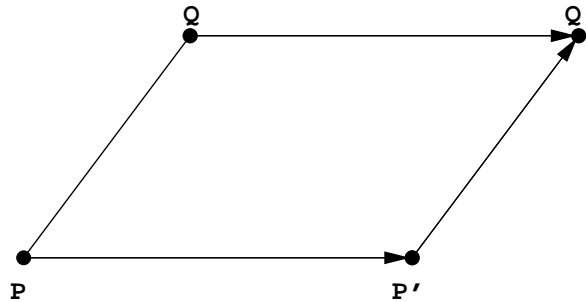
- i.) Wir setzen $\mathcal{P} = V$ und für $v, w \in \mathcal{P}$ $v(v, w) = w - v$. Dann ist $\mathbb{A} = (\mathcal{P}, V, v)$ ein affiner Raum.

- ii.) Wir betrachten den Lösungsraum \mathcal{L} eines inhomogenen linearen Gleichungssystems $Ax = b$. Sei \mathcal{L}_0 der Lösungsraum des zugehörigen homogenen Gleichungssystems $Ax = 0$. Dann ist $(\mathcal{L}, \mathcal{L}_0, v)$ ein affiner Raum, wenn

$$v : \mathcal{L} \times \mathcal{L} \longrightarrow \mathcal{L}_0$$

definiert ist als $v(x, y) = y - x$.

Die Dimension von \mathbb{A} ist definiert als die Dimension von V . In einem affinen Raum gilt das Parallelogrammgesetz, d.h. es gilt für Punkte $P, P', Q, Q' \in \mathcal{P}$ $v(P, Q) = v(P', Q')$ genau dann, wenn $v(P, P') = v(Q, Q')$.



In Zukunft identifizieren wir den affinen Raum \mathbb{A} mit seinen Punkten \mathcal{P} und schreiben $P \in \mathbb{A}$ für $P \in \mathcal{P}$. Ein affiner Unterraum \mathbb{A}' von \mathbb{A} ist eine Teilmenge von \mathbb{A} mit der Eigenschaft, daß die Menge der $v(P, Q)$ mit $P, Q \in \mathbb{A}'$ einen Untervektorraum von V bilden. Affine Unterräume der Dimension 1, 2, n-1 heißen Geraden, Ebenen und Hyperebenen. Zwei affine Unterräume $\mathbb{A}_1, \mathbb{A}_2$ mit zugehörigen Vektorräumen V_1, V_2 heißen parallel, falls $V_1 \subseteq V_2$ oder $V_2 \subseteq V_1$ gilt.

Definition 4 Eine Abbildung $\alpha : \mathbb{A} \longrightarrow \mathbb{A}$ heißt affine Abbildung, falls folgende Bedingungen erfüllt sind:

- i.) $P_1\vec{Q}_1 = P_2\vec{Q}_2 \Rightarrow \alpha(P_1)\vec{\alpha}(Q_1) = \alpha(P_2)\vec{\alpha}(Q_2)$.
- ii.) Die Abbildung $\vec{\alpha} : V \longrightarrow V$ gegeben durch $\vec{\alpha}(P\vec{Q}) = \alpha(P)\vec{\alpha}(Q)$ ist linear.

Eine bijektive affine Abbildung heißt affine Transformation. Die Menge der affinen Transformationen eines affinen Raumes bildet eine Transformationsgruppe.

Ist der Vektorraum V in der Definition eines affinen Raumes sogar ein euklidischer Vektorraum, so erhält man einen euklidischen Raum. Hier ist dann zusätzlich der Abstand $\rho(P, Q)$ von zwei Punkten P und Q erklärt durch

$$\rho(P, Q) = \langle \vec{PQ}, \vec{PQ} \rangle^{\frac{1}{2}}.$$

Ist α eine affine Transformation in einem euklidischen Raum, für die die Abbildung $\vec{\alpha}$ orthogonal ist, so nennt man α eine Bewegung. Die Gesamtheit der Bewegungen ist eine Teilmenge der Transformationsgruppe der affinen Transformationen und selbst Transformationsgruppe.

2.2 Die Bewegungsgruppe in der Euklidischen Ebene

Sei nun \mathbb{E} ein euklidischer Raum, d.h. $\dim \mathbb{E} = 2$. Dann gibt es neben der Identität I noch drei weitere Typen von Bewegungen:

- Translationen
- Drehungen
- Spiegelungen

Translationen haben keine Fixpunkte, Drehungen genau einen und bei Spiegelungen gibt es eine Gerade, die festgehalten wird. Man definiert zum Beispiel die Translationen folgendermaßen. Sei $w \in V$ ein Vektor. Dieser führt in der folgenden Weise zu einer Translation $T_w : \mathbb{E} \rightarrow \mathbb{E}$: Für $P \in \mathbb{E}$ gibt es genau ein $Q \in \mathbb{E}$ mit $\vec{PQ} = w$. Wir setzen $T_w(P) = Q$. Dies definiert eine affine Abbildung und sogar eine Bewegung. Ähnlich geht man bei Spiegelungen und Drehungen vor. Es gilt dann der folgenden Satz:

Satz 2.1 *Jede Bewegung in einer euklidischen Ebene ist entweder eine Translation oder die Hintereinanderschaltung einer Translation und einer Drehung oder Spiegelung.*

Beweis: siehe H. Knörrer, Geometrie.

In ähnlicher Weise kann man die Bewegung des euklidischen Raums beschreiben. Hier setzt sich eine solche Bewegung aus Translationen, Drehungen um eine Achse, Spiegelungen an einer Ebene sowie Punktspiegelungen zusammen.

2.3 Symmetrien

In einer euklidischen Ebene betrachten wir nun ein Dreieck. Die Bewegungen, die das Dreieck fest lassen, bilden die Symmetriegruppe des Dreiecks. Es gibt drei Möglichkeiten für ein Dreieck:

- i.) gleichseitig
- ii.) gleichschenkelig
- iii.) allgemeine Lage, d.h. weder i.) noch ii.)

Im Fall i.) erhält man als Symmetrien die Identität, die Drehung S um den Schwerpunkt um 120° und die Drehung S^2 um 240° . Daneben erhält man die drei Spiegelungen an den drei Winkelhalbierenden, die mit T_1, T_2, T_3 bezeichnet werden. Die Symmetriegruppe ist dann gegeben durch $D_3 = \{I, S, S^2, T, ST, S^2T\}$, wo $T \in \{T_1, T_2, T_3\}$ beliebig. Dies ist eine Diedergruppe. Sie ist in diesem Fall isomorph zur Gruppe γ_3 , die auf den drei Winkelhalbierenden operiert und diese permutiert.

Im Fall ii.) erhält man die zyklische Gruppe $\{I, T\}$, wobei S die Spiegelung an der von den gleichen Schenkeln definierten Winkelhalbierenden ist. Es gilt $\{I, T\} \cong \mathbb{Z}/2\mathbb{Z}$.

Im Fall iii.) ist die Symmetriegruppe die triviale Gruppe.

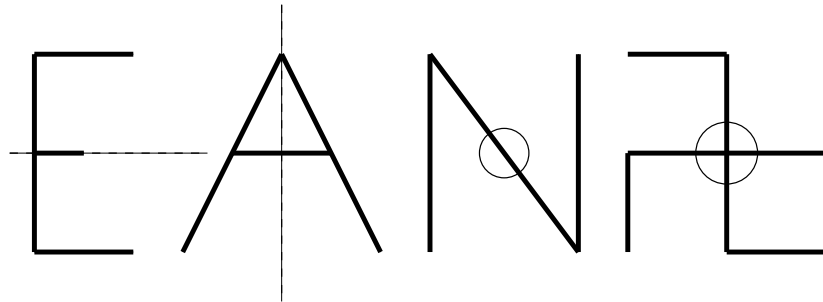
Allgemein können Transformationen, die ein Objekt festhalten, oft als die Menge der Symmetrien dieses Objekts interpretiert werden. Bezeichnet M dieses Objekt, $M \subset X$, und ist G eine Transformationsgruppe von X , so ist die Menge $\gamma(M)$ der Symmetrien von M gegeben durch

$$\gamma(M) = \{T \in G; T(M) = M\}.$$

Es ist klar, daß $I \in \gamma(M)$ und daß mit S, S_1, S_2 auch S^{-1} und $S_1 \circ S_2$ in $\gamma(M)$ liegen. Wir nennen $\gamma(M)$ die Symmetriegruppe von M .

Beispiele:

i.) $X = \mathbb{E} =$ euklidische Ebene

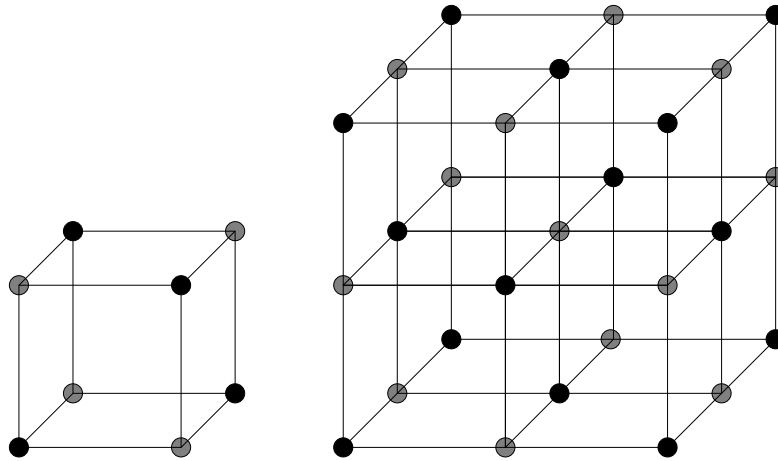


ii.) Symmetriegruppen von regulären Polyedern im euklidischen Raum, insbesondere die

(a) Platonischen Körper:

- Tetraeder
- Würfel
- Oktaeder
- Dodekaeder
- Ikosaeder

- (b) Fullerene: Das sind regelmäßige Polyeder, die in der Kohlenstoffchemie Bedeutung haben.
- (c) Kristalle, z.Bsp. NaCl



Symmetrien:

- Permutationen der Koordinatenachsen
- Spiegelung an den Koordinatenachsen
- Translationen mit Vektoren mit ganzzahligen Koordinaten

Teil II

Gruppentheorie

3 Gruppen

Definition 5 Eine Gruppe ist eine Menge G zusammen mit einer Operation $\circ : G \times G \rightarrow G$, $(g, h) \mapsto g \circ h$ mit

$$(G1) \quad \forall g \in G \forall h \in H \forall k \in G : (g \circ h) \circ k = g \circ (h \circ k),$$

$$(G2) \quad \exists e \in G \forall g \in G : e \circ g = g,$$

$$(G3) \quad \forall g \in G, \exists h \in G : h \circ g = e.$$

Die Gruppe G heißt abelsch oder kommutativ, falls zusätzlich noch gilt

$$(G4) \quad \forall g \in G \forall h \in G : g \circ h = h \circ g.$$

Beispiele:

- i.) $(\mathbb{Z}/n\mathbb{Z}, +)$
- ii.) $((\mathbb{Z}/n\mathbb{Z})^*, +)$
- iii.) $\mu_n = \{x \in \mathbb{C}; x^n = 1\}$
- iv.) γ_n symmetrische Gruppe
- v.) \mathbb{D}_n Diedergruppe
- vi.) V_4 Kleinsche Vierergruppe: $V_4 \cong \mathbb{D}_2$.

Realisierung der Diedergruppe:

S : Drehung um Achse g mit Winkel $2\pi/n$

T_j : Drehung um Achse g_j , $j = 1, \dots, n$, mit Winkel π

Dann gelten folgende Relationen:

$$\begin{aligned} S^n &= 1 \\ T_j^2 &= 1 \\ ST_j &= T_j S^{-1}. \end{aligned}$$

Übungsaufgabe: Gruppentafel für $\mathbb{D}_2, \mathbb{D}_3, \mathbb{D}_4$.

Proposition 3.1 Das Linksinverse ist gleich dem Rechtsinversen.

Beweis: Sei $g \in G$ und h ein Linksinverses von g , d.h. $h \circ g = e$, sowie k ein Linksinverses von h . Dann gilt:

$$\begin{aligned} g \circ h &= (e \circ g) \circ h = ((k \circ h) \circ g) \circ h = (k \circ (h \circ g)) \circ h \\ &= (k \circ e) \circ h = k \circ h = e. \end{aligned}$$

Proposition 3.2 *Jede Linkseins ist Rechtseins, und die Eins ist eindeutig bestimmt.*

Beweis: Sei $g \in G$ und $h \circ g = e$. Dann gilt $(g \circ e) = g \circ (h \circ g) = (g \circ h) \circ g = e \circ g = g$. Sind e, e' Einselemente, so gilt $e = e' \circ e = e \circ e' = e'$.

Proposition 3.3 *Seien $g, h \in G$.*

i.) $gx = h$ und $yg = h$ besitzen eine Lösung.

ii.) Es gilt die Kürzungsregel: $gx = gx' \Rightarrow x = x'$ und $xg = x'g \Rightarrow x = x'$.

Beweis: Multiplikation von links und rechts mit g^{-1} .

Proposition 3.4 i.) $(g^{-1})^{-1} = g$,

ii.) $(gh)^{-1} = h^{-1}g^{-1}$.

Beweis: Übungsaufgabe

Man kann leicht zeigen, daß ein Produkt von n Elementen aus G unabhängig von der Klammerung ist und schreibt dafür $g_1 \circ \dots \circ g_n$. Für $g \in G$ definieren wir

$$g^0 = e, g^1 = g, g^n = g^{n-1} \circ g, \text{ (induktiv)}$$

sowie

$$g^{-1}, g^{-2} = (g^{-1}) \circ (g^{-1}), \dots, g^{-n} = g^{-(n-1)} \circ g.$$

Rechenregeln: $g^r \circ g^s = g^{r+s}$, $(g^r)^s = g^{rs}$.

Definition 6 *Sei $g \in G$. Die Ordnung von g ist die kleinste positive Zahl n mit $g^n = e$. Gibt es keine solche Zahl, so hat g unendliche Ordnung. Wir bezeichnen die Ordnung von g mit $\text{ord } g$.*

Unter der Ordnung einer Gruppe versteht man die Anzahl ihrer Elemente.

Beispiele:

i.) $G = \gamma_4$, Zykel $\sigma = (124)$, $\sigma^2(1) = 4$, $\sigma^2(2) = 1$, $\sigma^2(4) = 2 \Rightarrow \sigma^2 = (142)$, $\sigma^3 = \text{id} \Rightarrow \text{ord } \sigma = 3$

ii.)

$$\begin{aligned} (\mathbb{Z}/30\mathbb{Z})^* &= \text{Menge der Restklassen } \bar{k} \text{ mit } (k, 30) = 1 \\ &= \{1, 7, 11, 13, 17, 19, 23, 29\} \\ |(\mathbb{Z}/30\mathbb{Z})^*| &= \phi(30) = \phi(2 \cdot 3 \cdot 5) = \phi(2) \cdot \phi(3) \cdot \phi(5) \end{aligned}$$

Da $\phi(p) = p - 1$ für Primzahlen p folgt $|(\mathbb{Z}/30\mathbb{Z})^*| = 1 \cdot 2 \cdot 4 = 8$. Weiter haben wir $7, 7^2 \equiv 19, 7^3 \equiv 13, 7^4 \equiv 1$, d.h. $\text{ord } 7 = 4$.

iii.) $S^1 \subset \mathbb{C}, S^1 = \{z \in \mathbb{C}; |z| = 1\}$. Wir definieren die Abbildung

$$D: S^1 \longrightarrow S^1, z \longmapsto e^{\sqrt{2}\pi i} z.$$

Dann gilt $D^n = 1 \Rightarrow e^{n\sqrt{2}\pi i} = 1 \Rightarrow n\sqrt{2} \in 2\mathbb{Z} \Rightarrow \sqrt{2} \in \mathbb{Q}$. Dies ist ein Widerspruch, somit $\text{ord } D = \infty$.

iv.) $A = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \in SO(2)$, d.h. $\alpha^2 + \beta^2 = 1$. Dann gilt $\alpha = \cos \phi, \beta = \sin \phi$ und

$$\text{ord } A = \begin{cases} \infty & \phi \notin 2\pi\mathbb{Q} \\ s & \phi = 2\pi \frac{r}{s}, (r, s) = 1 \end{cases}$$

Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ spielt in der Kryptologie eine wichtige Rolle. Eines der wichtigsten Verfahren ist die RSA-Kodierung, das von Rivest, Shamir und Adlema 1977 entwickelt wurde. Es beruht darauf, daß endliches Exponentieren polynomial in der Zeit ist, endliches Logarithmieren jedoch exponentiell. Man wählt große Primzahlen p, q und setzt $n = p \cdot q$. Dann werden e und f so bestimmt, daß $ef \equiv 1(\phi(n))$ ist. Eine Nachricht $M < p, q$ wird nun kodiert durch $E = M^e \text{ mod } n$, n und e werden veröffentlicht, der Empfänger kennt f und dekodiert durch Exponentieren von $E: E^d \equiv M^{ed} \equiv M^{\phi(n)} \equiv M \text{ mod } n$.

3.1 Untergruppen

Definition 7 Eine nichtleere Teilmenge $H \subseteq G$ ist eine Untergruppe, falls mit $g, h \in H$ auch $gh^{-1} \in H$ ist.

Lemma 3.1 Eine Untergruppe ist eine Gruppe.

Beweis: Sei $h \in H$. Dann gilt $e = hh^{-1} \in H$ und auch $h^{-1} = eh^{-1} \in H$. Mit $g, h \in H$ sind dann auch $gh = g(h^{-1})^{-1} \in H$.

Beispiele:

i.) $n\mathbb{Z} \subseteq \mathbb{Z}$ ist Untergruppe, und jede Untergruppe $H \subseteq \mathbb{Z}$ ist von der Form $H = n\mathbb{Z}$ für ein $n \in \mathbb{Z}$. Denn ist $H \neq 0$, so gibt es ein $n \in \mathbb{Z}$ mit $n > 0$ und minimal, sodaß $n \in H$ gilt. Daher gilt $n\mathbb{Z} \subseteq H \subseteq \mathbb{Z}$. Sei $m \in H$. Dann gilt $m = ln + r$ mit $0 \leq r < n$. Dann liegt aber auch $r \in H$ und somit gilt wegen Minimalität von n , daß $r = 0$, dh. $H \subseteq n\mathbb{Z}$ gilt. Zusammen folgt $H = n\mathbb{Z}$.

- ii.) $\mathcal{A}_n \subseteq \mathcal{S}_n$ alternierende Gruppe; die Elemente, die $\Delta = \prod_{i < j} (X_i - X_j)$ festhalten.
- iii.) G beliebige Gruppe, $g \in G$ fest. Dann ist $\langle g \rangle = \{g^n, n \in \mathbb{Z}\}$ eine Untergruppe.
- iv.) $S \subseteq G$ Teilmenge, $\langle S \rangle = \{s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}; s_j \in S, \epsilon_j \in \{\pm 1\}, n \in \mathbb{N}\}$ ist Untergruppe.
- v.) $H_i \subseteq G, i \in I$ Familie von Untergruppen. Dann ist $\bigcap_{i \in I} H_i$ Untergruppe.
- vi.) $S \subseteq G$ Teilmenge. Dann gilt $\langle S \rangle = \bigcap_{\substack{S \subseteq G \\ H \subseteq G \cup G}} H$.

Offensichtlich gilt $\langle S \rangle \subseteq \bigcap H$, da mit $s_1, \dots, s_n \in S, S \subseteq H$, d.h. $\langle S \rangle \subseteq \bigcap H$. Weil $S \subseteq \langle S \rangle$ gilt und $\langle S \rangle$ Untergruppe ist, folgt $\langle S \rangle \supseteq \bigcap H$. Zusammen somit $\langle S \rangle = \bigcap H$.
 Man nennt $\langle S \rangle$ die von S erzeugte Untergruppe von S .

3.2 Homomorphismen, Nebenklassen, Aktionen

Definition 8 Seien G, G' Gruppen. Eine Abbildung $\phi : G \rightarrow G'$ heißt Gruppenhomomorphismus, falls für alle $g, h \in G$ gilt:

$$\phi(gh) = \phi(g)\phi(h).$$

Die Menge $\ker \phi = \{g \in G; \phi(g) = e\}$ heißt Kern, die Menge $\text{Im} \phi = \{\phi(g); g \in G\}$ heißt Bild von ϕ .

Proposition 3.5 Sei $\phi : G \rightarrow G'$ ein Gruppenhomomorphismus.

- i.) $\ker \phi, \text{Im} \phi$ sind Untergruppen.
- ii.) Die Abbildung ϕ ist genau dann injektiv, wenn $\ker \phi = 0$.

Beweis: (i) trivial, (ii) folgt wegen $\phi(x) = \phi(y) \iff \phi(x-y) = 0 \iff x-y \in \ker \phi$.

Definition 9 Eine Aktion einer Gruppe H auf M ist ein Homomorphismus $\rho : H \rightarrow \gamma(M)$.

Ist ρ eine Aktion von H auf M , so erhält man eine Abbildung

$$\begin{aligned} H \times M &\longrightarrow M \\ (g, m) &\longmapsto \rho(g)(m). \end{aligned}$$

Man nennt dies auch eine Operation von H auf M und schreibt kurz $g.m$ anstelle von $\rho(g)(m)$. Es gilt

- $g \cdot (h \cdot m) = (gh) \cdot m$
- $e \cdot m = m$

für alle $g, h \in H$.

Beispiele für Operationen

- i.) Die triviale Operation ist definiert via $\rho(g) = id$ für alle $g \in H$, d.h.

$$g \cdot m = \rho(g)(m) = id(m) = m$$

für alle $g \in H$ und alle $m \in M$.

- ii.) Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe. Wir erhalten eine Aktion $ad : H \rightarrow Aut(G) \subseteq \gamma(G)$ durch

$$ad(h)(g) = hgh^{-1}, \quad h \in H, g \in G,$$

denn es gilt für $h, k \in H, g \in G$

$$\begin{aligned} ad(hk)(g) &= hkg(hk)^{-1} = h(kgk^{-1})h^{-1} \\ &= ad(h)(kgk^{-1}) \\ &= ad(h)(ad(k)(g)) \\ &= (ad(h)ad(k))(g) \end{aligned}$$

und somit $ad(hk) = ad(h)ad(k)$, d.h. ad ist ein Homomorphismus.

- iii.) Sei G eine Gruppe, $H \subseteq G$ eine Untergruppe. Die Linksmultiplikation mit Elementen aus H ergibt eine Aktion

$$\begin{aligned} l : H &\rightarrow \gamma(G) \\ h &\mapsto l(h) : g \mapsto hg. \end{aligned}$$

Man beachte, daß das Bild nicht in $Aut(G)$, der Automorphismengruppe von G , liegt.

- iv.) Die Gruppe

$$SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \in \mathbb{R} \text{ ad} - bc = 1 \right\}$$

operiert auf der oberen Halbebene $\mathcal{H} = \{z \in \mathbb{C}; \text{Im}z > 0\}$. Für $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ setzen wir

$$\gamma \cdot z = \frac{az + b}{cz + d}, \quad z \in \mathbb{C}.$$

Es gilt

$$\begin{aligned} \operatorname{Im} \gamma.z &= \operatorname{Im} \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2} = |cz+d|^{-2} \operatorname{Im}((az+b)(c\bar{z}+d)) \\ &= |cz+d|^2 \operatorname{Im} z \end{aligned}$$

Daher gilt $\gamma.z \in \mathcal{H}$ für $z \in \mathcal{H}$ und $SL_2(\mathbb{R})$ operiert auf \mathcal{H} .

Sei $\rho : G \longrightarrow \gamma(M)$ eine Aktion. Man nennt

$$G \cdot m = \{g \cdot m; g \in G\}$$

den *Orbit* oder die *Bahn* von m unter G . Ferner heißt

$$G_m = \{g \in G : g \cdot m = m\}$$

die *Stabilisatoruntergruppe* von m oder kurz der *Stabilisator* von m .

Proposition 3.6 i.) G_m ist eine Untergruppe von G .

ii.) $(G \cdot m) \cap (G \cdot m') \neq \emptyset \iff G \cdot m = G \cdot m'$.

Beweis: (i) ist klar.

Zu (ii): Es gilt $(G \cdot m) \cap (G \cdot m') \neq \emptyset \iff$ es gibt $g, g' \in G : g' \cdot m = g \cdot m' \iff (g^{-1}g') \cdot m = m' \iff G \cdot m = Gg^{-1}g' \cdot m \iff G \cdot m = G(g' \cdot m) \iff G \cdot m = G \cdot m'$.

Wählt man nun eine Menge $S \subset M$ mit $G \cdot s \neq G \cdot s'$ für $s \neq s', s, s' \in S$, so gilt

$$M = \bigcup_{s \in S} G \cdot s$$

und die Vereinigung ist disjunkt.

Beispiele:

- i.) $G = GL(n, K)$ $M = M_{n,n}(K)$ $K = \bar{K}$ Körper, ρ wie in 2), d.h. $\rho = \operatorname{ad}$. Ist \mathcal{J} die Menge der Jordanschen Normalformen, so erhält man nach dem bekannten Satz aus der Linearen Algebra eine disjunkte Zerlegung von M in Konjugationsklassen:

$$M_{n,n}(K) = \bigcup_{s \in \mathcal{J}} GL(n, K).s.$$

- ii.) $G = SL(2, \mathcal{Z}) \subseteq \mathcal{R}$ operiert auf \mathcal{H} . Wir können S in folgender Weise wählen.

eine disjunkte Vereinigung, d.h.

$$(G : K) = (G : H)(H : K).$$

Insbesondere gilt

$$(G : 1) = (G : H)(H : 1).$$

Beweis: Für $g, g' \in \{g_j, j \in J\}, h, h' \in \{h_i, i \in I\}$ folgt aus $Khg = Kh'g'$: $(HKh)g = (HKh')g' \Rightarrow Hg = Hg' \Rightarrow g = g' \Rightarrow Kh = Kh' \Rightarrow h = h'$. Die Vereinigung ist deswegen disjunkt.

3.3 Normalteiler und Faktorgruppen

Definition 10 Eine Untergruppe H einer Gruppe G heißt normal, falls für alle $g \in G$ gilt, daß $gH = Hg$. Normale Untergruppen nennt man auch Normalteiler.

Proposition 3.8 i.) $H \subseteq G$ ist Normalteiler genau dann, wenn $gH \subseteq Hg$ für alle g .

ii.) Der Kern eines Homomorphismus $\phi : G \rightarrow G'$ ist ein Normalteiler.

Beweis: (i): Die Richtung “ \Rightarrow ” ist klar. Umgekehrt: aus $gH \subseteq Hg$ für alle g folgt durch Ersetzen von g durch g^{-1} , daß $g^{-1}H \subseteq Hg^{-1}$ und somit $Hg \subseteq gH$, also $Hg = gH$ gilt.

(ii) Sei $H = \ker \phi$ und e' das neutrale Element von G' . Dann gilt $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e'$ und somit $ghg^{-1} \in H$ für alle $g \in G$, d.h. $gHg^{-1} \subseteq H$ für alle $g \in G$. Daher gilt $gH \subseteq Hg$.

Wir beweisen nun die Umkehrung von (ii) in Proposition 9.1.

Satz 3.9 Sei $H \subseteq G$ normal. Dann gibt es eine Gruppe G' und einen surjektiven Homomorphismus $\pi : G \rightarrow G'$ mit $H = \ker \pi$.

Beweis: Wir setzen $G' = \{gH \mid g \in G\}$ als Menge. Die Multiplikation von zwei Nebenklassen gH und $g'H$ ist wegen

$$(gH)(g'H) = g(Hg')H = g(g'H)H = (gg')H.$$

wieder eine Nebenklasse, d.h. in G' . Die Nebenklasse H ist neutrales Element von G' und die Nebenklasse $g^{-1}H$ invers zu gH . Die Abbildung $\pi : G \rightarrow G'$ ist definiert durch $g \mapsto gH$. Sie ist trivialerweise surjektiv und ein Element h liegt im Kern dieser Abbildung genau dann, wenn $H = hH$ gilt, d.h. h in H liegt.

Wir schreiben $G' = G/H$ und nennen diese Gruppe die Faktorgruppe von G nach der (normalen) Untergruppe H .

Satz 3.10 Die Gruppe G/H besitzt die folgende universelle Eigenschaft: Sei $\phi : G \rightarrow G'$ ein Gruppenhomomorphismus mit $H \subseteq \text{Ker}\phi$ dann existiert genau ein Homomorphismus $\phi_* : G/H \rightarrow G'$, so daß das Diagramm

$$\begin{array}{ccc} & G & \\ \pi \swarrow & & \searrow \phi \\ G/H & \xrightarrow{\phi_*} & G' \end{array}$$

kommutativ ist, d.h. $\phi = \phi_* \circ \pi$ gilt.

Beweis: Wir setzen $\phi_*(gH) := \phi(g)$. Die Abbildung ist wohldefiniert. Gilt nämlich $g'H = gH$, d.h. $g' = gh$ für ein $h \in H$, so folgt $\phi_*(g'H) = \phi(g')$ nach Definition von ϕ_* , dies ist gleich $\phi(gh)$ und wegen der Voraussetzung $H \subseteq \text{Ker}\phi$ weiter gleich $\phi(g) = \phi_*(g)$. Die Eindeutigkeit folgt aus der Kommutativität des Diagramms.

Satz 3.11 (1. Isomorphiesatz)

Sei G eine Gruppe, H eine Untergruppe und $K \subseteq H$ ein Normalteiler von G . Dann ist K Normalteiler von H , und es gilt

$$(G/H)/(G/K) \xrightarrow{\sim} G/H.$$

Beweis: Da K ein Normalteiler von G ist, ist a fortiori K auch ein Normalteiler von H . In dem vorangehenden Satz setzen wir $G' = G/H$. Die Abbildung $\phi : G/K \rightarrow G'$ sei gegeben durch $gK \mapsto gH$. Dann ist $\phi(gK) = 0$ genau dann, wenn $gH = H$, d.h. $g \in H$. Somit ist $\text{Ker}\phi = H/K$. Nach Konstruktion ist ϕ surjektiv und deswegen auch ϕ_* . Wir wissen, daß die Abbildung π surjektiv ist, und daher läßt sich jedes Element aus $\text{Ker}\phi_*$ schreiben als $\pi(\bar{g})$ für ein $\bar{g} \in G/K$. Aufgrund der Kommutativität des Diagramms gilt $\phi(\bar{g}) = \phi_*(\pi(\bar{g})) = 0$ und somit $\bar{g} \in H/K = \text{ker}\pi$. Also ist $\pi(\bar{g}) = 0$, woraus sich die Injektivität von ϕ_* ergibt. Zusammen folgt, daß ϕ_* ein Isomorphismus ist.

Satz 3.12 (2. Isomorphiesatz)

Sei G eine Gruppe, H ein Normalteiler von G und K eine Untergruppe. Dann ist $H \cap K \subseteq K$ normal in K , und es gilt

$$HK/H \xrightarrow{\sim} K/(H \cap K).$$

Beweis: Da H ein Normalteiler von G ist, ist wegen $(HK)(HK) \subseteq H^2K^2 \subseteq HK$ die Menge HK ist eine Untergruppe von G , die H als normale Untergruppe enthält. Weiter ist $H \cap K$ wegen $K(H \cap K) \subseteq KH \subseteq K \subseteq HK \cap K \subseteq (H \cap K)K$ eine normale Untergruppe von K . Wir setzen nun $G' = HK/H$ und definieren $\phi : K \rightarrow G'$ durch $k \mapsto kH \in HK/H$. Dann gilt $k \in \text{Ker}\phi$ genau dann, wenn $k \in H$, also $\text{Ker}\phi = H \cap K$. Weiter ist ϕ surjektiv nach Konstruktion, somit auch die induzierte Abbildung $\phi_* : HK/H \xrightarrow{\sim} K/(H \cap K)$.

Satz 3.13 (3. Isomorphiesatz)

Sei $\phi : G \rightarrow G'$ ein Homomorphismus, $H' \subseteq G'$ eine normale Untergruppe und $H = \phi^{-1}(H')$. Dann ist H ein Normalteiler von G , und es gibt einen kanonischen injektiven Homomorphismus

$$\bar{f} : G/H \rightarrow G'/H'.$$

Ist darüber hinaus ϕ surjektiv, so ist \bar{f} ein Isomorphismus.

Beweis: Die Komposition von ϕ und dem kanonischen Homomorphismus $\pi : G' \rightarrow G'/H'$ hat als Kern die Untergruppe H . Also gibt es eine kanonische Injektion $G/H \hookrightarrow G'/H'$. Diese Abbildung ist offensichtlich surjektiv, wenn ϕ surjektiv ist.

3.4 Zyklische Gruppen

Definition 11 Ein Gruppe G heißt zyklisch, falls es ein $g \in G$ gibt mit $\langle g \rangle = G$. Solch ein Element g nennt man ein erzeugendes Element von G .

Aus der Definition folgt sofort, daß eine Gruppe G zyklisch ist genau dann, wenn es ein g aus G gibt, sodaß der Homomorphismus $\varphi : \mathbb{Z} \rightarrow G$, definiert durch $m \mapsto g^m$, surjektiv ist. Ist die Gruppe G zyklisch und gilt $\ker \varphi = 0$, so nennt man die Gruppe *unendlich zyklisch*. In diesem Fall ist G isomorph zur Gruppe \mathbb{Z} . Gilt jedoch $\ker \varphi \neq 0$ so ist, wie wir gesehen haben, $\ker \varphi = d\mathbb{Z}$ für eine positive ganze Zahl d , die wir die *Ordnung* von g genannt haben. In diesem Fall nennt man die Gruppe eine *endliche zyklische Gruppe*. Ein Element $g \in G$ der Ordnung $\text{ord}(g) = d$ erzeugt g eine zyklische Untergruppe von G der Ordnung d . Ist allgemeiner m eine positive ganze Zahl mit $g^m = 1$, so gilt $m = ds$, und m heißt *Exponent* von g . Ist G eine endliche Gruppe, so nennt man m einen *Exponent* von G , falls $g^m = 1$ für alle $g \in G$.

Satz 3.14 (Satz von Lagrange) Seien G eine endliche Gruppe der Ordnung $\text{ord}(G) > 1$ und $e \neq g \in G$. Dann teilt $\text{ord}(g)$ die Ordnung $\text{ord}(G)$ von G . Ist diese eine Primzahl, so ist die Gruppe G zyklisch und wird von jedem Element $e \neq g \in G$ erzeugt.

Beweis: Sei $H = \langle g \rangle$ die von g erzeugte zyklische Untergruppe von G . Dann gilt aufgrund von Satz 0.1.3

$$G : 1 = (G : H)(H : 1) = (G : H)d$$

und deswegen $d | \text{ord}(G)$. Der zweite Teil des Satzes ist klar.

Satz 3.15 Sei G eine zyklische Gruppe und H eine Untergruppe von G . Dann ist H zyklisch. Ist $\varphi : G \rightarrow G$ ein Homomorphismus, so ist $\varphi(G)$ zyklisch. Insbesondere ist $\varphi(G) = \langle \varphi(g) \rangle$ falls $G = \langle g \rangle$ gilt.

Beweis: Wir haben gesehen, daß eine unendliche zyklische Gruppe isomorph zu \mathbb{Z} ist. Die Untergruppen hiervon haben wir bestimmt. Sie sind von der Gestalt $d\mathbb{Z}$ und somit zyklisch. Ist hingegen $G = \langle g \rangle$ endlich zyklisch und $H \neq 0$, so gibt es ein minimales $d > 0$ mit $g^d \in H$. Ein beliebiges Element von H läßt sich in der Form $h = g^m$ schreiben. Wir stellen nun m in der Form $m = kd + r$ mit $0 \leq r < d$ dar. Aufgrund der Minimalität von d folgt $r = 0$ und somit $h \in \langle g^d \rangle$. Also gilt $H = \langle g^d \rangle$. Der letzte Teil der Aussage ist offensichtlich.

Ein Element g aus einer Gruppe G heißt *primitives Element*, falls die von g erzeugte Untergruppe $\langle g \rangle$ in keiner zyklischen Untergruppe von G echt enthalten ist. Dies ist offensichtlich gleichbedeutend damit daß g eine maximale zyklische Untergruppe erzeugt.

Satz 3.16 Sei $G = \langle g \rangle$ eine endliche zyklische Gruppe. Dann ist $G = \langle g^r \rangle$ für alle $r \neq 0$ mit $(r, \text{ord}(g)) = 1$. Insbesondere ist die Anzahl der verschiedenen Erzeugenden von G gleich dem Wert der Eulerschen φ -Funktion $\varphi(\text{ord}(G))$.

Beweis: Sei m die Ordnung g^r . Dann wird mr durch die Gruppenordnung $d = \text{ord}(G)$ geteilt, d.h. $mr \equiv 0(d)$. Hieraus folgt $m \equiv 0(d)$ wegen $(r, d) = 1$ und somit $m = d$ wegen der Minimalität von m . Der zweite Teil der Behauptung folgt aus der Definition der Eulerschen φ -Funktion.

4 Die Sätze von Sylow

Sei G eine endliche Gruppe und H eine Untergruppe. Nach dem Satz von Lagrange teilt die Ordnung von H die Ordnung von G . Wenn p ein Primteiler von $|G|$ ist, so existiert zu jedem Teiler p^k von $|G|$ eine Untergruppe der Ordnung p^k . Dieses Resultat ist zuerst von L. Sylow (1832-1918) bewiesen worden. Die sogenannten Sylow-Sätze sind ein wichtiges Hilfsmittel, um die Struktur einer gegebenen endlichen Gruppe zu verstehen.

4.1 Die Klassengleichung einer endlichen Gruppe

Sei S eine Menge auf der eine Gruppe G operiert. Zu $s \in S$ heißt

$$Gs = \{g \cdot s \mid g \in G\}$$

die *Bahn* oder der *Orbit* von s unter der Operation von G . Die Gruppe

$$G_s = \{g \in G \mid g \cdot s = s\}$$

heißt der *Stabilisator* von s . Es bezeichne $|Gs|$ die Kardinalität der Bahn Gs . Dann gilt

$$|Gs| = (G : G_s).$$

Beweis Die Abbildung $gG_s \mapsto g \cdot s$ von G/G_s nach Gs ist eine Bijektion. \square

Sei S eine endliche Menge. Dann ist S die disjunkte Vereinigung endlich vieler Orbits, d.h. $S = \bigcup_{i=1}^n Gs_i$ für Elemente $s_i \in S$ und es gilt deswegen die folgende *Orbitzerlegungsformel*

$$|S| = \sum_{i=1}^n (G : Gs_i). \quad (1)$$

Wir betrachten nun die Situation, in der eine Gruppe G auf sich selbst durch *Konjugation* operiert, d.h. $S = G$ und für $x, g \in G$ ist $g \cdot x = \text{Ad}(g)x = gxg^{-1}$.

Definition 4.1 Der Stabilisator $Z_x = \{g \in G \mid gxg^{-1} = x\}$ von $x \in G$ unter der Konjugationsaktion heißt der Zentralisator von $x \in G$. Die Bahn $\text{Ad}(G)x$ heißt die Konjugationsklasse von x . Die Gruppe $Z(G) = \{z \in G \mid gzg^{-1} = z, \forall g \in G\}$ heißt das Zentrum von G .

Bemerkung $Z(G)$ ist ein Normalteiler von G . Es ist $x \in Z(G)$, genau dann wenn $|\text{Ad}(G)x| = 1$.

Ist G eine endliche Gruppe und C ein Repräsentantensystem für die unterschiedlichen Konjugationsklassen von G , dann schreibt sich (1) als die *Klassengleichung*

$$|G| = \sum_{x \in C} (G : Z_x) = |Z(G)| + \sum_{x \in C - Z(G)} (G : Z_x). \quad (2)$$

4.2 Exponenten

G sei eine Gruppe. Eine natürliche Zahl $m \in \mathbf{N}$ heißt *Exponent* für G , falls $\forall g \in G \ g^m = 1$.

Satz 4.2 Die Ordnung $|G|$ einer endlichen Gruppe G ist ein Exponent für G .

Beweis Sei $g \in G$ mit Ordnung $\text{ord}(g)$. Nach dem Satz von Lagrange gilt $\text{ord}(g) \mid |G|$, also $|G| = \text{ord}(g)k$. Dann ist $g^{|G|} = g^{\text{ord}(g)k} = (g^{\text{ord}(g)})^k = 1$. \square

Lemma 4.3 G sei abelsch, endlich und m ein Exponent für G . Dann gilt $|G|$ teilt m^l für ein $l \in \mathbf{N}$.

Beweis Durch Induktion nach der Gruppenordnung. Sei $1 \neq b \in G$ und $H = \langle b \rangle$ die von b erzeugte zyklische Gruppe. m ist Exponent für H und G/H . Für die zyklische Gruppe H gilt: $|H| \mid m$. Mit Induktion gilt für den Quotienten $|G/H| \mid m^{l'}$. Da $|G| = (G : H)|H|$ folgt $|G| \mid m^{l'+1}$. \square

Satz 4.4 G sei abelsch, endlich und p ein Primteiler von $|G|$. Dann gibt es eine Untergruppe H von G mit Ordnung p .

Beweis Aus dem vorhergehenden Lemma folgern wir, daß es ein $x \in G$ gibt mit $p \mid \text{ord}(x)$. (Das Produkt der Ordnungen aller Elemente von G ist ein Exponent für G) Also gilt $\text{ord}(x) = pk$ für ein $k \in \mathbf{N}$. Die zyklische Untergruppe $H = \langle x^k \rangle$ hat Ordnung p . \square

4.3 p-Sylow Untergruppen

p sei eine Primzahl.

Definition 4.5 Eine endliche Gruppe G heißt p -Gruppe, wenn ihre Ordnung eine Potenz von p ist.

Sei G eine endliche Gruppe und $H \subset G$ eine Untergruppe.

Definition 4.6 H heißt eine p -Sylow Untergruppe von G , wenn H eine p -Gruppe ist und $|H|$ die größte Potenz von p ist, die die Ordnung von G teilt.

G sei eine endliche Gruppe. Es gelten die Sylow-Sätze:

Satz 4.7 (Sylow) p sei eine Primzahl, $k \in \mathbf{N}$ und p^k teile $|G|$. Dann besitzt G eine Untergruppe der Ordnung p^k . Insbesondere hat G eine p -Sylow Untergruppe.

Zwei Untergruppen H, H' von G heißen konjugiert in G , wenn es ein $g \in G$ gibt mit $\text{Ad}(g)H = gHg^{-1} = H'$.

Satz 4.8 (Sylow)

- i.) Jede p -Untergruppe von G ist in einer p -Sylow Untergruppe enthalten.
- ii.) Alle p -Sylow Untergruppen von G sind konjugiert zueinander.
- iii.) Die Anzahl der p -Sylow Untergruppen von G teilt die Ordnung von G und ist $\equiv 1 \pmod{p}$.

Beweis von Satz 4.7 (Induktion nach der Ordnung von G)

Falls p die Ordnung $|Z(G)|$ des Zentrums teilt, so folgt nach Lemma 4.4, daß $Z(G)$ eine Untergruppe H der Ordnung p hat. H ist ein Normalteiler in G ; $\pi : G \rightarrow G/H$ sei der Quotientenhomomorphismus. Nun gilt $p^{k-1} \mid |G/H|$ und mit Induktion hat G/H also eine Untergruppe H' der Ordnung p^{k-1} . Sei $L = \pi^{-1}(H')$. Da $\text{Kern } \pi|_L = H$, folgt $|L| = p^k$.

Wir nehmen nun an, daß p nicht die Ordnung des Zentrums teilt. Die Klassengleichung für G lautet

$$|G| = |Z(G)| + \sum_{x \in C - Z(G)} (G : Z_x).$$

Es gibt wenigstens ein $x \in C - Z(G)$, so daß p den Index $(G : Z_x)$ nicht teilt. (Andernfalls wäre p kein Primfaktor von $|G|$) Da $|G| = |Z_x| (G : Z_x)$, muß gelten $p^k \mid |Z_x|$. Mit Induktion folgt, daß Z_x eine Untergruppe der Ordnung p^k hat, also auch G . \square

Die Gruppe G operiert durch Konjugation auf der Menge ihrer Untergruppen: Sei H eine Untergruppe von G , dann $g \cdot H = gHg^{-1}$. Die Bahn $\text{Ad}(G)H = \{gHg^{-1} \mid g \in G\}$ wird auch *Konjugationsklasse* von H genannt. Der Stabilisator von H unter Konjugation ist der *Normalisator* $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$

von H in G .

Beweis von Satz 4.8 Es sei \mathcal{S} die Menge der Sylow Untergruppen von G . G operiert auf \mathcal{S} durch Konjugation: sei $H \in \mathcal{S}$ eine Sylow Untergruppe dann ist auch $g \cdot H = gHg^{-1} \in \mathcal{S}$. Es sei $\mathcal{S}_H = \{gHg^{-1} \mid g \in G\}$ die Konjugationsklasse von $H \in \mathcal{S}$. Die Bahngleichung lautet

$$|G| = |N_G(H)| |\mathcal{S}_H|.$$

Da die Ordnung von $H \subset N_G(H)$ bereits die maximale Potenz von p in $|G|$ ist, ist p kein Teiler von $|\mathcal{S}_H|$. Wir lassen nun eine beliebige p -Untergruppe $L \subset G$ auf der Konjugationsklasse \mathcal{S}_H operieren. \mathcal{S}_H zerfällt in disjunkte L -Orbiten $\mathcal{S}_i = \text{Ad}(L)H_i$ für gewisse $H_i \in \mathcal{S}_H$ und es gilt

$$|\mathcal{S}_H| = \sum_i |\mathcal{S}_i|.$$

Da L eine p -Gruppe ist, ist $|\mathcal{S}_i| = p^{l_i}$. Da $|\mathcal{S}_H|$ keinen Teiler p hat, muß es ein j geben, so daß $|\mathcal{S}_j| = 1$. Das heißt, $L \subset N_G(H_j)$ normalisiert die Sylow Untergruppe H_j . Die Sequenz

$$H_j \hookrightarrow LH_j \rightarrow LH_j/H_j \cong L/(L \cap H_j)$$

zeigt, daß LH_j eine p -Untergruppe von G ist. Aus der Maximalität der Sylow Untergruppe H_j folgt $L \subset H_j$. Wir haben also gezeigt: jede p -Untergruppe L von G liegt in einer Konjugierten von H . Daraus folgen Behauptung 1. und 2. des Satzes.

Zu 3. : Wir haben bewiesen, daß $\mathcal{S} = \mathcal{S}_H$. Wir lassen nun die Sylow Untergruppe H auf \mathcal{S}_H operieren. Die Orbiten $\text{Ad}(H)H'_i$ für Orbitrepräsentanten $H'_i \in \mathcal{S}_H$ haben $p^{l'_i}$ Elemente. Es ist $l'_i = 0$, genau dann, wenn $H \subset N_G(H_i)$. Nach dem Argument von oben ist dies genau dann der Fall, wenn $H = H_i$. Die Orbitzerlegungsformel für die Operation von H auf \mathcal{S} ist deswegen von der Gestalt

$$|\mathcal{S}| = 1 + \sum_i p^{l'_i},$$

wobei $l'_i > 0$. Also gilt 3. . □

5 Normalreihen und der Satz von Jordan-Hölder

Definition 5.1 G sei eine Gruppe. Eine Folge von Untergruppen

$$G = G_0 \supset G_1 \dots \supset G_m = \{1\}$$

heißt Normalreihe von G , wenn G_{i+1} ein Normalteiler in G_i ist. Die Quotientengruppen G_i/G_{i+1} heißen Faktoren der Normalreihe.

5.1 Auflösbare und einfache Gruppen

Eine Gruppe G heißt *auflösbar*, falls G eine Normalreihe besitzt deren Faktoren alle abelsch sind. Eine Gruppe $G \neq \{1\}$ heißt *einfach*, wenn G und $\{1\}$ die einzigen Normalteiler von G sind.

Beispiele für einfache Gruppen sind:

- i.) abelsche Gruppen, deren Ordnung eine Primzahl ist
- ii.) $\text{PSL}(n, \mathbf{R}) = \text{SL}(n, \mathbf{R})/Z(\text{SL}(n, \mathbf{R}))$, $n \geq 2$. Hier bezeichnet $Z(\text{SL}(n, \mathbf{R}))$ das Zentrum von $\text{SL}(n, \mathbf{R})$ und ist die Gruppe der Diagonalmatrizen in $\text{SL}(n, \mathbf{R})$, die alle den gleichen Eintrag auf der Diagonalen haben.
- iii.) die alternierenden Gruppen A_n , $n \geq 5$
- iv.) $\text{PSL}(n, \mathbf{F}_q) = \text{SL}(n, \mathbf{F}_q)/Z(\text{SL}(n, \mathbf{F}_q))$. Hier ist q Potenz einer Primzahl, sowie $n > 2$ oder $n = 2$ und $q > 3$. \mathbf{F}_q ist der Körper mit q Elementen.
- v.) die 26 sporadischen endlichen Gruppen. Hierzu gehören die Mathieu-Gruppen, die Fischer-Gruppen, das Monster und das Baby-Monster.

Wir haben bereits gesehen, daß die Gruppen in 1. keine echten Untergruppen besitzen. Die Gruppen aus 2. sind Beispiele für *kontinuierliche* einfache Gruppen. Ende der Siebziger Jahre dieses Jahrhunderts ist die *Klassifikation der endlichen einfachen Gruppen* abgeschlossen worden. Die Liste dieser Gruppen besteht aus Familien in der Art von 3. und 4. sowie den sogenannten sporadischen einfachen Gruppen wie denen in 5. Wir werden die Mathieu-Gruppe M_{11} (das einfachste Beispiel einer sporadischen einfachen Gruppe) in Übung 8 kennenlernen. Die Einfachheit der Gruppen A_n , $n \geq 5$ werden wir später beweisen.

Definition 5.2 *Eine Sequenz von Gruppen und Homomorphismen*

$$1 \rightarrow H \xrightarrow{i} G \xrightarrow{j} L \rightarrow 1$$

heißt eine kurze exakte Sequenz (von Gruppen), wenn i injektiv ist, j surjektiv und $\text{Kern } j = \text{Bild } i$.

Bemerkung: Es gilt $L \cong G/\text{Kern } j = G/i(H)$. Die Gruppe G wird dann auch eine *Erweiterung von L durch H* genannt.

Beispiele für auflösbare Gruppen sind:

- i.) abelsche Gruppen
- ii.) endliche p -Gruppen
- iii.) $\text{Tr}(n, K) \subset \text{GL}(n, K)$, die Gruppe der oberen Dreiecksmatrizen in $\text{GL}(n, K)$, wobei K ein Körper ist
- iv.) Untergruppen auflösbarer Gruppen

v.) Erweiterungen auflösbarer Gruppen

Die Aussage, daß endliche p -Gruppen auflösbar sind, beweisen wir in Übung 7. Die Beweise von 3. - 5. sind nicht schwierig. Auflösbare Gruppen lassen sich mit Hilfe schrittweiser Erweiterung durch abelsche Gruppen gewinnen.

5.2 Verfeinerung von Normalreihen

Definition 5.3 Zwei Normalreihen $G = G_0 \supset \dots \supset G_r = \{1\}$ und $G = G'_0 \supset \dots \supset G'_s = \{1\}$ heißen isomorph, wenn es eine Bijektion $\sigma : \{0 \dots r\} \rightarrow \{0 \dots s\}$ gibt, so daß die Faktoren G_i/G_{i+1} und $G'_{\sigma(i)}/G'_{\sigma(i)+1}$ isomorph sind.

Definition 5.4 Die Normalreihe $G = G'_0 \supset \dots \supset G'_s = \{1\}$ heißt eine Verfeinerung von $G = G_0 \supset \dots \supset G_r = \{1\}$, falls es für alle $i \in \{1 \dots r\}$ ein $j \in \{1 \dots s\}$ gibt, so daß $G_i = G'_j$

Bemerkung Man erhält jede Verfeinerung der Normalreihe $G = G_0 \supset \dots \supset G_r = \{1\}$ durch Einfügen endlich vieler Gruppen in die Normalreihe.

Satz 5.5 (Schreier) Je zwei Normalreihen der Gruppe G besitzen isomorphe Verfeinerungen.

Eine wichtige Konsequenz aus diesem Resultat ist der folgende Satz von Jordan-Hölder:

Definition 5.6 Eine Normalreihe $G = G_0 \supset \dots \supset G_r = \{1\}$ heißt Kompositionsreihe von G , wenn alle Faktoren der Reihe einfache Gruppen sind.

Satz 5.7 (Jordan-Hölder) Je zwei Kompositionsreihen von G sind zueinander isomorph.

Beweis Es sei $G = G_0 \supset \dots \supset G_r = \{1\}$ eine Kompositionsreihe von G . Dann sind die Faktoren G_i/G_{i+1} einfach. Jeder Normalteiler N von G_i projiziert in einen Normalteiler von G_i/G_{i+1} . Wenn $G_i \supset N \supset G_{i+1}$, so folgt $N = G_i$ oder $N = G_{i+1}$. Dies zeigt, daß bei jeder Verfeinerung einer Kompositionsreihe nur triviale Faktoren hinzukommen. Also sind Kompositionsreihen mit isomorphen Verfeinerungen bereits isomorph. \square

Der Satz von Jordan-Hölder besagt, daß die in einer Kompositionsreihe auftretenden Faktoren und die zugehörigen Multiplizitäten nur von der Gruppe G abhängen und nicht von der Wahl der Kompositionsreihe. Wir zeigen in Übung 7, daß jede endliche Gruppe eine Kompositionsreihe besitzt. Die einfachen endlichen Gruppen lassen sich deswegen als Bausteine auffassen, aus denen man alle endlichen Gruppen durch schrittweise Erweiterung gewinnt.

Für den Beweis von Satz 5.5 benötigen wir ein Lemma:

Lemma 5.8 *Wenn $G = G_0 \supset \dots \supset G_r = \{1\}$ und $G = G'_0 \supset \dots \supset G'_r = \{1\}$ isomorphe Normalreihen sind, so gibt es zu jeder Verfeinerung der zweiten eine zu dieser isomorphe Verfeinerung der ersten.*

Beweis G'_{ij} sei Verfeinerung der zweiten Normalreihe, wobei $G'_{i0} = G'_i$ und $G'_i \supset G'_{ij} \supset G'_{i+1}$. $\sigma : \{1 \dots r\} \rightarrow \{1 \dots r\}$ sei die Bijektion so, daß G_i/G_{i+1} und $G'_{\sigma(i)}/G'_{\sigma(i)+1}$ isomorph sind durch einen Isomorphismus ϕ_i . Dann definiert

$$G_{\sigma(i)j} = \phi_i^{-1}(G'_{ij}/G_{i+1})$$

eine zu G'_{ij} isomorphe Verfeinerung von $G = G_0 \supset \dots \supset G_r = \{1\}$. □

Beweis von Satz 5.5 $G = G_0 \supset \dots \supset G_r = \{1\}$ und $G = G'_0 \supset \dots \supset G'_s = \{1\}$ seien Normalreihen von G . Wir führen, den Beweis durch Induktion nach der Länge s der zweiten Reihe und beginnen mit dem Fall $s=2$. (Für $s=1$ oder $r = 1$ ist die Behauptung des Satzes offensichtlich richtig) Es seien also

(*) $G = G_0 \supset \dots \supset G_r = \{1\}$ und

(**) $G = G'_0 \supset G'_1 \supset G'_2 = \{1\}$

Normalreihen von G . Betrachte $P = G_1G'_1$ und $D = G_1 \cap G'_1$ sowie die Normalreihen

i) $P \supset G_1 \supset D \supset \{1\}$

ii) $P \supset G'_1 \supset D \supset \{1\}$.

Da $P/G_1 \cong G'_1/D$ und $P/G'_1 \cong G_1/D$ sind die Reihen i) und ii) isomorph. Mit Induktion nach r gibt es eine Verfeinerung i)' von i), so daß i)' isomorph zu einer Verfeinerung von

$$P \supset G_1 \supset G_2 \supset \dots \supset G_r$$

ist. Nach dem vorhergehenden Lemma besitzt ii) eine zu i)' isomorphe Verfeinerung ii)'. Nun ist die Reihe i)' isomorph zu einer Verfeinerung von (*) und ii)' eine Verfeinerung von (**). Da i)' und ii)' isomorph sind folgt der Satz für $s = 2$.

Wir führen jetzt den Induktionsschritt für s . Es seien

(*) $G = G_0 \supset \dots \supset G_r = \{1\}$ und

(**) $G = G'_0 \supset \dots \supset G'_s = \{1\}$

Normalreihen von G . Betrachte nun

(***) $G \supset G'_1 \supset \{1\}$.

Nach dem ersten Teil des Beweises ($s = 2$) gibt es isomorphe Verfeinerungen i) und iii) von (*) und (***). Die Reihe iii) sei von der Gestalt

(iii) $G \supset \dots \supset G'_1 \supset \dots \supset \{1\}$.

Die Reststücke $G'_1 \supset \dots \supset \{1\}$ von iii) und $G'_1 \supset \dots \supset G'_s = \{1\}$ von (***) besitzen mit Induktion isomorphe Verfeinerungen. Diese lassen sich ergänzen zu isomorphen Verfeinerungen von iii) und (***). Da i) und iii) isomorph sind, läßt sich nach dem Lemma die Verfeinerung i) von (*) weiter verfeinern, so daß die neue Verfeinerung isomorph ist zu der Verfeinerung von (***). \square

6 Endliche erzeugte abelsche Gruppen

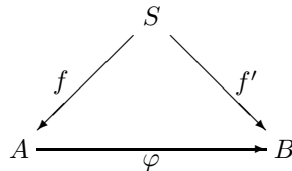
6.1 Freie abelsche Gruppen

Wir benutzen in diesem Abschnitt die additive Notation für abelsche Gruppen. Das heißt wir schreiben $+$ für die Verknüpfung und 0 für das neutrale Element in einer abelschen Gruppe. Für das direkte Produkt $A \times B$ zweier abelscher Gruppen A und B schreiben wir $A \oplus B$.

S sei eine Menge und $f : S \rightarrow A$ sei eine Abbildung von S in eine abelsche Gruppe A .

Definition 6.1 Eine abelsche Gruppe A zusammen mit $f : S \rightarrow A$ heißt freie abelsche Gruppe erzeugt von S , wenn gilt: für alle Abbildungen $f' : S \rightarrow B$ in eine abelsche Gruppe B gibt es eindeutigen Homomorphismus $\varphi : A \rightarrow B$ mit $\varphi \circ f = f'$.

Diagramm:



Bemerkungen

1. Eine freie abelsche Gruppe bezüglich S ist eindeutig bestimmt bis auf Isomorphie. Die Isomorphieklasse hängt nur von der Kardinalität von S ab. Seien hierzu $f : S \rightarrow A$ und $f' : S \rightarrow A'$ frei bezüglich S , dann gibt es eindeutige Homomorphismen $\varphi : A \rightarrow A'$, $\varphi' : A' \rightarrow A$ mit $\varphi \circ f = f'$ und $\varphi' \circ f' = f$. Nun ist $\varphi' \circ \varphi : A \rightarrow A$ ein Homomorphismus mit $(\varphi' \circ \varphi)f = f$. Also folgt $(\varphi' \circ \varphi) = id$. Ebenso folgt $(\varphi \circ \varphi') = id$. Also ist φ ein Isomorphismus.
2. Die Menge $f(S)$ erzeugt A als Gruppe und wir nennen $f(S)$ ein freies erzeugendes System für A , die Elemente von $f(S)$ freie Erzeuger.

Satz 6.2 $\mathbf{Z}^n = \mathbf{Z} \oplus \mathbf{Z} \oplus \dots \oplus \mathbf{Z}$ (n -mal) ist eine freie abelsche Gruppe bezüglich der Menge $S = \{s_1, \dots, s_n\}$ mit n verschiedenen Symbolen s_i .

Beweis Setze $f(s_i) = (0, \dots, 0, 1, 0, \dots, 0)$ (wobei die 1 an der i -ten Stelle steht). Dann bilden die $f(s_i)$ ein freies erzeugendes System (= \mathbf{Z} -Basis) von \mathbf{Z}^n . (Homomorphismen lassen sich auf der Basis eindeutig vorgeben.) \square

Lemma 6.3 *A und A' seien abelsche Gruppen und A' sei frei. $\varphi : A \rightarrow A'$ sei ein surjektiver Homomorphismus mit $B = \text{Kern } \varphi$. Dann gibt es eine Untergruppe $C \subset A$, so daß $A \cong B \oplus C$ und φ induziert einen Isomorphismus $\varphi : C \xrightarrow{\cong} A'$.*

Beweis Sei $\{x'_i\}$ freies Erzeugendes-System von A' . Und $x_i \in A$ mit $\varphi(x_i) = x'_i$. Sei C die von $\{x_i\}$ erzeugte Untergruppe. Dann ist $\varphi : C \rightarrow A'$ ein Isomorphismus, d.h. $C \cap B = \{0\}$. Bleibt zu zeigen, daß die Untergruppen C und B die Gruppe A erzeugen: sei $x \in A$, $\varphi(x) = \sum_{j=1}^n \alpha_j x'_j$. Dann $(x - \sum_{j=1}^n \alpha_j x_j) \in \text{Kern } \varphi = B$, also gilt $x \in B \oplus C$. \square

Satz 6.4 *Sei A eine freie abelsche Gruppe mit n freien Erzeugern, B eine Untergruppe, dann ist B frei mit $m \leq n$ freien Erzeugern. Jede Basis von A hat die gleiche Kardinalität n .*

Beweis Induktion nach Anzahl der Erzeuger von A . $A = \mathbf{Z}x_1 \oplus \dots \oplus \mathbf{Z}x_n$. Betrachte die Projektion $\varphi : A \rightarrow \mathbf{Z}x_1$. Nach dem Lemma gilt $B = \text{Kern } \varphi \oplus C$ und $C \cong \text{Bild } \varphi$, auf jeden Fall aber $\text{Kern } \varphi \subset \mathbf{Z}x_2 \oplus \dots \oplus \mathbf{Z}x_n$. Mit Induktion folgt, daß B frei ist mit $m \leq n$ Erzeugern. Für den Beweis, daß jede Basis von A genau n Elemente hat, betrachte für eine Primzahl p

$$A/pA = \bigoplus_{i=1}^n (\mathbf{Z}/p\mathbf{Z}),$$

wobei n also die Dimension von A/pA über \mathbf{F}_p ist. \square

Definition 6.5 *Die Anzahl der freien Erzeuger von A (= Kardinalität einer Basis) heißt der Rang von A .*

6.2 Torsion in endlich erzeugten abelschen Gruppen

Definition 6.6 *G sei eine Gruppe. $g \in G$ heißt Torsionselement, wenn $\exists n \in \mathbf{N}$ mit $g^n = 1$. Das kleinste n mit dieser Eigenschaft heißt die Periode von g .*

- Im allgemeinen ist die Menge $G_t = \{g \in G \mid g \text{ ist Torsionselement}\}$ keine Untergruppe. Beispiel: $G = \text{SO}(3)$, die Gruppe der eigentlichen orthogonalen Abbildungen von \mathbf{R}^3 . Torsionselemente von G sind genau die Drehungen mit rationalem Winkel $(\frac{m}{l})2\pi$.
- Für abelsche Gruppen gilt mit additiver Schreibweise

$$a \in A_t \Leftrightarrow \exists_{n \in \mathbf{N}} n \cdot a = 0.$$

Lemma 6.7 *A sei abelsch, dann ist A_t eine Untergruppe von A .*

Beweis a habe Periode $m \in \mathbf{N}$ und b Periode $n \in \mathbf{N}$, dann hat $a + b$ das kleinste gemeinsame Vielfache $\text{kgV}(m, n)$ als Periode. \square

Charakterisierung endlich erzeugter freier abelscher Gruppen:

Satz 6.8 *Eine endlich erzeugte abelsche Gruppe, die torsionsfrei ist, ist frei (und von endlichem Rang).*

Beweis Sei A abelsch, torsionsfrei mit endlichem Erzeugendensystem X . X besitzt eine maximale linear unabhängige Teilmenge $\{x_1, \dots, x_n\} \subset X$, d.h. es gilt

$$a_i \in A, \sum a_i x_i = 0 \Rightarrow a_i = 0.$$

Dann ist $B = \langle x_i \rangle$ frei ($\cong \mathbf{Z}^n$) und es gilt

$$\forall y \in X, \exists m \in \mathbf{N} \text{ mit } m \cdot y \in B.$$

Sei \tilde{m} das kgV der endlichen vielen $y \in X - \{x_i\}$. Multiplikation mit \tilde{m} definiert einen injektiven Homomorphismus

$$\varphi_{\tilde{m}} : A \rightarrow B$$

und Bild $\varphi_{\tilde{m}}$ ist frei mit Rang $\leq n$ nach Satz 6.4. Also ist A frei und hat Rang n . \square

Satz 6.9 *Eine endlich erzeugte abelsche Gruppe A zerfällt als direkte Summe*

$$A = A' \oplus A_t$$

wobei A' endlich erzeugt und frei mit endlichem Rang ist. (Der Rang von A' heißt dann auch der Rang von A .) Die Torsionsuntergruppe A_t ist endlich.

Beweis

- i) A/A_t ist torsionsfrei: Sei $x \in A$ ein Repräsentant von $[x] \in A/A_t$. Falls für ein $m \in \mathbf{N}$ $m[x] = 0$, so folgt $\Rightarrow mx \in A_t$. Dann gibt es $l \in \mathbf{N}$ mit $l \cdot (m \cdot x) = 0$, also $x \in A_t$, d.h. $[x] = 0$. Also ist nach Satz 6.2 A/A_t frei. Nach Lemma 6.3 folgt $A = A' \oplus A_t$ und $A' \cong A/A_t$ ist frei.
- ii) A_t ist endlich: A ist Quotient einer freien abelschen Gruppe F_{ab} mit endlich vielen Erzeugern, d.h. es gibt surjektiven Homomorphismus $\varphi : F_{ab} \rightarrow A$. Nach Satz 6.4 ist $\varphi^{-1}(A_t)$ endlich erzeugt, also auch A_t .

\square

6.3 Der Hauptsatz

A sei endlich erzeugte abelsche Torsionsgruppe, d.h. $A = A_t$. Dann ist, wie wir gesehen haben A eine endliche Gruppe. Für eine Primzahl p , ist

$$A(p) = \{a \in A \mid p^k \cdot a = 0, \text{ für ein } k \in \mathbf{N}\}$$

die p -Sylow Untergruppe von A .

Satz 6.10 A ist direkte Summe der Gruppen $A(p)$, wobei p die Primteiler von $|A|$ durchläuft. Es gilt also

$$A \cong \bigoplus_{p \mid |A|} A(p).$$

Beweis (Induktion nach der Anzahl der Primteiler von $|A|$) Wir zeigen zuerst $A = \sum A(p)$, i.e. die Untergruppen $A(p)$ erzeugen A . Sei p ein Primteiler von $|A|$ und $|A| = m \cdot p^k$ mit $(m, p^k) = 1$. Dann gibt es nach Bezout $k, l \in \mathbf{N}$ mit

$$1 = km + lp^k.$$

Es sei

$$A_m = \{a \mid m \cdot a = 0\}$$

Dann gilt für $a \in A$, daß

$$a = (km)a + (lp^k)a$$

Nun ist klarerweise $A(p) \cap A_m = 0$, da $|A(p)|$ und $|A_m|$ teilerfremd sind. Also gilt

$$A \cong A(p) \oplus A_m.$$

Sei p_2 ein weiterer Primteiler von $|A|$, d.h. von m . Da $A(p_2) = A_m(p_2)$ folgt die Behauptung mit Induktion. \square

Wir untersuchen nun die Struktur abelscher p -Gruppen. Es gilt hier:

Satz 6.11

i) Jede abelsche p -Gruppe A ist isomorph zu einer direkten Summe zyklischer Gruppen:

$$A \cong \mathbf{Z}/p^{r_1} \oplus \mathbf{Z}/p^{r_2} \oplus \dots \oplus \mathbf{Z}/p^{r_l}$$

wobei $r_1 \geq r_2 \geq \dots \geq r_l$.

ii) Das Zahlentupel (r_1, \dots, r_l) ist eindeutig bestimmt durch A und heißt der Typ von A .

Beweis

- i) Induktion nach der Potenz m von p . Es sei $|A| = p^m$. Sei $a_1 \in A$ ein Element mit maximaler Periode r_1 und es sei $A_1 = \langle a_1 \rangle$. Wir können die Induktionsvoraussetzung auf den Quotienten A/A_1 anwenden:

$$A/A_1 \cong \mathbf{Z}/p^{r_2}\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/p^{r_l}\mathbf{Z},$$

wobei $\mathbf{Z}/p^{r_i}\mathbf{Z} \cong \langle \bar{a}_i \rangle$, mit $\bar{a}_i \in A/A_1$. Gesucht ist nun ein direkter Summand $A' \subset A$ mit $A' \cong A/A_1$.

Nebenrechnung: Wenn $\bar{a} \in A/A_1$ ein Element der Periode p^r ist, dann gibt es einen Repräsentanten $a \in A$ von \bar{a} mit Periode p^r .

Beweis \tilde{a} sei ein Repräsentant von \bar{a} . Dann gilt $p^r \tilde{a} = na_1 \in A_1$. Wir zerlegen $n = p^k \mu$ mit $(\mu, p) = 1$. Dabei können wir annehmen, daß $k < r_1$. Die Periode von $p^r \tilde{a}$ ist also p^{r_1-k} und die Periode von \tilde{a} ist p^{r+r_1-k} . Da (Maximalität von r_1) $r+r_1-k \leq r_1$ folgt $k \geq r$, denn Periode von $p^r \tilde{a}$ ist $\leq p^{r_1-r}$ und also $r_1-k \leq r_1-r$. Somit also

$$p^r \tilde{a} = p^k \mu a_1 = p^r (\mu' a_1)$$

und es folgt $p^r (\tilde{a} - \mu' a_1) = 0$. Dann ist $a = \tilde{a} - \mu' a_1$ der gesuchte Repräsentant. \square

Sei nun a_i ein Repräsentant der Ordnung p_i^r von \bar{a}_i und $A' = \langle a_2, \dots, a_r \rangle$. Dann gilt

- (a) $A = A_1 + A'$. Denn sei $\varphi : A \rightarrow A/A_1$ die Quotientenabbildung und $a \in A$. Dann ist

$$\varphi(a) = \sum_{i>1} \alpha_i \bar{a}_i \text{ mit } \alpha_i \in \mathbf{N}$$

Also $a = (a - \sum_{i>1} \alpha_i a_i) + \sum_{i>1} \alpha_i a_i \in A_1 + A'$.

- (b) $A_1 \cap A' = \{0\}$. Denn für $\sum_{i=1}^n \alpha_i a_i = 0$ mit $\alpha_i < p^{r_i}$. Da $\alpha_i < p^{r_i}$ folgt für alle $i \geq 2$, daß $\alpha_i = 0$ und deswegen auch für $i = 1$.

- ii) Beweis der Eindeutigkeit mit Induktion: Es seien

$$(r_1, \dots, r_l), (s_1, \dots, s_k)$$

die Typen zweier Summenzerlegungen von A in zyklische Faktoren. Betrachte $pA \subset A$, dann hat pA Summenzerlegungen vom Typ

$$(r_1 - 1, \dots, r_s - 1), (s_1 - 1, \dots, s_k - 1).$$

Nach Induktion gilt also $r_i = s_i > 1$ für $i \leq m$. Und $r_i = 1, s_j = 1$ für die $i, j \geq m$. Da $|A| = |pA|p^{l-m} = |pA|p^{k-m}$ gilt $l = k$. Also stimmen die Typen $(r_1, \dots, r_l), (s_1, \dots, s_k)$ überein.

\square

Teil III

Ringtheorie

Ringe, kommutative Algebra

7 Ringe

Wir führen nun eine weitere algebraische Grundstruktur ein:

Definition 7.1 *Ein Ring ist $(R, +, \cdot)$ ist eine Menge mit zwei Verknüpfungen $+$ und \cdot , so daß*

- i) $(R, +)$ ist eine (additiv geschriebene) abelsche Gruppe.*
- ii) (R, \cdot) ist ein Monoid, d.h.
 - 1. \cdot ist assoziativ*
 - 2. Es gibt ein Einselement $1 \in R$, so daß $\forall_{x \in R} 1 \cdot x = x \cdot 1 = x$**
- iii) Es gelten die Distributivgesetze, d.h. es gilt $\forall_{x, y, z \in R}$
 - 1. $(x + y)z = xz + yz$*
 - 2. $z(x + y) = zx + zy$**

Für Ringe gelten die üblichen Rechenregeln. Zum Beispiel gilt $\forall_{x, y, z \in R}$:

1. $0 \cdot x = x \cdot 0 = 0 \quad \forall_{x \in R}$.
2. $(-x)y = -(xy)$
3. $(-x)(-y) = xy$
4. $(-1) \cdot x = x(-1) = -x$
5. $(\sum_{i=1}^n x_i)(\sum_{j=1}^m y_j) = \sum_{i=1}^n \sum_{j=1}^m x_i y_j$ (allgemeines Distributivgesetz)

Beweis

1. $0 \cdot x = (0 + 0)x = 0 \cdot x + 0 \cdot x$
 $x \cdot 0 = x(0 + 0) = x \cdot 0 + x \cdot 0$
2. $(-x) \cdot y + x \cdot y = (-x + x)y = 0 \cdot y = 0 \Rightarrow (-x) \cdot y = -(xy)$
3. $(-x)(-y) + -(x \cdot y) = (-x)(-y) + (-x) \cdot y = (-x)(-y + y) = 0$
4. folgt aus 3.
5. Übung

□

Definition 7.2 Ein Ring R heißt kommutativ, wenn die Multiplikation kommutativ ist. Ein Element $x \in R$ heißt eine Einheit von R , falls es ein $y \in R$ mit $x \cdot y = y \cdot x = 1$ gibt, dann schreiben wir $y = x^{-1}$.

Wir schreiben R^* für die Menge der Einheiten des Ringes R . (R^*, \cdot) bildet eine Gruppe. Wir zeigen hierzu $x, y \in R^* \Rightarrow x \cdot y \in R^*$. Nach dem Assoziativgesetz folgt

$$\begin{aligned}(x \cdot y)(y^{-1}x^{-1}) &= 1 \\ (y^{-1}x^{-1})(x \cdot y) &= 1\end{aligned}$$

und also $(y^{-1} \cdot x^{-1}) = (x \cdot y)^{-1}$.

Beispiele für Ringe:

- i.) K sei ein Körper, dann ist K ein kommutativer Ring mit $K^* = K - \{0\}$
- ii.) der Ring der ganzen Zahlen, \mathbf{Z} ist kommutativer Ring, $\mathbf{Z}^* = \{+1, -1\}$
- iii.) die Restklassengruppen $\mathbf{Z}/m\mathbf{Z}$ sind ein kommutativer Ring mit Restklassen-Multiplikation:

$$(a + m\mathbf{Z})(b + m\mathbf{Z}) := a \cdot b + m\mathbf{Z}$$

- iv.) V sei abelsche Gruppe. Der Endomorphismen-Ring von V ist die Menge

$$\text{End}(V) = \{\varphi : V \rightarrow V \mid \varphi(a+b) = \varphi(a) + \varphi(b)\}$$

mit Addition und Multiplikation wie folgt:

$$\begin{aligned}(\varphi_1 + \varphi_2)(v) &= \varphi_1(v) + \varphi_2(v) \\ \varphi_1 \cdot \varphi_2 &:= \varphi_1 \circ \varphi_2 \quad (\text{Komposition von Abb.})\end{aligned}$$

- v.) M sei eine Menge, R ein Ring.

$$\text{Abb}(M, R) = \{f : M \rightarrow R\}$$

ist ein Ring mit

$$\begin{aligned}(f + g)(x) &= f(x) + g(x) \\ (f \cdot g)(x) &= f(x) \cdot g(x)\end{aligned}$$

- vi.) R sei ein Ring, dann ist

$$\text{Mat}(n \times n, R) = \{n \times n \text{ Matrizen mit Einträgen in } R\}$$

ein Ring mit

$$\begin{aligned}+ &= \text{Addition von Matrizen} \\ \cdot &= \text{Multiplikation von Matrizen.}\end{aligned}$$

- vii.) Polynomringe, zum Beispiel reelle Polynome in einer Unbestimmten. Für Polynome mit Koeffizienten in einem Körper mit unendlich vielen Elementen lassen sich $+$, \cdot wie in 5. definieren.
- viii.) Funktionen-Ringe in der Analysis, zum Beispiel

$$C^k(U) = \{f : U \rightarrow \mathbf{R} \mid f \text{ ist } k\text{-mal stetig differenzierbar}\}$$

wobei $U \subset \mathbf{R}^n$ eine offene Teilmenge ist.

7.1 Strukturerhaltende Abbildungen, Unterringe

Definition 7.3 $R' \subset R$ heißt ein *Unterring*, wenn gilt

- i.) R' ist additive Untergruppe
- ii.) R' ist abgeschlossen bezüglich der Multiplikation
- iii.) $1 \in R'$.

Definition 7.4 R, R' seien Ringe. Eine Abbildung $\varphi : R \rightarrow R'$ heißt ein *Ringhomomorphismus*, wenn gilt

- i.) φ ist Homomorphismus der abelschen Gruppen $(R, +), (R', +)$
- ii.) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
- iii.) $\varphi(1) = 1$.

$\varphi : R \rightarrow R'$ sei ein Homomorphismus. Das Urbild $\varphi^{-1}(0) \subset R$ heißt dann auch der Kern von φ . Ein Homomorphismus $\varphi : R \rightarrow R$ heißt ein *Isomorphismus*, wenn φ invertierbar ist und φ^{-1} ein Ringhomomorphismus ist. Das Bild $\varphi(R) \subset R'$ eines Homomorphismus' ist ein Unterring.

7.2 Ideale und Quotientenringe

Sei R ein Ring.

Definition 7.5 $I \subset R$ sei eine Untergruppe von $(R, +)$. Dann heißt I

- i) *Links-Ideal*, falls $R \cdot I \subset I$
- ii) *Rechts-Ideal*, falls $I \cdot R \subset I$
- iii) *Zweiseitiges Ideal*, falls i) und ii) gelten

Beispiel: $\varphi : R \rightarrow R'$ sei ein Ringhomomorphismus, dann ist Kern φ ein zweiseitiges Ideal. (Beweis als Übung)

Satz 7.6 $I \subset R$ sei ein zweiseitiges Ideal. Dann ist $R/I = \{r + I \mid r \in R\}$ mit der Addition und Multiplikation von Restklassen ein Ring, so daß die Quotientenabbildung $\pi : R \ni r \mapsto r + I$ ein Ringhomomorphismus ist.

Beweis Die Addition von Restklassen macht R/I zu abelscher Gruppe (das ist bekannt). Wir zeigen, die Multiplikation von Restklassen ist wohldefiniert, d.h. die Definition $(r + I) \cdot (r' + I) := rr' + I$ ist unabhängig von der Wahl der Repräsentanten r, r' . Es gelte also

$$(r + I) = r_1 + I,$$

dann ist

$$\begin{aligned} (r_1 + I) \cdot (r' + I) &= r_1 r' + I \\ &= (r + (r_1 - r))r' + I \\ &= rr' + (r_1 - r)r' + I \end{aligned}$$

Da wegen ii) $(r_1 - r)r' \in I$ folgt

$$= rr' + I.$$

Ebenso folgt die Unabhängigkeit von der Wahl des Repräsentanten r' , dann mit Eigenschaft i). Die Restklassenabbildung π ist mit dieser Definition ein Homomorphismus und die Distributivgesetze folgen. Also ist R/I ein Ring. \square

Satz 7.7 Sei $I \subset R$ ein Ideal, und $\varphi : R \rightarrow R'$ ein Ringhomomorphismus mit Kern $\varphi \supset I$. $\pi : R \rightarrow R/I$ sei der Quotientenhomomorphismus. Dann gibt es eindeutigen Homomorphismus $\bar{\varphi} : R/I \rightarrow R'$ mit $\varphi = \bar{\varphi} \circ \pi$.

Diagramm:

$$\begin{array}{ccc} & R & \\ \pi \swarrow & & \searrow \varphi \\ R/I & \xrightarrow{\bar{\varphi}} & R' \end{array}$$

Beweis Es muß gelten $\bar{\varphi}(r + I) := \varphi(r)$. Da I Untergruppe von $(R, +)$ ist, haben wir bereits gezeigt, daß $\bar{\varphi}$ ein wohldefinierter Homomorphismus von $(R/I, +) \rightarrow (R', +)$ ist. Es bleibt zu zeigen, daß $\bar{\varphi}$ ein Ringhomomorphismus ist. Hierzu verifizieren wir, daß $\forall_{r, r' \in R}$ gilt:

$$\begin{aligned} \text{i.)} \quad \bar{\varphi}((r + I)(r' + I)) &= \bar{\varphi}(rr' + I) = \varphi(r \cdot r') \\ &= \varphi(r) \cdot \varphi(r') = \bar{\varphi}(r + I)\bar{\varphi}(r' + I) \end{aligned}$$

$$\text{ii.)} \quad \bar{\varphi}(1 + I) = \varphi(1) = 1$$

\square

Folgerung: $\varphi : R \rightarrow R'$ sei ein Ringhomomorphismus. Dann induziert φ einen Isomorphismus

$$\bar{\varphi} : R/\text{Kern } \varphi \xrightarrow{\cong} \text{Bild } \varphi.$$

7.3 Operationen mit Idealen

$I, J \subset R$ seien Ideale, dann gilt

- i.) $I \cap J$ ist ein Ideal (Schnitt)
- ii.) $I + J := \{a + b \mid a \in I, b \in J\}$ ist ein Ideal (Summe)
- iii.) $I \cdot J := \{\sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbf{N}_0\}$ ist ein Ideal (Produkt)
- iv.) Für alle Ideale $J_1, J_2 \subset R$ gilt

$$I \cdot (J_1 + J_2) = I \cdot J_1 + I \cdot J_2 \quad (\text{Distributivität})$$

- v.) $I \cdot J \subset I \cap J$

Beweis von 1. – 5. : einfache Übung

7.4 Ideale in kommutativen Ringen

Ab sofort nehmen wir an, daß alle Ringe kommutativ sind. (Die Begriffe Primideal und maximales Ideal, die wir jetzt einführen, lassen sich aber auch im Falle eines nichtkommutativen Ringes definieren)

Eine Untermege $I \subset R$ des kommutativen Ringes R ist ein Ideal, wenn I Untergruppe von $(R, +)$ ist und $R \cdot I \subset I$ gilt.

Definition 7.8 Ein Ideal $\mathcal{P} \subset R$, $\mathcal{P} \neq R$ heißt Primideal, wenn \mathcal{P} ein Ideal ist und falls für alle $a, b \in R$ gilt: $a \cdot b \in \mathcal{P} \Rightarrow a \in \mathcal{P}$ oder $b \in \mathcal{P}$.

Definition 7.9 $0 \neq n \in R$ heißt Nullteiler, wenn es ein $x \in R$, $x \neq 0$ gibt, so daß $n \cdot x = 0$. Ein Ring $R \neq \{0\}$ ohne Nullteiler heißt Integritäts-Ring oder auch nullteilerfrei.

Satz 7.10 $\mathcal{P} \subset R$ ist ein Primideal, genau dann, wenn R/\mathcal{P} ein Integritäts-Ring ist.

Beweis R/\mathcal{P} ist Integritäts-Ring \Leftrightarrow

$$\begin{aligned} (a \cdot b + \mathcal{P} = \mathcal{P} \Rightarrow a \in \mathcal{P} \text{ oder } b \in \mathcal{P}) &\Leftrightarrow \\ (a \cdot b \in \mathcal{P} \Rightarrow a \in \mathcal{P} \text{ oder } b \in \mathcal{P}) &\Leftrightarrow \end{aligned}$$

\mathcal{P} ist Primideal □

Definition 7.11 Ein Ideal $\mathcal{M} \subset R$, $\mathcal{M} \neq R$ heißt maximal, falls für alle Ideale $I \subset R$ mit $I \supset \mathcal{M} \Rightarrow I = \mathcal{M}$ oder $I = R$.

Satz 7.12 $\mathcal{M} \subset R$ ist ein maximales Ideal $\Leftrightarrow R/\mathcal{M}$ ist ein Körper.

Beweis

„ \Rightarrow “ Wir müssen zeigen, daß für $r \notin \mathcal{M}$ die Restklasse $r + \mathcal{M}$ ein Inverses Element in R/\mathcal{M} besitzt, d.h. gesucht ist ein $r' \in R$ mit $r \cdot r' + \mathcal{M} = 1 + \mathcal{M} \Leftrightarrow r \cdot r' - 1 \in \mathcal{M}$. Da \mathcal{M} maximal ist und $r \notin \mathcal{M}$ gilt

$$R = R \cdot r + \mathcal{M}$$

Also ist $1 \in R \cdot r + \mathcal{M}$, was zu zeigen war.

„ \Leftarrow “ Sei K ein Körper. Die einzigen Ideale von K sind $\{0\}$ und K selbst. Falls R/\mathcal{M} ein Körper ist, und $I \supset \mathcal{M}$ ein Ideal von R , $\pi(I) \subset R/\mathcal{M}$ das Bild unter der Quotientenabbildung, so gilt für das Ideal $\pi(I)$, $\pi(I) = 0$ oder $\pi(I) = R/\mathcal{M}$. Es folgt also $I = \mathcal{M}$ oder $I = R$. □

Bemerkung Maximale Ideale sind insbesondere auch Primideale.

Beispiel 7.1 $R = \mathbf{Z}$, der Ring der ganzen Zahlen. Die Ideale in \mathbf{Z} sind von der Gestalt $m\mathbf{Z}$. Primideale sind die Ideale $\mathcal{P} = p\mathbf{Z}$ für p eine Primzahl und $\{0\}$. Die maximalen Ideale sind die Ideale $p\mathbf{Z}$ für p eine Primzahl. Insbesondere sind die Ringe $\mathbf{Z}/p\mathbf{Z}$ auch Körper.

Zur Existenz maximaler Ideale:

Satz 7.13 $I \subset R$ sei ein echtes Ideal, dann ist I in einem maximalen Ideal enthalten.

Beweis Sei $M = \{I' \mid I \subset I' \subset R, I' \text{ Ideal und } I' \neq R\}$. Die Relation \supset definiert eine Ordnung \geq auf M , i.e. $I_1 \geq I_2 \Leftrightarrow I_1 \supset I_2$. Jede total geordnete Teilmenge $T \subset M$ besitzt eine obere Schranke in M :

$$(I^T = \bigcup_{Y \in T} Y) \in M,$$

denn $I^T \neq R$, da $1 \notin I^T$ und I^T ist ein Ideal. Dazu zeigen wir $x \in I_1, y \in I_2$ (wobei I_1, I_2 Elemente aus T sind), dann ist $x + y \in I^T$. O.b.d.A. können wir annehmen, daß $I_1 \supset I_2$. Also ist $x + y \in I_1 \subset I^T$. Nach dem Lemma von Zorn besitzt die Menge M ein maximales Element. □

Bemerkung \geq ist eine Ordnung auf M , bedeutet \geq ist eine Relation mit

- i) $x \geq x$
- ii) $x \geq y$ und $y \geq x \Rightarrow x = y$
- iii) $x \geq y$ und $y \geq z \Rightarrow x \geq z$

Eine Menge T mit Ordnung ist total geordnet, wenn gilt $x, y \in T \Rightarrow x \geq y$ oder $y \geq x$. Ein Element $m \in M$ heißt maximales Element, wenn für alle $y \in M$ gilt $y \geq m \Rightarrow y = m$.

Satz 7.14 (Lemma von Zorn) (M, \geq) sei eine geordnete Menge und jede total geordnete Teilmenge habe eine obere Schranke in M . Dann hat M ein maximales Element.

7.5 Der chinesische Restsatz

R sei ein kommutativer Ring, $I \subset R$ sei ein Ideal. Wir benutzen hier die Kongruenz-Schreibweise:

$$x, y \in R, \quad x \equiv y \pmod{I} : \Leftrightarrow x - y \in I.$$

Klassisches Beispiel ist $R = \mathbf{Z}$, $I = m\mathbf{Z} \subset \mathbf{Z}$. Dann bedeutet

$$x \equiv y \pmod{m}$$

„ x und y haben den gleichen Rest bei Division durch m “.

Simultanes lösen von Kongruenzen:

Satz 7.15 (Chinesischer Restsatz) *R sei kommutativer Ring, I_1, I_2, \dots, I_n seien Ideale, so daß $I_i + I_j = R$, für $i \neq j$. Gegeben seien $x_1, \dots, x_n \in R$, dann gibt es $x \in R$ mit*

$$x \equiv x_i \pmod{I_i}.$$

Beweis Wir betrachten zuerst den Fall $n = 2$. Dann ist $I_1 + I_2 = R$. Gesucht ist $x \in R$, so daß

$$\begin{aligned} x &\equiv x_1 \pmod{I_1} \\ x &\equiv x_2 \pmod{I_2} \end{aligned}$$

Es gilt nun $1 = a_1 + a_2$, mit $a_i \in I_i$. Setze $x = x_2 a_1 + x_1 a_2$, dann gilt

$$\begin{aligned} x &\equiv x_1 a_2 \pmod{I_1} \equiv x_1 \pmod{I_1} \\ x &\equiv x_2 a_1 \pmod{I_2} \equiv x_2 \pmod{I_2}. \end{aligned}$$

Im allgemeinen Fall, $n > 2$, gehen wir folgendermaßen vor: Es ist

$$I_1 + \prod_{i=2}^n I_i = R,$$

denn es gibt $a_i \in I_1, b_i \in I_i$ mit $a_i + b_i = 1$. Also

$$1 = \prod_{i=2}^n (a_i + b_i) \in I_1 + \prod_{i=2}^n I_i.$$

Es gibt also $y_1 \in R$ mit

$$\begin{aligned} y_1 &\equiv 1 \pmod{I_1} \\ y_1 &\equiv 0 \pmod{\prod_{i=2}^n I_i}, \text{ insbesondere} \\ y_1 &\equiv 0 \pmod{I_i}, \text{ für } i \geq 2 \end{aligned}$$

Ebenso gibt es für $i \geq 2$ Elemente $y_i \in I_i$ mit

$$\begin{aligned} y_i &\equiv 1 \pmod{I_i}, \\ y_i &\equiv 0 \pmod{I_j}, \quad \text{für } i \neq j. \end{aligned}$$

Die $\{y_i\}, i = 1, \dots, n$ heißen auch orthogonale Idempotente und

$$x = x_1 y_1 + x_2 y_2 + \dots + x_n y_n$$

ist Lösung des Kongruenzsystems. □

Wir definieren nun den Produktring:

Definition 7.16 R_1, R_2 seien Ringe, dann ist $R = R_1 \times R_2$ ein Ring mit

$$\begin{aligned} (r_1, r_2) + (r'_1, r'_2) &= (r_1 + r_2, r'_1 + r'_2) \\ (r_1, r_2) \cdot (r'_1, r'_2) &= (r_1 \cdot r'_1, r_2 \cdot r'_2) \\ 1_R &= (1_{R_1}, 1_{R_2}). \end{aligned}$$

R heißt auch Produktring von R_1 und R_2 .

Aus dem chinesischen Restsatz folgern wir nun

Korollar 7.17 R sei ein Ring. $I_i \subset R, i = 1, \dots, n$, seien Ideale mit $I_i + I_j = R$ für $i \neq j$. Die Abbildung

$$\begin{aligned} f : R &\rightarrow R/I_1 \times R/I_2 \times \dots \times R/I_n \\ x &\mapsto (r + I_1, r + I_2, \dots, r + I_n) \end{aligned}$$

ist ein surjektiver Homomorphismus mit Kern $f = I_1 \cap I_2 \cap \dots \cap I_n =: I$, d.h. f induziert einen Isomorphismus

$$\bar{f} : R/I \xrightarrow{\cong} R/I_1 \times R/I_2 \times \dots \times R/I_n.$$

Beweis f ist offenbar ein Homomorphismus. Kern $f = I_1 \cap I_2 \cap \dots \cap I_n$ ist ebenfalls klar. Der Chinesische Restsatz impliziert nun, daß f surjektiv ist. □

Anwendung: $R = \mathbf{Z}$. m_1, m_2, \dots, m_n seien paarweise teilerfremde natürliche Zahlen und $m = m_1 \cdot m_2 \cdot \dots \cdot m_n$. Dann gilt

$$\mathbf{Z}/m\mathbf{Z} \cong \mathbf{Z}/m_1\mathbf{Z} \times \mathbf{Z}/m_2\mathbf{Z} \times \dots \times \mathbf{Z}/m_n\mathbf{Z}.$$

Insbesondere, wenn

$$m = \prod_i p_i^{r_i}$$

die Zerlegung von m in seine verschiedenen Primfaktoren ist, so erhalten wir einen Ringisomorphismus

$$\mathbf{Z}/m\mathbf{Z} \cong \prod_i \mathbf{Z}/p_i^{r_i}\mathbf{Z}.$$

8 Lokalisierung

R sei ein kommutativer Ring. Eine Teilmenge $S \subset R$ heißt multiplikative Teilmenge, wenn die Bedingungen

- i) $1 \in S$
- ii) $a, b \in S \Rightarrow a \cdot b \in S$

erfüllt sind. Wir betrachten nun folgende Relation \sim auf der Menge $R \times S$:

$$(a, s_1) \sim (b, s_2) \quad :\Leftrightarrow \quad \exists s \in S \text{ mit } s \cdot (as_2 - bs_1) = 0.$$

Die Relation \sim ist eine Äquivalenzrelation und wir bezeichnen die Menge der Äquivalenz-Klassen mit $S^{-1}R$. Für die Klasse von (r, s) schreiben wir $\frac{r}{s}$.

Beweis, daß \sim eine Äquivalenzrelation ist: Reflexivität und Symmetrie der Relation sind klar. Für die Transitivität ist zu zeigen:

$$(a, s_1) \sim (b, s_2) \text{ und } (b, s_2) \sim (c, s_3) \quad \Rightarrow \quad (a, s_1) \sim (c, s_3).$$

Die Voraussetzung bedeutet, daß es Elemente $s', s'' \in S$ gibt mit $0 = s'(a \cdot s_2 - bs_1) = s''(bs_3 - c \cdot s_2)$. Dies bedeutet

$$\begin{aligned} 0 &= s' s'' (as_2 s_3 - bs_1 s_3) \\ &= s' s'' (as_2 s_3 - s_1 c s_2) \\ &= s' s'' s_2 (as_3 - cs_1). \end{aligned}$$

□

Satz 8.1

- i) \sim ist Äquivalenzrelation auf $R \times S$.
- ii) Die Menge der Äquivalenzklassen $S^{-1}R$ ist ein kommutativer Ring mit

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &= \frac{at + bs}{s \cdot t} \\ \frac{a}{s} \cdot \frac{b}{t} &= \frac{a \cdot b}{s \cdot t} \\ 0_{S^{-1}R} &= \frac{0}{1}, \quad 1_{S^{-1}R} = \frac{1}{1}. \end{aligned}$$

- iii) Die Abbildung $\nu : r \mapsto \frac{r}{1}$ von R nach $S^{-1}R$ ist ein Ringhomomorphismus mit $\nu(S) \subset (S^{-1}R)^*$. Ist $0 \notin S$, so ist ν injektiv, genau dann, wenn S keine Nullteiler enthält.

Zum Beweis des Satzes

- i) Ist bereits gezeigt.
- ii) Zu zeigen ist im wesentlichen, daß die Definition der Addition und Multiplikation wohldefiniert sind. Dann rechnet man sofort nach, daß $S^{-1}R$ ein (kommutativer) Ring ist. Wir zeigen hier nur, daß $+$ wohldefiniert ist. Es sei also $\frac{a_1}{s_1} = \frac{a_2}{s_2}$ und $\frac{b_1}{t_1} = \frac{b_2}{t_2}$. Dann gilt für gewisse $s, t \in S$,

$$\begin{aligned} 0 &= s(a_1s_2 - a_2s_1)tt_2t_1 \\ 0 &= t(b_1t_2 - b_2t_1)ss_2s_1. \end{aligned}$$

Addieren der beiden Gleichungen liefert

$$0 = st(s_2t_2(a_1t_1 + b_1s_1) - s_1t_1(a_2t_2 + b_2s_2)).$$

Es gilt also $\frac{a_1t_1 + b_1s_1}{s_1 \cdot t_1} = \frac{a_2t_2 + b_2s_2}{s_2 \cdot t_2}$.

- iii) Die Abbildung $\nu: r \mapsto \frac{r}{1}$ ist offenbar ein Homomorphismus. Wenn $s \in S$, dann ist $\nu(s) = \frac{s}{1}$ invertierbar in $S^{-1}R$, denn $\frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1}$. Es ist $\text{Kern } \nu = \{r \mid \frac{r}{1} = \frac{0}{1}\}$, das heißt für $0 \neq r \in \text{Kern } \nu$ gibt es $0 \neq s \in S$ mit $s \cdot r = 0$. Also ist s ein Nullteiler.

□

Definition 8.2 Der Ring $S^{-1}R$ mit $+, \cdot$ wie im Satz definiert heißt *Lokalisierung von R bezüglich S* oder auch *Quotientenring von R bezüglich S* .

Beispiel 8.1 Beispiele für multiplikative Mengen und Quotienten-Ringe:

1. Falls $0 \in S$, so gilt $S^{-1}R = \{0\}$.
2. $\mathcal{P} \subset R$ sei ein Primideal, dann ist $S = R \setminus \mathcal{P}$ multiplikativ und $S^{-1}R =: R_{\mathcal{P}}$ heißt lokaler Ring von R an der Stelle \mathcal{P} .
3. Wenn $S = R^*$, so ist $\nu: R \rightarrow S^{-1}R$ ein Isomorphismus, denn $\frac{r}{s} = \nu(rs^{-1})$.
4. $R = \mathbf{Z}$, $S = \mathbf{Z} - \{0\}$, $S^{-1}R = \mathbf{Q}$.
5. $R = \mathbf{Z}$, p sei eine Primzahl. Dann ist \mathbf{Z}_p ein Unterring von \mathbf{Q} . $\mathbf{Z}_p = \{\frac{a}{b} \mid (a, b) = 1, p \nmid b, a, b \in \mathbf{Z}\}$.

Wir verallgemeinern die Konstruktion der rationalen Zahlen aus \mathbf{Z} durch

Definition 8.3 R sei ein Integritätsring, $S = R - \{0\}$. Dann ist $S^{-1}R$ ein Körper mit $R \subset S^{-1}R$. Dieser Körper heißt der *Quotientenkörper von R* .

Beispiel 8.2 R sei ein Integritätsring. Es sei $R[X]$ der Ring der Polynome mit Koeffizienten in R und $S = R[X] - \{0\}$. Dann ist $S^{-1}R[X]$ der Körper der rationalen Funktionen von über R .

Satz 8.4 (Universelle Eigenschaft der Lokalisierung) $S \subset R$ sei eine multiplikative Menge und $\varphi: R \rightarrow R'$ sei ein Homomorphismus mit $\varphi(S) \subset (R')^*$. Dann gibt es einen eindeutigen Homomorphismus $\varphi_S: S^{-1}R \rightarrow R'$, so daß $\varphi_S \circ \nu = \varphi$.

Diagramm:

$$\begin{array}{ccc} & R & \\ \nu \swarrow & & \searrow \varphi \\ S^{-1}R & \xrightarrow{\varphi_S} & R' \end{array}$$

Beweis Notwendig ist, daß

$$\varphi_S\left(\frac{r}{s}\right) = \varphi(r)\varphi(s)^{-1}.$$

Also ist folgt die Eindeutigkeit. Wir müssen zeigen, daß hierdurch ein wohldefinierter Homomorphismus φ_S bestimmt ist. Es sei also $\frac{r_1}{s_1} = \frac{r_2}{s_2}$. Dann gibt es $s \in S$ mit

$$\begin{aligned} s(r_1s_2 - r_2s_1) &= 0, \text{ also auch} \\ \varphi(s)(\varphi(r_1)\varphi(s_2) - \varphi(r_2)\varphi(s_1)) &= 0 \end{aligned}$$

Da $\varphi(s)$ invertierbar ist folgt

$$\varphi(r_1)\varphi(s_2) - \varphi(r_2)\varphi(s_1) = 0.$$

Und deswegen auch $\varphi(r_1)\varphi(s_1)^{-1} = \varphi(r_2)\varphi(s_2)^{-1}$. Somit ist φ_S wohldefiniert und offensichtlich auch ein Homomorphismus ist. \square

8.1 Abbildungsverhalten von Idealen unter Lokalisierung

Es sei

$$\nu: R \rightarrow S^{-1}R$$

die Lokalisierung bezüglich S und $I \subset R$ sei ein Ideal. Dann ist

$$S^{-1}I = \left\{ \frac{a}{s} \in S^{-1}R \mid a \in I \right\}$$

ein Ideal in $S^{-1}R$. $S^{-1}I$ ist eine additive Untergruppe, denn für $a_1, a_2 \in I$ ist $\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2a_1 + s_1a_2}{s_1 \cdot s_2} \in S^{-1}I$. Denn aus $a_1, a_2 \in I$ folgt $a_1s_2, s_1a_2 \in I$. Ebenso folgt $S^{-1}R \cdot S^{-1}I \subset S^{-1}I$.

Satz 8.5 $I_1, I_2 \subset R$ seien Ideale, dann gilt

1. $S^{-1}(I_1 + I_2) = S^{-1}I_1 + S^{-1}I_2$
2. $S^{-1}(I_1 \cdot I_2) = S^{-1}I_1 \cdot S^{-1}I_2$

$$3. S^{-1}(I_1 \cap I_2) = S^{-1}I_1 \cap S^{-1}I_2$$

Beweis

1. Es seien $a_i \in I_i$ und $s, s_1, s_2 \in S$. Dann ist

$$S^{-1}(I_1 + I_2) \ni \frac{a_1 + a_2}{s} = \frac{a_1}{s} + \frac{a_2}{s} \in S^{-1}I_1 + S^{-1}I_2$$

und umgekehrt

$$S^{-1}I_1 + S^{-1}I_2 \ni \frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2} = \frac{a_1 s_2}{s_1 s_2} + \frac{a_2 s_1}{s_1 s_2} \in S^{-1}I_1 + S^{-1}I_2 .$$

2. + 3. Übung. □

9 Hauptidealringe und faktorielle Ringe

R sei ein kommutativer Ring.

Definition 9.1 Ein Ideal $I \subset R$ heißt *Hauptideal*, wenn $I = R \cdot a$ für ein $a \in R$. Ein Ring heißt *Hauptidealring*, wenn jedes Ideal ein Hauptideal ist.

Beispiel 9.1 \mathbf{Z} : alle Ideale sind von der Gestalt $m\mathbf{Z}$, für ein $m \in \mathbf{N}$, also \mathbf{Z} ist ein Hauptideal-Ring.

Für Hauptidealring verwenden wir manchmal die Abkürzung HIR. Wir schreiben (a_1, \dots, a_n) für das von den Elementen $a_i \in R$ erzeugte Ideal in R .

9.1 Faktorielle Ringe

Es sei R ein Integritätsring.

Definition 9.2 $a \in R, a \neq 0$ heißt *irreduzibel*, wenn a keine Einheit ist und wenn aus $a = b \cdot c$ folgt, daß entweder b oder c eine Einheit ist.

Beispiel 9.2 Wenn $(a) \subset R$ ein Primideal ist, dann ist a irreduzibel.

Beweis Es sei $a = b \cdot c$. Nun folgt (da (a) Prim ist) ohne Einschränkung, daß $b \in (a)$ ist, das heißt $b = ra$ für ein $r \in R$. Also ist $a = (rc)a$. Da R ein Integritätsring ist, ist $rc = 1$, also ist c eine Einheit. □

Beispiel 9.3 Die irreduziblen Elemente in \mathbf{Z} sind die Zahlen $\pm p$, mit $p \in \mathbf{N}$ eine Primzahl.

Eine wichtige Eigenschaft des Ringes der ganzen Zahlen ist, daß jede Zahl eine eindeutige Primfaktor-Zerlegung hat.

Definition 9.3 $a \in R$ hat eine *eindeutige Faktorisierung in irreduzible Elemente*, wenn

1. $a = \mu \cdot \prod_{i=1}^r p_i$, wobei $\mu \in R$ ein Einheit ist und die Elemente $p_i \in R$ irreduzibel sind.
2. Für jede weitere Zerlegung $a = \mu' \cdot \prod_{i=1}^s p'_i$ gilt $r = s$ und (nach möglicher Permutation der Indizes) gilt $p'_i = \mu_i p_i$ für Einheiten $\mu_i \in R^*$.

Definition 9.4 R sei ein Integritätsring. R heißt faktorieller Ring, wenn jedes $0 \neq r \in R$ eine eindeutige Faktorisierung in irreduzible Elemente hat.

9.2 Der grösste gemeinsame Teiler

R sei ein Integritätsring und $a, b \in R$. Wir sagen $a \mid b$ (a teilt b), wenn $b = ra$ für ein $r \in R$. Ein Teiler c von a und b heißt *grösster gemeinsamer Teiler* von a und b (bezeichnet mit $\text{ggT}(a, b)$), wenn für alle $d \in R$ gilt

$$d \mid a \quad \text{und} \quad d \mid b \quad \implies \quad d \mid c.$$

Satz 9.5 R sei ein Integritätsring und ein HIR. Es seien $a, b \in R$. Dann ist ein $c \in R$ mit $(c) = (a, b)$ ein ggT von a und b .

Beweis $(c) = (a, b)$. Dann folgt $c \mid a$ und $c \mid b$ und weiter $c = s_1 a + s_2 b$, für gewisse $s_1, s_2 \in R$. Wenn $d \mid a$ und $d \mid b$, so gibt es $t_1, t_2 \in R$ mit $dt_1 = a$ und $dt_2 = b$. Dann

$$\begin{aligned} c &= s_1 \cdot t_1 \cdot d + s_2 \cdot t_2 \cdot d \\ &= (s_1 \cdot t_1 + s_2 \cdot t_2) \cdot d, \end{aligned}$$

also $d \mid c$. □

Satz 9.6 R sei ein Integritätsring und ein HIR, dann ist R faktoriell.

Beweis Wir zeigen zuerst die Existenz der Zerlegung in irreduzible Elemente. Sei $S = \{a \in R \mid a \text{ hat keine Zerlegung}\}$. Betrachte eine aufsteigende Kette

$$(*) \quad (a_1) \subseteq (a_2) \subseteq \dots$$

mit $a_i \in S$. Dann ist $\bigcup_{i=1}^{\infty} (a_i) = I$ ein Ideal und also $I = (a)$ mit $a \in (a_n)$ für ein n . Also

$$(a) \subset (a_n), \quad \text{das heißt} \quad I = (a_n)$$

und die Kette $(*)$ ist endlich. Die Menge S besitzt also maximale Elemente, d.h. Elemente a , so daß gilt für alle $b \in S$ folgt aus $(a) \subset (b)$, daß $(a) = (b)$. Insbesondere gilt für jedes Ideal $I = (d)$ mit $I \supseteq (a)$ und $I \neq (a)$, daß d eine Zerlegung in irreduzible Element hat. Da $a \in S$ ist, hat a eine Zerlegung $a = a_1 \cdot a_2$ mit $(a_i) \supseteq (a)$, somit haben die a_i eine Zerlegung in irreduzible Elemente, also auch a . Dies ist ein Widerspruch zur Annahme, daß $S \neq \emptyset$. □

Zum Beweis der Eindeutigkeit einer Zerlegung benötigen wir das folgende

Lemma 9.7 *R sei ein HIR, $p \in R$ sei ein irreduzibles Element und $p \mid a \cdot b$. Dann gilt $p \mid a$ oder $p \mid b$.*

Beweis des Lemmas Wir nehmen an, daß a nicht von p geteilt wird, dann ist $\text{ggT}(a, p) = 1$, also $(a, p) = (1)$ und $1 = a \cdot r_1 + r_2 \cdot p$ für gewisse $r_i \in R$. Also ist

$$b = (a \cdot b)r_1 + (b \cdot r_2) \cdot p$$

und insbesondere gilt $p \mid b$. □

Fortsetzung des Beweises von Satz 9.6 Wir müssen noch die Eindeutigkeit einer Zerlegung von $a \in R$ in irreduzible Elemente zeigen. Es sei

$$a = \mu \cdot \prod_{i=1}^r p_i = \mu' \cdot \prod_{i=1}^s p'_i .$$

Au dem Lemma folgt, daß $p'_1 \mid p_j$ für ein j also $p'_1 = \mu_1 p_j$ und deswegen

$$a = (\mu \mu_1) p'_1 \prod_{\substack{i=1 \\ i \neq j}}^r p_i = \mu' p'_1 \prod_{i=2}^s p'_i .$$

Also gilt

$$(\mu \mu_1) \prod_{\substack{i=1 \\ i \neq j}}^r p_i = \mu' \prod_{i=2}^s p'_i$$

und die Behauptung folgt durch Induktion. □

Beispiel 9.4 (Ganze Gaußsche Zahlen) Der Ring

$$\mathbf{Z}[i] = \{m + ni \mid m, n \in \mathbf{Z}\} \subset \mathbf{C}$$

ist ein Unterring der komplexen Zahlen und wird Ring der ganzen Gaußschen Zahlen genannt. Die Gruppe der Einheiten von $\mathbf{Z}[i]$ ist $\mathbf{Z}[i]^* = \{1, -1, i, -i\}$. Wir werden später sehen, daß $\mathbf{Z}[i]$ faktoriell, sogar ein Hauptidealring ist und die irreduziblen Elemente dieses Ringes bestimmen. Zum Beispiel hat die Primzahl $2 \in \mathbf{Z}$ die folgende Zerlegung in $\mathbf{Z}[i]$:

$$2 = (1 + i)(1 - i) .$$

Das heißt 2 ist nicht irreduzibel in $\mathbf{Z}[i]$. Jedoch $(1 + i)$ ist irreduzibel in $\mathbf{Z}[i]$.

10 Euklidische Ringe

R sei ein Integritätsring. Eine Funktion

$$d : R - \{0\} \rightarrow \mathbf{N} \cup \{0\}$$

heißt Gradfunktion, wenn es in R eine Division mit Rest bezüglich d gibt, das heißt

$$\forall a, b \in R, b \neq 0 \exists q, r \in R \quad a = q \cdot b + r,$$

und es gilt wenn $r \neq 0$, daß $d(r) < d(b)$.

Definition 10.1 Wenn R eine Gradfunktion und Division mit Rest hat, dann heißt R ein euklidischer Ring.

Beispiel 10.1 \mathbf{Z} ist ein euklidischer Ring mit dem Absolutbetrag als Gradfunktion. D.h. für $m \in \mathbf{Z}$ ist $d(m) = |m|$.

Satz 10.2 Euklidische Ringe sind Hauptidealringe (und also insbesondere faktoriell).

Beweis $I \subset R$ sei ein Ideal. Dann existiert ein $0 \neq a \in I$, das ein Element kleinsten Grades in I ist. Für $b \in I$ führen wir die Division mit Rest durch a aus und erhalten

$$b = a \cdot q + r.$$

Wobei dann $r \in I$ und falls $r \neq 0$ ist $\deg(r) < \deg(a)$. Also ist $r = 0$ und deswegen $I = (a)$ \square

10.1 Der euklidische Algorithmus

Sei R ein euklidischer Ring und $d : R - \{0\} \rightarrow \mathbf{N} \cup \{0\}$ die Grad-Funktion. R ist ein Hauptidealring und je zwei Elemente in R besitzen einen größten gemeinsamen Teiler. Wir erinnern an die Definition des größten gemeinsamen Teilers: Für $a, b \in R$, heißt $c \in R$ mit $c \mid a$ und $c \mid b$ der ggT von a und b , wenn für alle $d \in R$ mit $d \mid a$ und $d \mid b$ auch $d \mid c$.

Satz 10.3 (Euklidischer Algorithmus) Es gibt einen Algorithmus, der zu $a, b \in R$ Elemente $u, v \in R$ berechnet mit

1. $c = au + bv$ ist der ggT von a und b .
2. $d(u) < d(\frac{b}{c})$ und $d(v) < d(\frac{a}{c})$.

Beweis Der euklidische Algorithmus berechnet den ggT durch wiederholte Division mit Rest. Betrachte die Folge von Divisionen mit Rest

$$\begin{aligned} a &= q_1 b + r_1, & r_0 &= b \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_{k+1} r_k + r_{k+1} \\ r_k &= q_{k+2} r_{k+1} \end{aligned}$$

Die Folge r_j wird schließlich 0 and der Stelle $k+2$, da in jedem Schritt $d(r_{j+1}) < d(r_j)$ gilt. Setze $c = r_{k+1}$, dann gilt $c \mid r_{j+1}$ und $c \mid r_j$ für alle j , also auch $c \mid a$ und $c \mid b$. Umgekehrt falls $d \mid a$ und $d \mid b$ dann (induktiv aufsteigend) $d \mid r_j$ für alle j , also auch $d \mid r_{k+1} = c$. Also ist c ein ggT von a und b .

Zur Berechnung von u und v : Setze $u_1 = 1$ und $u_0 = 0$, sowie für $j > 1$

$$u_j = u_{j-2} - q_j u_{j-1}.$$

Dann gilt in jedem Schritt

$$r_j = u_j \cdot a + v_j \cdot b.$$

Insbesondere gilt

$$c = r_k = u_k \cdot a + v_k \cdot b,$$

also $u = u_k$ und $v = v_k = \frac{(c-u \cdot a)}{b}$. Sei $y = \frac{b}{c}$ und $x = \frac{a}{c}$, dann sind alle Lösungen von

$$c = u' \cdot a + v' \cdot b$$

von der Gestalt

$$u' = u + \lambda \cdot y, \quad v' = v - \lambda \cdot x$$

mit $\lambda \in R$.

□

Beispiel 10.2 $R = \mathbf{Z}[X]$, $a = X, b = 2$. Dann ist $\text{ggT}(X, 2) = 1$. Aber es ist

$$\mathbf{Z}[X] \supset (X, 2) \supset (X) \supset (0)$$

eine echt absteigende Folge von Idealen in $\mathbf{Z}[X]$. Die Ideale $(X, 2)$, (X) , (0) sind sogar Primideale. Das Ideal $(X, 2)$ ist kein Hauptideal. Betrachten wir $(X, 2)$ in $\mathbf{Q}[X]$, so ist $(X, 2) = \mathbf{Q}[X]$ ein Hauptideal, erzeugt von $\text{ggT}(X, 2) = 1$.

10.2 Polynome in einer Variablen

R sei ein Ring. Wir geben eine Konstruktion für den Ring der Polynome mit Koeffizienten in R . Hierzu betrachten wir Abbildungen $f : \mathbf{N} \cup \{0\} \rightarrow R$ mit der Eigenschaft $f(j) = 0$ für alle bis auf endlich viele j . Die Abbildungen $X^i :$

$\mathbf{N} \cup \{0\} \rightarrow R$ seien definiert durch $X^i(i) = 1$, $X^i(j) = 0$ für $j \neq i$. Dann können wir schreiben $f = \sum_i a_i X^i$ mit $a_i \in R$, wobei nur endlich viele a_i verschieden von 0 sind. Die Menge solcher Abbildungen bildet mit der Addition

$$(f + g)(i) = f(i) + g(i)$$

und der Multiplikation

$$(f \cdot g)(i) = \sum_{k_1+k_2=i} f(k_1)g(k_2)$$

einen Ring, den Polynomring $R[X]$. Falls $f \neq 0$, so heißt die grösste Zahl n mit $f(n) \neq 0$ der Grad von f und wir schreiben $n = \deg f$. (Für $f \equiv 0$ definiert man oft $\deg f := -\infty$). Ein Polynom $0 \neq f \in R[X]$ vom Grad n ist also von der Gestalt

$$f(X) = \sum_{i=0}^n a_i X^i \quad a_i \in R, \quad a_n \neq 0.$$

Bemerkung Polynome definieren Funktionen auf dem Ring R durch „Einsetzen“: Wenn

$$f(X) = \sum_{i=0}^n a_i X^i \in R[X],$$

dann setzen wir für $r \in R$

$$\tilde{f}(r) = \sum_{i=0}^n a_i r^i.$$

Dann ist $\tilde{f}: R \rightarrow R$ die zu f gehörende Funktion.

Beispiel 10.3 $R = \mathbf{Z}/2\mathbf{Z}$. Es sei

$$f(X) = X^2 + X \neq 0, \in \mathbf{Z}/2\mathbf{Z}[X].$$

Dann ist f ein Polynom vom Grad 2 und verschieden von 0. Jedoch ist $\tilde{f}(r) = r + r = 2r = 0$ für alle $r \in \mathbf{Z}/2\mathbf{Z}$. Also ist \tilde{f} die Nullfunktion.

Satz 10.4 Wenn R ein Integritätsring ist, dann ist $R[X]$ ein Integritätsring und es gilt

$$\deg(p_1 \cdot p_2) = (\deg p_1) + (\deg p_2)$$

für $0 \neq p_1, p_2 \in R[X]$.

Anwendung: R sei ein Integritätsring, dann ist $f \in R[X]$ eine Einheit, genau dann, wenn $f(X) = a_0$ mit $a_0 \in R^*$.

Satz 10.5 (Polynomdivision) Sei K ein Körper, $p_1, p_2 \in K[X]$, dann gibt es eindeutige Polynome $q, r \in K[X]$ mit

$$p_1 = q \cdot p_2 + r$$

und $\deg r < \deg p_2$. Insbesondere gilt: $K[X]$ ist ein euklidischer Ring.

Beweis Für ein Polynom $0 \neq p = \sum_{i=0}^n a_i X^i \in R[X]$ bezeichne $LC(p)$ den „Leitkoeffizienten“ von p , d.h. $LC(p)$ ist der Koeffizient $a_{\deg p}$. Der folgende Algorithmus berechnet q und r . „Pseudo-Code“:

$q = 0, r = p_1$. WHILE ($\deg r \geq \deg p_2$) DO

$$q := q + \frac{LC(r)}{LC(p_2)} \cdot X^{(\deg r - \deg p_2)}$$

$$r := r - \frac{LC(r)}{LC(p_2)} \cdot X^{(\deg r - \deg p_2)} \cdot p_2$$

{ $p_1 = q \cdot p_2 + r$ } END

Die Eindeutigkeit ist klar. □

$a \in R$ heißt eine Nullstelle von $p \in R[X]$, wenn $p(a) = 0$.

Satz 10.6 *R sei ein Integritätsring, dann hat ein Polynom $p[X] \in R[X]$ vom Grad n höchstens n Nullstellen.*

Beweis Da $R \subset \text{Quot}(R)$ in seinem Quotientenkörper enthalten ist, genügt es, das Resultat für den Fall $R = K$, wobei K ein Körper ist, zu zeigen. Für jedes $a \in K$ gibt es dann q, r , so daß

$$p(X) = q(X) \cdot (X - a) + r(X)$$

mit $\deg r < 1$. Es sei nun $p(a) = 0$. Falls $r = 0$ ist, so folgt die Behauptung mit Induktion, denn $\deg q = (\deg p) - 1$. Sonst ist r eine Konstante $r_0 \neq 0$. Dies kann aber nicht sein, da

$$0 = p(a) = q(a)(a - a) + r_0 = r_0 .$$

□

Beispiel 10.4

- i) $R = \mathbf{Z}/8\mathbf{Z}$, $p(X) = X^2 - 1$. Dann hat p die Nullstellen 1, 3, 5, 7 in R .
- ii) Nach dem Fundamentalsatz der Algebra ist \mathbf{C} ein algebraisch abgeschlossener Körper. Jedes Polynom $p \in \mathbf{C}[X]$ von Grad n schreibt sich als Produkt von Linearfaktoren.

Anwendung:

Satz 10.7 *K sei ein Körper, dann ist jede endliche (multiplikative) Untergruppe $U \subset K^*$ zyklisch.*

Beweis Es ist

$$U = \prod_{p \mid \text{ord}(U)} U(p)$$

ein Produkt von p -Gruppen $U(p)$. Deswegen reicht es zu zeigen, daß $U(p)$ zyklisch ist. Sei $m = |U(p)|$. Falls $U(p)$ nicht zyklisch ist, so ist $p^l < m$ ein Exponent für $U(p)$, das heißt $x^{p^l} - 1 = 0, \forall x \in U(p)$. Das kann aber nicht sein, also ist $U(p)$ zyklisch. □

11 Ganze Zahlen in quadratischen Zahlkörpern

$0 \neq d \in \mathbf{Z}$ sei eine ganze Zahl, die quadratfrei ist und es sei

$$\alpha = \sqrt{d} \quad \text{für } d \equiv 2 \pmod{4} \text{ oder } d \equiv 3 \pmod{4}$$

$$\alpha = \frac{1 + \sqrt{d}}{2} \quad \text{für } d \equiv 1 \pmod{4}$$

Dann ist

$$\mathbf{Q}(\sqrt{d}) = \{r + s\sqrt{d} \mid r, s \in \mathbf{Q}\} \subset \mathbf{C}$$

ein Körper. $(\mathbf{Q}(\sqrt{d}))$ heißt „reell quadratischer Zahlkörper“ falls $d > 0$, sonst heißt $\mathbf{Q}(\sqrt{d})$ „imaginär quadratischer Zahlkörper“. Die Ringe

$$\mathcal{O}_d = \mathbf{Z}[\alpha] = \{m + n\alpha \mid m, n \in \mathbf{Z}\} \subset \mathbf{Q}[\sqrt{d}]$$

heißen die Ringe ganzer Zahlen in $\mathbf{Q}[\sqrt{d}]$.

Beispiel 11.1 $d = -5$, $\alpha = \sqrt{-5}$. $\mathbf{Z}[\sqrt{-5}]$ ist nicht faktoriell (Übung 11). Das heißt $\mathbf{Z}[\sqrt{d}]$ ist im allgemeinen nicht faktoriell.

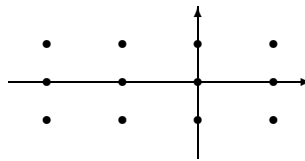
Satz 11.1 Die Ringe \mathcal{O}_d sind euklidisch für $d = -11, -7, -3, -2, -1, 2, 3, 5, 13$.

Bemerkung \mathcal{O}_d ist faktoriell für $d < 0$ genau dann, wenn $-d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Für $d > 0$ wird vermutet, daß unendlich viele \mathcal{O}_d faktoriell sind.

Zum Beweis des Satzes Wir beweisen nur den Fall $d = -1$, $\mathcal{O}_{-1} = \mathbf{Z}[i]$. Betrachte die komplexe Konjugation $\sigma : \mathbf{Z}[i] \rightarrow \mathbf{Z}[i]$, das heißt

$$\sigma : m + ni \mapsto m - ni$$

und die zugehörige Normfunktion $N(x) = x \cdot \sigma(x) = m^2 + n^2$. Es gilt $N(x \cdot y) = N(x)N(y)$ und N ist definiert auf dem Körper $\mathbf{Q}(i)$. Wir wollen zeigen, daß N eine Gradfunktion auf $\mathbf{Z}[i]$ ist. Wir zeigen hier für, daß es für $a, b \in \mathbf{Z}[i]$ ein $q \in \mathbf{Z}[i]$ gibt mit $N(a - b \cdot q) < N(b)$. Dann ist N eine Grad-Funktion. Nun folgt $N(a - b \cdot q) < N(b)$ aus $N(\frac{a}{b} - q) < 1$. Also reicht es zu zeigen: Für jedes $\beta = \frac{a}{b} \in \mathbf{Q}[i]$ gibt es ein $q \in \mathbf{Z}[i]$ mit $N(\beta - q) < 1$. Die Menge $\mathbf{Z}[i] \subset \mathbf{C}$ ist ein Gitter in \mathbf{C} :



und N ist das Quadrat des euklidischen Abstandes. Das Gitter $\mathbf{Z}[i]$ hat nun die Eigenschaft, daß alle Elemente $z \in \mathbf{C}$ Abstand < 1 zu den Gitter-Punkten haben, d.h. im Innern eines Balls vom Radius 1 mit Zentrum z liegt wenigstens ein Punkt aus $\mathbf{Z}[i]$. \square

Bemerkung Für die Ringe $\mathbf{Q}(\sqrt{d})$ existiert eine multiplikative Funktion N , wie im Fall $d = -1$. Vergleiche Übung 11.

11.1 Primelemente im Ring der ganzen Gaußschen Zahlen

Unser Ziel ist es, die Primelemente im Ring der ganzen Gaußschen Zahlen

$$\mathbf{Z}[i] = \{m + in \mid m, n \in \mathbf{Z}\} \subset \mathbf{Q}(i)$$

zu bestimmen. Die Normfunktion

$$N : \mathbf{Z}[i] \rightarrow \mathbf{N}_0$$

definiert durch

$$N(m + in) = m^2 + n^2$$

macht, wie wir gesehen haben, $\mathbf{Z}[i]$ zu einem euklidischen, also insbesondere auch zu einem faktoriellen Ring. In einem faktoriellen Ring sind die irreduziblen Elemente sogar Primelemente, d.h. es gilt für $\pi \in \mathbf{Z}[i]$ irreduzibel, daß $\pi \mid a \cdot b \Rightarrow \pi \mid a$ oder $\pi \mid b$, für alle $0 \neq a, b \in \mathbf{Z}[i]$.

Satz 11.2 $p \in \mathbf{Z}$ sei eine Primzahl in \mathbf{Z} . Dann gilt entweder

- i) p bleibt ein Primelement in $\mathbf{Z}[i]$ oder
- ii) $p = \pm \pi \cdot \bar{\pi}$ für ein Primelement $\pi \in \mathbf{Z}[i]$. (wobei $\bar{\pi}$ = das zu π komplex konjugierte Primelement ist)

Es gilt weiter: Jedes Primelement $\pi \in \mathbf{Z}[i]$ teilt eine eindeutige Primzahl $p \in \mathbf{Z}$.

Beweis Für ein Primelement $\pi \in \mathbf{Z}[i]$ ist $N(\pi) = \pi \cdot \bar{\pi} \in \mathbf{Z}$. Somit gilt $\pi \mid N(\pi)$. Da $N(\pi) \neq \pm 1$, teilt π also auch eine Primzahl p . Da $\mathbf{Z}[i]$ ein Hauptidealring ist, bleiben zwei in \mathbf{Z} teilerfremde Primzahlen p, q auch teilerfremd in $\mathbf{Z}[i]$. Deswegen ist die zu π gehörige Primzahl p eindeutig bestimmt.

Da $\pi \mid p$ können wir schreiben

$$p = \pi \cdot \pi',$$

für ein $\pi' \in \mathbf{Z}[i]$. Es folgt $N(\pi) \cdot N(\pi') = p^2$. Im Fall, daß $N(\pi') = 1$ ist, ist p ein Primelement in $\mathbf{Z}[i]$. Also gilt Fall i). Sonst ist $N(\pi) = p = \pi \cdot \bar{\pi}$. Also gilt Fall ii). \square

Satz 11.3 $p \in \mathbf{Z}$ sei eine Primzahl. Dann gilt:

- i) p bleibt eine Primzahl in $\mathbf{Z}[i]$, genau dann wenn $p \equiv 3 \pmod{4}$.
- ii) $p = \pm \pi \cdot \bar{\pi}$, wobei π und $\bar{\pi}$ nicht assoziiert zueinander sind, genau dann wenn $p \equiv 1 \pmod{4}$.
- iii) $p = 2 = (1 + i)(1 - i) = -i(1 + i)^2$.

Wir erhalten aus dem Satz die Liste der Primelemente in $\mathbf{Z}[i]$:

$$(1 + i), 3, (1 + 2i), (1 - 2i), 7, 11, (3 + 2i), (3 - 2i), (4 + i)(4 - i), 19, \dots$$

Beweis

- i) Wenn $p = \pm \pi \cdot \bar{\pi} = m^2 + n^2$ so folgt, daß $p \equiv 1 \pmod{4}$, da 0 und 1 die einzigen Quadrate mod 4 sind. Es folgt somit i).
- ii) Falls $p \equiv 1 \pmod{4}$, so ist $p - 1 \equiv 0 \pmod{4}$. Da \mathbf{F}_p^* zyklisch ist, ist $-1 = \mu^k$, wobei $\mathbf{F}_p^* = \langle \mu \rangle$, $k = \frac{1}{2}(p - 1) = 2k'$, also ist $-1 = \mu^{2k'} = (\mu^{k'})^2$ ein Quadrat in \mathbf{F}_p . Deswegen gibt es ein $0 < x < p$ mit $x^2 + 1 = p \cdot m$, wobei $m < p$. Für $\tau = x + i \in \mathbf{Z}[i]$ ist

$$N(\tau) = p \cdot m .$$

Also gilt für einen der Primteiler von τ :

$$N(\pi) = p, \quad \text{d.h. } p = \pi \cdot \bar{\pi} .$$

iii) Übung.

□

Korollar 11.4 *Eine Primzahl p ist genau dann Summe zweier Quadrate, wenn $p = 2$ oder $p \equiv 1 \pmod{4}$.*

12 Polynomringe

Sei R ein Ring. In diesem Abschnitt wollen wir den Ring der Polynome in n -Variablen mit Koeffizienten in R konstruieren.

12.1 Monome

\mathbf{N}_0 bezeichne die Menge der ganzen Zahlen ≥ 0 . S sei eine endliche Menge. Dann sei $\mathbf{N}_0\langle S \rangle := \{\varphi : S \rightarrow \mathbf{N}_0\}$ und für $\varphi, \psi \in \mathbf{N}_0\langle S \rangle$ sei das Produkt durch

$$(\varphi\psi)(x) := \varphi(x) + \psi(x)$$

erklärt. Für $x \in S$, definieren wir die Funktion $x^i \in \mathbf{N}_0\langle S \rangle$ durch $x^i(x) = i$ und $x^i(y) = 0$ für $y \neq x$. Dann schreibt sich $\varphi \in \mathbf{N}_0\langle S \rangle$ als

$$\varphi = \prod_{x \in S} x^{\nu(x)} \quad \text{für } \nu : S \rightarrow \mathbf{N}_0, \nu = \varphi$$

und es gilt für $\mu, \nu : S \rightarrow \mathbf{N}_0$

$$\left(\prod_{x \in S} x^{\nu(x)} \right) \left(\prod_{x \in S} x^{\mu(x)} \right) = \prod_{x \in S} x^{\nu(x) + \mu(x)} .$$

Für ein $\nu : S \rightarrow \mathbf{N}_0$ definieren wir:

$$M_\nu = \prod_{x \in S} x^{\nu(x)} .$$

Die Ausdrücke M_ν nennen wir primitive Monome. Sie bilden einen Monoid mit dem auf $\mathbf{N}_0\langle S \rangle$ definierten Produkt.

Wir betrachten nun formale Summen der Gestalt

$$\sum_{(\nu)} a_{(\nu)} M_{(\nu)},$$

wobei ν über alle Abbildungen $S \rightarrow \mathbf{N}_0$ läuft, $a_{(\nu)} \in R$ und $a_{(\nu)} = 0$ für alle bis auf endlich viele ν . Die Menge aller solcher Summen bezeichnen wir mit $R[N_0 \langle S \rangle]$. Mit der Addition

$$\sum_{(\nu)} a_{(\nu)} M_{(\nu)} + \sum_{(\nu)} b_{(\nu)} M_{(\nu)} = \sum_{(\nu)} (a_{(\nu)} + b_{(\nu)}) M_{(\nu)}$$

und Multiplikation

$$\left(\sum_{(\nu)} a_{(\nu)} M_{(\nu)} \right) \cdot \left(\sum_{(\nu)} b_{(\nu)} M_{(\nu)} \right) = \sum_{(\nu)} \sum_{(\mu_1)+(\mu_2)=(\nu)} a_{(\mu_1)} b_{(\mu_2)} M_{(\nu)}$$

bildet $R[N\langle S \rangle]$ einen Ring.

Es sei $S = \{X_1, \dots, X_n\}$ die Menge der verschiedenen Symbole X_1, X_2, \dots, X_n . Dann schreiben wir $R[X_1, \dots, X_n]$ für $R[N\langle S \rangle]$. Die Elemente $p \in R[X_1, \dots, X_n]$ sind von der Gestalt

$$p = \sum a_\nu X^\nu = \sum a_\nu X_1^{\nu(1)} \dots X_n^{\nu(n)}.$$

Wir nennen $R[X_1, \dots, X_n]$ den Ring der Polynome in den n -Variablen X_1, \dots, X_n mit Koeffizienten in R .

12.2 Elementare Eigenschaften von Polynomen

i) Polynome als Funktionen auf R^n :

$p = \sum_\nu a_\nu X^\nu \in R[X_1, \dots, X_n]$ definiert eine Funktion $p: R^n \rightarrow R$ durch

$$p(r_1, \dots, r_n) = \sum_\nu a_\nu r_1^{\nu(1)} \dots r_n^{\nu(n)}.$$

ii) $(a_1, \dots, a_n) \in R^n$ definiert einen Ringhomomorphismus

$$R[X_1, \dots, X_n] \rightarrow R$$

(„Einsetzungshomomorphismus“) durch

$$p \mapsto p(a_1, \dots, a_n).$$

iii) Es gibt einen kanonischen Isomorphismus

$$R[X_1, \dots, X_n] \cong R[X_1, \dots, X_{n-1}][X_n],$$

denn wir können durch

$$p(X_1, \dots, X_n) = \sum_j p_j(X_1, \dots, X_{n-1})X_n^j$$

jedes Polynom $p \in R[X_1, \dots, X_n]$ als ein Polynom mit Koeffizienten in $R[X_1, \dots, X_{n-1}]$ auffassen. (Beweis als Übung)

Nach Satz 10.4 folgt aus iii):

Satz 12.1 *R sei ein Integritätsring. Dann ist auch der Polynomring $R[X_1, \dots, X_n]$ ein Integritätsring.*

Wir haben schon gesehen (Satz 10.6), daß der folgende Satz gilt:

Satz 12.2 *Sei K ein Körper, $p \in K[X]$ mit $\text{grad } p = n$. Dann hat p höchstens n Nullstellen.*

Hieraus folgt nun das

Korollar 12.3 *K habe unendlich viele Elemente. Wenn $p \in K[X_1, \dots, X_n]$ die Nullfunktion auf K^n induziert, dann ist $p = 0$.*