Algebraische Strukturen
und
Diskrete Mathematik 1

Günter Törner*

Stand 14.11.2006

Inhaltsverzeichnis

*Dies ist im eigentlichen Sinne keine Vorlesungsausarbeitung, sondern nur das LaTeX-Manuskript einer aus Zeitgründen nicht überarbeiteten Vorlesungsmitschrift. Für Hinweise auf Inkorrektheiten oder Flüchtigkeitsfehler ist der Autor dankbar.

Bei der Erstellung der Vorlesung wurde, nicht an jeder Stelle explizit kenntlich gemacht, auf die folgenden Bücher zurückgegriffen. Der ursprüngliche Vorlesungstext in einer früheren, noch teilweise erkennbaren Version folgte auf weite Strecken dem Text von Biggs [5]. In einer späteren Version wurde Teile aus dem Buch von Aigner [1] eingearbeitet. Historische Hinweise auf Mathematiker/innen sind oft dem Lexikon [14] entnommen.

Literatur

[1] Aigner, M.: *Diskrete Mathematik.* Braunschweig: Vieweg Verlag. 2003.

[2] Artin, M.: *Algebra.* Basel: Birkhäuser. 1993.

[3] Artmann, B.: *Einfhrung in die neuere Algebra.* Gttingen: Vandenhoeck & Ruprecht. 1973.

[4] Beutelspacher, A.; Rosenbaum, U.: *Projektive Geometrie.* Braunschweig: Vieweg. 1992.

[5] Biggs, N.L.: *Discrete Mathematics.* Oxford: Oxford Science Publications. Clarendon Press. 1985.

[6] Cohn, P.M.: *Algebra 1* (Second edition). London: Wiley. 1989.

[7] Dummit, D. S.; Foote, R. M.: *Abstract Algebra.* London: Prentice-Hall International. 1991.

[8] Fischer, G.; Sacher, R.: *Einführung in die Algebra.* Stuttgart: Teubner. 1974.

[9] Lang, S.: *Algebra.* New York: Addison-Wesley.

[10] Kline, M. *Mathematical Thought from Ancient to Modern Times.* New York: Oxford University Press. 1972.

[11] van Lint, J.H. & Wilson, R.M. *A Course in Combinatorics.* Cambridge: Cambridge University Press. 1998.

[12] Schulz, R.-H.: *Codierungstheorie. Eine Einführung.* Braunschweig: Vieweg. 1991.

[13] Waerden, B. L. van: *A History of Algebra.* Berlin: Springer Verlag. 1980.

[14] Spektrum: *Lexikon der Mathematik in sechs Bänden.* Heidelberg: Spektrum Akademischer Verlag. 2000.

1 Die ganzen Zahlen

Wir beginnen diese Vorlesung, indem wir uns zunächst mit einem vertrauten Objekt, den *ganzen Zahlen*[1], beschäftigen. Viele Begriffsbildungen der Algebra wie auch allgemeine Problemstellungen leiten sich von den ganzen Zahlen ab. Für den Zuhörer mag am Anfang der Eindruck entstehen, dass es sich um weitgehend bekannte Inhalte handelt; Ziel ist es allerdings, am konkreten algebraischen Objekt Strukturen deutlich zu machen, die über das Objekt als solche hinausweisen und somit den Blick für Verallgemeinerungen zu weiten.

1.1 Die Arithmetik der ganzen Zahlen

Im Folgenden bezeichnen wir mit $\mathbb{Z}$ die Menge der ganzen Zahlen, über deren Existenz wir hier nicht philosophieren wollen. Sie erscheint uns auch selbstverständlich, weil Mathematiker mit diversen Grundlagenpositionen auf jeden Fall an die *natürlichen Zahlen*[2] $\mathbb{N}$ glauben. Wir postulieren gleichsam die Existenz eines solchen Objektes mit vorgeschriebenen Eigenschaften, die wir als *Axiome* bezeichnen. Umgekehrt können diese Axiome auch als Handlungsanweisungen verstanden werden, ein solches Objekt zu gewinnen. Ob alle sich aus den Axiomen abzuleitenden ergebenden Objekte im Wesentlichen dieselben sind, ob also das Axiomensystem *monomorph* ist, ist eine sich anschließende Frage.

Die Vorgabe von Axiomen in der Mathematik erfolgt zumeist nicht willkürlich. Wir orientieren uns selbstverständlich an den uns naiv vertrauten Eigenschaften vom Rechnen mit den ganzen Zahlen. In jenem $\mathbb{Z}$ sind bekanntlich zwei *Verknüpfungen*[3] $+$ bzw. $\cdot$ definiert. Schreibtechnisch ist es vielfach hilfreich, den Multiplikationspunkt wegzulassen. Die uns vertrauten Eigenschaften der ganzen Zahlen stellen wir zusammen; dabei bezeichnen a, b, c beliebige Zahlen und 0 bzw. 1 speziell zu beschreibende Objekte:

I1. Auf $\mathbb{Z}$ sind zwei Verknüpfungen erklärt, eine Addition $+$ und eine Multiplikationen $\cdot$, d.h. es gelten $a + b$, $a \cdot b \in \mathbb{Z}$ für alle $a, b \in \mathbb{Z}$.

I2. Addition und Multiplikation auf $\mathbb{Z}$ sind *kommutativ*, d.h. für alle $a, b \in \mathbb{Z}$ gelten $a + b = b + a$ und $ab = ba$.

I3. Addition und Multiplikation genügen *Assoziativgesetzen*, d.h. $(a+b)+c = a+(b+c)$, $(ab)c = a(bc)$ für alle Elemente $a, b, c \in \mathbb{Z}$.

I4. Es existieren *neutrale Elemente* der Addition und Multiplikation, nämlich $a + 0 = 0 + a = a, a \cdot 1 = 1 \cdot a = a$ für alle $a \in \mathbb{Z}$.

I5. Addition und Multiplikation sind durch *Distributivgesetze* verschränkt, d.h. $a(b+c) = ab+ac$ für alle $a, b, c \in \mathbb{Z}$.

I6. Für jedes $a \in \mathbb{Z}$ gibt es genau eine Zahl $-a \in \mathbb{Z}$ mit $a + (-a) = 0$. (Existenz von inversen Elementen bei der Addition)

I7. Ist $a \neq 0$, so folgt aus $ab = ac$ stets $b = c$. (Nullteilerfreiheit)

Diese uns vertrauten Eigenschaften von $\mathbb{Z}$ weisen über diese Menge hinaus. Wir definieren:

Definition 1.1 *Eine Menge R, auf der zwei Verknüpfungen $+$ und $\cdot$ definiert sind, also eine Struktur $(R, +, \cdot)$ mit den Regel* **I1.** *bis* **I7.** *bezeichnet man als einen kommutativen, nullteilerfreien Ring.*

Somit bildet die Menge $(\mathbb{Z}, +, \cdot)$ einen kommutativen Ring. Im Kapitel 8 werden wir ausführlicher Ringe kennenlernen und ihre Eigenschaften studieren.

[1] im Englischen: integer
[2] im Englischen: natural numbers
[3] Eine Verknüpfung $*$ auf einer Menge M ist eine Abbildung von $M \times M$ in die Menge M.

Bemerkungen 1.2 1. *Es soll nicht detailliert auf Feinheiten des Regelsystems eingegangen werden: In* **I6.** *wird die Existenz eines inversen Elements bezüglich der Addition gefordert; daraus lässt sich eine weitere Verknüpfung, nämlich die* Subtraktion *ableiten, in dem wir setzen* $a - b = a + (-b)$. 2. *Mit Rückbezug auf die obigen Axiome folgt: Es gilt für* $m, n \in \mathbb{Z}$ *stets*

$$m - (-n) = m + n.$$

1.2 Die Anordnung in den ganzen Zahlen

Die obigen Axiome regeln gleichsam die *arithmetischen Eigenschaften* von $\mathbb{Z}$. Ebenfalls bedeutsam ist die Anordnung oder lineare Ordnung der Elemente dieses Zahlenbereichs. Diese lineare Ordnung der ganzen Zahlen nehmen wir zum Anlass, den Anordnungsbegriff algebraisch zu fundieren.

Eine *lineare Ordnung* $\leq$ auf $\mathbb{Z}$ ist eine Relation[4] mit der Eigenschaft: Für Elemente $a, b \in \mathbb{Z}$ gelten stets: $a \leq b$ oder $b \leq a$. Diese Relation in $\mathbb{Z} \times \mathbb{Z}$ genügt den folgenden Axiomen, wobei wie oben a, b, c beliebige Elemente aus $\mathbb{Z}$ bezeichnen:

I8. (Reflexivität) $a \leq a$

I9. (Antisymmetrie) $a \leq b$ und $b \leq a$ impliziert $a = b$.

I10. (Transitivität) $a \leq b$ und $b \leq c$ impliziert $a \leq c$.

I11. (Monotoniegesetz der Addition) $a \leq b$ impliziert $a + c \leq b + c$.

I12. (Monotoniegesetz der Multiplikation) $a \leq b$ und $0 \leq c$ impliziert $ac \leq bc$.

Elemente, die größer als 0 sind, nennen wir sinngemäß *positiv*, solche die kleiner als 0 sind, entsprechend *negativ*. Es ist eine leichte Aufgabe, die Vorzeichenregel nachzuweisen: das Produkt zweier negativer Elemente ist positiv, das Produkt eines positiven und eines negativen Elementes ist negativ usw. Insbesondere gilt $0 < 1$, wobei wir das strikte Kleiner-Zeichen verwenden, wenn Gleichheit ausgeschlossen ist.

Insofern ist auch naheliegend, was wir in unserer axiomatischen Charakterisierung unter *natürlichen Zahlen* verstehen wollen: $\mathbb{N} = \{n \in \mathbb{Z} \mid 1 \leq n\}$ bzw. $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Allgemeiner:

Definition 1.3 *Ein Ring* $(R, +, \cdot, \leq)$ *heißt* angeordnet[5]*, falls eine lineare Ordnung* $\leq$ *auf* R *definiert ist, die reflexiv, antisymmetrisch und transitiv ist und dabei den Monotoniegesetzen der Addition und Multiplikation genügt.*

In dieser Sprechweise ist also $(\mathbb{Z}, +, \cdot, \leq)$ ein angeordneter Ring.

Um weitere Aussagen formulieren zu können, benötigen wir die folgende Begriffsbildung. Es sei $X \subseteq \mathbb{Z}$ eine Teilmenge. Dann heißt b eine *untere Schranke*[6] von X, falls $b \leq x$ für alle $x \in X$ gilt. Ist die untere Schranke selbst Element der Menge, so sprechen wir von einer *unteren Grenze*[7]. Damit ergibt sich als abschließendes Axiom für $\mathbb{Z}$:

I13. Jede nichtleere Teilmenge von $\mathbb{Z}$, die eine untere Schranke besitzt, enthält eine untere Grenze, d.h. ein kleinstes Element.

Die Eigenschaft **I13.** wird auch als *Wohlordnungsaxiom* für $\mathbb{Z}$ bezeichnet. Allgemeiner: Eine linear geordnete Menge M, die das Axiom **I13.** erfüllt, heißt wohlgeordnet.

Das Fordern der Wohlordnungseigenschaft für $\mathbb{Z}$ hat weitreichende Konsequenzen, die uns zwar selbstverständlich erscheinen, gerade sich über dieses Axiom begründen. Wir formulieren diese Beobachtung als ein Lemma.

[4] Eine Relation R auf einer Menge M ist eine Teilmenge R des kartesischen Produktes $M \times M$.

[5] Wir verweisen auf das klassische Buch von Fuchs, L. 1966. *Teilweise geordnete algebraische Strukturen.* Göttingen: Vandenhoeck & Ruprecht.

[6] Im Englischen: lower bound

[7] Im Englischen: least member

Lemma 1.4 *Es gibt keine ganze Zahl $x \in \mathbb{Z}$, die größer ist als alle durch fortgesetzte Addition von* 1 *entstehenden Zahlen*[8] *ist.*

Beweis: Unterstellen wir nun die Existenz eines solchen Elements x. Dann wären die additiven Inversen dieser Zahlen, also $-\langle 1\rangle$, eine durch $-x$ nach unten beschränkte Teilmenge von $\mathbb{Z}$, die aufgrund des Wohlordnungsaxioms ein kleinstes Element $y_0 = -x_0$ besitzen würde. Das additiv Inverse dieses Elementes, nämlich x_0, wäre gleichsam eine 'größte' natürliche Zahl; eine solche Zahl kann es nicht geben, da mit n auch stets $n+1$ in $\mathbb{N}$ liegen muss, was unsere Annahme widerlegt. Mithin ist jedes Element aus $\mathbb{N}$ eine endliche Summe von 1, d.h. $\mathbb{N} = \langle 1\rangle$. ∎

Eine weitere Konsequenz ist offensichtlich: die durch die Axiome **I.1** - **I.13** beschriebene Struktur ist eindeutig, m.a.W. alle Ringe, die diese Eigenschaften erfüllen, sind strukturgleich. Damit haben wir die intuitiv verstandene Menge $\mathbb{Z}$ axiomatisch fundiert.

Dieses Wohlordnungsaxiom gestattet zwei weitere unmittelbare Anwendungen, nämlich Objekte in $\mathbb{Z}$ *rekursiv zu definieren* und bei Aussagen über $\mathbb{N}$ das Beweisprinzip der *vollständigen Induktion* zu bemühen.

Bei der Rekursion führt man zu berechnende, mit $\mathbb{N}$ oder $\mathbb{Z}$ indizierte Grössen auf Daten mit kleinerem Index zurück. Der Grundgedanke lässt sich dann wie folgt beschreiben: Sei U die Menge der Indizes aus $\mathbb{N}$, für die die Werte (noch) unbekannt sind. Da diese Menge (unter schwachen weiteren Voraussetzungen) ein kleinstes Element besitzt, das sich selbst auf bekannte kleinere Indizes bezieht, ist insgesamt eine Ermittlung sichergestellt, d.h. die Rekursion greift.

Beispiel 1.5 (aus Duden: Informatik, S. 496) (1) Collatz-Funktion $c : \mathbb{N} \longrightarrow \mathbb{N}_0$:

(a) $c(1) = 0$,

(b) $c(n) = \begin{cases} 1 + c\left(\frac{n}{2}\right) & n \text{ gerade} \\ 1 + c(3n+1), & n \text{ ungerade} \end{cases}$

(2) McCarthy 91 - Funktion

$mc : \mathbb{N} \longrightarrow \mathbb{N}$: (a) $mc(n) = n - 10$ für $n > 100$, (b) $mc(n) = mc(mc(n+11))$ sonst.

Die Collatz-Funktion besitzt beispielsweise die Funktionswerte: $c(2) = 1, c(3) = 7, c(4) = 2, \ldots,$ $c(27) = 111$. Bei der McCarthy-91-Funktion tritt die Funktion darüber hinaus zugleich als eigenes Argument auf.

Das hinlänglich bekannte Induktionsprinzip formuliert sich dann auf der axiomatisch beschriebenen Menge $\mathbb{N}$ wie folgt als Satz:

Satz 1.6 *Es sei S eine Teilmenge von $\mathbb{N}$, die die folgenden Aussagen erfüllt:*

(i) $1 \in S$.

(ii) *Für jedes $k \in \mathbb{N}$ folgt mit $k \in S$ stets $k + 1 \in S$.*

Dann gilt $S = \mathbb{N}$.

Beweis: Wir nehmen an: $S \neq \mathbb{N}$. Es sei $\overline{S} = \{r \in \mathbb{N} \mid r \notin S\}$ die nichtleere Komplementmenge. Folglich hat $\overline{S}$ ein kleinstes Element m, das wegen (i) sicher von 1 verschieden ist. Nun ist $m - 1 \in \mathbb{N} \cap S$, mit (ii) also auch $m \in S$, was unserer Annahme widerspricht. ∎

Es gibt Modifikationen dieses Induktionsprinzips: ohne Gefahr kann man die Aussage des obigen Satzes auch für $\mathbb{N}_0$ formulieren. Eine weitere Variante besteht darin, die Aussage (ii) von der Tatsache abhängig zu machen, dass alle $k' \leq k$ in S angenommen werden.

[8] Mit anderen Worten: das von 1 erzeugte additive Monoid $\langle 1\rangle$

1.3 Division mit Rest

Wir werden nun einen Satz formulieren, der im Weiteren oftmals, zum Teil ohne Referenz, benutzt werden wird.

Proposition 1.7 (Division mit Rest) *Für beliebige ganze Zahlen $a, b \in \mathbb{Z}$ mit $b \in \mathbb{N}$ gibt es eindeutig bestimmte ganze Zahlen $q, r \in \mathbb{Z}$, so dass gilt:*

$$a = bq + r \text{ und } 0 \leq r < b.$$

Beweis: Wir wenden das Wohlordnungsaxiom wie folgt an: Es sei

$$R = \{x \in \mathbb{N}_0 \mid a = by + x \text{ für ein } y \in \mathbb{Z}\}.$$

Wegen $a = b \cdot 0 + a$, falls $a \geq 0$ bzw. $a = ba + (1-b)a$ für $a < 0$ ist $a \in R$ bzw. $(1-b)a \in R$, also ist R nicht leer. R hat als Teilmenge von $\mathbb{N}_0$ somit ein kleinstes Element r. Es gibt nun ein $q \in \mathbb{Z}$ mit $a = bq + r$. Überdies folgt aus $a = bq + r$ auch $a = b(q+1) + (r-b)$, so dass, falls $r \geq b$ angenommen wird, auch $r - b \in R$ folgt. Nun ist aber $r - b < r$. Da nach Annahme r kleinstes Element in R ist, folgt schließlich $r < b$.

Es bleibt noch die Eindeutigkeit von q, r nachzuweisen. Sei

$$a = bq' + r' \text{ und } 0 \leq r' < b.$$

O.B.d.A. kann $q' \leq q$ vorausgesetzt werden. Wäre $q' < q$, also $q - q' \geq 1$, so ergibt sich

$$r' = a - bq' = (a - bq) + b(q - q') \geq r + b.$$

Wegen $r + b \geq b$ muss unsere Annahme verworfen werden, also gilt $q = q'$ und somit $a - bq = a - bq'$, mithin auch $r = r'$. ∎

Wir wenden nun diese Aussage auf folgende Situation an. Es sei $t \geq 2$ eine natürliche Zahl und $x \geq 0$ beliebig. Fortgesetzte Anwendung der Proposition 1.7 liefert

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ &\vdots \quad\quad \vdots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n. \end{aligned}$$

Hierbei ist jeder Rest r_i eine der Zahlen $0, 1, \ldots, t-1$, und der Algorithmus bricht ab, falls $q_n = 0$ ist. Zurückrechnen liefert

$$x = r_n t^n + r_{n-1} t^{n-1} + \cdots + r_1 t + r_0,$$

was eine Darstellung bezüglich der Basis t liefert.

1.4 Teilbarkeit und größter gemeinsamer Teiler

Definition 1.8 *Es seien $x, y \in \mathbb{Z}$. Die ganze Zahl y heißt* Teiler der Zahl *x, in Zeichen $y \mid x$, wenn es ein $q \in \mathbb{Z}$ mit $x = yq$ gibt. Anders betrachtet ist dann x ein Vielfaches von y.*

Man beachte, dass im Falle von $y \mid x$ die Schreibweise $\dfrac{x}{y}$ sinnvoll ist. Die Zahlen 1 bzw. x heißen *triviale Teiler*. Überdies erfüllt die Teilbarkeitsrelation die Bedingungen **I8.** bis **I10.**.

Ohne Beweis vermerken wir:

Lemma 1.9 *Für die nachstehend genannten Elemente aus $\mathbb{Z}$ gelten die folgenden Aussagen:*

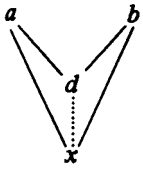

Abbildung 1: $\mathrm{ggT}\,(a,b) = d$

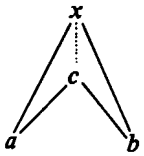

Abbildung 2: $\mathrm{kgV}\,(a,b) = d$

(i) $1 \mid a$ *und* $a \mid a$.

(ii) $c \mid b$ *und* $b \mid a$ *impliziert* $c \mid a$.

(iii) $b \mid a_1, \ldots, a_n$ *impliziert* $b \mid (x_1a_1 + \cdots + x_na_n)$.

(iv) $b \mid 1$ *impliziert* $b \in \{1, -1\}$.

(v) *Es gelte* $d \mid n$ *und* $c \mid \dfrac{n}{d}$. *Dann gilt* $c \mid n$ *und* $d \mid \dfrac{n}{c}$.

Definition 1.10 *Es seien* $a, b, d \in \mathbb{Z}$ *derart, dass die folgenden Aussagen gelten:*

(i) $d \mid a$ *und* $d \mid b$*;*

(ii) *Für alle* $x \in \mathbb{Z}$ *folgt aus* $x \mid a$ *und* $x \mid b$ *stets* $x \mid d$.

Dann heißt $d \in \mathbb{Z}$ *ein größter gemeinsamer Teiler (greatest common divisor) von* a *und* b*, in Zeichen* $ggT(a, b)$.

Das Diagramm in Abbildung 1, das wir dem Buch von [3] entnommen haben, zeigt die funktionale Abhängigkeit der Variablen in dieser Definition im Teilergraph von $\mathbb{N}$.

In dualer Weise erhält man durch 'Spiegelung' an der Horizontalen den Begriff eines *kleinsten gemeinsamen Vielfaches* (kgV). Wir verweisen auf das Diagramm in der Abbildung 2.

Die formale Definition lautet demzufolge:

Definition 1.11 *Es seien* $a, b, c \in \mathbb{Z}$ *derart, dass die folgenden Aussagen gelten:*

(i) $a \mid c$ *und* $b \mid c$*;*

(ii) *Für alle* $x \in \mathbb{Z}$ *folgt aus* $a \mid x$ *und* $b \mid x$ *stets* $c \mid x$.

Dann heißt $c \in \mathbb{Z}$ *ein kleinstes gemeinsames Vielfaches (least common multiple) von* a *und* b*, in Zeichen* $kgV(a, b)$.

Proposition 1.12 *Es seien* $a, b \in \mathbb{Z}$. *Dann gelten:*

(i) *Für je zwei ganze Zahlen existiert ein größter gemeinsamer Teiler.*

(ii) *Der größte gemeinsame Teiler ist bis auf den Faktor* (-1) *eindeutig festgelegt.*

(iii) *Ist* d *ein größter gemeinsamer Teiler von* a, b*, so gibt es Zahlen* $m, n \in \mathbb{Z}$ *mit*

$$d = ma + nb.$$

Beweis: (i) Wir führen den Existenzbeweis durch die Angabe eines konstruktiven Algorithmus. Dieses Verfahren ist in der Literatur als *Euklid-scher Algorithmus* bekannt. Nach Proposition 1.7 gibt es ganze Zahlen q_1, r_1 mit

$$a = q_1 b + r_1 \text{ mit } 0 \leq r_1 < b.$$

Wir zeigen $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r_1)$.

Es sei d ein gemeinsamer Teiler von a, b. Wegen $r_1 = a - bq_1$ teilt d auch r_1 und ist insofern auch gemeinsamer Teiler von b und r_1.

Ist umgekehrt d ein Teiler von b und r_1, so teilt d auch die Zahl $a = bq_1 + r_1$. Mithin ist jeder gemeinsamer Teiler von b, r_1 auch ein gemeinsamer Teiler von a und b, d.h. die entsprechenden Teilermengen beider Paare stimmen überein, weshalb sie gleiche größte gemeinsame Teiler haben, kurz

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r_1).$$

Diese Argumentation wenden wir auf die nächsten Herleitungsschritte an:

$$\begin{array}{lcll} a & = & bq_1 + r_1 & (0 \leq r_1 < b) \\ b & = & r_1 q_2 + r_2 & (0 \leq r_2 < r_1) \\ r_1 & = & r_2 q_3 + r_3 & (0 \leq r_3 < r_2) \end{array}$$

Es ist klar, dass dieser Algorithmus abbricht; somit lauten die letzten Schritte:

$$\begin{array}{lcll} r_{k-4} & = & r_{k-3} q_{k-2} + r_{k-2} & (0 \leq r_{k-2} < r_{k-3}) \\ r_{k-3} & = & r_{k-2} q_{k-1} + r_{k-1} & (0 \leq r_{k-1} < r_{k-2}) \\ r_{k-2} & = & r_{k-1} q_k & \end{array}$$

Es folgt, dass $r_{k-1} = \mathrm{ggT}(r_{k-2}, r_{k-1}) = \cdots = \mathrm{ggT}(a, b)$ gilt. Mithin existiert ein größter gemeinsamer Teiler für die Elemente a, b.

(ii) Seien d, d' größte gemeinsame Teiler von a und b, was bedeutet $d \mid d'$ und $d' \mid d$. Daraus ergibt sich, dass sich d und d' höchstens um einen Faktor (-1) unterscheiden.

(iii) Wie in (i) belegt wurde, ist $d = r_{k-1}$. Daraus folgt $r_{k-1} = r_{k-3} - r_{k-2} q_{k-1}$. Also lässt sich d in der Form $m' r_{k-2} + n' r_{k-3}$ schreiben, wobei $m' = -q_{k-1}$ und $n' = 1$ ist. Den Faktor r_{k-2} ersetzen wir durch einen linearen Term in Abhängigkeit von r_{k-3} und r_{k-4} usw. ∎

Beschränkt man sich auf natürliche Zahlen, so ist $\mathrm{ggT}(a, b)$ ein Kennzeichnungsterm.

Der folgende Sonderfall führt zu einer eigenen Bezeichnungsweise.

Definition 1.13 *Natürliche Zahlen* a, b *heißen* coprim *oder auch* relativ prim*, wenn* $ggT(a, b) = 1$ *gilt.*

Wir erwähnen noch folgendes Lemma:

Lemma 1.14 *Es seien* a, b, a', b' *natürliche Zahlen mit*

(i) $ab' = a'b$*,*

(ii) $ggT(a, b) = ggT(a', b')$*.*

Dann folgt $a = a'$ *und* $b = b'$*.*

Beweis: Es ist leicht einzusehen, dass man sich auf den Fall $\mathrm{ggT}(a,b) = 1$ beschränken kann. Wegen $\mathrm{ggT}(a,b) = 1$ gibt es ganze Zahlen m und n mit $ma + nb = 1$. Folglich ergibt sich

$$b' = (ma + nb)b' = mab' + nbb' = ma'b + nbb' = (ma' + nb')b$$

und daher $b \mid b'$. Unter analogen Argumenten folgt $b' \mid b$. Also ist $b = b'$ oder $b = -b'$. Da aber b, b' natürliche Zahlen sind, ergibt sich die Behauptung im Falle $ggT(a,b) = 1$. Den allgemeinen Fall führt man ohne weiteres auf die spezielle Situation zurück. ∎

Schließlich erwähnen wir ohne Beweis:

Lemma 1.15 *Es seien $a, b \in \mathbb{N}$. Dann gilt $ggT(a,b) \cdot kgV(a,b) = a \cdot b$.*

Die Anzahl der zu einer natürlichen Zahl n relativ primen (teilerfremden) Zahlen interessierte schon von je her die Mathematiker und hat Anlass zur Definition der Euler'schen[9] ϕ-Funktion gegeben.

[9] Euler, Leonhard, Mathematiker und Physiker, geb. 15.4.1707 Basel, gest. 18.9.1783 St. Petersburg.

Euler wurde als Sohn eines Pfarrers geboren. Beide Eltern waren sehr gebildet und mit mehreren bedeutenden Mathematikern freundschaftlich verbunden. Euler wurde zunächst von seinem Vater unterrichtet, später besuchte er die Lateinschule und erhielt, als der Vater sein mathematisches Talent erkannt hatte, von Johann I Bernoulli ((Stichwort) Bernoulli-Familie) mathematische Unterweisungen zusammen mit dessen Söhnen Daniel und Niklas.

Im Herbst 1720 begann Euler sein Studium an der philosophischen Fakultät der Universität Basel 1723 an der theologischen Fakultät, widmete sich dann aber verstärkt der Mathematik. 1727 ging er nach St. Petersburg, wo Daniel und Niklas Bernulli an der Akademie tätig waren. 1730 wurde er dort Professor für Physik und drei Jahre später Professor für Mathematik. Damit begann eine erste erfolgreiche Schaffensperiode im Leben Eulers.

Innenpolitische Unsicherheiten veranlassten ihn, 1741 einen Ruf an die Berliner Akademie anzunehmen. Ab 1746 war er dort Direktor der mathematischen Klasse und leitete faktisch nach dem Tod des Akademiepräsidenten de Maupertuis die Akademie. Zunehmende Differenzen mit dem König von Preußen bewogen Euler, seine Entlassung zu betreiben und 1766 wieder nach Petersburg zurückzukehren. Noch 1766 erblindete Euler, trotzdem war er, unterstützt von seinem Sohn und von Fuß, bis zu seinem Tod schöpferisch tätig.

Euler hat wohl wie kein zweiter Gelehrter die Mathematik und die mathematischen Naturwissenschaften des 18. Jahrhunderts beeinflusst. Seine umfangreichen Schriften reichen von den verschiedenen Teilgebieten der Mathematik, über die Hydromechanik und die Astronomie bis zur Physik, und schließen dabei Geodäsie, Kartographie und Navigation ebenso ein, wie die Theorie der Turbinen und die Schiffswissenschaften. Mit mehr als 850 Veröffentlichungen zählt Euler zu den produktivsten Mathematikern aller Zeiten.

Euler war ein typischer Geometer des 18. Jahrhunderts, der neben der mathematischen Theorie auch stets die Anwendungen im Blick hatte. Viele seiner mathematischen Methoden entwickelte er zur Lösung von Problemen der Mechanik. Astronomie, Geodäsie oder Physik. Dabei strebte er stets danach, das vorgelegte Problem mathematisch zu erfassen, und scheute sich nicht, über die eigentliche Fragestellung hinaus weitergehende theoretische Überlegungen durchzuführen.

Den ersten Platz in `Eulers` mathematischen Schaffen nimmt die (Stichwort) Analysis ein. Mit den Lehrbüchern zur Analysis des Unendlichen (1748), zur Differential- (1755) und Integralrechnung (1768-70) gab er eine erste systematische Darstellung der Theorie, wobei er viele heute übliche Begriffe und Bezeichnungen einführte. Dazu gehörten u. a. die Bezeichnung für die trigonometrischen Funktionen, die Schreibweise $f(x)$ für eine Funktion der Veränderlichen x, die Buchstaben (Stichwort) e ür die Basis der natürlichen Logarithmen und i für die imaginäre Einheit, sowie das Summenzeichen $\sum$

Ausgehend von einem gründlichen Studium der Funktionen formulierte er eine klare Definition des Funktionsbegriffs und entwickelte die Analysis als eine Lehr von den Funktionen, rückte den Funktionsbegriff also in den Mittelpunkt der Betrachtungen. Wichtigstes Mittel zur Darstellung und Untersuchung von Funktionen waren Potenzreihen. So stellte er die Potenzreihenentwicklung für die elementaren Funktionen auf und leitete durch z. T. virtuoses Rechnen mit den Reihen wichtige Eigenschaften der Funktionen und Beziehungen zwischen ihnen ab, etwa die nach ihm benannte Relation $e^{ic} = \cos c + i \sin c$ (1743). Man muss jedoch beachten, dass die Mathematiker des 18. Jahrhunderts, auch Euler, zwar zwischen konvergenten und divergenten Reihen unterschieden, aber keine allgemeine Grenzwerttheorie besaßen und durch teilweise intuitiven Gebrauch divergenter Reihen richtige Ergebnisse erzielten.

Als weitere Formen zur Darstellung von Funktionen benutzte Euler auch unendliche Produkte und Reihen von Partialbrüchen, Verfahren, die im 19. Jahrhundert wesentlich weiterentwickelt wurden. Doch Euler hat auch die Kenntnisse über transzendente Funktionen wesentlich bereichert. Die von ihm analysierten Beta- und Γ-Funktionen ((Stichwort) Eulersche Γ-Funktion), die ζ-Funktion und die heute als Bessel-Funktion bekannten Funktionen gehören zu den wichtigsten transzendenten Funktionen. Von allen enthüllte Euler zahlreiche Eigenschaften und wurde einer der Begründer des Studiums spezieller Funktionen.

Verschiedene Fragestellungen führten Euler zur Betrachtung komplexer Zahlen. Etwa zeitgleich mit d' Alembert, aber unabhängig von diesem, gab er mehrere Anwendungen der Funktionen einer komplexen Variablen und kam zu ersten Ergebnissen über analytische Funktionen. Doch obwohl er geschickt mit verschiedenen Darstellungen komplexer Zahlen umging, sah er in den imaginären Zahlen nur eine formale Bildung zur Vereinfachung der Rechnungen ohne reale Bedeutung. Wie d'Alembert folgerte er (in moderner Terminologie formuliert) die algebraische Abgeschlossenheit der Menge der komplexen Zahlen (1751) und leitete die Cauchy-Riemannschen Differentialgleichungen ab. Beide Mathematiker formulierten und bewiesen auch den Fundamentalsatz der Algebra, die Beweise waren jedoch noch

Definition 1.16 *Es sei n eine natürliche Zahl. Dann bezeichnet $\phi(n) = |\{k \in \mathbb{N}|\ ggT(n,k) = 1\}|$ die Anzahl der zu n relativ primen natürlichen Zahlen.*

Unmittelbar ergibt sich:

$$n \text{ ist prim } \Leftrightarrow \phi(n) = n - 1$$

.

Proposition 1.17 *Für jede natürliche Zahl $n \in \mathbb{N}$ gilt:*

$$\sum_{d|n} \phi(d) = n.$$

Beweis: Es bezeichne S die Menge der Paare von natürlichen Zahlen (d, f) mit

$$d \mid n, \qquad 1 \leq f \leq d, \qquad \text{ggT}(f, d) = 1.$$

Stellt man die zu S gehörigen Paare in einer Matrixtabelle dar, so stehen in einer Zeile, d.h. bei festem d, genau $\phi(d)$ Einträge, also gilt

$$|S| = \sum_{d|n} \phi(d).$$

Es bleibt zu zeigen, dass $|S| = n$. Also haben wir eine Bijektion β von S nach $\mathbb{N}_n$ anzugeben. Wir definieren

$$\beta(d, f) = fn/d.$$

Da n/d ganzzahlig und $1 \leq f \leq d$ ist, ist $\beta(d, f) \in \mathbb{N}_n$. Wir zeigen, dass β injektiv ist:

$$\beta(d, f) = \beta(d', f') \Longrightarrow fn/d = f'n/d' \quad \Longrightarrow \quad fd' = f'd.$$

Aus der Tatsache, dass jeweils d, f bzw. d', f' relativ prim sind, folgt $d = d'$ und $f = f'$ (vgl. Lemma 1.14).

Es bleibt zu zeigen, dass β eine surjektive Abbildung ist. Es sei $x \in \mathbb{N}_n$ und g_x der größte gemeinsame Teiler von x und n. Sei ferner

$$d_x = n/g_x, \quad f_x = x/g_x.$$

Man sieht nun wieder ein, dass $\beta(d_x, f_x) = f_x n/d_x = x$ gilt, folglich ist β surjektiv. ∎

1.5 Faktorisierung in Primzahlen

Definition 1.18 *Eine natürliche Zahl p heißt* prim *oder auch* Primzahl*, falls $p \geq 2$ und p nur triviale Teiler besitzt*[10].

Zur Vorbereitung des Hauptsatzes der elementaren Zahlentheorie beweisen wir:

---

lückenhaft.

Grundlegende Fortschritte gelangen Euler bei der Lösung von Differentialgleichungen. So löste er homogene lineare Differentialgleichungen mit konstanten Koeffizienten mit Hilfe des Ansatzes $y = e^{\lambda}$, und die zugehörige inhomogene Gleichung mit der Methode des integrierten Faktors. Er formulierte notwendige Bedingungen für die Existenz eines totalen Differentials und schuf 1768 mit seiner Polygonzugmethode ein Verfahren zur numersichen Lösung der Gleichung $y' = f(x, y)$ bei vorgegebenen Anfangswerten $y(x_0) = y_0$, das er dann auf Gleichungen zweiter Ordnung ausdehnte. Auch die Methode der Variation der Konstanten findet sich in Ansätzen bei Euler (1741).

Umfangreiche Forschungen führte er zur Theorie der partiellen Differentialgleichungen durch, meist verbunden mit der Untersuchung physikalischer Probleme. Eine für die Mathematikentwicklung äußerst anregende Frage war die Untersuchung der schwingenden Saite. Bezüglich der Lösung der zugehörigen Differentialgleichung kam es zu einem längeren Streit zwischen Euler, `d'Alembert` und D. `Bernoulli`, aus dem sich letztlich das Problem herauskristallisierte, welche Funktionen durch trigonometrische Reihen darstellbar sind.

[10] Diese Eigenschaft spielt in der Ringtheorie als Irreduzibilitätskriterium eine Rolle.

Lemma 1.19 *Ist p eine Primzahl und sind $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, so folgt aus*

$$p \mid x_1 x_2 \ldots x_n$$

stets $p \mid x_i$ für wenigstens ein x_i $(1 \leq i \leq n)$.

Beweis: Wir beweisen diese Aussage durch Induktion über die Anzahl der Faktoren des Produktes. Im Falle $n = 1$ sind wir fertig. Wir nehmen also an, dass die Aussage richtig ist für $n = k$. Sei nun $x = x_1 x_2 \ldots x_k$ und $p \mid x x_{k+1}$. Teilt nun p die Zahl x, so sind wir fertig. Teilt allerdings p nicht das Element x, so ist der größte gemeinsame Teiler von x und p gleich 1, d.h. es gibt $r, s \in \mathbb{Z}$ mit $rp + sx = 1$. Also ist

$$x_{k+1} = (rp + sx)x_{k+1} = (rx_{k+1})p + s(xx_{k+1}),$$

und da p beide Faktoren teilt, folgt $p \mid x_{k+1}$, was den Induktionsschritt rechtfertigt. ∎

Die nächste Aussage bezeichnet man gelegentlich als den *Hauptsatz der elementaren Zahlentheorie*. Diesen Satz findet man schon bei Euklid von Alexandria[11] .

Satz 1.20 *Jede natürliche Zahl $n \geq 2$ besitzt eine eindeutige Primfaktorzerlegung.*

Beweis: Wäre diese Aussage nicht richtig, so gäbe es ein kleinstes Gegenbeispiel n_0. Dann kann n_0 selbst keine Primzahl sein. Also können wir ansetzen

$$n_0 = p_1 p_2 \ldots p_k \text{ und } n_0 = p_1' p_2' \ldots p_l',$$

wobei p_i und p_i' nicht notwendig verschiedene Primzahlen sind. Aus $p_1 \mid n_0$ folgt $p_1 \mid p_1' p_2' \ldots p_l'$, also mit Lemma 1.19 o.B.d.A. $p_1 \mid p_1'$. Da beide Elemente prim sind, folgt $p_1 = p_1'$. Somit lässt sich auf beiden Seiten p_1 kürzen. Da n_0 das kleinste Gegenbeispiel war, gilt für n_0/p_1 die Aussage des Satzes, was zu einem Widerspruch führt. ∎

Der Vollständigkeit halber erwähnen wir hier bereits, obgleich die formale Begriffsdefinition, was man unter einer unendlichen Menge versteht, erst endgültig in Kapitel 2 festgelegt wird:

Satz 1.21 *Die Menge $\mathbb{P}$ der Primzahlen ist unendlich.*

Beweis: Natürlich ist P nicht leer, da $2 \in P$ gilt. Wäre P endlich, so seien $p_1, p_2 \ldots, p_n$ alle Primzahlen. Wir werden zeigen, dass es dann weitere Primzahlen geben muss, was einen Widerspruch zur Annahme liefert.

Wir betrachten die Zahl

$$m = p_1 p_2 \ldots p_n + 1.$$

[11] Euklid von Alexandria, Mathematiker, lebte um 300 v. Chr.

Über die Person des Euklid und dessen Leben ist fast nichts bekannt. Was man über ihn weiß, sind Anekdoten aus der Spätantike oder sind Schlussfolgerungen aus seinem Werk. Man nimmt an, dass er seine Jugend in Athen verbracht hat. Um 307 v. Chr. Wurde das Museion in Alexandria gegründet und man vermutet, dass Euklid, wohl schon als angesehener Gelehrter, um 320 auf Einladung der Ptolomäerdynastie nach Alexandria kam. In Alexandria sind die Werke des Euklid entstanden, möglicherweise für den Lehrbetrieb am Museion. Zwischen 290 und 260 v. Chr. Ist Euklid in Alexandria (?) gestorben.

Euklid sind sieben mathematische Werke, eine astronomische, eine optische und eine musiktheoretische Schrift zuzuschreiben. Oft wurde er noch als Verfasser einer Schrift über Spiegel und von Abhandlungen über Mechanik benannt, beides möglicherweise unrichtig. Die 'Optika' ist ein elementares Werk über Perspektive. Die astronomische Schrift ('Phainomena') behandelt die Geometrie der Bewegung der Himmelsköper und enthält vielleicht die Meinung des Eudoxos zur Himmelsmechanik.

Das erste grosse Verdienst des Euklid bestand in der Zusammenstellung wichtigen historischen mathematischen Materials. Diese Materialzusammenstellung war bei ihm keine unkritische Aneinanderreihung erreichter Ergebnisse, sondern er hat das Material systematisch bearbeitet. Er präsentierte es in Form von Definitionen, Axiomen, Postulaten, Sätzen, Aufgaben und Beweisen. Hierin liegt wohl das Hauptverdienst des Euklid und der Höhepunkt der Mathematik der frühen Kulturen.

Man darf allerdings an den deduktiven Aufbau gerade der 'Elemente' nicht die Messlatte moderner Mathematik anlegen. Eine Reihe von 'Definitionen' des Euklid sind 'nicht zur Sache gehörig' - man kann mit ihnen nichts beweisen. Desgleichen entspricht die Unterscheidung von Axiomen und Postulaten - durchaus nicht modernen Ansprüchen.

Keine der Primzahlen $p_1, p_2, \ldots, p_n$ teilt m; auf der anderen Seite wissen wir aber, dass m eine eindeutige Zerlegung in Primfaktoren besitzt. Ob nun m selbst Primzahl ist oder sich als Produkt darstellen lässt, die dabei auftretenden Primzahlen sind nicht in der obigen Liste enthalten. ∎

Die mathematische Disziplin, die sich mit Primzahlen beschäftigt, heißt *Zahlentheorie*. Als mathematisches Basiswissen kann der Satz angesehen werden, der Aussagen über die Verteilung von Primzahlen $\pi(n)$[12] macht:

Satz 1.22 (Primzahlsatz)

$$\lim_{n\to\infty} \pi(n) \cdot \frac{\ln n}{n} = 1.$$

Der Beweis dieser Aussage, deren Richtigkeit schon von Gauss vermutet wurde, gelang im Jahre 1896 den beiden Mathematikern Hadamard und de la Vallée-Poussin.

Schließlich erwähnen wir zur Information noch den folgenden Satz von Dirichlet[13]:

Satz 1.23 *Jede arithmetische Progression $a_n = q \cdot n + r$, in der q und r teilerfremd sind, enthält unendlich viele Primzahlen.*

Wir beschließen dieses Kapitel mit wenigen Bemerkungen:

Bemerkung 1.24 (1) Fermat[14] *behauptete 1640, dass alle Zahlen der Form $F_n = 2^{2^n} + 1$ Primzahlen seien. Im Jahre 1732 zeigte* Euler, *dass die Zahl F_5 den Teiler 641 hat. Primzahlen von diesem Bautyp heißen* Fermat'*sche Primzahlen.*

[12] Dabei bezeichnet $\pi(n)$ die Anzahl der Primzahlen bis n.

[13] Peter Gustav Lejeune Dirichlet (geboren 13. Februar 1805 in Düren, gestorben am 5. Mai 1859 in Göttingen) war ein deutscher Mathematiker.

Dirichlet lehrte in Berlin und Göttingen und arbeitete hauptsächlich auf den Gebieten der Analysis und der Zahlentheorie.

Er war seit 1831 verheiratet mit Rebecca geb. Mendelssohn Bartholdy, einer Schwester des Komponisten Felix Mendelssohn Bartholdy. Dirichlets Großeltern stammten aus dem Ort Richelet in Belgien. Dies erklärt den französisch klingenden Namen: Le jeune de Richelet bedeutet sinngemäß Der Junge von Richelet.

Mit 12 Jahren besuchte Dirichlet zunächst ein Gymnasium in Bonn; zwei Jahre später wechselte er zum Jesuiten-Gymnasium in Köln, wo er u.a. von Georg Simon Ohm unterrichtet wurde. Im Mai 1822 begann er ein Mathematikstudium in Paris und traf hier mit den bedeutendsten französischen Mathematikern dieser Zeit - u.a. Biot, Francoeur, Hachette, Laplace, Lacroix, Legendre und Poisson - zusammen.

1825 machte er erstmals auf sich aufmerksam, indem er zusammen mit Adrien-Marie Legendre für den Spezialfall $n = 5$ die Fermat'sche Vermutung bewies: Es gibt keine ganzen Zahlen a, b, c und $n > 2$, welche die Bedingung $a^n + b^n = c^n$ erfüllen. Später lieferte er noch einen Beweis für den Spezialfall $n = 14$.

1827 wurde er von der Universität Bonn ehrenhalber promoviert und habilitierte sich 1827 - auf Empfehlung Alexander von Humboldts - als Privatdozent an der Universität in Breslau. 1827 zog ihn Alexander von Humboldt nach Berlin. Hier unterrichtete er zunächst an der allgemeinen Kriegsschule und später lehrte er an der Bauakademie. 1829 wurde er Privatdozent, 1831 a.o. Professor und 1839 o. Professor der Mathematik an der Berliner Universität. 1855 trat er in Göttingen als Professor der höheren Mathematik die Nachfolge von Carl Friedrich Gauss an. Diese Position hatte er bis an sein Lebensende 1859 inne.

Dirichlet forschte im Wesentlichen auf den Gebieten der partiellen Differentialgleichungen, der periodischen Reihen und bestimmten Integrale, sowie der Zahlentheorie. Er verknüpfte die bis dahin getrennten Gebiete der Zahlentheorie und der angewandten Mathematik. Er bewies die Konvergenz von Fourierreihen und eine Eigenschaft von Primzahlen in arithmetischen Progressionen. Nach ihm benannt ist der Dirichletsche Einheitensatz über algebraische Zahlenkörper. Seine neue Art von Betrachtungen der Potentialtheorie wurden später von Bernhard Riemann verwendet und weiterentwickelt.

Siehe auch: Dirichlet-Funktion, Dirichlet-Randbedingung, Schubfachprinzip, Dirichletscher Einheitensatz

In Dirichlets Haus in Göttingen musizierten der Geiger Joseph Achim und Agathe von Siebold, die Jugendliebe von Brahms. Dort besuchte ihn Karl August Varnhagen von Ense aus Berlin und beschreibt in seinen Tagebüchern das Haus, den Garten und dessen Pavillon.

[14] Als Geburtsdatum galt bis vor kurzem der 17. August 1601, sorgfältige Recherchen (siehe unten: Richtigstellung von Fermats Geburtsdatum) haben jedoch ergeben, dass Fermat Ende 1607 oder Anfang 1608 geboren wurde.

Fermat studierte Rechtswissenschaften an den Universitäten in Toulouse, Bordeaux und Orlans. 1631 wurde er Anwalt und Beamter der Regierung in Toulouse, wo er bis zu seinem Tod lebte. Aufgrund dieser Position wurde er geadelt.

1652 wurde er an das oberste Strafgericht befördert. 1643 bis 1654, als in Europa Bürgerkrieg und Pest wüteten, brach Fermat seine Kontakte nach Paris ab und widmete sich verstärkt der Zahlentheorie. 1653 erkrankte er ebenfalls an der Pest und wurde irrtümlich für tot erklärt.

Fermat studierte von 1623 bis 1626 Zivilrecht an der Universität Orléans und schloss dieses Studium im Juli 1626 mit dem baccalaureus juris civilis ab. Im Herbst desselben Jahres ließ er sich als Anwalt am parlement de Bordeaux

(2) *Eine Primzahl der Form* $M_n = 2^n - 1$ *heißen* MERSENNE'sche Primzahlen*, benannt nach dem Mathematiker* MERSENNE[15] .

(3) *Die* FERMAT'*zahlen sind wie die* MERSENNE'*zahlen ideale Prüfsteine für Primzahltests und Faktorisierungsmethoden. Man weiss nämlich, dass jeder Primfaktor einer* FERMAT'*zahl die Form* $2^{n+2}k + 1$ *hat.*

Der derzeitige Rekord (4.9.2006) lautet:

$$2^{32.582.657} - 1,$$

eine Zahl, die 9 808 358 Stellen aufweist und durch Dr. CURTIS COOPER and Dr. STEVEN BOONE 'entdeckt' wurde. Es ist die 44. bekannte MERSENNE'sche Primzahl[16].

---

nieder, wo er bis Ende 1630 blieb. Er hat weder in Bordeaux noch in Toulouse studiert. Dann kaufte er das Amt eines conseiller du parlement de Toulouse und wurde am 14. Mai 1631 in diesem Amt vereidigt.

In der Zeit von 1643 bis 1653 widmete sich FERMAT nicht verstärkt der Zahlentheorie (die Zeit seiner großen zahlentheoretischen Entdeckungen lag da bereits hinter ihm). Vielmehr wurde er durch die mannigfachen Verpflichtungen aus seinem Amt als conseiller so sehr in Anspruch genommen, dass ihm praktisch keine Zeit für seine mathematischen Forschungen blieb. Bauernaufstände im Languedoc wegen brutaler Steuereintreibungen, deren ungesetzliche und unmenschliche Praktiken von FERMAT aufgedeckt wurden, und die in Südfrankreich besonders heftigen kriegerischen Auseinandersetzungen mit der Fronde, die auch FERMATS Geburtsstadt Beaumont-de-Lomagne in Mitleidenschaft zogen, hielten das für den größten Teil Südfrankreichs politisch verantwortliche Parlament von Toulouse und auch FERMAT in Atem. So gehörte FERMAT zum Beispiel zu der Verhandlungskommission des königstreuen Parlaments von Toulouse, die mit den Generalständen des Languedoc, die sich auf die Seite der Fronde geschlagen hatten, langwierige Verhandlungen zur Wiederherstellung des Rechtsfriedens führte. Auch verhinderte FERMAT durch mutigen persönlichen Einsatz die Zerstörung seiner Heimatstadt Beaumont durch königliche Truppen.

FERMAT war einer der bedeutendsten 'Amateure' in der Geschichte der Mathematik, freilich zu einer Zeit, als sich noch kaum ein Forscher ausschließlich mit Mathematik beschäftigte. So beschränkte sich FERMATS Einfluss auf seine Korrespondenz mit vielen bedeutenden Gelehrten seiner Zeit (wie z. B. CARCAVI, BEAUGRAND, DESCARTES und MERSENNE) und auf die von seinem Sohn vorgenommene Ausgabe seines Nachlasses, einschließlich der von ihm kommentierten Arithmetik des Diophant (siehe unten). Er hat wichtige Beiträge zur Zahlentheorie, Wahrscheinlichkeitsrechnung, Variations- und Differentialrechnung geleistet. Dabei hat er seine Resultate oft nur in Form von 'Denksportaufgaben' - von Problemen ohne Angabe der Lösung - mitgeteilt.

Nach FERMAT sind unter anderem benannt:

Das FERMAT'*sche Prinzip* ist ein Variationsprinzip der Optik: 'Licht nimmt seinen Weg immer so, dass es ihn in der kürzesten Zeit zurücklegt.' Hieraus leitet sich das Reflexionsgesetz und das Snelliussche Brechungsgesetz ab.

Als FERMAT'*sche Zahlen* werden Zahlen der Form $F_n = 2^{2^n} + 1$ bezeichnet. FERMAT vermutete 1637, dass alle FERMAT-Zahlen Primzahlen sind. Dies wurde jedoch 1732 von EULER widerlegt.

Der FERMAT'*sche Zwei-Quadrate-Satz* lautet: Eine ungerade Primzahl p ist genau dann die Summe zweier Quadrate, wenn sie eine Zahl der Form $4n+1$ ist, und diese Darstellung ist (bis auf die Reihenfolge) eindeutig. $p = a^2 + b^2 \iff p = 4n + 1$ Der erste Beweis dieses Satzes geht auf EULER zurück. Die beiden kleinsten Primzahlen mit dieser Eigenschaft sind $5(= 12 + 22)$ und $13(= 22 + 32)$.

Kleiner FERMAT'*scher Satz*: Für jede Primzahl p gilt: $a^p \equiv a \pmod p$ für alle $a \in \mathbb{Z}$. Auf diesem Satz beruht der FERMATsche Primzahltest. Auch in diesem Fall findet sich der erste erhaltene Beweis bei EULER.

FERMAT'*sche Vermutung* oder *Großer* FERMAT'*scher Satz* (als wörtliche Übersetzung der englischen Bezeichnung oft auch als FERMATS letzter Satz bezeichnet): Diese berühmteste auf FERMAT zurückgehende Behauptung besagt, dass die diophantische Gleichung $a^n + b^n = c^n$ mit $a, b, c \in \mathbb{N}$ für keine natürliche Zahl $n > 2$ erfüllt ist. Es gibt also keine Analoga zu den pythagoräischen Tripel für die dritte oder höhere Potenzen. Seine Berühmtheit erlangte dieser Satz dadurch, dass FERMAT in einer Randnotiz seines Exemplars der Arithmetica des Diophant behauptete, dafür einen 'wunderbaren' Beweis gefunden zu haben, für den aber ?auf dem Rand nicht genug Platz? sei. Der Fall $n = 4$ wurde von FERMAT an anderer Stelle bewiesen, weitere Fälle später von anderen Mathematikern. In seiner Allgemeinheit blieb die Aussage bis vor kurzem eines der berühmtesten ungelösten Probleme der Mathematik. Erst 1993 (publiziert 1995 mit einem Beitrag von Richard Taylor) gelang es dem britischen Mathematiker Andrew Wiles, die FERMAT'sche Vermutung zu beweisen. Daher wird diese auch als Satz von *Fermat* auch Satz von WILES oder Satz von WILES-TAYLOR bezeichnet.

[15]MERSENNE, Marin, französischer Mathematiker, geboren 8.9.1588 Soultière bei Bourg d' Oiz, gestorben 1.9.1648 Paris.

1604 bis 1909 wurde MERSENNE am Jesuitenkolleg in La Flèche zusammen mit Descartes ausgebildet. Von 1609 bis 1611 studierte er Theologie an der Sorbonne. 1611 wurde er Mönch und gehörte ab 1619 in Paris zum Konvent.

MERSENNE hatte durch seine umfangreiche Korrespondenz Kontakt mit vielen Gelehrten seiner Zeit, unter anderem mit FERMAT, PASCAL, GASSENDI, ROBERVAL und BEAUGRAND. 1626 veröffentlichte er Arbeiten zur Mathematik, Mechanik, Optik und Akustik. 1644 versuchte er, eine Formel für Primzahlen zu finden. Das Ergebnis war eine Liste derjenigen Primzahlen m bis 257, für die $2^m - 1$ ebenfalls eine Primzahl ist. Wie sich später jedoch herausstellte, enthielt diese Liste einige 'falsche'Primzahlen, und es fehlten einige wirkliche Primzahlen. Daneben befasste sich MERSENNE auch mit den Arbeiten von DESCARTES und GALILEO.

[16]mehr dazu, siehe http://www.MERSENNE.org/

2 Funktionen und erste Zählprinzipien

2.1 Grundideen der Diskreten Mathematik

Als Ausgangstext hat für dieses Kapitel auf weite Strecken der vorzügliche und kompakte Text aus [1] gedient, den wir allerdings mit Kommentaren nachbearbeitet haben und teilweise neuorganisiert haben.

Die Diskrete Mathematik studiert endliche Mengen, und als erstes wollen wir uns fragen, wie viele Elemente eine gegebene Menge besitzt. Zum Beispiel können wir fragen, wie viele Paare die Menge $\{1, 2, 3, 4\}$ enthält. Die Antwort ist 6, wie jeder weiß, sehr aufregend ist das Ergebnis aber nicht, da wir daraus nicht erkennen, wie viele Paare $\{1, 2, \ldots, 6\}$ oder $\{1, 2, \ldots, 1000\}$ enthalten. Interessant wird die Sache erst, wenn wir die Anzahl der Paare in der n-Menge $\{1, \ldots, n\}$ für beliebiges n bestimmen können.

Ein typisches diskretes Abzählproblem sieht demnach folgendermaßen aus: Gegeben sei eine unendliche Familie von endlichen Mengen S_n, (wobei n eine Indexmenge I durchläuft, z.B. die natürlichen Zahlen), und die Aufgabe besteht darin, die Zählfunktion $f : I \longrightarrow N_0,\ f(n) = |S_n|,\ n \in I$ zu bestimmen. Meist sind die Mengen S_n durch einfach kombinatorische Bedingungen gegeben.

Als erstes, mehr philosophisches Problem, stellt sich die Frage, was man unter einer „Bestimmung“ von f zu verstehen hat. Am befriedigendsten ist natürlich eine geschlossene Formel. Ist z. B. S_n die Menge der Permutationen einer n-Menge, so haben wir $f(n) = n!$, und jeder wird dies als ausreichende Bestimmung akzeptieren. Leider ist in den allermeisten Fällen solch eine Formel nicht zu erreichen. Was macht man dann?

2.1.1 Summation - die Grundidee

Angenommen, wir wollen nicht alle Permutationen von $\{1, \ldots n\}$ abzählen, sondern nur die fixpunktfreien, d.h. jene Permutationen, bei denen i nicht an i-ter Stelle auftritt, für alle i. Sei D_n die Anzahl dieser Permutationen. Zum Beispiel sind 231, 312 die einzigen fixpunktfreien Permutationen[17] (Derangement) für $n = 3$, also ist $D_3 = 2$. Wir werden später beweisen, dass

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

für alle n gilt. Hier liegt also eine Summationsformel vor.

2.1.2 Rekursion - die Grundidee

Aus kombinatorischen Erwägungen folgt, wie wir sehen werden, die Beziehung $D_n = (n-1)(D_{n-1} + D_{n-2})$ für $n \geq 3$. Aus den Anfangswerten $D_1 = 0,\ D_2 = 1$ folgt daraus die allgemeine Formel. Beispielsweise erhalten wir $D_3 = 2,\ D_4 = 9,\ D_5 = 44$. Eine Rekursion ist manchmal einer geschlossenen Formel durchaus vorzuziehen. Die Fibonacci-Zahlen F_n sind definiert durch $F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2}$ $(n \geq 2)$. Später werden wir daraus die Formel

$$F_n = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n)$$

ableiten, aber wahrscheinlich wird jeder (oder zumindest jeder Computer aufgrund der Irrationalität von $\sqrt{5}$) die Rekursion bevorzugen.

[17] Die Aufgabe wurde zuerst von Niclaus Bernoulli I. (1687 bis 175) , dem Neffen der beiden großen Mathematiker Jakob und Johann Bernoulli behandelt. Später wurde auch Euler auf das Problem geführt, das er als ‘quaestio curiosa ex doctrina combinationis’ bezeichnete und unabhängigk von Bernoulli löste.

2.1.3 Erzeugende Funktionen - die Grundidee

Eine Methode, die sich als besonders fruchtbar erwiesen hat, besteht darin, die Werte $f(n)$ der Zählfunktion als Koeffizienten einer Potenzreihe aufzufassen,

$$F(z) = \sum_{n \geq 0} f(n) z^n$$

mit $F(z)$ heißt Erzeugende Funktion der Zählfunktion f. Fragen wir z.B. nach der Anzahl der n-Untermengen einer r-Menge für festes r, so ist $f(n) = \binom{r}{n}$ (Binomialkoeffizient), und wir wissen aus dem Binomialsatz, dass

$$\sum_{n \geq 0} \binom{r}{n} z^n = (1+z)^r$$

gilt. Wir werden sehen, wie sich daraus auf verblüffend einfache Weise Identitäten für Binomialkoeffizienten ableiten lassen.

2.1.4 Asymptotische Analyse - die Grundidee

In späteren Kapiteln werden wir Algorithmen für die verschiedensten Probleme studieren. Neben der Korrektheit des Algorithmus interessiert natürlich besonders, wie schnell er ist, wir fragen also nach der Laufzeit des Algorithmus. Sehr oft ist der Algorithmus durch eine Rekursion gegeben. In Sortierproblemen wird uns beispielsweise die Rekursion

$$f(n) = \frac{2}{n} \sum_{k=0}^{n-1} f(k) + an + b$$

mit $a > 0$ begegnen. In diesem Fall ist eine Lösung leicht zu erhalten, aber allgemein kann die Bestimmung von $f(n)$ äußerst schwierig sein. Wir werden dann versuchen, $f(n)$ durch leichter zugängliche Funktionen $a(n)$ und $b(n)$ mit $a(n) \leq f(n) \leq b(n)$ abzuschätzen, und uns zufriedengeben, wenn wir das Problem asymptotisch gelöst haben, das heißt eine bekannte Funktion $g(n)$ gefunden haben (z.B. ein Polynom oder eine Exponentialfunktion), welche dieselbe Größenordnung wie $f(n)$ hat.

2.2 Begriffliches und endliche Mengen

Wie hinlänglich bekannt ist, verstehen wir unter einer Funktion $f : X \longrightarrow Y$ eine eindeutige Zuordnung (= linkstotale, rechtseindeutige Relation), bei der jedem $x \in X$ genau ein $y \in Y$ zugeordnet ist. In der Algebra ist es sinnvoll - im Unterschied zur Analysis - Funktionen als Tripel, nämlich (f, X, Y) zu verstehen. Die Sprechweisen *Funktionen* und *Abbildungen* benutzen wir synonym.

Die Verknüpfung von Funktionen $f : X \longrightarrow Y$ und $g : Y \longrightarrow Z$ ist nichts anderes als die Hintereinanderausführung von g *nach* f, d.h. $gf : X \longrightarrow Z$ wird durch $(gf)(x) = g(f(x))$ definiert.

Wir erwähnen noch die im Prinzip bekannten sprachlichen Vereinbarungen:

Definition 2.1 *Es sei $f : X \longrightarrow Y$ eine Funktion. Die Funktion f heißt* injektiv *genau dann, wenn $f(x_1) = f(x_2)$ stets $x_1 = x_2$ impliziert. Die Funktion f heißt* surjektiv*, wenn für jedes $y \in Y$ ein $x \in X$ mit $f(x) = y$ existiert. f heißt* bijektiv*, wenn sie zugleich injektiv und surjektiv ist.*

Ist X eine Teilmenge von Y, so verstehen wir unter der *Inklusionsfunktion* oder auch *Insertion* die Funktion $i : X \longrightarrow Y$ mit $i(x) = x$ für alle $x \in X$. Im Falle $X = Y$ sprechen wir von der *Identität* auf X.

Der Vollständigkeit halber erwähnen wir die folgende, leicht zu rechtfertigende Aussage:

Lemma 2.2 *Es seien $f : X \longrightarrow Y$ und $g : Y \longrightarrow Z$. Sind beide Funktionen injektiv (surjektiv), so ist auch die Verkettung $gf : X \longrightarrow Z$ injektiv (surjektiv).*

Definition 2.3 *Eine Funktion $g : Y \longrightarrow X$ heißt zur Funktion $f : X \longrightarrow Y$* invers*, wenn für alle $x \in X, y \in Y$ gilt*

$$(gf)(x) = x \quad \text{und} \quad (fg)(y) = y.$$

Die Funktion g heißt dann auch die Inverse *von f und wir schreiben vielfach $g = f^{-1}$.*

Ohne Beweis erwähnen wir die bekannte Aussage:

Proposition 2.4 *Eine Funktion besitzt genau dann eine Inverse, wenn sie bijektiv ist.*

Die nächste Aussage **Gleichheitsregel** basiert auf unserem naiven Anzahlbegriff; genau genommen *definieren* wir die *Anzahl* einer (endlichen) Menge als Klassencharakteristik unter der Äquivalenzrelation *gleichmächtig*. Insofern ist eigentlich $|S|$ die Klasse der zur Menge S gleichmächtigen Mengen, wobei die Gleichmächtigkeit über Bijektionen vermittelt wird. Bei dieser Interpretation ist diese *Gleichheitsregel* eine triviale Aussage:

Lemma 2.5 (Gleichheitsregel) *Es seien S, T Mengen; dann gilt $|S| = |T|$ genau dann, wenn es eine Bijektion zwischen den Mengen S und T gibt.*

Die typische Anwendung der Gleichheitsregel sieht folgendermaßen aus: Wir wollen eine Menge S abzählen. Gelingt es uns, S bijektiv auf eine Menge T abzubilden, deren Größe wir kennen, so können wir $|S| = |T|$ schließen.

Beispiel 2.6 *Wie viele verschiedene Untermengen besitzt eine n-Menge X, z. B. $X = \{1, \ldots, n\}$? Zu jeder Untermenge A betrachten wir den charakteristischen Vektor $w(A) = a_1 a_2 \ldots a_n$ von A mit $a_i = 1$, falls $i \in A$ ist, und $a_i = 0$, falls $i \notin A$. Jeder Vektor $w(A)$ ist also ein $0,1$-Wort der Länge n, und man sieht sofort, dass die Abbildung w eine Bijektion zwischen der Menge S aller Untermengen von $\{1, \ldots, n\}$ und der Menge T aller $0,1$-Wörter der Länge n ergibt. Die Mächtigkeit von T kennen wir schon, $|T| = 2^n$, also folgt nach der Gleichheitsregel auch $|S| = 2^n$.*

Ohne Rücksicht auf Konsistenz verabreden wir die folgende Abkürzung:

$$\mathbb{N}_n = \{1, 2, \ldots, n\}.$$

Eigentlich offensichtlich, jedoch erwähnenswert ist die folgende Aussage, da sie als Ausgangspunkt einer Definition genommen werden kann:

Proposition 2.7 *Es seien $m < n$ natürliche Zahlen. Dann gibt es keine injektive Abbildung von $\mathbb{N}_n$ nach $\mathbb{N}_m$.*

Beweis: Es bezeichne S die Menge der natürlichen Zahlen n, für die ein $m < n$ und eine injektive Abbildung von $\mathbb{N}_n$ nach $\mathbb{N}_m$ existiert. Wenn S nicht leer ist, gibt es in S ein kleinstes Element k, also eine injektive Abbildung i von $\mathbb{N}_k$ nach $\mathbb{N}_l$ für ein geeignetes $l < k$. Wie man leicht sieht, ist $l \neq 1$. Also ist $l - 1$ ebenfalls eine natürliche Zahl. Ziel ist es nun, ein kleineres Gegenbeispiel zu konstruieren.

Ist keines der Werte $i(1), i(2), \ldots, i(k-1)$ gleich l, dann schränken wir i auf $\mathbb{N}_{k-1}$ ein, als Bildmenge wählen wir $\mathbb{N}_{l-1}$. Widerspruch zur Minimalität des Gegenbeispiels.

Ist $i(b) = l$ für ein b mit $1 \leq b \leq k-1$, dann ergibt sich notwendigerweise $i(k) = c \neq l$, da i eine injektive Abbildung ist. In diesem Fall konstruieren wir eine injektive Abbildung i^* von $\mathbb{N}_{k-1}$ nach $\mathbb{N}_{l-1}$ gemäß

$$i^*(b) = c, \qquad i^*(r) = i(r) \quad (r \neq b).$$

Erneut ergibt sich ein Widerspruch zur Minimalität von k. ∎

Als unmittelbare Konsequenz ergibt sich: Hätte eine Menge X insgesamt n Elemente, auf der anderen Seite auch m Elemente für ein $m \leq n$, so gäbe es Bijektionen

$$\beta : \mathbb{N}_n \longrightarrow X, \qquad \gamma : \mathbb{N}_m \longrightarrow X,$$

und schließlich wäre $\gamma^{-1}\beta$ eine injektive Abbildung von $\mathbb{N}_n$ nach $\mathbb{N}_m$, was dem letzten Satz widerspricht. Damit ist die eindeutige Elementzuweisung einer endlichen Menge gerechtfertigt. Wir schreiben $| X |$ für die Kardinalität von X.

2.3 Elementare Zählprinzipien

Wir wollen einige fundamentale Regeln zusammenfassen, auf denen alle Abzählung basiert. Die ersten beiden Regeln, die so einsichtig sind, dass sie nicht bewiesen werden müssen, beruhen auf einer Klassifikation der Elemente, der abzuzählenden Menge.

2.3.1 Summenregel

Eine oft unreflektiert benutzte Regel beschreibt das folgende Lemma:

Lemma 2.8 (Summenregel) *E sei* $S = \sum_{i=1}^{t} S_i$ *eine disjunkte Vereinigung von Mengen* $S_i, i = 1, \ldots t$*, dann gilt*

$$|S| = \sum_{i=1}^{t} |S_i|.$$

In der Anwendung tritt die Summenregel meist in folgender Gestalt auf: Wir klassifizieren die Elemente von S nach gewissen Eigenschaften E_i, $(i = 1, \ldots, t)$, die sich gegenseitig ausschließen, und setzen: $S_i = \{x \in S \mid \ x \text{ hat die Eigenschaft } E_i\}$.

Die Summenregel bildet die Grundlage für die meisten Rekursionen. Betrachten wir folgendes Beispiel:

Beispiel 2.9 *Für eine n-Menge X sei* $S = \binom{X}{k}$ *die Menge aller k Untermengen von X, also* $|S| = \binom{n}{k}$*. Sei* $a \in X$*. Wir klassifizieren die k Untermengen A, je nachdem ob* $a \in A$*, oder* $a \notin A$ *ist,* $S_1 = \{A \in S \mid \ a \in A\}$*,* $S_2 = \{A \in S \mid \ a \notin A\}$*. Wir erhalten die Mengen aus* S_1*, indem wir alle* $(k-1)$*-Untermengen von* $X \setminus \{a\}$ *nehmen, also* $|S_2| = \binom{n-1}{k}$*. Nach der Summenregel erhalten wir daraus die fundamentale Rekursion für die Binomialkoeffizienten:*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \ (n \geq 1)$$

Auf Seie 17 werden wir ausführlich auf die Binomialzahlen eingehen.

2.3.2 Produktregel

Ebenfalls im Kern selbstverständlich erscheint die nachfolgende Aussage, die als *Produktregel* bezeichnet wird.

Lemma 2.10 ***Produktregel.*** *Sei* $S = S_1 \times S_2 \times \ldots \times S_t$ *ein Mengenprodukt, dann gilt:* $|S| = \prod_{s=1}^{t} |S_i|$.

Angenommen, wir können auf 3 Wegen von Köln nach Düsseldorf und auf 5 Wegen von Düsseldorf nach Münster fahren. Dann gibt es $15 = 3 \cdot 5$ Wege, um von Köln nach Münster über Düsseldorf zu gelangen.

Es ist oft nützlich, die Produktregel als Baumdiagramm zu verdeutlichen. Seien a, b, c die Wege von Köln nach Düsseldorf und 1,2,3,4,5 die Wege von Düsseldorf nach Münster, dann zeigt das Diagramm auf Seite 16 die 15 Wege von Köln nach Münster.

Eine Folge von 0 und 1 nennen wir ein 0, 1-Wort und die Anzahl der 0 'en und 1'en die Länge des Wortes. Wie viele verschiedene 0, 1-Wörter der Lange n gibt es? Für jede Stelle des Wortes gibt es 2 Möglichkeiten, also ist die Antwort nach der Produktregel 2^n.

Für unsere letzte Regel benötigen wir ein paar Begriffe. Ein *Inzidenzsystem* (S, T, I) besteht aus zwei Mengen S und T und einer Relation I (genannt Inzidenz) zwischen den Elementen aus S und T. Falls eine Relation aIb zwischen $a \in S$ und $b \in T$ besteht, so nennen wir a und b inzident, ansonsten nicht-inzident. Ein bekanntes Beispiel liefert die Geometrie: S ist eine Punktmenge, T eine Geradenmenge, und pIg bedeutet, dass der Punkt p auf der Geraden g liegt.

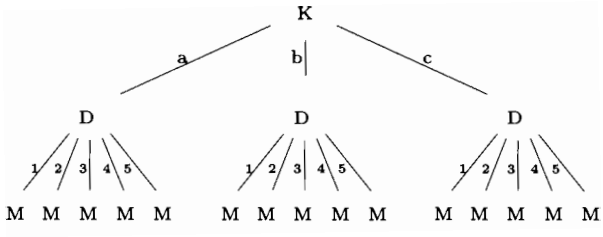

Abbildung 3: Wege von Köln nach Münster

	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2		1		1		1		
3			1			1		
4				1				1
5					1			
6						1		
7							1	
8								1

Tabelle 1: Inzidenzmatrix der Teilerrelation auf der Menge $\{1, \ldots, 8\}$ (vgl. Beispiel 2.12)

2.3.3 Regel vom zweifachen Abzählen

Die nächste Regel versteht sich eigentlich als 'Prinzip'.

Lemma 2.11 (Regel vom zweifachen Abzählen) *Es sei (S, T, I) ein Inzidenzsystem, und für $a \in S$ bezeichne $r(a)$ die Anzahl der zu a inzidenten Elemente aus T, und analog $r(b)$ für $b \in T$ die Anzahl der zu b inzidenten Elemente aus S. Dann gilt*

$$\sum_{a \in S} r(a) = \sum_{b \in T} r(b)$$

Die Regel wird sofort einsichtig, wenn wir das Inzidenzsystem als Rechteckschema darstellen. Wir nummerieren die Elemente aus $S = \{a_1, \ldots, a_m\}$ und $T = \{b_1, \ldots b_n\}$. Nun stellen wir eine $m \times n$-Matrix $M = (m_{ij})$ auf, genannt die Inzidenzmatrix, indem wir

$$m_{ij} = \begin{cases} 1 & \text{falls } a_i I b_i \\ 0 & \text{sonst} \end{cases}$$

setzen. Die Größe $r(a_i)$ ist dann genau die Anzahl der 1'en in der i-ten Zeile, und analog $r(b_j)$ die Anzahl der 1'en in der j-ten Spalte. Die Summe $\sum_{i=1}^{m} r(a_i)$ ist somit gleich der Gesamtzahl der 1'en (zeilenweise gezählt), während $\sum_{j=1}^{n} r(b_j)$ dieselbe Zahl (spaltenweise gezählt) ergibt.

Beispiel 2.12 *Es sei $S = \{1, \ldots, 8\} = T$ und wir erklären $i \in S,\ j \in T$ inzident, wenn i ein Teiler von j ist, in Zeichen $i \mid j$. Die zugehörige Inzidenzmatrix hat demnach folgende Gestalt, wobei wir der Übersichtlichkeit halber nur die 1'en eintragen:*

Die Anzahl der 1'en in Spalte j ist genau gleich der Anzahl der Teiler von j, die wir mit $t(j)$ bezeichnen wollen, also z. B. $t(6) = 4, t(7) = 2$. Wir stellen uns nun die Frage, wie viele Teiler

eine Zahl von 1 bis 8 im Durchschnitt hat, d. h. wir wollen $\bar{t}(8) = \frac{1}{8}\sum_{j=1}^{8} t(j)$ berechnen. In unserem Beispiel ist $\bar{t}(8) = \frac{5}{2}$. Aus der Tafel erkennen wir folgende Werte:

n	1	2	3	4	5	6	7	8
$\bar{t}(n)$	1	$\frac{3}{2}$	$\frac{5}{3}$	2	2	$\frac{7}{3}$	$\frac{16}{7}$	$\frac{5}{2}$

Wie groß ist nun $\bar{t}(n)$ für beliebiges n? Das scheint auf den ersten Blick eine hoffnungslose Angelegenheit. Für Primzahlen p gilt $t(p) = 2$, während für 2-er Potenzen ein großer Wert $t(2^k) = k+1$ resultiert. Versuchen wir dennoch unsere Regel des zweifachen Abzählens. Nach Spalten gezählt erhalten wir, wie gesehen, $\sum_{j=1}^{n} t(j)$. Wie viele 1'en sind in der i-ten Zeile? Offenbar entsprechen die 1'en den Vielfachen von i, nämlich $1 \cdot i, 2 \cdot i, \ldots$ und das letzte Vielfache $\leq n$ ist $\lfloor \frac{n}{i} \rfloor \cdot i$, also ist $r(i) = \lfloor \frac{n}{i} \rfloor$. Unsere Regel ergibt daher:

$$\bar{t}(n) = \frac{1}{n}\sum_{j=1}^{n} t(j) = \frac{1}{n}\sum_{j=1}^{n} \lfloor \frac{n}{i} \rfloor \sim \frac{1}{n}\sum_{i=1}^{n} \frac{n}{i} = \sum_{i=1}^{n} \frac{1}{i}$$

wobei der Fehler beim Übergang von $\lfloor \frac{n}{i} \rfloor$ auf $\frac{n}{i}$ für alle i kleiner als 1 ist, also auch in der Summe. Die letzte Größe $\sum_{i=1}^{n} \frac{1}{i}$ wird uns noch oft begegnen, sie heißt die n-te harmonische Zahl H_n. Aus der Analysis wissen wir, dass $H_n \sim \log n$ etwa so groß ist wie der natürliche Logarithmus, und wir erhalten das erstaunliche Ergebnis, dass die Teilerfunktion trotz aller Unregelmäßigkeit im Durchschnitt sich vollkommen regelmäßig verhält, nämlich $\bar{t}(n) \sim \log n$.

2.4 Die fundamentalen kombinatorischen Grundfiguren und zugehörige Zählkoeffizienten

2.4.1 k-Teilmengen einer n-Menge

Einige Zahlen wie die Binomialkoffizienten $\binom{n}{k}$ tauchen immer wieder auf. Wir wollen die wichtigsten Zahlen nun systematisierend besprechen und dabei unser Augenmerk auf die dahinter stehenden kombinatorischen Grundfiguren richten.

Die ersten Begriffe, die wir mit einer Menge assoziieren, sind Untermengen.

Definition 2.13 *Es sei $n \in \mathbb{N}$ eine natürliche Zahl, N eine n-Menge und $k \leq n$. Eine k-Menge in N ist eine k-elementige Teilmenge von N; $\binom{n}{k}$ bezeichnet deren Anzahl. Diese Zählkoeffizienten $\binom{n}{k}$ heißen Binomialkoeffizienten oder auch Binomialzahlen.*

Wir listen einige grundlegende Eigenschaften der Binomialzahlen resp. Binomialkoeffizienten auf:

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!} = \frac{n^{\underline{k}}}{k!} \qquad (n \geq k \geq 0) \tag{1}$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \qquad (n \geq k \geq 0) \tag{2}$$

$$\text{insbesondere also} \qquad \binom{n}{k} = \binom{n}{n-k} \qquad (n \geq k \geq 0). \tag{3}$$

Die Größen $n(n-1)\ldots(n-k+1)$, die bei der Berechnung des Binomialkoeffizieten auftauchen, erscheinen so häufig in Abzählproblemen, dass wir ihnen einen eigenen Namen geben:

Definition 2.14 *Es seien n, k natürliche Zahlen. Dann nennen wir*

$$n^{\underline{k}} := n(n-1)\ldots(n-k+1)$$

die fallenden Faktoriellen (von n der Länge k). Analog dazu setzen wir:

$$n^{\overline{k}} := n(n+1)\dots(n+k-1)$$

und nennen $n^{\overline{k}}$ die steigenden Faktoriellen.

Es ist nützlich auch für negative Zahlen, ja auch für beliebige komplexe Zahlen n zu erklären, und k für beliebige ganze Zahlen. Zuerst setzen wir $\binom{0}{0} = 1$, das ist sinnvoll, da die leere Menge $\emptyset$ genau eine 0-Untermenge, nämlich $\emptyset$ enthält. Ebenso setzen wir $n^{\underline{0}} = n^{\overline{0}} = 1$ für die fallenden und steigenden Faktoriellen, und $0! = 1$.

Der Ausdruck $r^{\underline{k}} = r(r-1)\dots(r-k+1)$ oder $r^{\overline{k}} = r(r+1)\dots(r+k-1)$ ist für beliebiges $r \in \mathbb{C}$ sinnvoll, z.B. $(-\frac{1}{2})^{\underline{3}} = (-\frac{1}{2})(-\frac{3}{2})(-\frac{5}{2}) = -\frac{15}{8}$, $(-2)^{\overline{2}} = (-2)(-1) = 2$. Für $k!$ müssen wir allerdings zunächst $k \geq 0$ voraussetzen, da die Fakultätsfunktion für $k < 0$ nicht ohne weiteres erklärt werden kann. Wir geben daher die allgemeine Funktion für $r \in \mathbb{C}$:

$$\binom{r}{k} = \begin{cases} \frac{r(r-1)\dots(r-k+1)}{k!} = \frac{r^{\underline{k}}}{k!} & (k \geq 0) \\ 0 & (k < 0) \end{cases} \tag{4}$$

2.4.2 Ungeordnete Mengen- und Zahlpartitionen

Nun wenden wir uns den Partitionen zu:

Definition 2.15 *Es sei $n \in \mathbb{N}$ eine natürliche Zahl, N eine n-Menge und $k \leq n$.*

(i) *Unter einer (ungeordneten) k-Mengenpartition von N verstehen wir eine disjunkte Zerlegung von N in k Teilmengen (= Blöcke). Die Anzahl der k-Mengenpartitionen einer n-Menge wird durch die Stirling-Zahlen $S_{n,k}$ zweiter Art*[18] *repräsentiert.*

(ii) *Unter einer k-gliedrigen (ungeordneten) Zahlpartition von n verstehen wir eine additive Zerlegung von n als Summe $n_1+n_2+\ldots+n_k$ von k Summanden n_i. Die Anzahl der k-Zahlpartitionen einer Zahl n wird mit $P_{n,k}$ bezeichnet. Da es auf die Reihenfolge der $n_i's$ nicht ankommt, können wir $n_1 \geq n_2 \geq \ldots \geq n_k$ voraussetzen.*

Die Zahlen sind nach dem Mathematiker James Stirling[19] benannt. Wir gehen auf Seite 18 näher auf Eigenschaften dieser Zahlen ein, während wir uns auf Seite 19 den Zahlpartionenparametern vom Typ $P_{n,k}$ widmen.

Beispiele 2.16 (i) $N = \{1,2,3,4,5\}$ *besitzt die folgenden 2-Mengenpartitionen, wobei wir die Klammern weglassen:*

$$\begin{aligned} 12345 = \quad & 1234+5, \quad 1235+4, \quad 1245+3, \\ & 1345+2, \quad 2345+1, \quad 123+45, \\ & 124+35, \quad 125+34, \quad 134+25, \\ & 135+24, \quad 145+23, \quad 234+15, \\ & 235+14, \quad 245+13, \quad 345+12, \end{aligned}$$

[18] warum zweiter Art hat historische Gründe und wird bald klar werden, vgl. auch Seite 22

[19] Stirling, James, schottischer Mathematiker, geboren 1692 Garden (Stirlingshire, Schottland), gestorben 5.12.1770 Edingburgh).

Stirling nahm 1710 sein Studium in Oxford auf, und blieb dort auch nach dem Studium bis 1717. In der Folgezeit weilte er in verschiedenen Städten Europas, unter anderem in Venedig und Padua. Ab 1724 war er als Lehrer in London tätig und wurde 1726 Mitglied der Londoner Mathematischen Gesellschaft. 1735 wurde er Geschäftsführer der Schottischen Bergbaugesellschaft Leadhills in Lanarksshire.

In seinem ersten Buch 'Lineare tertii ordinis neutonianae', das 1717 erschien, erweiterte Stirling Newtons Theorie der ebenen Kurven dritten Grades, indem er weitere Kurventypen ergänzte. In folgenden Arbeiten ('Methodus differentialis', 1730) setzte er sich mit der Differenzenrechnung, der Konvergenz von unendlichen Reihen und unendlichen Produkten, mit Interpolation und Quadraturformeln auseinander. Er fand eine Näherungsformel für n! (Stirlingsche Formel) und Darstellungen für spezielle Werte der Eulerschen Γ-Funktion.

Neben diesen mathematischen Arbeiten untersuchte er die Gravitation, die Gestalt der Erde, und beschäftigte sich mit Fragen des Bergbaus.

also ist $S_{5,2} = 15$.

(ii) *Für* $n = 8$ *erhalten wir die folgenden* 4*-Zahlpartitionen:* $8 = 5+1+1+1,\ 4+2+1+1,\ 3+3+1+1,\ 3+2+2+1,\ 2+2+2+2$, *also ist* $P_{8,4} = 5$.

2.4.3 Geordnete Mengen- und Zahlpartitionen

Wir haben eben erwähnt, dass es auf die Reihenfolge der Summanden in einer Zahlpartition nicht ankommt, wir können daher auch von *ungeordneten* Zahlpartitionen sprechen. Ebensowenig spielt bei den Untermengen oder Mengenpartitionen die Reihenfolge eine Rolle. Insofern macht es Sinn, die eben definierten kombinatorischen Figuren auch als *geordnete* Strukturen anzudenken. Daher generieren wir in Analogie zur Definition entsprechende *geordnete Begriffe*.

Definition 2.17 *Es sei* $n \in \mathbb{N}$ *eine natürliche Zahl,* N *eine* n*-Menge und* $k \leq n$.

(i) *Unter den* k*-Permutationen der* n*-Menge* N *versteht man die Menge aller Wörter aus* N *mit* k *lauter verschiedenen Einträgen.*

(ii) *Unter den geordneten* k*-Mengenpartitionen einer Menge von* n *Elementen versteht man formal die disjunkte Zerlegung in* k*-Teilmengen (unter Berücksichtigung der Reihenfolgen).*

(iii) *Unter den geordneten* k*-Zahlpartionen versteht man sinngemäss die additive Zerlegung der Zahl* n *in* k *Summanden unter Berücksichtigung der Reihenfolgen.*

Beispiele 2.18 1. *Sei* N *eine* n*-Menge, z.B.* $N = \{1, 2, \ldots, n\}$. *Wir betrachten Wörter der Länge* k *mit lauter verschiedenen Einträgen; wir nennen sie* k*-Permutationen von* N. *Z.B. sind 1234 und 5612 zwei* 4*-Permutationen von* $N = \{1, \ldots, 6\}$.

2. *Geordnet heißt also, dass die geordnete Untermenge* $\{1, 2, 3\}$ *von* $\{3, 1, 2\}$ *oder* $\{3, 2, 1\}$ *verschieden ist, obwohl sie als gewöhnliche Mengen gleich sind. Desgleichen sind die geordneten Mengen-Partitionen* $123+45$ *und* $45+123$ *verschieden, oder die Zahl-Partitionen* $3+3+1+1$ *und* $3+1+3+1$.

Korollar 2.19 (i) *Die Anzahl der* k*-Permutationen einer* n*-Menge beträgt* $n(n-1)\ldots(n-k+1)$.

(ii) *Die Anzahl der* n*-Permutationen einer* n*-Menge beträgt* $n!$.

Zurück zu unserem Problem der Abzählung geordneter Objekte. Für Untermengen und Mengen-Partitionen ist dies ganz einfach. Jede k-Untermenge ergibt $k!$ geordnete k-Untermengen und jede k-Mengenpartition ergibt $k!$ geordnete k-Mengen-Partitionen, da die verschiedenen Elemente bzw. Blöcke auf $k!$ Arten permutiert werden können. Also erhalten wir für die entsprechenden Anzahlen:

Korollar 2.20 *Die Zahl der geordneten* k*-Mengenpartitionen ist das* $k!$*-fache der (ungeordneten) Mengenpartitionen einer* n*-Menge, also* $k!S_{n,k}$.

Nun ist klar, dass die geordneten k-Untermengen nichts anderes als die k-Permutationen von N sind, also erhalten wir für $\binom{n}{k}$ die übliche Formel:

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!} = \frac{n^k}{k!}$$

Die Abzählung geordneter Zahlpartitionen ist ein wenig subtiler, da die Summanden ja nicht verschieden zu sein brauchen, einige Permutationen daher die gleiche geordnete Partition ergeben. Zum Beispiel erhalten wir aus $3+1+1$ nicht $6 = 3!$ verschiedene geordnete Partitionen sondern nur 3, nämlich $3 + 1 + 1$, $1 + 3 + 1$, $1 + 1 + 3$. Die folgende Formel ist eine schöne Illustration der Gleichheitsregel:

Korollar 2.21 *Die Anzahl der geordneten* k*-Zahlpartitionen von* n *beträgt* $\binom{n-1}{k-1}$.

Beweis: Zum Beweis konstruieren wir eine Bijektion von der Menge S aller geordneten k-Partitionen auf die Menge T aller $(k-1)$-Untermengen in $\{1, 2, \ldots, n-1\}$. Sei $n = n_1+n_2+\ldots+n_k \in S$, dann erklären wir $f : S \longrightarrow T$ durch $f(n_1+\ldots+n_k) = \{n_1, n_1+n_2, \ldots, n_1+\ldots+n_{k-1}\}$. Wegen $n_i \geq 1$ ist $1 \leq n_1 < n_1+n_2 < \ldots < n_1+\ldots+n_{k-1} \leq n-1$, d.h. $f(n_1+\ldots+n_k) \in T$, die Umkehrabbildung ist $g(\{a_1 < a_2 < \ldots < a_{k-1}\}) = a_1 + (a_2 - a_1) + \ldots + (a_{k-1} - a_{k-2}) + (n - a_{k-1})$, und f, g sind offensichtlich invers zueinander. Den Rest besorgt die Gleichheitsregel. ∎

Beispiel 2.22 *Als Beispiel erhalten wir für $n = 6, k = 3$ die folgenden $\binom{5}{2} = 10$ geordneten 3-Zahlpartitionen von 6:*

$4+1+1, 1+4+1, 1+1+4, 3+2+1, 3+1+2, 2+3+1, 2+1+3, 1+3+2, 1+2+3, 2+2+2$

Als letztes wollen wir noch den Begriff einer *Multimenge* einführen.

Definition 2.23 *Eine Menge $M = \{1, \ldots, n\}$ heißt Multimenge (M, m), wenn mit M eine (zusätzliche) Abbildung $m : M \to \mathbb{N} \cup \{\infty\}$ assoziiert wird; die Werte der Funktion m sind die Vielfachheiten, mit denen die Elemente aus M gezählt werden sollen.*

Wenn die Vielfachheiten nicht weiter spezifiziert sind, kann verabredungsgemäß davon ausgegangen werden, dass sie größtmöglich angesetzt werden können.

Beispiel 2.24 *$M = \{1, 1, 2, 2, 3\}$ ist z. B. eine Multimenge über $\{1, 2, 3\}$, wobei 1 und 2 mit der Vielfachheit 2 auftreten, 3 mit der Vielfachheit 1. Die Mächtigkeit einer Multimenge ist die Anzahl der Elemente gezählt mit ihrer Vielfachheit, in unserem Beispiel ist $|M| = 5$.*

Die folgende Formel zeigt uns neu die Bedeutung der steigenden Faktoriellen; dabei kann die Anzahl der k-Multimengen über einer n-Mengen können auch als die Möglichkeiten interpretiert werden, aus einer n-Menge mit Zurücklegen k Objekte ungeordnet auszuwählen:

Lemma 2.25 *Die Anzahl der k-Multimengen über einer n-Menge beträgt*

$$\frac{n(n+1)\ldots(n+k-1)}{k!} = \frac{n^{\overline{k}}}{k!}$$

Beweis: Wiederum liefert die Gleichheitsregel den Beweis. Sei S die Menge aller k-Multimengen über $\{1, 2, \ldots, n\}$ und T die Menge aller k-Untermengen von $\{1, 2, \ldots, n+k-1\}$, also

$$|T| = \binom{n+k-1}{k} = \frac{n^{\overline{k}}}{k!}.$$

Für $\{a_1 \leq a_2 \leq \ldots \leq a_k\} \in S$ setzen wir $f(\{a_1 \leq \ldots \leq a_k\}) = \{a_1, a_2+1, a_3+2, \ldots, a_k+(k-1)\}$. Es gilt $1 \leq a_1 < a_2+1 < \ldots < a_k+(k-1)$, also ist $f(\{a_1 \leq \ldots \leq a_k\}) \in T$. Die inverse Abbildung ist $g(\{b_1 < \ldots < b_k\}) = \{b_1 \leq b_2 - 1 \leq \ldots \leq b_k - (k-1)\}$, und der Beweis ist fertig. ∎

2.4.4 Zählkoeffizienten und Funktionen endlicher Mengen

Unsere fundamentalen Zählkoeffizienten treten in ganz natürlicher Weise beim Abzählen von Abbildungen auf. Betrachten wir die Abbildungen $f : N \longrightarrow R$, wobei $|N| = n$, $|R| = r$ sein soll. Die Gesamtzahl der Abbildungen ist r^n, da wir für jedes Element r mögliche Bilder haben, so dass wir mit der Produktregel r^n erhalten. Desgleichen liefert die Produktregel für die Anzahl der injektiven Abbildungen $r(r-1)\ldots(r-n+1)$.

Wie sieht es mit den surjektiven Abbildungen aus? Jede Abbildung f kann durch die Urbilder $\{f^{-1}(y) \mid y \in R\}$ beschrieben werden. Zum Beispiel entspricht die Abbildung f, mit

$$f(i) = \begin{cases} a & i = 1, 2, 4 \\ b & i = 3, 5 \end{cases}$$

wobei $N = \{1, 2, 3, 4, 5\}$ und $R = \{a, b, c\}$, also $f^{-1}(c) = \emptyset$. Ist insbesondere f surjektiv, so bilden die Urbilder eine geordnete r-Mengenpartition von N, und umgekehrt ergibt jede solche Partition genau eine surjektive Abbildung. In Zusammenfassung haben wir also:

$$\begin{aligned} |Abb\ (N, R)| &= r^n \\ |Inj\ (N, R)| &= r^{\underline{n}} \\ |Surj\ (N, R)| &= r! S_{n,r}. \end{aligned}$$

Jede Abbildung $f : N \longrightarrow R$ hat ein eindeutiges Bild $A \subseteq R,\ A = \{f(x) \mid x \in N\}$, und f ist surjektiv von N auf A. Klassifizieren wir daher die Abbildungen nach ihren Bildern, so ergibt die Summenregel

$$\begin{aligned} r^n = |Abb\ (N, R)| &= \sum_{A \subseteq R} |Surj\ (N, A)| \\ &= \sum_{k=0}^{r} \sum_{|A|=k} |Surj\ (N, A)| \\ &= \sum_{k=0}^{r} \binom{r}{k} k! S_{n,k} \\ &= \sum_{k=0}^{r} S_{n,k} r^{\underline{k}}, \end{aligned}$$

und wir erhalten eine Formel, welche die Potenzen, fallenden Faktoriellen und Stirling-Zahlen verknüpft:

$$r^n = \sum_{k=0}^{n} S_{n,k} r^{\underline{k}}. \tag{5}$$

Dabei können wir die Summation bei n abbrechen, da es offenbar keine k-Mengenpartitionen von N mit $k > n$ gibt, d.h. $S_{n,k} = 0$ für $k > n$.

2.4.5 Ziehen aus einer Urne bzw. Verteilen auf Fächer

Besonders einprägsam werden unsere Zählkoeffizienten, wenn wir die Menge N als Bälle ansehen, R als Fächer und eine Abbildung $f : N \longrightarrow B$ als Verteilung der Bälle in die Fächer. Injektiv heißt dann, dass in ein Fach höchstens ein Ball kommt, surjektiv, dass jedes Fach mindestens einen Ball enthält. Angenommen, die Bälle können nicht unterschieden werden, die Fächer aber schon. Wie viele Verteilungen gibt es dann?

Injektiver Fall: wir wählen jedesmal n der r Fächer, die einen Ball enthalten (welcher ist gleichgültig, da wir die Bälle nicht unterscheiden können), und erhalten somit genau die n-Untermengen von R mit der Anzahl $\binom{r}{n}$. Erlauben wir beliebige Verteilungen, so ergeben sich genau die n-Multimengen von R, deren Anzahl wir als $\frac{r^{\overline{n}}}{n!}$ berechnet haben.

Surjektiver Fall: Diese Verteilungen kennen wir schon. Das Fach i enthält $n_i \geq 1$ Bälle, insgesamt ist also $n = n_1 + \ldots + n_r$. eine geordnete Zahlpartition von n, und deren Anzahl ist $\binom{n-1}{r-1}$ (Korollar 2.21). Kombinieren wir alle Fälle, je nachdem ob die Bälle und Fächer unterscheidbar bzw. nicht unterscheidbar sind, so erhalten wir das folgende Diagramm, welches alle unsere fundamentalen Koeffizienten auf einen Blick ergibt:

2.4.6 Permutationen

Permutationen einer Menge, z.B. von $N = \{1, 2, \ldots, n\}$ können auf mehrfache Weisen dargestellt werden. Zunächst ist eine Permutation π einfach eine bijektive Abbildung

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}.$$

$\lvert N\rvert = n,\ \lvert R\rvert = r$	beliebig	injektiv	surjektiv	bijektiv
N unterscheidbar R unterscheidbar	r^n	$r^{\underline{n}}$	$r!S_{n,r}$	$r! = n!$
N nicht unterscheidbar R unterscheidbar	$\frac{r^{\overline{n}}}{n!}$	$\frac{r^{\underline{n}}}{n!} = \binom{r}{n}$	$\binom{n-1}{r-1}$	1
N unterscheidbar R nicht unterscheidbar	$\sum_{k=1}^{r} S_{n,k}$	0 oder 1	$S_{n,r}$	1
N nicht unterscheidbar R nicht unterscheidbar	$\sum_{k=1}^{r} P_{n,k}$	0 oder 1	$P_{n,r}$	1

Tabelle 2: Zählkoeffizienten als Anzahlen von geeigneten Funktionen

Halten wir die Ausgangsmenge in der Reihenfolge $1, 2, \ldots, n$ fest, so können wir π eindeutig als das Wort $\pi = \pi(1)\pi(2)\ldots\pi(n)$ schreiben. Jede Permutation π ist äquivalent zu einer Menge von Zyklen. Sei z.B.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 3 & 1 & 9 & 7 & 6 & 2 & 4 \end{pmatrix},$$

dann geht 1 nach 5, 5 nach 9, 9 nach 4 und 4 nach 1. Die Elemente $(1, 5, 9, 4)$ bilden einen Zyklus. Verfahren wir genau so mit den restlichen Elementen, so erhalten wir die Zyklendarstellung von π, π = (1,5,9,4)(2, 8)(3)(6,7). Die Anzahl der Elemente in einem Zyklus ist die *Länge des Zyklus*. Zyklen der Länge 1 nennen wir Fixpunkte. Besitzt sie keine Fixpunkte, so nennen wir sie *fixpunktfrei* (vgl. Abschnitt 2.1.1) oder sprechen auch von einem *Derangement*. Wir bemerken zwei Dinge: Zum einen kommt es bei der Zyklendarstellung nicht auf die Reihenfolge der Zyklen an, wir könnten in unserem Beispiel auch π = (6,7)(1,5,9,4)(3)(2,8) schreiben - es ist immer noch dieselbe Permutation. Zweitens können wir innerhalb eines Zyklus mit jedem beliebigen Element beginnen, dann ist die Reihenfolge allerdings festgelegt. Zum Beispiel ist auch $(7, 6)(9, 4, 1, 5)(8, 2)(3)$ eine Zyklendarstellung von π.

Für $n = 3$ erhalten wir beispielsweise die 6 Permutationen geschrieben als Wörter

$$123 \qquad 132 \qquad 213 \qquad 231 \qquad 312 \qquad 321$$

und in Zyklendarstellung

$$(1)(2)(3) \quad (1)(2,3) \quad (1,2)(3) \quad (1,2,3) \quad (1,3,2) \quad (1,3)(2).$$

Die Zyklendarstellung von π ergibt insbesondere eine Partition von N mit den Zyklen als Blöcken.

Definition 2.26 *Es seien $n, k \geq 0$. Die Anzahl $s_{n,k}$ der Permutationen einer n-Menge mit k Zykeln heißt Stirling-Zahl erster Art.*

Beispiel 2.27 *Als Beispiel haben wir $s_{n,1} = (n-1)!$, da wir in einem Zyklus der Länge n als Anfangselement 1 nehmen können, und dann die restlichen Elemente beliebig permutieren können. Ein weiteres Beispiel ist $s_{n,n-1} = \binom{n}{2}$, da eine Permutation mit $n-1$ Zyklen aus $n-2$ Fixpunkten und einem 2-er Zyklus besteht, den wir ersichtlich auf $\binom{n}{2}$ Arten wählen können.*

Natürlich folgt aus der Definition

$$n! = \sum_{k=1}^{n} s_{n,k} \ (n \geq 1).$$

Fur eine Permutation π bezeichne $b_i(\pi)$ die Anzahl der Zyklen der Länge i $(i = 1, \ldots, n)$ und $b(\pi)$ die Gesamtzahl der Zyklen, also

$$n \quad = \quad \sum_{i=1}^{n} i b_i(\pi)$$

Partition	Typ
5	5^1
$4+1$	$1^1 4^1$
$3+2$	$2^1 3^1$
$3+1+1$	$1^2 3^1$
$2+2+1$	$1^1 2^2$
$2+1+1+1$	$1^3 2^1$
$1+1+1+1+1$	1^5

Tabelle 3: Typen von 5-Permutationen

$$b(\pi) \quad = \quad \sum_{i=1}^{n} b_i(\pi).$$

Der *Typ der Permutation* π ist der formale Ausdruck $t(\pi) = 1^{b_1(\pi)} \dots n^{b_n(\pi)}$. In unserem obigen Beispiel haben wir $t(\pi) = 1^1 2^2 4^1$. (Die Zahlen i mit $b_i(\pi) = 0$ lassen wir weg.)

Wir sehen sofort, dass es genau soviele mögliche Typen von Permutationen gibt wie Zahl-Permutationen von n. Tabelle 3 listet die möglichen Typen einer 5-Permutation auf.

Wieviele Permutationen gibt es nun zu einem gegebenen Typ $1^{b_1} 2^{b_2} \dots n^{b_n}$? Wir schreiben die vorderhand leeren Zyklen hin

$$\underbrace{(\dots)\dots(\dots)}_{b_1}\underbrace{(\dots)\dots(\dots)}_{b_2}\underbrace{(\dots)\dots(\dots)}_{b_3}\dots$$

und füllen die Plätze der Reihe nach mit den $n!$ Wörtern. Auf diese Weise erhalten wir sicherlich die Permutationen von dem angegebenen Typ. Im allgemeinen werden wir jedoch dieselbe Permutation mehrfach produzieren. Da es auf die Reihenfolge der Zyklen nicht ankommt, können wir die b Zyklen der Länge i als ganzes permutieren, dies ergibt $b_1! b_2! \dots b_n!$ Mehrfachzählungen. Schließlich können wir das Anfangselement eines Zyklus fest angeben, also erhalten wir innerhalb der Zyklen weitere $1^{b_1} 2^{b_2} \dots n^{b_n}$ Mehrfachzählungen (diesmal ist damit ein echtes Produkt gemeint).

Lemma 2.28 *Es sei* $\sum_{i=1}^{n} i b_i = n$. *Die Anzahl der Permutationen vom Typ* $1^{b_1} 2^{b_2} \dots n^{b_n}$ *beträgt*

$$\frac{n!}{b_1! \dots b_n! 1^{b_1} 2^{b_2} \dots n^{b_n}}.$$

Insbesondere gilt

Korollar 2.29

$$s_{n,k} \quad = \quad \sum_{(b_1,\dots,b_n)} \frac{n!}{b_1! \dots b_n! 1^{b_1} 2^{b_2} \dots n^{b_n}} \; mit \; \sum_{i=1}^{n} i b_i = n, \sum_{i=1}^{n} b_i = k$$

$$n! \quad = \quad \sum_{(b_1,\dots,b_n)} \frac{n!}{b_1! \dots b_n! 1^{b_1} 2^{b_2} \dots n^{b_n}} \; mit \; \sum_{i=1}^{n} i b_i = n.$$

Tabelle 4 auf Seite 24 ergänzt unsere Liste (vgl. Tabelle 3 von Seite 23) der $5! = 120$ Permutationen hinsichtlich der Verteilung.

Permutationen werden uns noch oft begegnen, insbesondere bei Sortierproblemen. Betrachten wir eine Permutation $a_1, a_2, \dots, a_n$ von $\{1, \dots, n\}$ als Liste, so wollen wir diese Liste durch möglichst wenige Vertauschungen in die richtige Reihenfolge $1, 2, \dots, n$ bringen.

Anzahl der Permutationen	Stirlingzahlen
24	$s_{5,1} = 24$
30, 20	$s_{5,2} = 50$
20, 15	$s_{5,3} = 35$
10	$s_{5,4} = 10$
1	$s_{5,5}$

Tabelle 4: Anzahl für die Typen von 5-Permutationen

2.5 Rekursionen

2.5.1 Rekursion der Binomialkoeffizienten

Für die Binomialkoeffizienten haben wir bereits eine befriedigende geschlossene Formel

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!}$$

abgeleitet, für Stirling-Zahlen $s_{n,k}$ erster Art eine etwas unhandliche Summenformel (vgl. Seite 22 (die noch dazu wegen der unbekannten Anzahl der Summanden $= P_{n,k}$ Schwierigkeiten bereitet)). Für die Zahlen $S_{n,k}$ existiert vorläufig nur die Definition (vgl. Seite 18). Rekursionen helfen uns hier weiter.

Prominentestes Beispiel ist die Rekursionsgleichung für die Binomialkoeffizieten:

$$\binom{r}{k} = \binom{r-1}{k-1} + \binom{r-1}{k} \qquad (r \in \mathbb{C}\ \ k \in \mathbb{Z}) \tag{6}$$

Die Formel folgt direkt aus (4). Wir geben noch einen zweiten Beweis, der die sogenannte *Polynommethode* verdeutlicht. Für $k < 0$ sind beide Seiten von (6) gleich 0, und für $k = 0$, sind beide Seiten gleich 1. Sei also $k \geq 1$. Wir wissen schon, dass (6) für alle natürlichen Zahlen r richtig ist. Ersetzen wir r durch eine Variable x, so erhalten wir

$$\binom{x}{k} \stackrel{?}{=} \binom{x-1}{k-1} + \binom{x-1}{k}.$$

Auf den beiden Seiten stehen jeweils Polynome in x über $\mathbb{C}$ vom Grad k, und wir wissen, dass diese beiden Polynome denselben Wert für alle natürlichen Zahlen annehmen. Nun besagt ein Satz aus der Algebra, dass Polynome vom Grad k, die an mindestens $k+1$ Stellen übereinstimmen, identisch sind. Hier stimmen sie sogar für unendlich viele Werte überein, also gilt tatsächlich die Polynomgeichung

$$\binom{x}{k} = \binom{x-1}{k-1} + \binom{x-1}{k} \qquad (k \geq 1) \tag{7}$$

und daher ist (6) für alle $x = r \in \mathbb{C}$ richtig.

Die Polynome

$$\begin{aligned} x^{\underline{k}} &= x(x-1)\dots(x-k+1) \text{ bzw.} \\ x^{\overline{k}} &= x(x+1)\dots(x+k-1) \end{aligned}$$

mit $x^{\underline{0}} = x^{\overline{0}} = 1$ nennen wir wieder die fallenden bzw. steigenden Faktoriellen. Übrigens können wir auch aus der offensichtlichen Gleichung $x^k = x(x-1)^{\underline{k-1}} = (k(x-k))(x-1)^{\underline{k-1}} = k(x-1)^{\underline{k-1}} + (x-1)^{\underline{k-1}}(x-k) = k(x-1)^{\underline{k-1}} + (x-1)^{\underline{k}}$ durch Division mit $k!$ sofort auf (7) schließen.

n \ k	0	1	2	3	4	5	6	7	...
0	1								
1	1	1							
2	1	2	1						
3	1	3	3	1					
4	1	4	6	4	1				
5	1	5	10	10	5	1			
6	1	6	15	20	15	6	1		
7	1	7	21	35	35	21	7	1	
:									

Tabelle 5: Pascal'sches Dreieck $\binom{n}{k}$

Die Rekursion (6) ergibt für $n, k \in \mathbb{N}_0$ das *Pascal'sche Dreieck* (vgl. Tabelle 5), wobei die leeren Stellen jeweils 0 sind, da $\binom{n}{k} = 0$ ist für $n < k$. Die Geheimnisse und Schönheiten des Pascal'schen Dreiecks füllen ganze Bände. Wir verweisen auf www.wikipedia.com, was die Person sc Blaise Pascal[20] anbetrifft. Wir wollen nur drei Formeln festhalten. Erstens ist die Zeilensumme mit Index n, nämlich

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n, \tag{8}$$

da wir hierbei ja genau die Untermengen einer n-Menge abzählen. Betrachten wir nun eine Spaltensumme mit Index k bis zur Zeile n, also $\sum\limits_{m=0}^{n} \binom{m}{k}$. Für $k = 2$, $n = 6$ erhalten wir $35 = \binom{7}{3}$ und für $k = 1$, $n = 5, 15 = \binom{6}{2}$.

Allgemein gilt

$$\sum_{m=0}^{n} \binom{m}{k} = \binom{n+1}{k+1} \qquad (n, k \geq 0) \tag{9}$$

Für $n = 0$ ist dies sicherlich richtig, und mit Induktion erhalten wir aus (5)

$$\sum_{m=0}^{n+1} \binom{m}{k} = \sum_{m=0}^{n} \binom{m}{k} + \binom{n+1}{k} = \binom{n+1}{k+1} + \binom{n+1}{k} = \binom{n+2}{k+1}$$

Schließlich betrachten wir noch die Diagonalen links und rechts unten, also den Ausdruck

$$\sum_{k=0}^{n} \binom{m+k}{k},$$

wobei m die Anfangszeile und n die Endspalte bezeichnet. Betrachte im Dreieck die Diagonale mit $m = 3$, $n = 3$, die Summe ist $35 = \binom{7}{3}$.

$$\sum_{k=0}^{n} \binom{m+k}{k} = \binom{m+n+1}{n} \qquad (m, n \geq 0) \tag{10}$$

Der Beweis wir wiederum durch Induktion geliefert. Übrigens gilt (10) für beliebiges $m \in \mathbb{C}$.

[20] Blaise Pascal (geboren 19. Juni 1623 in Clermont-Ferrand; gestorben 19. August 1662 in Paris) war ein französischer Mathematiker, Physiker, Literat und Philosoph. In der Mathematik sind noch ihm benannt: das Pascal'sche Dreieck, der Satz von Pascal in der Geometrie, die Pascal'sche Schnecke, ebene Kurve und manche Einsichten in der Wahrscheinlichkeitsrechnung.

2.5.2 Negation und das Reziprozitätsgesetz

$$\binom{-r}{k} = (-1)^k \binom{r+k-1}{k} \qquad (r \in \mathbb{C},\, k \in \mathbb{Z}) \tag{11}$$

Wir haben $(-x)^{\underline{k}} = (-x)(-x-1)\dots(-x-k+1) = (-1)^k x(x+1)\dots(x+k-1)$, also die allgemeine Polynomgleichung

$$(-x)^{\underline{k}} = (-1)^k x^{\overline{k}}. \tag{12}$$

Division durch $k!$ ergibt hieraus sofort (11). Die Formel (12) heißt das *Reziprozitätsgesetz* zwischen den fallenden und steigenden Faktoriellen.

Wir können aus (11) sofort eine weitere erstaunliche Eigenschaft des Pascal'schen Dreieckes ableiten. Betrachten wir die alternierenden Summen einer Zeile, z. B. der 7-ten Zeile. Wir erhalten $1, 1-7 = -6, 1-7+21 = 15$ und so weiter $-20, 15, -6, 1, 0$, also genau die darüberstehenden Zahlen mit wechselnden Vorzeichen. Tatsächlich, mit (11) und (10) sehen wir

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = \sum_{k=0}^{m} \binom{k-n-1}{k} = \binom{m-n}{m} = (-1)^m \binom{n-1}{m}$$

2.5.3 Binomialsatz

Durch Ausmultiplizieren des linken Produktes erhalten wir

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \qquad (n \geq 0).$$

Insbesondere ergibt dies für $y = 1$:

$$(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Setzen wir hier $x = 1$, bzw. $x = -1$, so resultieren die uns schon bekannten Formeln

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \text{ bzw. } 0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \qquad (n \geq 1) \tag{13}$$

2.5.4 Vandermonde-Identität

Als letztes wollen wir eine der wichtigsten Formeln überhaupt ableiten, die als VANDERMONDE[21]-Identität in der Literatur angesprochen wird.

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} \qquad (n \geq 0) \tag{14}$$

Wir beweisen die Gleichung für natürliche Zahlen $x = r, y = s$. Der Rest folgt dann mit unserer Polynommethode. Seien R und S disjunkte Mengen mit $|R| = r$, $|S| = s$. Links steht $\binom{r+s}{n}$, also die Anzahl aller n-Untermengen von $R+S$. Wir klassifizieren nun diese Untermengen A nach ihrem Durchschnitt $|A \cap R| = k$, $k = 0, \dots, n$. Gilt $|A \cap R| = k$, so muss $|A \cap S| = n-k$ sein, d. h. es gibt genau $\binom{r}{k}\binom{s}{n-k}$ k-Untermengen mit $|A \cap R| = k$ (Produktregel). Anwendung der Summenregel liefert nun das Ergebnis.

[21] Alexandre-Thophile Vandermonde (geboren 28. Februar 1735 in Paris, gestorben 1. Januar 1796 in Paris) war ein französischer Musiker, Mathematiker und Chemiker.

Vandermondes Leidenschaft war das Violinenspielen. Das Interesse an mathematischen Problemen kam erst, als er etwa 35 Jahre alt war. Vandermonde beschäftige sich unter anderem mit symmetrischen Funktionen, der Lösung von zyklischen Polynomen, der Galoistheorie und den Springerzügen im Schachspiel.

Nach ihm benannt ist die Vandermonde-Matrix, eine speziellen Form einer Matrix.

n \ k	0	1	2	3	4	5	6	7	...
0	1								
1	0	1							
2	0	1	1						
3	0	1	3	1					
4	0	1	7	6	1				
5	0	1	15	25	10	1			
6	0	1	31	90	65	15	1		
7	0	1	63	301	350	140	21	1	
:									

Tabelle 6: Stirling-Zahlen $S_{n,k}$ zweiter Art

2.5.5 Rekursionsgleichungen der Stirling-Zahlen

Betrachten wir zunächst die Stirling-Zahlen zweiter Art $S_{n,k}$, also k-Mengenpartitionen einer n-Menge. Ähnlich wie für Binomialzahlen haben wir jedenfalls $S_{n,k} = 0$ für $n < k$, da eine n-Menge höchstens eine n-Partition gestattet. Wir setzen zusätzlich $S_{0,0} = 1$ und $S_{0,k} = 0$ für $k > 0,\ S_{n,0} = 0$ für $n > 0$.

Lemma 2.30 *Die Stirling-Zahlen $S_{n,k}, (n, k > 0)$ zweiter Art genügen der folgenden Rekursion:*

$$S_{n,k} = S_{n-1,k-1} + kS_{n-1,k} \tag{15}$$

Beweis: Zum Beweis verwenden wir natürlich die Summenregel. Sei N eine n-Menge. Wir klassifizieren die k-Partitionen nach einem festen Element $a \in N$. Bildet $\{a\}$ für sich einen Block, so bilden die restlichen Blöcke eine $(k-1)$-Partition von $N \setminus \{a\}$. Dies ergibt den Summanden $S_{n-1,k-1}$. Andernfalls entfernen wir a. $N \setminus \{a\}$ ist in diesem Fall in k Blöcke zerlegt, und wir können a in jeden dieser k Blöcke einfügen, also erhalten wir $kS_{n-1,k}$ Partitionen im zweiten Fall. ∎

Aus der Rekursion (15) ergibt sich das Stirling-Dreieck zweiter Art (vgl. Tabelle 6).

Einige spezielle Werte fallen sofort auf:

$$S_{n,1} = 1,\ S_{n,2} = 2^{n-1} - 1,\ S_{n,n-1} = \binom{n}{2},\ S_{n,n} = 1.$$

$S_{n,n-1} = \binom{n}{2}$ ist klar, da eine $(n-1)$-Partition aus einem Paar und $n-2$ einzelnen Elementen besteht. Zerlegen wir N in zwei disjunkte Blöcke, so sind diese beiden Mengen $A, N \setminus A$ komplementär zueinander und $A \neq \emptyset, N$. Also gilt $S_{n,2} = \frac{2^n - 2}{2} = 2^{n-1} - 1$.

Wir wenden uns nun den Stirlingzahlen $s_{n,k}$ erster Art zu und erinnern, dass diese die Anzahl der Permutationen eine n-Menge beschreiben, die in k Zyklen zerfallen. Wie üblich setzen wir $s_{0,0} = 1,\ s_{0,k} = 0\ (k > 0),\ s_{n,0} = 0\ (n > 0)$. Die Rekursion lautet in diesem Fall:

Lemma 2.31 *Die Stirling-Zahlen $s_{n,k}, n, k > 0$ erster Art genügen der folgenden Rekursion:*

$$s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k} \tag{16}$$

Beweis: Wie gewohnt klassifizieren wir die Permutationen von N mit k Zyklen nach einem Element $a \in N$. Es gibt $s_{n-1,k-1}$ solcher Permutationen, die a als 1-Zyklus enthalten. Ansonsten zerfällt $N \setminus \{a\}$ in k Zyklen und wir können a vor jedes der $n-1$ Elemente aus $N \setminus \{a\}$ in einem Zyklus eintragen. ∎

Die kleinen Werte des Stirling-Dreiecks erster Art werden in Tabelle 7 aufgelistet. Einige Werte kennen wir schon:

$$s_{n,1} = (n-1)!,\ s_{n,n-1} = \binom{n}{2},\ s_{n,n} = 1.$$

n \ k	0	1	2	3	4	5	6	7
0	1							
1	0	1						
2	0	1	1					
3	0	2	3	1				
4	0	6	11	6	1			
5	0	24	50	35	10	1		
6	0	120	274	225	85	15	1	
7	0	720	1764	1624	735	175	21	1

Tabelle 7: Stirling-Zahlen $s_{n,k}$ erster Art

Zur Berechnung von $s_{n,2}$ verwenden wir (16). Division durch (n-1)! ergibt

$$\frac{s_{n,2}}{(n-1)!} = \frac{(n-2)!}{(n-1)!} + \frac{(n-1)s_{n-1,2}}{(n-1)!} = \frac{s_{n-1,2}}{(n-2)!} + \frac{1}{n-1}$$

also durch die Iteration

$$s_{n,2} = (n-1)!(\frac{1}{n-1} + \frac{1}{n-2} + \ldots + 1) = (n-1)!H_{n-1},$$

wobei H_{n-1} die uns schon bekannte $(n-1)$-te harmonische Zahl bezeichnet.

Warum heißen $s_{n,k}$ und $S_{n,k}$ Stirling-Zahlen erster und zweiter Art? Hier ist der Grund. Wir haben bereits gezeigt, dass $r^n = \sum_{k=0}^{n} S_{n,k} r^{\underline{k}}$ für alle $r \in \mathbb{N}$ gezeigt. Mit unserer bewährten Polynommethode können wir somit auf die Polynomgleichung

$$x^n = \sum_{k=0}^{n} S_{n,k}\, x^{\underline{k}} \tag{17}$$

schließen. Drücken wir umgekehrt die fallenden Faktoriellen $x^{\underline{n}}$ durch die Potenzen x^k aus, so behaupten wir

$$x^n = \sum_{k=0}^{n} (-1)^{n-k} s_{n,k}\, x^k. \tag{18}$$

Für $n = 0$ ist dies offensichtlich richtig. Induktion liefert nun mit Hilfe von (16)

$$\begin{aligned}
x^{\underline{n}} &= x^{\underline{n-1}}(x-n+1) \\
&= \sum_{k=0}^{n-1} (-1)^{n-1-k} s_{n-1,k}\, x^k (x-n+1) \\
&= \sum_{k=0}^{n-1} (-1)^{n-1-k} s_{n-1,k}\, x^{k+1} + \sum_{k=0} n-1(-1)^{n-k}(n-1)s_{n-1,k}\, x^k \\
&= \sum_{k=0}^{n} (-1)^{n-k} (s_{n-1,k-1} + (n-1)s_{n-1,k})\, x^k \\
&= \sum_{k=0}^{n} (-1)^{n-k} s_{n,k}\, x^k
\end{aligned}$$

Dies ist der Grund für die Bezeichnung erster und zweiter Art. Die Polynomfolgen (x^n) und $(x^{\underline{n}})$ können eindeutig wechselweise als Linearkombination dargestellt werden, und die Verbindungskoeffizienten von $x^{\underline{n}}$ ausgedrückt durch x^k bzw. x^n ausgedrückt durch $x^{\underline{k}}$ sind (bis auf das Vorzeichen) genau die Stirling Zahlen erster bzw. zweiter Art. Später werden wir diesen Gedanken bei der Ableitung von allgemeinen Inversionsformeln aufgreifen. Übrigens werden in der Literatur die Stirling-Zahlen erster Art auch durch $(-1)^{n-k}s_{n,k}$ bezeichnet, also mit wechselndem Vorzeichen.

2.6 Existenzaussagen

Bei den allermeisten Problemen werden wir die genaue Anzahl von vorgegebenen Objekten nicht bestimmen können. Wir müssen uns dann mit Abschätzungen und Aussagen über die Größenordnung zufriedengeben - mehr darüber in Kapitel 5 in [1]. Einen ganz anderen Charakter erhält das Problem, wenn wir uns die Frage stellen, ob überhaupt ein Objekt mit den angegebenen Bedingungen existiert. Eine Antwort erhalten wir, wenn es uns gelingt, ein solches Objekt direkt zu konstruieren, oder umgekehrt die Nichtexistenz zu beweisen. Wir konzentrieren uns hier auf den Existenzaspekt. Alle möglichen Objekte durchzuprobieren, um zu sehen, ob eines den Bedingugen genügt, wird meist aufwendig sein. Gesucht ist also eine Aussage, die es uns erlaubt, die Existenz zu behaupten, ohne alle Objekte durchzugehen, ja ohne das gesuchte Objekt überhaupt zu kennen.

Ein Beispiel möge das erläutern. Es seien $a_1, a_2, \ldots, a_n$ ganze Zahlen, die nicht verschieden zu sein brauchen. Existiert dann eine Teilmenge der Zahlen, deren Summe ein Vielfaches von n ist? Da es 2^n Teilsummen gibt, ist Durchprobieren für großes n unmöglich. Können wir trotzdem die Existenz einer solchen Summe behaupten? Für kleine Zahlen $n = 2, 3, 4$ oder 5 kann man ohne weiteres nachprüfen, dass so eine Teilmenge stets existiert. Aber stimmt dies auch für beliebiges n?

2.6.1 Schubfachprinzip

Die einfachste, aber zugleich sehr anwendungsreiche Methode ist das Schubfachprinzip (im Englischen pigeonhole principle, also Taubenschlagprinzip, genannt).

(1) Verteilt man n Elemente auf r Fächer, $n > r$, so existiert ein Fach, das mindestens zwei Elemente erhält.

Völlig klar, da ist nichts zu beweisen. In der Sprache der Abbildungen lautet das Prinzip: Sind N und R zwei Mengen mit $|N| = n > r = |R|$ und f eine Abbildung von N nach R, so existiert ein $a \in R$ mit $|f^{-1}(a)| \geq 2$. Wir können (1) sofort verschärfen:

(2) Sei $f : N \to R$ mit $|N| = n > r = |R|$, so existiert ein $a \in R$ mit $|f^{-1}(a)| \geq \left\lfloor \frac{n-1}{r} \right\rfloor + 1$.

Wäre nämlich $|f^{-1}(a)| < \left\lfloor \frac{n-1}{r} \right\rfloor + 1$ für alle $a \in R$, so hätten wir

$$n = \sum_{a \in R} |f^{-1}(a)| \leq r \cdot \left\lfloor \frac{n-1}{r} \right\rfloor < n,$$

was nicht geht.

Mit dem Schubfachprinzip können wir mühelos unser Zahlenproblem lösen. Wir zeigen sogar mehr:

Lemma 2.32 *Es sei n eine natürliche Zahl und $a_1, \ldots, a_k, a_{k+1}, a_{k+2}, \ldots a_l$ eine Folge von Zahlen. Dann gibt es unter den Summen*

$$\sum_{i=k+1}^{l} a_i$$

stets eine solche, bei der der Summenwert ein Vielfaches von n ist.

Beweis: Wir setzen $N = \{0, a_1, a_1 + a_2, a_1 + a_2 + a_3, \ldots, a_1 + a_2 + \ldots + a_n\}$. Teilen wir eine beliebige ganze Zahl m durch n, so erhalten wir als Rest $0, 1, \ldots$ oder $n-1$. Wir schreiben $R = \{0, 1, 2, \ldots, n-1\}$ und erklären $f : N \to R$, indem wir $f(m)$ gleich dem Rest bei Division durch n setzen. Da $|N| = n+1 > n = |R|$ ist, folgt aus (1), dass es zwei Summen $a_1 + \ldots + a_k, a_1 + \ldots + a_l, k > l$, gibt, die denselben Rest bei Division durch n ergeben (wobei eine der beiden Summen die leere Summe sein könnte, die wir mit 0 bezeichnet haben). Also hat

$$\sum_{i=k+1}^{l} a_i = \sum_{i=1}^{l} a_i - \sum_{i=1}^{k} a_i$$

den Rest 0, und ist somit ein Vielfaches von n. ∎

Wir bemerken noch, dass die Anzahl n der Summanden kleinstmöglich ist, da wir nur $a_1 = a_2 = \ldots = a_{n-1} = 1$ zu setzen brauchen.

Eine weitere schöne Anwendung des Schubfachprinzips ist folgendes Beispiel:

Beispiel 2.33 *Sei $a_1, \ldots, a_{n^2+1}$ eine Folge von $n^2 + 1$ verschiedenen reellen Zahlen. Dann gibt es entweder eine monoton steigende Unterfolge $a_{k_1} < a_{k_2} < \ldots < a_{k_{n+1}}$ mit $k_1 < k_2 < \ldots < k_{n+1}$ von $n+1$ Zahlen oder eine monton fallende Unterfolge $a_{l_1} > a_{l_2} > \ldots > a_{l_{n+1}}$ von $n+1$ Zahlen.*

Hier bedarf es schon einigen Geschicks, das Schubfachprinzip anzuwenden.

Beweis: Zu a_i assoziieren wir die Zahl t_i, welche die Länge einer längsten monoton steigenden Unterfolge mit Anfangsglied a_i angibt; t_i ist also eine Zahl zwischen 1 und n^2+1. Gilt $t_i \geq n+1$ für ein i, so haben wir eine gesuchte ansteigende Folge gefunden. Nehmen wir also an, $t_i \leq n$ für alle i. Die Abbildung $f : a_i \to t_i$ zeigt uns laut (2), dass es ein $s \in \{1, \ldots, n\}$ gibt, so dass $\left\lfloor \frac{n^2}{n} \right\rfloor + 1 = n+1$ Zahlen $a_{l_1}, a_{l_2}, \ldots, a_{l_{n+1}}$, $(l_1 < l_2 < \ldots < l_{n+1})$ alle die maximale Länge s mit Anfangsglied a_{l_i} haben. Betrachten wir zwei aufeinanderfolgende Glieder $a_{l_i}, a_{l_{i+1}}$ dieser Teilfolge. Wäre $a_{l_i} < a_{l_{i+1}}$, so gäbe es eine ansteigende Unterfolge $a_{l_{i+1}} < \ldots$ der Länge s und damit eine der Länge $s+1$ mit Anfangsglied a_{l_i}, im Widerspruch zu $f(a_{l_i}) = s$. Die a_{l_i} erfüllen also $a_{l_1} > a_{l_2} > \ldots > a_{l_{n+1}}$, und wir haben unsere gewünschte absteigende Folge erhalten. Der Leser kann sich mühelos überlegen, dass die Aussage für n^2 Zahlen nicht mehr richtig ist, $n^2 + 1$ also wieder bestmöglich ist. ∎

2.6.2 Der Satz von Ramsey

Eine weitreichende Verallgemeinerung des Schubfachprinzips wurde von dem Logiker Frank Plumpton Ramsey[22,23] gefunden und im gleichen Jahr publiziert. Sehen wir uns nochmals das Schubfachprinzip an. Es ist vorteilhaft, die r Fächer als Farben zu interpretieren. Eine Abbildung $f : N \to R$

[22] 1903-1930

[23] aus Wikipedia, der freien Enzyklopädie. Frank Plumpton Ramsey (geboren 22. Februar 1903 in Cambridge; gestorben: 19. Januar 1930) war ein britischer Mathematiker und Logiker.

Ramsey wurde in Cambridge geboren, wo sein Vater Präsident des Magdalene College war. Er besuchte das College in Winchester bevor er nach Cambridge zurückkehrte um Mathematik am Trinity College zu studieren. Er erhielt den Grad 'Senior Wrangler', den höchsten Abschluss, der im Fach Mathematik zu erreichen war.

Ramseys überragende Intelligenz beeindruckte viele Akademiker in Cambridge. Er war auf verschiedenen Gebieten belesen und interessierte sich für fast alles. Politisch war er links-orientiert und wie seine Ehefrau ein 'militanter Atheist'. In einem Gespräch mit Charles Kay Ogden äußerte er seinen Wunsch Deutsch zu lernen. Ogden gab ihm ein Wörterbuch, dazu eine deutsche Grammatik und eine schwer verständliche philosophische Abhandlung und sagte zu ihm: 'Benutze die Grammatik und das Wörterbuch; komm wieder und sag uns was du darüber denkst.' Ungefähr eine Woche später hatte er nicht nur deutsch gelernt, sondern hatte Einwendungen gegen die Theorien der Abhandlung vorzubringen. Er benutzte seine neuerworbene Fähigkeit um Ludwig Wittgenstein's Tractatus Logico-Philosophicus zu lesen, welches jener 1918 fertigstellte.

Die Lektüre beeindruckte Ihn tief. Er übersetzte daraufhin einen großen Teil davon ins Englische und veröffentlichte eine erste Rezension in der philosophischen Zeitschrift Mind. 1923 reiste er für kurze Zeit nach österreich und diskutierte in dieser Zeit mit Wittgenstein, der in Puchberg zu der Zeit als Lehrer tätig war. 1924 schloss sich ein weiterer Besuch in österreich an für eine Psychoanalyse bei Theodor Reik in Wien und weiteren Besuchen bei Wittgenstein. Einige Philosophen sehen in Ramsey ein größeres Genie als Wittgenstein. Tatsächlich war er ein scharfer Kritiker Wittgensteins, hatte aber keinen so großen Einfluß auf ihn als z.B. Piero Sraffa.

Offenbar hin und hergerissen zwischen vergangenen und gegenwärtigen Ereignissen der Politik und unter dem Eindruck eines Genies wie Wittgenstein, schreibt er in dieser Zeit an seine Mutter: 'We really live in a great time for

ist also eine Färbung von N, und das Prinzip besagt: *Wenn mehr Elemente als Farben vorliegen, so müssen bei jeder Färbung mindestens zwei Elemente dieselbe Farbe erhalten.*

Wir können dies noch genauer spezifizieren.

> *Es seien natürliche Zahlen $l_1, \ldots, l_r$ gegeben, und eine $n-$Menge N mit $n \geq l_1 + \ldots + l_r - r + 1$. Dann muss es bei jeder Färbung von N eine Farbe i geben, so dass l_i Elemente mit der Farbe i gefärbt sind.*

Wir nennen dies die *Ramsey-Eigenschaft* für $(l_1, \ldots, l_r)$. Der ursprüngliche Fall (1) bezieht sich auf $l_1 = \ldots = l_r = 2$.

Hat eine n-Menge die Ramsey-Eigenschaft, so natürlich auch jede größere Menge. Es interessiert uns daher das kleinste solche n und dies ist offenbar genau $l_1 + \cdots + l_r - r + 1$, da für

$$m = \sum_{i=1}^{r} (l_i - 1) = \sum_{i=1}^{r} l_i - r$$

ja die Färbung vorliegen könnte, in der für jedes i genau $l_i - 1$ Elemente mit i gefärbt sind. Der Satz von Ramsey besagt nun, dass ein analoges Ergebnis für Färbungen von h-Mengen gilt ($h = 1$ ist das Schubfachprinzip). Wir wollen dies nur für $h = 2$, also Paare, zeigen und für zwei Farben. Der allgemeine Fall[24] folgt dann leicht.

Satz 2.34 *(Ramsey, $n = 2$) Es seien k und l natürliche Zahlen ≥ 2. Dann gibt es eine kleinste Zahl $R(k, l)$, genannt die Ramsey-Zahl, so dass folgendes gilt: Ist N eine n-Menge mit $n \geq R(k, l)$ und färben wir alle Paare aus N beliebig mit rot oder blau, dann gibt es entweder ein k-Menge in N, deren Paare alle rot gefärbt sind oder eine l-Menge, deren Paare alle blau gefärbt sind.*

Offenbar gilt $R(k, 2) = k$, da in einer k-Menge entweder alle Paare rot gefärbt sind oder ein Paar blau gefärbt ist ($l = 2$). Analog haben wir $R(2, l) = l$. Nun verwenden wir Induktion nach $k + l$. Wir nehmen an, dass $R(k-1, l)$ und $R(k, l-1)$ existieren und zeigen

$$R(k, l) \leq R(k-1, l) + R(k, l-1)$$

Es sei also die Menge N mit $N = n = R(k-1, l) + R(k, l-1)$ gegeben, deren Paare beliebig mit rot und blau gefärbt sind. Sind $a \in N$, dann zerfällt $N \setminus a$ in $R \cup B$, wobei $x \in R$ ist, falls $\{a, x\}$ rot gefärbt ist bzw. $y \in B$, falls $\{a, y\}$ blau gefärbt ist. Da

$$|R| + |B| = R(k-1, l) + R(k, l-1) - 1$$

ist, so muss entweder $|R| \geq R(k-1, l)$ sein oder $|B| \geq R(k, l-1)$. Nehmen wir den ersten Fall an (der zweite geht analog). Nach Induktion gibt es in R entweder $k-1$ Elemente, deren Paare rot gefärbt sind, dann haben wir zusammen mit a unsere gesuchte k-Menge. Oder es gibt eine l-Menge, deren Paare alle blau gefärbt sind, und wir sind wieder fertig.

---

thinking, with Einstein Freud and Wittgenstein all alive, and all in Germany or Austria, those foes of civilisation!'

Zurück in England wird er im jugendlichen Alter von 21 Jahren als Fellow ans King's College berufen und war College's Director of Studies in Mathematics.

Die beiden Existenzsätze, die von Ramsey in seiner Arbeit *On a problem of formal logic* aufgestellt wurden, wirkten als Initialzündung für weitere Arbeiten auf dem Gebiet der Graphentheorie und der Kombinatorik und sind als Ramsey-Theorem bekannt. Den in der Kombinatorik daraus entstandener Korpus nennt man Ramsey-Theorie.

Ramsey, befreundet mit John Maynard Keynes, veröffentlichte auch die zwei wichtigen ökonomischen Arbeiten A contribution to the theory of taxation und A mathematical theory of saving. Er stellte 1928 die Ramsey-Regel auf, mit der er das phelpsche Theorem erweiterte.

Am 19. Januar 1930 starb Frank Plumpton Ramsey mit 26 Jahren an den Folgen einer Operation.

[24] zitiert aus [11]: Let $r \geq 1$ and $q_i \geq r$, $i = 1, 2, \ldots, s$ be given. There exists a minimal positive integer $N(q_1, \ldots q_s; r)$ with the following property. Let S be a set set with n elements. Suppose that all $\binom{n}{r}$ r-subsets of S are divided into s mutually exclusive families $T_1, \ldots T_s$ ('colors'. Then if $n \geq N(q_1, \ldots, q_s; r)$ there is an i with $1 \leq i \leq s$, and some q_i-subset of S for which every r-subset is in T_i.

Aus der 'Pascal'-Rekursion $R(k,l) \leq R(k-1,l) + R(k,l-1)$ und den Anfangsbedingungen erkennen wir sofort

$$R(k,l) \leq \binom{k+l-2}{k-1}.$$

Zum Beispiel erhalten wir für den ersten interessanten Fall $R(3,3) \leq \binom{4}{2} = 6$; man kann sich überlegen, dass $R(3,3)$ nicht 5 sein kann; dazu färbe man Paare, deren Elemente modulo 2 gleich sind 'blau', ansonsten 'rot'. Dann kann es keine 3-Menge geben, die die Ramsey-Eigenschaft erfüllt.

Mit der folgenden Interpretation wird der Satz von Ramsey in vielen Büchern über mathematische Puzzles erwähnt.

Beispiel 2.35 *N ist eine Menge von Personen, ein rotes Paar bedeutet, dass sich die beiden kennen, und ein blaues, dass sie sich nicht kennen. Die Ramsey-Zahl $R(3,3) = 6$ besagt somit: In jeder Gruppe von 6 Personen gibt es immer drei, die untereinander bekannt sind, oder drei, die sich gegenseitig nicht kennen.*

Eine ganz andere außerordentlich nützliche Methode ist wahrscheinlichkeitstheoretischer Natur. Wir definieren auf unseren Objekten einen Wahrscheinlichkeitsraum und zeigen, dass die Wahrscheinlichkeit für ein Objekt, die gegebenen Bedingungen zu erfüllen, größer als 0 ist. Dann muss es ein solches Objekt geben.

Als Illustration betrachten wir folgendes Färbungsproblem, das auf den berühmten ungarischen Mathematiker Paul Erdös[25,26] zurückgeht. Es sei F eine Familie von d-Mengen, $d \geq 2$, aus einer Grundmenge X. Wir sagen, dass F 2-färbbar ist, falls es eine Färbung der Elemente von X mit zwei Farben gibt, so dass in jeder Menge $A \in F$ beide Farben auftreten.

Es ist klar, dass man nicht jede Familie F so färben kann. Ist zum Beispiel F die Familie aller d-Untermengen einer $(2d-1)$-Menge, so muss es (nach dem Schubfachprinzip) eine gleichgefärbte d-Menge geben. Andererseits ist aber auch klar, dass jede Teilfamilie einer 2-färbbaren Familie selber 2-färbbar ist. Wir interessieren uns also für die kleinste Zahl $m = m(d)$, für die es eine Familie F mit $|F| = m$ gibt, welche nicht 2-färbbar ist. Das obige Beispiel zeigt also $m(d) \leq \binom{2d-1}{d}$. Wie ist es mit einer unteren Schranke für $m(d)$?

(4) Wir haben $m(d) > 2^{d-1}$, das heißt: Jede Familie mit höchstens 2^{d-1} d-Mengen ist 2-färbbar.

[25] 1913 - 1996

[26] Babai, László; Pomerance, Carl; Vértesi, Péter. The mathematics of Paul Erdös. (English) [J] Notices Am. Math. Soc. 45, No.1, 19-31 (1998). [ISSN 0002-9920; ISSN 1088-9477] This memorial triptych surveys Paul Erdös's contribution to and influence of mathematics. It consists of 'Paul Erdös, Number Theorist Extraordinaire' by Carl Pomerance, 'Finite and Transfinite Combinatorics'by László Babai, and "Approximation Theory" by Péter Vértesi. Carl Pomerance surveys Paul Erdös's contribution to number theory, which numbers over 600 articles. He details Erdös's theorems, conjectures, and Erdös's influence on the mathematical work of Pomerance. László Babai discusses at length Paul Erdös's work in set theory, combinatorics (including graph theory), combinatorial geometry, combinatorial number theory and probability theory, which number over 800 articles. Péter Vértesi briefly reviews Paul Erdös's contribution to approximation theory and polynomials.

This is a fine survey. It shows a great breadth of Paul Erdös's mathematical interests and the enormity of his contributions and influence. The survey implicitly shows the classic quality of the problems posed by Erdös: simplicity of their formulations combined with their depth and often level of difficulty that has to be overcome in their solutions. In the case of combinatorics, Babai's is explicit about it: "If combinatorics is the art of finding patterns under virtually no assumption, Erdös was the master of this art." The survey lists a number of Paul Erdös's conjectures, whose proof will occupy mathematicians for decades if not centuries to come. Here is a $3,000 conjecture, which for a long time was Paul Erdös' favorite: Let S be a subset of positive integers such that the sum of the reciprocals of the numbers from S is infinite; then S contains arbitrarily long arithmetic progressions.

Each part of the triptych offers its own bibliography. The reviewer would like to add that a number of books dedicated to Paul Erdös's open problems has or soon will come out: Erdös on graphs: His legacy of unsolved problems by *F. Chung* and *R. Graham*. Wellesley, MA : AK Peters (1998; Zbl 0890.05049); Old and new problems and results in combinatorial number theory by *P. Erdös*, *R. L. Graham*, *M. B. Nathanson* and *X. Jia* (a new, expanded edition of the rare 1980 book, Berlin, Springer (1998); Problems of pgom Erdös by *P. Erdös* and *A. Soifer* (to be published by Center for Excellence in Mathematical Education, Colorado Springs in 2001). [A.Soifer (Colorado Springs)]

Sei F mit $|F| \leq 2^{d-1}$ gegeben. Wir färben X zufällig mit 2 Farben, wobei alle Färbungen gleich wahrscheinlich sind. Für $A \in F$ sei E_A das Ereignis, dass die Elemente von A alle dieselbe Farbe erhalten. Da es genau zwei solche Färbungen auf A gibt, erhalten wir

$$p(E_A) = \frac{2}{2^d} = \frac{1}{2^{d-1}}.$$

Also gilt mit $|F| \leq 2^{d-1}$ (wobei die Ereignisse nicht disjunkt sind)

$$p\left(\bigcup_{A \in F} E_A\right) < \sum_{A \in F} p(E_A) = m\frac{1}{2^{d-1}} \leq 1$$

$\bigcup_{A \in F} E_A$ ist nun das Ereignis, dass irgendeine Menge aus F einfarbig ist, und wir schließen wegen

$$p\left(\bigcup_{A \in F} E_A\right) < 1,$$

dass es eine 2-Färbung von S ohne einfarbige Mengen geben muss - und genau das wollten wir zeigen.

Eine obere Schranke für $m(d)$ von der Größenordnung $d^2 2^d$ ist ebenfalls bekannt, wobei diesmal zufällige Mengen und eine feste Färbung verwendet werden. An exakten Werten kenn man nur die ersten beiden: $m(2) = 3$ und $m(3) = 7$.

3 Summation

Als Ausgangstext hat auch für dieses Kapitel auf weite Strecken der vorzügliche und kompakte Text aus [1] gedient, den wir allerdings mit Kommentaren nachbearbeitet haben. In der Vorlesung wurde er nur in Teilen thematisiert.

Viele Abzählprobleme reduzieren sich auf die Auswertung von Summen, und umgekehrt lassen sich Zählkoeffizienten oft als eine Summe darstellen. Einige der Standardmethoden, wie man Summen berechnet wollen wir nun kennenlernen.

3.1 Direkte Methoden

Wir schreiben eine Summe üblicherweise in der Form

$$\sum_{k=0}^{n} a_k \text{ oder } \sum_{0\le k\le n} a_k.$$

Der Laufindex wird meist mit k bezeichnet. Wollen wir die geraden Zahlen zwischen 0 und 100 aufsummieren, so könnten wir $\sum_{k=0,\ k\ gerade}^{100} k$ schreiben oder $\sum_{k=1}^{50} 2k$. Bequemer ist die folgende Wahr-Falsch-Notation:

$$\sum_{k=0}^{100} k \quad [k = \text{ gerade }].$$

Der Klammerausdruck bedeutet

$$[k \text{ hat Eigenschaft } E] = \begin{cases} 1 & \text{falls } k \text{ die Eigenschaft } E \text{ erfüllt} \\ 0 & \text{falls nicht.} \end{cases}$$

Eine der elementarsten (und nützlichsten) Techniken ist die *Indextransformation*. Sei $i \ge 0$, dann ist

$$\sum_{k=m}^{n} a_k = \sum_{k=m+i}^{n+i} a_{k-i} = \sum_{k=m-i}^{n-i} a_{k+i}.$$

Also: Erniedrigung im Laufindex um i entspricht Erhöhung der Summationsgrenzen um i, und umgekehrt. Als weiteres Beispiel erhalten wir durch die Transformation $k \to n-k$ bzw. $k \to m+k$

$$\sum_{k=m}^{n} a_k = \sum_{k=0}^{n-m} a_{n-k} = \sum_{k=0}^{n-m} a_{m+k}.$$

Betrachten wir z.B. die *arithmetische Summe*

$$S = 0\cdot a + 1\cdot a + ... + n\cdot a = \sum_{k=0}^{n} ka.$$

Durch die Transformation $k \to n-k$ sehen wir $S = \sum_{k=0}^{n}(n-k)a$, und daher

$$\begin{aligned} 2S &= \sum_{k=0}^{n} ka + \sum_{k=0}^{n}(n-k)a \\ &= \sum_{k=0}^{n} na \\ &= n\sum_{k=0}^{n} a = n(n+1)a, \end{aligned}$$

d.h. $S = \frac{n(n+1)}{2}a$.

Angenommen, wir haben ein quadratisches Schema von reellen Zahlen $a_i a_j$ gegeben $(i, j = 1, ..., n)$. Summieren wir alle Zahlen auf, so erhalten wir $S = \sum_{1 \le i,j \le n} a_i a_j = (\sum_{i=1}^n a_i)(\sum_{j=1}^n a_j) = (\sum_{k=1}^n a_k)^2$. Unsere Aufgabe lautet nun, alle Produkte $a_i a_j$ unterhalb (und einschließlich) der Hauptdiagonale zu summieren, also $\underline{S} = \sum_{1 \le j \le i \le n} a_i a_j$ zu bestimmen. Zunächst sehen wir, dass die Summe oberhalb (und einschließlich) der Hauptdiagonale $\overline{S} = \sum_{1 \le i \le j \le n} a_i a_j = \sum_{1 \le i \le j \le n} a_j a_i = \underline{S}$ ist. Aus $S = \underline{S} + \overline{S} - \sum_{i=1}^n a_i^2 = 2\underline{S} - \sum_{k=1}^n a_k^2$ berechnen wir nun sofort

$$\underline{S} = \frac{1}{2}((\sum_{k=1}^n a_k)^2 + \sum_{k=1}^n a_k^2).$$

Welche direkte Methode wird man zur Berechnung von Summen zuerst ausprobieren? Zuallererst sicherlich *Induktion*. Ein einfaches Beispiel ist die Summation der ersten n ungeraden Zahlen $S_n = \sum_{k=1}^n (2k-1)$. Man beginnt mit einer Tafel kleiner Werte:

n	1	2	3	4	5	6
S_n	1	4	9	16	25	36

Das sollte genügen, um die Antwort $S_n = n^2$ zu vermuten. Für $n = 1$ haben wir $S_1 = 1^2 = 1$. Aus der Annahme $S_n = n^2$ folgt nun $S_{n+1} = S_n + (2n+1) = n^2 + 2n + 1 = (n+1)^2$, und die Richtigkeit der Aussage folgt mit Induktion.

Der Nachteil der Induktionsmethode ist klar. Wir müssen die richtige Antwort "raten". Außerdem ist der Schluss von n auf $n+1$ des öfteren gar nicht einfach. Bei dieser zweiten Schwierigkeit kann man sich manchmal mit einer raffinierteren Variante der Induktion behelfen.

Betrachten wir die geometrisch-arithmetische Ungleichung: Seien $a_1, ..., a_n$ reelle Zahlen ≥ 0, dann gilt für alle $n \ge 1$:

$$\begin{array}{lrcll} (Pn) & \sqrt[n]{a_1 a_2 ... a_n} & \le & \frac{a_1 + ... + a_n}{n} & \text{oder} \\ & a_1 a_2 ... a_n & \le & (\frac{a_1 + ... + a_n}{n})^n. & \end{array}$$

Für $n = 1$ ist dies klar, für $n = 2$ haben wir

$$a_1 a_2 \le (\frac{a_1 + a_2}{2})^2 \Leftrightarrow 4a_1 a_2 \le a_1^2 + 2a_1 a_2 + a_2^2 \Longleftrightarrow 0 \le a_1^2 - 2a_1 a_2 + a_2^2 = (a_1 - a_2)^2,$$

also ist auch (P2) richtig. Der Schluss von n auf $n+1$ bereitet jedoch einige Mühe. Wir gehen statt dessen in zwei Schritten vor:

(a) $(Pn) \Rightarrow (P(n-1))$

(b) $(Pn) \wedge (P2) \Rightarrow P(2n)$.

Die Kombination dieser beiden Schritte liefert ebenfalls die volle Aussage. Zum Beweis von (a) setzen wir $b = \sum_{i=1}^{n-1} \frac{a_i}{n-1}$ und erhalten

$$\begin{array}{rcl} \left(\prod_{k=1}^{n-1} a_k\right) \sum_{k=1}^{n-1} \frac{a_k}{n-1} & = & \left(\prod_{k=1}^{n-1} a_k\right) b \overset{(Pn)}{\le} \left(\frac{\sum_{k=1}^{n-1} a_k + b}{n}\right)^n = \left(\frac{n \sum_{k=1}^{n-1} a_k}{n(n-1)}\right)^n \\ & = & \left(\frac{\sum_{k=1}^{n-1}}{n-1} a_k\right)^n \end{array}$$

also

$$\prod_{k=1}^{n-1} a_k \leq \left(\frac{\sum_{k=1}^{n-1} a_k}{n-1} \right)^{n-1}$$

Zu (b) haben wir

$$\begin{aligned}
\prod_{k=1}^{2n} a_k &= (\prod_{k=1}^{n} a_k)(\prod_{k=n+1}^{2n} a_k) \\
&\overset{(Pn)}{\leq} (\sum_{k=1}^{n} \frac{a_k}{n})^n (\sum_{k=n+1}^{2n} \frac{a_k}{n})^n \\
&\overset{(P2)}{\leq} \left(\frac{\sum_{k=1}^{2n} \frac{a_k}{n}}{2} \right)^{2n} \\
&= \left(\frac{\sum_{k=1}^{2n} a_k}{2n} \right)^{2n},
\end{aligned}$$

und wir sind fertig.

Eine weitere nützliche Methode besteht darin, den ersten und letzten Term einer Summe zu *isolieren*. Sei $S_n = \sum_{k=0}^{n} a_k$, dann gilt mit der Indextransformation

$$S_{n+1} = S_n + a_{n+1} = a_0 + \sum_{k=1}^{n+1} a_k = a_0 + \sum_{k=0}^{n} a_{k+1}.$$

Die Idee ist, die letzte Summe zu S_n in Beziehung zu setzen. Zwei Beispiele mögen dies erläutern.

Zunächst betrachten wir die *geometrische Summe* $S_n = 1 + a + a^2 + \ldots + a^n = \sum_{k=0}^{n} a^k$. Isolieren der Terme ergibt

$$S_{n+1} = S_n + a^{n+1} = 1 + \sum_{k=0}^{n} a^{k+1} = 1 + a \sum_{k=0}^{n} a^k = 1 + aS_n,$$

und wir erhalten $S_n + a^{n+1} = 1 + aS_n$, d.h. $S_n = \frac{a^{n+1}-1}{a-1}$ für $a \neq 1$. Für $a = 1$ ist das Ergebnis natürlich $S_n = n + 1$. Als nächstes sei $S_n = \sum_{k=0}^{n} k2^k$ zu berechnen. Unsere Methode ergibt

$$\begin{aligned}
S_{n+1} &= S_n + (n+1)2^{n+1} = \sum_{k=0}^{n} (k+1)2^{k+1} = 2\sum_{k=0}^{n} k2^k + 2\sum_{k=0}^{n} 2^k \\
&= 2S_n + 2^{n+2} - 2,
\end{aligned}$$

und daraus

$$S_n = (n-1)2^{n+1} + 2$$

Sobald eine Formel bewiesen ist, sollte man sie zur Sicherheit für kleine Werte verifizieren: Für $n = 4$ erhalten wir $S_4 = 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + 4 \cdot 2^4 = 2 + 8 + 24 + 64 = 98$ und rechts $3 \cdot 2^5 + 2 = 96 + 2 = 98$.

Wir wollen uns noch kurz dem zweiten Aspekt der Einleitung zuwenden: Darstellung einer Zählfunktion durch eine Summenformel. Die einfachste Form ist die folgende: Angenommen, die gesuchten Koeffizienten T_n $(n \geq 0)$ sind als Rekursion gegeben:

$$\begin{aligned} T_0 &= \alpha \\ a_n T_n &= b_n T_{n-1} + c_n \qquad (n \geq 1). \end{aligned}$$

Wir können darin T_{n-1} durch T_{n-2} ausdrücken, T_{n-2} durch T_{n-3} usw., bis wir bei T_0 angelangt sind. Das Ergebnis wird ein Ausdruck in a_k, b_k, c_k und α sein. Der folgende Ansatz erleichtert die Rechnung erheblich. Wir multiplizieren beide Seiten der Rekursion mit einem *Summationsfaktor* s_n, der

$$s_{n-1} a_{n-1} = s_n b_n \tag{19}$$

erfüllt. Mit $S_n = s_n a_n T_n$ erhalten wir daraus

$$S_n = s_n(b_n T_{n-1} + c_n) = S_{n-1} + s_n c_n$$

also

$$S_n = \sum_{k=1}^{n} s_k c_k + s_0 a_0 T_0$$

und somit

$$T_n = \frac{1}{s_n a_n}\Big(\sum_{k=1}^{n} s_k c_k + s_0 a_0 T_0\Big). \tag{20}$$

Wie finden wir nun die Summationsfaktoren s_n? Durch Iteration der definierenden Gleichung (19) erhalten wir

$$s_n = \frac{a_{n-1} s_{n-1}}{b_n} = \frac{a_{n-1} a_{n-2} s_{n-2}}{b_n b_{n-1}} = \ldots = \frac{a_{n-1} a_{n-2} \ldots a_0}{b_n b_{n-1} \ldots b_1},\ s_0 = 1, \tag{21}$$

oder irgendein Vielfaches. Allerdings müssen wir darauf achten, dass alle $a_i, b_j \neq 0$ sind.

3.1.1 Derangements

Als Beispiel wollen wir die Anzahl D_n der fixpunktfreien Permutationen, der sogenannten Derangements, berechnen. Wir haben $D_1 = 0, D_2 = 1$ und setzen $D_0 = 1$. Sei $n \geq 3$. Wir klassifizieren die fixpunktfreien Permutationen π nach dem Bild $\pi(1)$ von 1. Offfensichtlich kann $\pi(1)$ eine der Zahlen $2, 3, \ldots, n$ sein. Sei $\pi(i) = 1$. Nun unterscheiden wir zwei Fälle: $\pi(i) = 1$ oder $\pi(i) \neq 1$. Im ersten Fall haben wir $\pi = \binom{1 \ldots i \ldots n}{i \ldots 1 \ldots \pi(n)}$, das heißt die Zahlen $k \neq 1, i$ können auf alle Arten fixpunktfrei abgebildet werden, und wir erhalten demnach D_{n-2} Permutationen. Im zweiten Fall haben wir $\pi = \begin{pmatrix} 1 & \ldots & i & \ldots & n \\ i & \ldots & \pi(i) \neq 1 & \ldots & \pi(n) \end{pmatrix}$. Ersetzen wir nun in der ersten Zeile i durch 1 und entfernen die erste Stelle, so erhalten wir eine fixpunktfreie Permutation auf $\{1, \ldots, n\} \setminus \{i\}$, und umgekehrt ergibt jede solche Permutation durch Wiederersetzung $1 \to i$ eine Permutation von $\{1, \ldots, n\}$ mit $\pi(i) \neq 1$. Aus der Gleicheitsregel folgt, dass im zweiten Fall genau D_{n-1} Permutationen resultieren. Da $\pi(1)$ die $n-1$ Werte $2, \ldots, n$ annehmen kann, ergibt die Summenregel die Rekursion

$$D_n = (n-1)(D_{n-1} + D_{n-2}) \tag{22}$$

und diese Rekursion gilt auch für $n = 2$, da wir $D_0 = 1$ gesetzt haben. Um unsere Technik der Summationsfaktoren anwenden zu können, benötigen wir aber eine Rekursion erster Ordnung. Aus (22) ersehen wir

$$\begin{aligned} D_n - nD_{n-1} &= -(D_{n-1} - (n-1)D_{n-2}) \\ &= D_{n-2} - (n-2)D_{n-3} \\ &\vdots \\ &= (-1)^{n-1}(D_1 - D_0) = (-1)^n, \end{aligned}$$

also

$$D_n = nD_{n-1} + (-1)^n \qquad (n \geq 1), \tag{23}$$

und jetzt haben wir die gewünschte Form. Mit $a_n = 1, b_n = n, c_n = (-1)^n$ erhalten wir laut (21) den Summationsfaktor $s_n = \frac{1}{n!}$ und daraus mit (20)

$$D_n = n!(\sum_{k=1}^{n} \frac{(-1)^k}{k!} + 1) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!},$$

oder

$$\frac{D_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Aus der Analysis wissen wir, dass $\sum_{k=0}^{n} \frac{(-1)^k}{k!}$ mit $n \to \infty$ gegen e^{-1} konvergiert. Daraus können wir das überraschende Ergebnis ableiten: Ziehen wir zufällig eine Permutation, so ist die Wahrscheinlichkeit, eine fixpunktfreie Permutation zu erhalten, für große n, etwa $e^{-1} \sim \frac{1}{2{,}71} > \frac{1}{3}$. Amüsante Interpretation: Werden durch einen Windstoß die geordneten Manuskriptblätter eines Buches beliebig aufgewirbelt, so ist die Wahrscheinlichkeit, dass nachher keiner mehr am richtigen Platz liegt, größer als $\frac{1}{3}$ eine wahrhaft betrübliche Erkenntnis.

3.2 Differenzenrechnung

Die Summation $\sum_{k=a}^{b} g(k)$ können wir als diskretes Analogon des bestimmten Integrals $\int_a^b g(x)dx$ auffassen. Der Hauptsatz der Differential-Integralrechnung liefert uns bekanntlich folgende Methode zur Auswertung des Integrals. Sei D der Differentialoperator. Es sei f eine Stammfunktion von g, also $g = Df$, dann gilt

$$\int_a^b g(x)dx = f(b) - f(a) \tag{24}$$

Wir wollen untersuchen, ob wir auch im diskreten Fall einen solchen "Differentialoperator" finden können, der eine Berechnung der Summe wie in (19) erlaubt.

In der Analysis wird $Df(x)$ durch die Quotienten $\frac{f(x+h)-f(x)}{h}$ angenähert. Im diskreten Fall steht uns als beste Näherung $h = 1$ zur Verfügung, also $f(x+1) - f(x)$.
Für eine Funktion $f(x)$ erklären wir den *Translationsoperator* E^a mit Schrittweite a durch $E^a : f(x) \to f(x+a)$, wobei wir $E = E^1$ setzen und $I = E^0$. I ist die Identität. Nun erklären wir die beiden fundamentalen Differenzenoperatoren: $\Delta = E - I$ und $\nabla = I - E^{-1}$, also

$$\begin{aligned} \Delta: \ f(x) &\to f(x+1) - f(x) \\ \nabla: \ f(x) &\to f(x) - f(x-1). \end{aligned}$$

Δ heißt der *(Vorwärts-)Differenzenoperator* und ∇ der *(Rückwärts-)Differenzenoperator.*

Als Beispiel erhalten wir $\Delta(x^3) = (x+1)^3 - x^3 = 3x^2 + 3x + 1$, d.h.$\Delta$ blidet das Polynom x^3 auf das Polynom zweiten Grades $3x^2 + 3x + 1$ ab. Allgemein erniedrigt Δ den Grad einen Polynoms um 1, da sich die höchsten Potenzen wegkürzen.

Operatoren können wir auf die übliche Weise addieren, mit einem Skalarfaktor multiplizieren, und wir haben auch ein Produkt, die Komposition:

$$\begin{aligned} (P+Q)f &= Pf + Qf \\ (\alpha P)f &= \alpha(Pf) \\ (QP)f &= Q(Pf). \end{aligned}$$

Alle Rechenregeln gelten für die Operatoren wir für reelle Zahlen, mit Ausnahme der Existenz eines mulitplikativen Inversen. Berechnen wir beispielsweise Δ^n. Wegen $\Delta = E - I$ ist $\Delta^n = (E-I)^n$, und nach dem Binomialsatz, angewandt auf $(E-I)^n$ erhalten wir die wichtige Formel:

$$\begin{aligned} \Delta^n f(x) &= (E-I)^n f(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} E^k f(x) && (25) \\ &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(x+k). && (26) \end{aligned}$$

Insbesondere gilt dies für $x = 0$

$$\Delta^n f(0) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k). \tag{27}$$

Wir können also $\Delta^n f(x)$ an der Stelle $x = 0$ (oder an irgendeiner anderen Stelle) berechnen, ohne das Polynom $\Delta^n f(x)$ zu kennen. Betrachten wir als Beispiel $\Delta^3(x^4)$. Hier ergibt sich $\Delta^3(x^4)_{x=0} = \sum_{k=0}^{3} (-1)^{3-k} \binom{3}{k} k^4 = -0 + 3 \cdot 1 - 3 \cdot 2^4 + 3^4 = 36$. Zurück zu unserer eigentlichen Aufgabe. Eine wichtige Regel des Differenzierens besagt $Dx^n = nx^{n-1}$ für $n \in \mathbb{Z}$. Auch für die Differenzenoperatoren Δ und ∇ gibt es Folgen mit diesen Eigenschaften, die fallenden und steigenden Faktoriellen $x^{\underline{n}} = x(x-1)....(x-n+1)$ bzw. $x^{\overline{n}} = x(x+1)...(x+n-1)$, die wir schon in Abschnitt 2.5 kennengelernt haben.

Wir haben $(x+1)^{\underline{n}} = (x+1)x^{\underline{n-1}}, x^{\underline{n}} = x^{\underline{n-1}}(x-n+1)$ und daher

$$\Delta x^{\underline{n}} = (x+1)^{\underline{n}} - x^{\underline{n}} = (x+1)x^{\underline{n-1}} - x^{\underline{n-1}}(x-n+1) = nx^{\underline{n-1}}, \tag{28}$$

und analog

$$\nabla x^{\overline{n}} = x^{\overline{n}} - (x-1)^{\overline{n}} = x^{\overline{n-1}}(x+n-1) - (x-1)x^{\overline{n-1}} = nx^{\overline{n-1}} \tag{29}$$

Wir wollen (28) und (29) auf beliebiges $n \in \mathbb{Z}$ erweitern. Wie sollen wir $x^{\underline{n}}$ bzw. $x^{\overline{n}}$ für $n < 0$ erklären? Betrachten wir die Quotienten $x^{\underline{n}}/x^{\underline{n-1}}$, so erhalten wir $x - n + 1$, also z.B. $x^{\underline{3}}/x^{\underline{2}} = x - 2$, $x^{\underline{2}}/x^{\underline{1}} = x - 1$, $x^{\underline{1}}/x^{\underline{0}} = x$. Als nächsten Quotienten sollten wir $x^{\underline{0}}/x^{\underline{-1}} = 1/x^{\underline{-1}} = x + 1$ erhalten, also definieren wir $x^{\underline{-1}} = \frac{1}{x+1}$, und dann $x^{\underline{-2}} = \frac{1}{(x+1)(x+2)}$ usw. Analog gehen wir für $x^{\overline{n}}$ vor. In Zusammenfassung geben wir folgende Definition:

$$\begin{cases} x^{\underline{n}} &= x(x-1)...(x-n+1) & n \geq 0 \\ x^{\underline{-n}} &= \frac{1}{(x+1)..(x+n)} & n > 0 \end{cases} \tag{30}$$

$$\begin{cases} x^{\overline{n}} &= x(x+1)...(x+n-1) & n \geq 0 \\ x^{\overline{-n}} &= \frac{1}{(x-1)..(x-n)} & n > 0 \end{cases} \tag{31}$$

Die Formeln (28) und (29) gelten nun für alle $n \in \mathbb{Z}$. Prüfen wir dies für Δ nach:

$$\begin{aligned} \Delta x^{\underline{-n}} = (x+1)^{\underline{-n}} - x^{\underline{-n}} &= \frac{1}{(x+2)...(x+n+1)} - \frac{1}{(x+1)...(x+n)} \\ &= \frac{1}{(x+1)...(x+n+1)}(x+1-x-n-1) \\ &= (-n)\frac{1}{(x+1)...(x+n+1)} \\ &= (-n)x^{\underline{-n-1}} \end{aligned}$$

In Zusammenfassung gilt also für alle $n \in \mathbb{Z}$:

$$\Delta x^{\underline{n}} = nx^{\underline{n-1}} \tag{32}$$

$$\nabla x^{\overline{n}} = n x^{\overline{n-1}}. \tag{33}$$

Im Folgenden konzentrieren wir uns auf den Operator Δ. Rufen wir uns nochmals die analytische Methode in Erinnerung. Um $\int_a^b g(x)dx$ zu berechnen, bestimmen wir die Stammfunktion f, d.h. $Df = g$, und erhalten dann $\int_a^b g(x)dx = f(b) - f(a)$.

Wir gehen nun genauso vor: f heißt eine (diskrete) Stammfunktion von g, falls $\Delta f = g$ gilt. Wir schreiben dann $f = \sum g$ und nennen g eine unbestimmte Summe, also

$$\Delta f = g \Longleftrightarrow f = \sum g.$$

Das folgende Resultat ist das genaue Gegenstück zum Hauptsatz der Differentialrechnung:

Satz 3.1 *Es sei f eine Stammfunktion von g, dann gilt*

$$\sum_{k=a}^{b} g(k) = f(b+1) - f(a).$$

Beweis. Wegen $\Delta f = g$ gilt $f(k+1) - f(k) = g(k)$ für alle k, und wir erhalten

$$\sum_{k=a}^{b} g(k) = \sum_{k=a}^{b} (f(k+1) - f(k)) = f(b+1) - f(a).$$

Vorsicht: Die Summationsgrenzen für f sind a und $b+1$! Um unsere Methode effektiv anwenden zu können, benötigen wir also eine Liste von Stammfunktionen. Ein Beispiel kennen wir schon:

$$\sum x^{\underline{n}} = \frac{x^{\underline{n+1}}}{n+1} \qquad \text{für } n \neq -1.$$

Was ist $\sum x^{\underline{-1}}$? Aus $x^{\underline{-1}} = \frac{1}{x+1} = f(x+1) - f(x)$ folgt sofort $f(x) = 1 + \frac{1}{2} + ... + \frac{1}{x}$, d.h. $f(x) = H_x$, unsere wohlbekannte harmonische Zahl. In Zusammenfassung:

$$\sum x^{\underline{n}} = \begin{cases} \frac{x^{\underline{n+1}}}{n+1} & n \neq -1 \\ H_x & n = -1. \end{cases} \tag{34}$$

H_x ist also das direkte Analogon zum Logarithmus, und die ist auch der Grund, warum die harmonischen Zahlen in vielen Summationsformeln erscheinen. Was ist das Analogon zu e^x? Gesucht ist eine Funktion $f(x)$ mit $f(x) = \Delta f(x) = f(x+1) - f(x)$. Daraus folgt $f(x+1) = 2f(x)$, d.h. $f(x) = 2^x$. Betrachten wir eine beliebige Exponentialfunktion c^x $(c \neq 1)$. Aus $\Delta c^x = c^{x+1} - c^x = (c-1)c^x$ schließen wir

$$\sum c^x = \frac{c^x}{c-1} \qquad (c \neq 1). \tag{35}$$

Wir bemerken noch, dass die Operatoren Δ und $\sum$ linear sind, das heißt es gilt stets $\Delta(\alpha f + \beta g) = \alpha \Delta f + \beta \Delta g$ und $\sum(\alpha f + \beta g) = \alpha \sum f + \beta \sum g$.

Nun ist es aber an der Zeit, unsere Ergebnisse anzuwenden. Wollen wir zum Beispiel $\sum_{k=0}^{n} k^2$ berechnen, so benötigen wir eine Stammfunktion von x^2. Die kennen wir nicht, aber wir haben $x^2 = x(x-1) + x = x^{\underline{2}} + x^{\underline{1}}$ und erhalten nunmehr

$$\begin{aligned} \sum_{k=0}^{n} k^2 &= \sum_{0}^{n+1} x^2 = \sum_{0}^{n+1} x^{\underline{2}} + \sum_{0}^{n+1} x^{\underline{1}} = \frac{x^{\underline{3}}}{3} \,|_0^{n+1} + \frac{x^{\underline{2}}}{2} \,|_0^{n+1} \\ &= \frac{(n+1)^{\underline{3}}}{3} + \frac{(n+1)^{\underline{2}}}{2} = \frac{(n+1)n(n-1)}{3} + \frac{(n+1)n}{2} \\ &= \frac{n(n+\frac{1}{2})(n+1)}{3}. \end{aligned}$$

Es ist klar, wie diese Methode auf beliebige Potenzsummen $\sum_{k=0}^{n} k^m$ angewandt werden kann. Wir wissen aus Formel (17) in Abschnitt 2.5.5, dass $x^m = \sum_{k=0}^{m} S_{m,k} x^{\underline{k}}$ ist. Daraus folgt für $m \geq 1$

$$\begin{aligned}\sum_{k=0}^{n} k^m &= \sum_{0}^{n+1} x^m = \sum_{0}^{n+1} (\sum_{k=0}^{m} S_{m,k} x^{\underline{k}}) = \sum_{k=0}^{m} S_{m,k} \sum_{0}^{n+1} x^{\underline{k}} \\ &= \sum_{k=0}^{m} S_{m,k} \frac{x^{\underline{k+1}}}{k+1} \mid_0^{n+1} = \sum_{k=0}^{m} \frac{S_{m,k}}{k+1} x^{\underline{k+1}} \mid_0^{n+1} \\ &= \sum_{k=0}^{m} \frac{S_{m,k}}{k+1} (n+1)n...(n-k+1).\end{aligned}$$

Wir haben also die Potenzsumme auf lauter elementare Größen zurückgeführt, Stirlingzahlen und fallende Faktorielle. Insbesondere sehen wir, dass $\sum_{k=0}^{n} k^m$ ein Polynom in n vom Grad $m+1$ mit höchstem Koeffizienten $\frac{1}{m+1}$ und konstantem Glied 0 ist (wegen $S_{m,0} = 0$ für $m \geq 1$).

Auch eine Regel für die partielle Summation gibt es. Aus

$$\begin{aligned}\Delta(u(x)v(x)) &= u(x+1)v(x+1) - u(x)v(x) \\ &= u(x+1)v(x+1) - u(x)v(x+1) \\ &\quad + u(x)v(x+1) - u(x)v(x) \\ &= (\Delta u(x))v(x+1) + u(x)(\Delta v(x))\end{aligned}$$

folgt

$$\sum u \Delta v = uv - \sum (Ev) \Delta u,$$

also genau das Analogon zur Partiellen Integration, abgesehen von der zusätzlichen Translation E.

Unsere schon bekannte Summe $\sum_{k=0}^{n} k2^k$ können wir nun wir folgt berechnen. Wir setzen $u(x) = x, \Delta v(x) = 2^x$ und erhalten wegen $\sum 2^x = 2^x, \Delta x = 1$

$$\begin{aligned}\sum_{k=0}^{n} k2^k &= \sum_{0}^{n+1} x2^x = x2^x \mid_0^{n+1} - \sum_{0}^{n+1} 2^{x+1} = (n+1)2^{n+1} - 2^{x+1} \mid_0^{n+1} \\ &= (n+1)2^{n+1} - 2^{n+2} + 2 = (n-1)2^{n+1} + 2.\end{aligned}$$

Beispiel 3.2 *Wir wollen die ersten n harmonischen Zahlen aufsummieren. Mit* $u(x) = H_x,\ \Delta v(x) = 1 = x^{\underline{0}}$ *ergibt dies unter der Beachtung von (34)*

$$\begin{aligned}\sum_{k=1}^{n} H_k &= \sum_{1}^{n+1} H_x x^{\underline{0}} = H_x \mid_1^{n+1} - \sum_{1}^{n+1} \frac{1}{x+1}(x+1) = H_x x \mid_1^{n+1} - x \mid_1^{n+1} \\ &= (n+1)H_{n+1} - 1 - (n+1) + 1 = (n+1)(H_{n+1} - 1).\end{aligned}$$

Natürlich können wir dieses Ergebnis auch mit unseren direkten Methoden aus den vorigen Kapiteln herleiten, aber mit wesentlich mehr Mühe. Die Differenzenrechnung läuft dagegen vollkommen automatisch ab. Da dies für $\sum H_k$ so gut geklappt hat, noch ein etwas komplizierteres Beispiel:

Was ist $\sum_{k=1}^{n} \binom{k}{m} H_k$? Aus der *binomialen Rekursion* haben wir $\binom{x+1}{m+1} = \binom{x}{m} + \binom{x}{m+1}$, also $\Delta\binom{x}{m+1} = \binom{x}{m}$ oder $\sum \binom{x}{m} = \binom{x}{m+1}$. Partielle Summation mit $u(x) = H_x,\ \Delta v(x) = \binom{x}{m}$ ergibt:

$$\begin{aligned}\sum_{k=1}^{n} \binom{k}{m} H_k &= \sum_{1}^{n+1} \binom{x}{m} H_x = \binom{x}{m+1} H_x \mid_1^{n+1} - \sum_{1}^{n+1} \frac{1}{x+1} \binom{x+1}{m+1} \\ &= \binom{x}{m+1} H_x \mid_1^{n+1} - \frac{1}{m+1} \sum_{1}^{n+1} \binom{x}{m}\end{aligned}$$

$$\begin{aligned} &= \binom{x}{m+1} H_x \,|_1^{n+1} - \frac{1}{m+1}\binom{x}{m+1}\,|_1^{n+1} \\ &= \binom{n+1}{m+1}(H_{n+1} - \frac{1}{m+1}) \qquad (m \geq 0), \end{aligned}$$

da sich die unteren Grenzen wegkürzen.

Und noch einen Satz aus der Analysis können wir übertragen. Sei $f(x)$ ein Polynom, $f(x) = \sum_{k=0}^{n} a_k x^k$, dann wissen wir, dass für die Koeffizienten a_k gilt: $a_k = \frac{f^{(k)}(0)}{k!} = \frac{D^k f(0)}{k!}$, $D^k f$ die k-te Ableitung von f. $f(x) = \sum_{k=0}^{n} \frac{D^k f(0)}{k!} x^k$ heißt bekanntlich die Taylor-Entwicklung von f (an der Stelle 0). In der Differenzenrechnung entspricht Δ dem Differentialoperator D, $x^{\underline{k}}$ entspricht x^k, und es gilt tatsächlich für ein Polynom vom Grad n:

$$f(x) = \sum_{k=0}^{n} \frac{\Delta^k f(0)}{k!} x^{\underline{k}} = \sum_{k=0}^{n} \Delta^k f(0) \binom{x}{k}. \tag{36}$$

Die Form (36) heißt die Newton-Darstellung von f. Zum Beweis bemerken wir zunächst, dass f eindeutig in der Gestalt $f(x) = \sum_{k=0}^{n} b_k x^{\underline{k}}$ dagestellt werden kann. Hat f den Grad 0, so ist dies offensichtlich richtig, $f = a_0 = a_0 x^{\underline{0}}$. Ist nun a_n der höchste Koeffizient von f, so hat das Polynom $g(x) = f(x) - a_n x^{\underline{n}}$ Grad $n-1$, und das Resultat folgt mit Induktion. Es bleibt also zu zeigen, dass $b_k = \frac{\Delta^k f(0)}{k!}$ ist. Wir bemerken zunächst $\Delta^k x^{\underline{i}} = i(i-1)...(i-k+1)x^{\underline{i-k}} = i^{\underline{k}} x^{\underline{i-k}}$. Aus $f(x) = \sum_{i=0}^{n} b_i x^{\underline{i}}$ folgt wegen der Linearität von Δ somit $\Delta^k f(x) = \sum_{i=0}^{n} b_i i^{\underline{k}} x^{\underline{i-k}}$. Für $i < k$ ist $i^{\underline{k}} = 0$ und für $i > k$ ist $x^{\underline{i-k}}$ an der Stelle 0 gleich 0. Wir erhalten daher

$$\Delta^k f(0) = b_k k^{\underline{k}} = k! b_k \text{ also } b_k = \frac{\Delta^k f(0)}{k!}.$$

Betrachten wir als Beispiel $f(x) = x^n$. In diesem Fall wissen wir aus Formel (17) in Abschnitt 2.5.5, dass $b_k = S_{n,k}$ ist, und wir schließen $k! S_{n,k} = (\Delta^k x^n)_{x=0}$. Aus (27) ergibt sich daraus (mit dem Laufindex i)

$$k! S_{n,k} = (\Delta^k x^n)_{x=0} = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^n,$$

und wir erhalten eine Summenformel für die Stirling Zahlen zweiter Art

$$S_{n,k} = \frac{1}{k!} \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^n. \tag{37}$$

3.3 Inversion

Betrachten wir die beiden Formeln (27) und (36) des vorigen Abschnitts, wobei wir $x = n$ in (36) setzen:

$$\begin{aligned} \Delta^n f(0) &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k) \\ f(n) &= \sum_{k=0}^{n} \binom{n}{k} \Delta^k f(0). \end{aligned}$$

Setzen wir $u_k = f(k)$, $v_k = \Delta^k f(0)$, so sehen wir, dass die erste Formel die Größe v_n durch $u_0, u_1, ..., u_n$ ausdrückt, und die zweite die Zahl u_n durch $v_0, v_1, ..., v_n$. Wir sagen, dass hier eine *Inversionsformel* vorliegt. Überlegen wir uns, ob dieser Formel ein allgemeineres Prinzip zugrundeliegt. Den ersten Teil haben wir aus der Gleichung

$$\Delta^n = (E - I)^n \tag{38}$$

geschlossen, d.h. wir haben Δ mittels E ausgedrückt. Drehen wir die Sachen um, so sehen wir

$$E^n = (\Delta + I)^n, \tag{39}$$

und dies ergibt natürlich die zweite Formel, da $E^n = (\Delta + I)^n = \sum_{k=0}^{n} \binom{n}{k} \Delta^k$ angewandt auf f impliziert

$$f(x+n) = \sum_{k=0}^{n} \binom{n}{k} \Delta^k f(x),$$

also mit $x = 0$

$$f(n) = \sum_{k=0}^{n} \binom{n}{k} \Delta^k f(0).$$

Entscheidend ist also der Zusammenhang (38) und (39), und dies ist nichts anderes als die zweimalige Anwendung des Binomialsatzes. Setzen wir $E = x$ und $\Delta = x - 1$, so reduzieren (38) und (39) zu den Formeln

$$\begin{aligned} (x-1)^n &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} x^k \\ x^n &= \sum_{k=0}^{n} \binom{n}{k} (x-1)^k \end{aligned}$$

Nun liegt das allgemeine Prinzip auf der Hand. Eine *Basisfolge* $(p_0(x), p_1(x), ...)$ ist eine Folge von Polynomen mit Grad $p_n = n$. Also, $p_0(x)$ ist eine Konstante $\neq 0$, $p_1(x)$ hat Grad 1, usw. Unsere Standardbeispiele sind die Potenzen (x^n) und die fallenden bzw. steigenden Faktoriellen $(x^{\underline{k}})$ bzw. $(x^{\overline{k}})$. Ist $f(x)$ irgendein Polynom vom Grad n, so können wir $f(x)$ eindeutig als Linearkombination der $p_k(x)$, $0 \leq k \leq n$ darstellen. Den Beweis haben wir im vorigen Abschnitt schon für die fallenden Faktoriellen $(x^{\underline{k}})$ durchgeführt, und er funktioniert wortwörtlich für jede Basisfolge. Oder in der Sprache der Linearen Algebra:: Die Polynome $p_0(x), p_1(x), ..., p_n(x)$ bilden eine Basis im Vektorraum aller Polynome vom Grad $\leq n$.

Es seien nun $(p_n(x))$ und $(q_n(x))$ zwei Basisfolgen, dann können wir also jedes $q_n(x)$ eindeutig durch $p_0(x), ..., p_n(x)$ ausdrücken, und umgekehrt jedes $p_n(x)$ durch $q_0(x), ..., q_n(x)$. Das heißt, es gibt eindeutige Koeffizienten $a_{n,k}$ und $b_{n,k}$ mit

$$q_n = \sum_{k=0}^{n} a_{n,k} p_k(x) \tag{40}$$

$$p_n(x) = \sum_{k=0}^{n} b_{n,k} q_k(x). \tag{41}$$

Wir nennen $a_{n,k}$, $b_{n,k}$ die *Zusammenhangskoeffizienten*, wobei wir $a_{n,k} = b_{n,k} = 0$ für $n < k$ setzen. Die Koeffizienten $(a_{n,k})$ und $(b_{n,k})$ bilden zwei untere (unendliche) Dreiecksmatrizen. Die Beziehungen (40) und (41) drücken sich als Matrizengleichungen folgendermaßen aus: Seien $A = (a_{i,j})$, $B = (b_{i,j})$, $0 \leq i, j \leq n$, dann gilt

$$\sum_{k \geq 0} a_{n,k} b_{k,m} = [n = m],$$

d.h. die Matrizen A und B sind invers zueinander, $A = B^{-1}$.

Satz 3.3 *Seien $(p_n(x))$ und $(q_n(x))$ zwei Basisfolgen mit Zusammenhangskoeffizienten $a_{n,k}$ bzw. $b_{n,k}$. Dann gilt für zwei Folgen von Zahlen $u_0, u_1, u_2, ...$ und $v_0, v_1, v_2, ...$*

$$v_n = \sum_{k=0}^{n} a_{n,k} u_k \ (\forall n) \Leftrightarrow u_n = \sum_{k=0}^{n} b_{n,k} v_k \ (\forall n).$$

Beweis: Da die Matrizen $A = (a_{i,j}),\ B = (b_{i,j}),\ 0 \leq i, j \leq n$, invers zueinander sind, gilt für zwei Vektoren $u = (u_0, ..., u_n),\ v = (v_0, ..., v_n)$

$$v = Au \Leftrightarrow u = Bv$$

■

Jedes Paar von Basisfolgen liefert uns also eine Inversionsformel, sofern wir die Zusammenhangskoeffizienten bestimmen können. Schreiben wir unser erstes Beispiel

$$\begin{aligned} x^n &= \sum_{k=0}^{n} \binom{n}{k} (x-1)^k \\ (x-1)^n &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} x^k \end{aligned}$$

noch einmal hin. Für zwei Folgen $u_0, ..., u_n; v_0, ..., v_n$ gilt daher nach 3.3

$$v_n = \sum_{k=0}^{n} \binom{n}{k} u_k \ (\forall n) \Leftrightarrow u_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} v_k \ (\forall n). \tag{42}$$

Die Formel (42) heißt *Binomial-Inversion*. Wir können sie durch die Ersetzung $u_n \to (-1)^n u_n$ auch auf eine symmetrische Form bringen:

$$v_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} u_k \ (\forall n) \Leftrightarrow u_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} v_k (\forall n). \tag{43}$$

Die Methode der Inversion lautet also folgendermaßen: Wir wollen eine Zählfunktion (also eine Koeffizientenfolge) bestimmen. Können wir eine bekannte Folge durch die zu bestimmende mittels einer Seite der Inversionsformel ausdrücken, so ist die gewünschte Folge durch die andere Seite der Formel ausgedrückt.

Betrachten wir als Beispiel nochmals die Derangement-Zahlen D_n. Sei $d(n,k)$ die Anzahl der Permutationen der Länge n mit genau k Fixpunkten, somit $d(n,0) = D_n$. Da wir die k Fixpunkte auf $\binom{n}{k}$ Arten wählen können, gilt

$$d(n,k) = \binom{n}{k} D_{n-k},$$

und daher

$$n! = \sum_{k=0}^{n} d(n,k) = \sum_{k=0}^{n} \binom{n}{k} D_{n-k} = \sum_{k=0}^{n} \binom{n}{k} D_k. \tag{44}$$

Wenden wir nun die Binomial-Inversion auf (42) mit $u_n = D_n,\ v_n = n!$ an, so erhalten wir unsere alte Summenformel

$$D_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k! = n! \sum_{k=0}^{n} \frac{(-1)^{n-k}}{(n-k)!} = n! \frac{(-1)^k}{k!}.$$

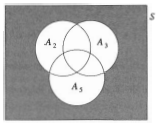

Abbildung 4: Mengendiagramm der Teiler von 30

Sehen wir uns noch die Basisfolgen (x^n) und $(x^{\underline{n}})$ an. Aus den Beziehungen

$$\begin{aligned} x^n &= \sum_{k=0}^{n} S_{n,k} x^{\underline{k}} \\ x^{\underline{n}} &= \sum_{k=0}^{n} (-1)^{n-k} s_{n,k} x^k. \end{aligned}$$

aus den Formeln (17) und (17) in Abschnitt 2.5.5 folgt die *Stirling-Inversion*

$$v_n = \sum_{k=0}^{n} S_{n,k} u_k \ (\forall n) \Leftrightarrow u_n = \sum_{k=0}^{n-k} s_{n,k} v_k \ (\forall n),$$

und insbesondere auch $\sum_{k\geq 0} S_{n,k}(-1)^{k-m} s_{k,m} = [n = m]$.

Prüfen wir dies anhand unserer Stirling-Tabellen für $n = 7,\ m = 3$ nach, so erhalten wir $\sum_{k\geq 0} S_{7,k}(-1)^{k-3} s_{k,3} = 301 - 350 \cdot 6 + 140 \cdot 35 - 21 \cdot 225 + 1624 = 0$.

3.4 Inklusion - Exklusion

Betrachten wir das folgende Problem: Wie viele Zahlen zwischen 1 und 30 gibt es, die relativ prim zu 30 sind? Wir können die Zahlen von 1 bis 30 natürlich hinschreiben und dann die relativ primen unter ihnen ablesen. Wie immer wollen wir aber die Aufgabe für allgemeines n lösen - und da helfen unsere bisherigen Methoden nicht weiter. Versuchen wir es mit folgendem Ansatz. Da $30 = 2 \cdot 3 \cdot 5$ die Primzerlegung von 30 ist, suchen wir alle Zahlen, die weder ein Vielfaches von 2, noch von 3 und auch nicht von 5 sind. Setzen wir $S = \{1, 2, \ldots, 30\}$ und erklären wir A_2 als die Menge der Vielfachen von 2, welche ≤ 30 sind, und analog A_3 (Vielfache von 3) und A_5 (Vielfache von 5), so müssen wir also die Anzahl der Elemente in $S \setminus (A_2 \cup A_3 \cup A_5)$ bestimmen. Die gesuchte Menge ist demnach der schraffierte Teil des folgenden Mengendiagramms (Bild 3.4).

Jedes Element aus S fällt in genau einen der 8 Teile des Diagramms. Beginnen wir mit $|S| - |A_2| - |A_3| - |A_5|$, dann haben wir alle Elemente aus $A_2 \cup A_3 \cup A_5$ abgezogen, aber einige doppelt, da ein Element aus, sagen wir $A_2 \cap A_3$, ja zweimal abgezogen wurde. Geben wir diese Elemente wieder hinzu, so erhalten wir $|S| - |A_2| - |A_3| - |A_5| + |A_2 \cap A_3| + |A_2 \cap A_5| + |A_3 \cap A_5|$. Jetzt ist die Formel schon fast richtig: Alle Elemente sind genau einmal abgezogen, mit Ausnahme derer in $|A_2 \cap A_3 \cap A_5|$. Diese Elemente haben wir dreimal abgezogen, aber auch dreimal dazugezählt, also insgesamt noch nicht berücksichtigt. Ziehen wir diese letzte Gruppe ab, so erhalten wir die Formel:

$$\begin{aligned} |S \setminus \cup A_i| &= |S| - |A_2| - |A_3| - |A_5| + |A_2 \cap A_3| + |A_2 \cap A_5| + \\ &\quad |A_3 \cap A_5| - |A_2 \cap A_3 \cap A_5|. \end{aligned}$$

Um unsere Ausgangsfrage zu beantworten, müssen wir $|A_i|, |A_i \cap A_j|, |A_2 \cap A_3 \cap A_5|$ bestimmen. Das ist aber leicht. A_2 sind die Vielfachen von 2, also $|A_2| = \frac{30}{2} = 15$, und analog $|A_3| = 10, |A_5| = 6$. $A_2 \cap A_3$ enthält offenbar die Vielfachen von 6, also $|A_2 \cap A_3| = \frac{30}{6} = 5$, und analog $|A_2 \cap A_5| = 3, |A_3 \cap A_5| = 2$, und schließlich ist $|A_2 \cap A_3 \cap A_5| = 1$, da nur 30 ein Vielfaches von $2, 3$ und 5 ist. Damit ist das Problem gelöst: Die Anzahl der Zahlen ≤ 30, welche zu 30 relativ prim sind, ist $30 - 15 - 10 - 6 + 5 + 3 + 2 - 1 = 8$. Diese Zahlen sind $1, 7, 11, 13, 17, 19, 23, 29$.

Zur Berechnung von $S \setminus (A_2 \cup A_3 \cup A_5)|$ schließen wir also Zahlen aus, schließen dann die zuviel abgezogenen Zahlen wieder ein, die jetzt zuviel gezählten wieder aus, usf. Das Ganze ist also eine Inklusion-Exklusions-Methode und sie funktioniert für beliebige Mengen S und beliebige Untermengen $B_1, B_2, \ldots, B_m$ von S.

Proposition 3.4 *Seien $B_1, B_2, \ldots, B_m$ Untermengen von S, dann gilt:*

$$|S \setminus \bigcup_{i=1}^{m} B_i| = |S| - \sum_{i=1}^{m} |B_i| + \sum_{1 \le i < j \le m} |B_i \cap B_j| - \ldots + (-1)^m |B_1 \cap \ldots \cap B_m|.$$

Zum Beweis brauchen wir uns nur zu überlegen, wie oft ein Element $x \in S$ gezählt wird. Ist $x \in S \setminus \bigcup_{i=1}^{m} B_i$, so wird x auf der rechten Seite einmal gezählt, nämlich in $|S|$. Sei also $x \in \bigcup_{i=1}^{m} B_i$, genauer x sei in $B_{i_1}, \ldots, B_{i_k}$, aber nicht in den anderen B_j's. Dann wird x zunächst einmal gezählt (in $|S|$), dann k-mal abgezogen (in $|B_{i_1}|, \ldots, |B_{i_k}|$, dann $\binom{k}{2}$ dazugezählt (in $|B_{i_1} \cap B_{i_2}|, |B_{i_1} \cap B_{i_3}|, \ldots$), dann $\binom{k}{3}$ abgezählt, usf. Insgesamt wird x also genau

$$1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \ldots + (-1)^k \binom{k}{k}$$

mal gezählt, und das ergibt 0, wie wir schon längst wissen (Abschnitt 1.1.4).

Für die Anwendungen wird die Formel meist in folgender Form benutzt, und ist das eigentliche **Prinzip der Inklusion - Exklusion**; gelegentlich spricht man auch von dem *Sieb-Prinzip*.

Proposition 3.5 *Es sei S eine Menge mit n Elementen, und $E_1, \ldots, E_m$ eine Menge von Eigenschaften, die die Elemente aus S besitzen oder nicht. Mit $N(E_{i_1}, \ldots, E_{i_k})$ bezeichnen wir die Anzahl der Elemente, welche die Eigenschaften $E_{i_1}, \ldots, E_{i_k}$ besitzen (und möglicherweise noch weitere). Dann gilt für die Anzahl $\bar{N}$ der Elemente, die überhaupt keine der Eigenschaften besitzen:*

$$\bar{N} = n - \sum_{i=1}^{m} N(E_i) + \sum_{1 \le i < j \le m} N(E_i, E_j) - \ldots + (-1)^m N(E_1, \ldots, E_m) \tag{45}$$

Beweis: Zum Beweis brauchen wir nur $B_i = \{x \in S : x \text{ besitzt } E_i\}$ zu setzen. Dann ist

$$N(E_{i_1}, \ldots, E_{i_k}) = |B_{i_1} \cap \ldots \cap B_{i_k}|, \bar{N} = |S \setminus \bigcup_{i=1}^{m} B_i|,$$

und (45) ist nichts anderes als unsere obige Formel. ∎

In unserem Ausgangsbeispiel war E_2 die Eigenschaft durch 2 teilbar, E_3 durch 3 teilbar, E_5 durch 5 teilbar, und das Problem liegt somit genau darin, die Anzahl $\bar{N}$ zu bestimmen.

In vielen Beispielen hängt $N(E_{i_1}, \ldots, E_{i_k})$ nur von der Anzahl k ab, das heißt es gilt

$$N(E_{i_1}, \ldots, E_{i_k}) = N(E_{j_1}, \ldots, E_{j_k})$$

für zwei k-Untermengen von $\{E_1, \ldots, E_m\}$. Wir können also $N_k = N(E_{i_1}, \ldots, E_{i_k})$ für beliebige k-Mengen setzen, und Formel (45) nimmt die folgende einfach Gestalt an (mit $N_0 = n$):

$$\bar{N} = \sum_{k=0}^{m} (-1)^k \binom{m}{k} N_k \tag{46}$$

Das Prinzip der Inklusion-Exklusion ist von bestechender Einfachheit und gerade darum vielseitig anwendbar. Ein paar weitere Beispiele mögen dies illustrieren.

Beispiel 3.6 *Zunächst noch einmal unsere altbekannten Derangement-Zahlen D_n. Die Vorgangsweise ergibt sich fast von selbst. S ist die Menge der n- Permutationen, und für $i = 1, \ldots, n$ ist E_i die Eigenschaft, dass i Fixpunkt ist. Wählen wir die Fixpunkte $i_1, \ldots, i_k$, so kann der Rest beliebig permutiert werden. Somit ist $N(E_{i_1}, \ldots, E_{i_k}) = (n-k)!$ für jede k-Menge $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$, und wir erhalten laut Formel (46)*

$$D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Im Abschnitt 3.1.1 haben wir die Formel für D_n mittels Binomial-Inversion bewiesen, und tatsächlich kann man zeigen, dass auch das Prinzip der Inklusion-Exklusion eine Inversion über einer geeigneten Struktur darstellt, ohne dass wir hier näher darauf eingehen wollen.

Beispiel 3.7 *Als ein etwas schwierigeres Beispiel betrachten wir eine n- Menge $\{a_1, \ldots, a_n\}$ und fragen uns, wie viele Wörter der Länge $2n$ gebildet werden können, die jedes a_i genau zweimal enthalten, so dass gleiche Elemente niemals nebeneinander auftauchen. Für $n = 2$ erhalten wir zum Beispiel als einzige Wörter $a_1a_2a_1a_2$ und $a_2a_1a_2a_1$. Als Interpretation können wir uns eine lange Tafel vorstellen, und fragen, auf wie viele Arten n Ehepaare platziert werden können, so dass Ehepartner niemals nebeneinander sitzen. S sei die Menge aller Wörter der Länge $2n$ aus $\{1, 2, \ldots, n\}$, in denen jedes i genau zweimal auftritt. Ist E_i die Eigenschaft, dass ein Wort die Zahl i nebeneinander enthält, so fragen wir also genau nach $\bar{N}$. Betrachten wir eine k-Menge $\{i_1, \ldots, i_k\}$. Wie viele Wörter enthalten $i_1, i_2 \ldots, i_k$ jeweils nebeneinander? Zunächst überlegen wir uns, wie oft wir die $2k$ Zahlen $i_1, i_1, \ldots, i_k, i_k$ nebeneinander platzieren können. Betrachten wir die k Anfangsstellen der k Paare. Dies sind k Stellen zwischen 1 und $2n-1$, die sich jeweils um mindestens 2 unterscheiden (da die Stelle danach ja von dem zweiten Element besetzt ist). Die Anzahl dieser k Wahlen aus $\{1, 2, \ldots, 2n-1\}$ ist $\binom{2n-k}{k}$. Nun können wir die k Paare auf $k!$ Arten permutieren, und die restlichen $n-k$ Paare auf $\frac{(2n-2k)!}{2^{n-k}}$ und daher nach (46)*

$$\bar{N} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{2n-k}{k} k! \frac{(2n-2k)!}{2^{n-k}}$$

Die Transformation $k \to n-k$ und Kürzen ergibt das endgültige Ergebnis

$$\begin{aligned} \bar{N} &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \binom{n+k}{n-k} (n-k)! \frac{(2k)!}{2^k} \\ &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \frac{(n+k)!}{2^k} \end{aligned}$$

Kommen wir kurz zu Zahl-Partitionen zurück. Wie viele Partitionen von 7 gibt es, in denen alle Summanden ungerade sind und wie viele gibt es, in denen alle Summanden verschieden sind? Diese Anzahlen wollen wir mit $p_u(7)$ und $p_v(7)$ bezeichnen.

ungerade	verschieden
7	7
5+1+1	6+1
3+3+1	5+2
3+1+1+1+1	4+3
1+1+1+1+1+1+1	4+2+1

Also $p_u(7) = p_v(7) = 5$. Probieren wir andere kleine Zahlen, so kommen wir immer auf dasselbe Ergebnis $p_u(n) = p_v(n)$. Ist dies immer richtig? Kein Problem mit Inklusion-Exklusion. Sei $p(n)$ die Anzahl aller Partitionen von n. Wir berechnen zuerst $p_u(n)$. S ist die Menge aller Partitionen von

n und E_i die Eigenschaft, dass ein gerader Summand i vorkommt. Wie viele Partitionen enthalten 2? Offenbar $p(n-2)$ viele, da wir 2 jeweils wegstreichen. Nun ist klar, was herauskommt:

$$\begin{aligned} p_u(n) = \quad & p(n) \\ - \quad & p(n-2) - p(n-4) - p(n-6) - \dots \\ + \quad & p(n-2-4) + p(n-2-6) + p(n-2-8) + \dots \\ - \quad & p(n-2-4-6) - \dots \end{aligned}$$

Nun zu $p_v(n)$. Hier ist E_i die Eigenschaft, dass i mehrmals als Summand auftritt. Also erhalten wir:

$$\begin{aligned} p_v(n) = \quad & p(n) \\ - \quad & p(n-1-1) - p(n-2-2) - p(n-3-3) - \dots \\ + \quad & p(n-1-1-2-2) + p(n-1-1-3-3) + \dots \end{aligned}$$

und wir sehen, dass die beiden Berechnungen Zeile für Zeile übereinstimmen, also gilt tatsächlich $p_u(n) = p_v(n)$.

Auch in der Wahrscheinlichkeitsrechnung können wir das Prinzip oft verwenden. Gegeben n Bälle und r Fächer, $n \geq r$. Wir werfen die n Bälle zufällig in die Fächer. Wie groß ist die Wahrscheinlichkeit, dass kein Fach leer bleibt? Ω ist also die Menge aller r^n Verteilungen, alle gleich wahrscheinlich. Bezeichnen wir mit A_i das Ereignis, dass das Fach i leer bleibt, so besagt das Prinzip der Inklusion-Exklusion, das für die gesuchte Wahrscheinlichkeit $\bar{p}$ gilt:

$$\bar{p} = 1 - \sum_{i=1}^{r} p(A_i) + \sum_{1 \leq i < j \leq r} p(A_i \cap A_j) \mp \dots$$

Die Wahrscheinlichkeit für $A_{i_1} \cap \dots A_{i_k}$ ist nun offenbar $p(A_{i_1} \cap \dots A_{i_k}) = \frac{(r-k)^n}{r^n}$ (günstige durch mögliche Fälle), und es folgt

$$\bar{p} = \sum_{k=0}^{r} (-1)^k \binom{r}{k} \frac{(r-k)^n}{r^n} = \frac{1}{r^n} \sum_{k=0}^{r} (-1)^{r-k} \binom{r}{k} k^n.$$

Da $\bar{p}$ die Anzahl $r! S_{n,r}$ der surjektiven Abbildungen (günstig) geteilt durch die Anzahl r^n aller Abbildungen (möglich) ist, haben wir mittels Inklusion-Exklusion wiederum die Formel (37) aus Abschnitt 3.2 bewiesen.

3.5 Einige arithmetische Anwendungen; Möbius-Inversionsformel

Durch den nächsten Satz wollen wir eine Berechnungsvorschrift für die Euler'sche ϕ-Funktion (vgl. Definition 1.16) angeben, wobei $\phi(n)$ die Zahl der zu n relativ primen natürlichen Zahlen darstellt.

Satz 3.8 *Es sei eine natürliche Zahl $n \geq 2$ mit der Primfaktorzerlegung*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

gegeben. Dann ist

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

Beweis: Mit A_j bezeichnen wir die Vielfachenmengen von p_j $(1 \leq j \leq r)$. Dann ist mit Satz 3.5

$$\begin{aligned} \phi(n) &= n - |A_1 \cup A_2 \cup \dots \cup A_r| \\ &= n - \alpha_1 + \alpha_2 - \dots + (-1)^r \alpha_r, \end{aligned}$$

wobei α_i wie in Satz 3.5 verstanden wird. Eine typische Durchschnittsbildung ist

$$A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_i}$$

welche die Vielfachen $p = p_{j_1} p_{j_2} \dots p_{j_i}$ in $\mathbb{N}_n$ enthält, und dies sind gerade die Zahlen

$$p,\ 2p,\ 3p, \dots \left(\frac{n}{p}\right) p.$$

Also ist die Mächtigkeit eines typischen Durchschnittes gerade

$$\frac{n}{p} = \frac{n}{p_{j_1} p_{j_2} \cdot p_{j_i}} = n(\frac{1}{p_{j_1}})(\frac{1}{p_{j_2}}) \dots (\frac{1}{p_{j_i}}).$$

Es ergibt sich

$$\begin{aligned} \phi(n) &= n - n\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r}\right) + n\left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdots\right) + \cdots \\ &\quad \cdots + (-1)^r n\left(\frac{1}{p_1 p_2 \cdots p_r}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right), \end{aligned}$$

was den Satz beweist. ∎

Wir erwähnen eine weitere zahlentheoretische Funktion, die in diesem Zusammenhang bedeutsam ist.

Definition 3.9 *Es sei $d \in \mathbb{N}$ eine natürliche Zahl. Die Funktion*

$$\mu(d) = \begin{cases} 1 & \text{falls } d = 1, \\ (-1)^k & \text{falls } d \text{ das Produkt von } k \text{ verschiedenen Primzahlen ist,} \\ 0 & \text{falls } d \text{ einen mehrfachen Primfaktor hat} \end{cases}$$

heißt Möbius'sche Funktion[27].

Diese Funktion spielt eine große Rolle innerhalb der algebraischen Zahlentheorie. Wir werden zunächst belegen, dass für jede natürliche Zahl $n \geq 2$ die Summe aller Funktionswerte $\mu(d)$ über alle Teiler d dieser vorgegebenen Zahl n verschwindet:

Lemma 3.10 *Es sei $n \geq 2$ eine natürliche Zahl. Dann ist*

$$\sum_{d|n} \mu(d) = 0.$$

[27] Möbius, August Ferdinand, deutscher Mathematiker und Astronom, geb. 17.11.1790 Schulpforta, gest. 26.9.1868 Leipzig.

Möbius studierte an der Universität Leipzig Mathematik, Physik und Astronomie, unter anderem bei Mollweide. 1813 unternahm er Studienreisen nach Göttingen zu Gauß und nach Halle zu Pfaff. 1815 promovierte er. Durch Vermittlung von Mollweide bekam er 1816 eine Stelle als außerordentlicher Professor für Astronomie und höhere Mathematik an der Universität Leipzig. Gleichzeitig erhielt er eine Stelle als Observator an der Sternwarte Leipzig. 1820 wurde er Direktor der Leipziger Sternwarte, aber erst 1844 ordentlicher Professor für Astronomie und Mechanik.

Möbius' wichtigste Arbeit 'Der barycentrische Calkül' erschien 1827 und befasste sich mit der analytischen Geometrie. Es wurde zu einem klassischen Lehrbuch und fasste viele seine Resultate zur projektiven und affinen Geometrie zusammen. In dem Buch führte er homogene Koordinaten ein und diskutierte projektive Transformationen *Möbius-Transformationen* . Er war einer der ersten, die geometrische Objekte anhand der sie erhaltenden affinen Transformationen studierte.

Neben diesen axiomatisch-geometrischen Untersuchungen wandte sich Möbius auch topologischen Fragen zu und entwickelte hierfür viele neue Methoden. Im Zusammenhang mit der Geometrie von Polyedern untersuchte er 1858 als Beispiel für eine einseitige Fläche das *Möbius-Band*, welches auch die Erstentdeckung dieser Fläche wohl auf Listing zurückgeht. Weitere wichtige Arbeiten von Möbius betreffen die Möbius-Funktion der Zahlentheorie. Er schrieb außerdem Lehrbücher zur Astronomie ('Die Elemente der Mechanik des Himmels').

Beweis: Um dies zu zeigen, setzen wir $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Jeder Teiler d hat nach dem Hauptsatz der elementaren Zahlentheorie die Form $p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$ mit $0 \leq f_i \leq e_i$ und $\mu(d)$ ist Null, es sei denn, für alle i ist $f_i = 0$ oder $f_i = 1$. Daher entspricht jeder Teiler d mit $\mu(d) \neq 0$ einer Teilmenge der Primteiler $\{p_1, p_2, \dots, p_r\}$, wobei gerade jene p_i die Teilmenge konstituieren, für die $f_i = 1$ ist. Die Anzahl dieser Teilmengen der Größe k beträgt $\binom{r}{k}$ und wegen $\mu(d) = (-1)^k$ folgt

$$\sum_{d|n} \mu(d) = 1 - \binom{r}{1} + \binom{r}{2} - \dots + (-1)^r \binom{r}{r} = 0.$$

■

Nun soll eine weitere charakteristische Eigenschaft der Möbius'schen Funktion aufgezeigt werden, die meist als *Möbius-Inversionsformel* bezeichnet wird.

Satz 3.11 *Es sei $g : \mathbb{N} \longrightarrow \mathbb{N}$ eine Funktion und f definiert durch*

$$f(n) = \sum_{d|n} g(d).$$

Dann gilt

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right). \tag{47}$$

Beweis: Substituiert man $f(n/d)$ in der rechten Seite der Gleichung (47), so ergibt sich

$$\begin{aligned} \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{c|\, n/d} g(c) \\ &= \sum_{(c,d)\in S} \mu(d) g(c). \end{aligned}$$

Dabei läuft die Doppelsumme über alle Paare (c, d) von S mit $d \mid n$ und $c \mid \frac{n}{d}$. Diese Menge stimmt aber mit jener Menge von Paaren überein, wenn die Nebenbedingung $c \mid n$ und $d \mid \frac{n}{c}$ lautet, so dass wir die Summation neu organisieren können:

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{c|n} g(c) \Big(\sum_{d|n/c} \mu(d) \Big).$$

Die Summe in der Klammer ist Null, wenn $n/c \geq 2$ ist (vgl. Lemma 3.10). Der einzige Term, der übrig bleibt, ist $n = c$, was zu

$$g(n) \sum_{d|1} \mu(d) = g(n)\mu(1) = g(n)$$

führt. ■

4 Erzeugende Funktionen

Als Ausgangstext hat auch für dieses Kapitel auf weite Strecken der vorzügliche und kompakte Text aus [1] gedient, den wir allerdings mit Kommentaren nachbearbeitet haben.

Wir kommen nun zur dritten und weitaus anwendungsreichsten Methode der Zähltheorie. Wir fassen die gesuchten Zählkoeffizienten $a_0, a_1, a_2, \ldots$ als Koeffizienten einer Potenzreihe $\sum_{i\geq 0}^{n} a_i z^i$ auf. Mit diesen Potenzreihen können wir rechnen, das heißt wir operieren mit den Koeffizienten als *Ganzes*. Wir werden sehen, dass sich manche bisher unzugänglichen Probleme erstaunlich leicht bewältigen lassen.

4.1 Definition und Beispiele

Definition 4.1 *Es sei eine Folge $a_0, a_1, a_2, \ldots$ gegeben. Die erzeugende Funktion von (a_n) ist die formale Reihe $A(z) = \sum_{n\geq 0} a_n z^n$.*

Zwei Bemerkungen sind angebracht: Die Variable z drückt aus, dass wir über den komplexen Zahlen $\mathbb{C}$ rechnen, obwohl wir es meistens mit ganzen Zahlen zu tun haben. Mit 'formal' ist gemeint, dass wir die Potenzen z^n nur als 'Aufhänger' für das Rechnen verwenden. Konvergenzfragen werden völlig außer acht gelassen. Manchmal ist es vorteilhaft, den Indexbereich nicht einzuschränken. Wir schreiben dann $\sum_n a_n z^n$ mit dem Einverständnis, dass $a_n = 0$ ist für $n < 0$. Für den Koeffizienten a_n von z^n setzen wir auch $a_n = [z^n]A(z)$.

Mit den formalen Reihen können wir rechnen. Die *Summe* von $\sum a_n z^n$ und $\sum b_n z^n$ ist natürlich $\sum(a_n + b_n)z^n$, und ein *Vielfaches* $c\sum a_n z^n$ ist die Reihe $\sum(ca_n)z^n$. Wir haben auch ein Produkt. Ist $A(z) = \sum a_n z^n, B(z) = \sum b_n z^n$, so setzen wir

$$A(z)B(z) = \sum_{n\geq 0}(\sum_{k=0}^{n} a_k b_{n-k})z^n. \tag{48}$$

Das Produkt (48) heißt die *Konvolution* von $A(z)$ und $B(z)$. Es ergibt sich einfach durch Ausmultiplizieren. Was ist der Beitrag zur Potenz z^n in $A(z)B(z)$? Wir müssen alle Potenzen z^k aus $A(z)$ und z^{n-k} aus $B(z)$ berücksichtigen mit den Koeffizienten a_k bzw. b_{n-k}, und dann die Summe bilden. Wir sehen, dass die Reihen $A(z) = 0$ bzw. $A(z) = 1$ Nullelement bzw. Einselement in bezug auf Addition und Multiplikation von Reihen bilden.

Die formalen Reihen erfüllen alle üblichen Rechenregeln mit der Ausnahme, dass $A(z)$ kein multiplikatives Inverses besitzen muss. Aber auch diese Frage, wann $A(z)$ eine inverse Reihe $B(z)$ mit $A(z)B(z) = 1$ besitzt, ist leicht zu beantworten. Da $a_0 b_0 = 1$ gelten muss, ist $a_0 \neq 0$ eine notwendige Bedingung dafür, dass $A(z)$ ein Inverses besitzt. Das ist aber auch schon hinreichend. Sei $A(z) = \sum a_n z^n$ mit $a_0 \neq 0$. Für die gesuchte inverse Reihe $B(z) = \sum b_n z^n$ muss $b_0 = a_0^{-1}$ gelten. Nehmen wir nun an, dass $b_0, b_1, \ldots, b_{n-1}$ schon bestimmt sind, so folgt aus $\sum_{k=0}^{n} a_k b_{n-k} = 0$, dass $b_n = a_0^{-1} \sum_{k=1}^{n} a_k b_{n-k}$ wohlbestimmt ist.

Betrachten wir als Beispiel die *geometrische* Reihe $\sum_{n\geq 0} z^n$. Aus (48) folgt sofort$(\sum_{n\geq 0} z^n)(1 - z) = 1$, also ist die Reihe $1 - z$ das Inverse von $\sum z^n$ und wir schreiben $\sum_{n\geq 0} z^n = \frac{1}{1-z}$.

Beispiele 4.2 *Stellen wir eine Liste der wichtigsten erzeugenden Funktionen zusammen:*

$$\text{(a)} \qquad \sum_{n\geq 0} z^n = \frac{1}{1-z}$$

$$\text{(b)} \qquad \sum_{n\geq 0} (-1)^n z^n = \frac{1}{1+z}$$

$$\text{(c)} \qquad \sum_{n\geq 0} z^{2n} = \frac{1}{1-z^2}$$

$$\text{(d)} \qquad \sum_{n\geq 0}\binom{c}{n}z^n = (1+z)^c \ (c\in\mathbb{C})$$

$$\text{(e)} \qquad \sum_{n\geq 0}\binom{c+n-1}{n}z^n = (1-z)^{-c} \ (c\in\mathbb{C})$$

$$\text{(f)} \qquad \sum_{n\geq 0}\binom{m+n}{n}z^n = \frac{1}{(1-z)^{m+1}}$$

$$\text{(g)} \qquad \sum_{n\geq 0}\frac{z^n}{n!} = e^z$$

$$\text{(h)} \qquad \sum_{n\geq 1}\frac{(-1)^{n+1}z^n}{n} = \log(1+z)$$

Formel (d) ist für $c\in\mathbb{N}_0$ gerade der Binomialsatz. Der allgemeine Fall wird in der Analysis bewiesen. Für (e) verwenden wir die Negationsformel (11) aus Abschnitt 2.5. Wir haben $\binom{c+n-1}{n}z^n = \binom{-c}{n}(-z)^n$, und das Resultat folgt aus (d). Formel (f) folgt aus (e) mit $m = c-1$, und die letzten beiden Ausdrücke sind wohlbekannte Reihenentwicklungen.

Eine Anwendung des Konvolutionsproduktes können wir sofort notieren. Sei $A(z) = \sum_{n\geq 0} a_n z^n$ gegeben. Dann ist

$$\frac{A(z)}{1-z} = \sum_{n\geq 0}(\sum_{k}^{n} a_k)z^n,$$

da alle Koeffizienten von $\frac{1}{1-z} = \sum_{n\geq 0} z^n$ gleich 1 sind. Zum Beispiel erhalten wir mit $A(z) = \frac{1}{1-z}$, dass

$$\frac{1}{(1-z)^2} = \sum_{n\geq 0}(n+1)z^n$$

ist, oder allgemein

$$\frac{1}{(1-cz)^2} = \frac{\sum(cz)^n}{1-cz} = \sum_{n\geq 0}(n+1)(cz)^n = \sum_{n\geq 0}(n+1)c^n z^n.$$

Die Indextransformation lässt sich ebenfalls leicht ausdrücken. Ist $A(z) = \sum_n a_n z^n$, so haben wir $z^m A(z) = \sum_n a_n z^{n+m} = \sum_n a_{n-m} z^n$, d. h. Multiplikation mit z^m entspricht einer Indexverminderung um m. Zum Beispiel erhalten wir aus Formel (f) die Gleichung $\sum_n \binom{n}{m}z^n = \sum_n \binom{n}{n-m}z^n = z^m(1-z)^{-m-1}$.

4.2 Lösung von Rekursionen

Erzeugende Funktionen geben uns eine wichtige Methode an die Hand, um beliebige Rekursionen mit konstanten Koeffizienten zu lösen. Als Beispiel betrachten wir die einfachste aller zweistelligen Rekursionen

$$F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2} \qquad (n\geq 2). \tag{49}$$

Die Zahlen F_n heißen nach ihrem Entdecker Leonardo von Pisa Fibonacci[28] die *Fibonacci-Zahlen*. Sie tauchen in so vielen Problemen auf, dass ihrer Untersuchung eine eigene mathematische

[28] Fibonacci, Leonardo von Pisa , italienischer Mathematiker, geb. um 1170 Pisa, gest. nach 1240 Pisa.

Fibonacci, Sohn eines Notars und Leiters der Niederlassung pisanischer Kaufleute in Bougie (Algerien), lernte Mathematik in Bougie und auf ausgedehnten Reisen im Mittelmeerraum. Um 1200 kehrte er nach Pisa zurück. Er wirkte in seiner Heimatstadt als Privatgelehrter und mathematischer Schriftsteller. Fibonacci gilt als der erste bedeutende Mathematiker des europäischen Mittelalters.

Von ihm sind fünf Werke überliefert. Grundlegend wurde davon sein 'Liber abbaci' (1202, 1228). Darin verwendete Fibonacci die indisch-arabischen Ziffern und das dezimale Stellenwertsystem. Er ließ die Null als Wurzel einer quadratischen Gleichung zu, deutete die Möglichkeit der Einführung negativer Zahlen an, untersuchte irrationale Zahlen, verbreitete arabische Methoden zur Lösung von (linearen) Gleichungen und (linearen) Gleichungssystemen und stellte die berühmte 'Kaninchenaufgabe' (Fibonacci-Folge). In weiteren Werken behandelte er, immer im Gewand konkreter Problemstellungen oder von 'Denksportaufgaben', elementare geometrische Fragen, Aufgaben des Typs $x^2 \pm a = y^2$ (a, x, y positiv ganzzahlig), die Lösung einer 'nichttrivialen' kubischen Gleichung und kaufmännische Rechenaufgaben.

Zeitschrift gewidmet ist.

Eine Tabelle der ersten Fibonacci-Zahlen sieht so aus:

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55

Wie berechnen wir nun die n-te Fibonacci-Zahl F_n? Die folgende Vorgehensweise ist bereits typisch für alle Rekursionen.

1. Drücke die Rekursion in einer einzigen Formel aus, inklusive der Anfangsbedingungen. Wie immer ist $F_n = 0$ für $n < 0$, $F_n = F_{n-1} + F_{n-2}$ gilt auch für $n = 0$, aber für $n = 1$ ist $F_1 = 1$, aber die rechte Seite 0. Also ist die vollständige Rekursion der Fibonacci-Zahlen

$$F_n = F_{n-1} + F_{n-2} + [n = 1].$$

2. Interpretiere die Gleichung in 1. mit Hilfe von erzeugenden Funktionen. Wir wissen schon, dass Indexerniedrigung einer Multiplikation mit einer Potenz von z entspricht. Also erhalten wir

$$\begin{aligned} F(z) &= \sum F_n z^n = \sum F_{n-1} z^n + \sum F_{n-2} z^n + \sum [n = 1] z^n \\ &= zF(z) + z^2 F(z) + z. \end{aligned}$$

3. Löse die Gleichung in $F(z)$. Das ist leicht:

$$F(z) = \frac{z}{1 - z - z^2}$$

4. Drücke die rechte Seite als formale Reihe aus und ermittle daraus die Koeffizienten.

Dies ist der schwierigste Schritt. Zunächst schreiben wir $1 - z - z^2$ in der Form $1 - z - z^2 = (1 - \alpha z)(1 - \beta z)$ und ermitteln dann durch Partialbruchzerlegung Konstanten a und b mit

$$\frac{1}{(1 - \alpha z)(1 - \beta z)} = \frac{a}{1 - \alpha z} + \frac{b}{1 - \beta z}.$$

Nun ist die Arbeit getan, denn es gilt:

$$\begin{aligned} F(z) &= z\left(\frac{a}{1 - \alpha z} + \frac{b}{1 - \beta z}\right) = z(a \sum \alpha^n z^n + b \sum \beta^n z^n) \\ &= \sum_n (a\alpha^{n-1} + b\beta^{n-1}) z^n \end{aligned}$$

und somit

$$F_n = a\alpha^{n-1} + b\beta^{n-1}. \tag{50}$$

Um eine vollständige Lösung (50) zu erhalten, müssen wir also erstens α und β ermitteln, und zweitens a und b.

Setzen wir $q(z) = 1 - z - z^2$, so heißt $q^R(z) = z^2 - z - 1$ das *reflektierte Polynom*, und wir behaupten, aus $q^R(z) = (z - \alpha)(z - \beta)$ folgt $q(z) = (1 - \alpha z)(1 - \beta z)$, d.h. α und β sind genau die Nullstellen des reflektierten Polynoms.

Wir wollen dies gleich allgemein beweisen. Sei $q(z) = 1 + q_1 z + \ldots + q_d z^d$ ein Polynom über $\mathbb{C}$ vom Grad $d \geq 1$ und konstantem Koeffizienten 1. Das reflektierte Polynom $q^R(z)$ entsteht durch Reflektion der Potenzen z^i, also $q^R(z) = z^d + q_1 z^{d-1} + \ldots + q_d$, $q_d \neq 0$. Offenbar gilt $q(z) = z^d q^R(\frac{1}{z})$.

Seien nun $\alpha_1, \ldots, \alpha_d$ die Nullstellen von $q^R(z)$, also $q^R(z) = (z-\alpha_1)\ldots(z-\alpha_d)$. Über $\mathbb{C}$ ist so eine Darstellung immer möglich, wobei die α_i's natürlich nicht alle verschieden zu sein brauchen. Aus $q(z) = z^d q^R(\frac{1}{z})$ folgt

$$q(z) = z^d(\frac{1}{z} - \alpha_1)\ldots(\frac{1}{z} - \alpha_d) = (1-\alpha_1 z)\ldots(1-\alpha_d z),$$

wie behauptet. Die Bestimmung von $\alpha_1, \ldots, \alpha_d$ (oder α, β in unserem Beispiel der Fibonacci-Zahlen) ist also nichts anderes als die Nullstellenbestimmung von $q^R(z)$.

Für die Fibonacci-Zahlen erhalten wir

$$\begin{aligned} q^R(z) = z^2 - z - 1 &= (z - \frac{1+\sqrt{5}}{2})(z - \frac{1-\sqrt{5}}{2}), \\ q(z) = 1 - z - z^2 &= (1 - \frac{1+\sqrt{5}}{2}z)(1 - \frac{1-\sqrt{5}}{2}z) \end{aligned}$$

Die übliche Bezeichnung für diese Nullstellen ist $\phi = \frac{1+\sqrt{5}}{2}$, $\hat{\phi} = \frac{1-\sqrt{5}}{2}$ (auch $\tau, \hat{\tau}$ ist gebräuchlich). Die Zahl ϕ heißt der *goldene Schnitt*, sie ist eine der fundamentalen Zahlen der gesamten Mathematik und war schon in der Antike bekannt. Der Name goldener Schnitt rührt von folgendem Problem her: Gegeben sei ein Rechteck mit Seitenlängen r und $s, r \geq s$. Welches Verhältnis $\frac{r}{s}$ müssen r und s erfüllen, so dass nach Wegschneiden eines Quadrates der Seitenlänge s wiederum ein Rechteck mit dem gleichen Verhältnis resultiert?

Ist $z = \frac{r}{s}$, so soll also $x = \frac{r}{s} = \frac{s}{r-s} = \frac{1}{x-1}$ gelten. Das Verhältnis x muss demnach die Gleichung $x^2 - x - 1 = 0$ erfüllen, also ist $x = \phi$, da $x \geq 1$ vorausgesetzt ist. Aus der Gleichung $z^2 - z - 1 = (z-\phi)(z-\hat{\phi}))$ folgen die Beziehungen

$$\hat{\phi} = -\phi^{-1}, \ \phi + \hat{\phi} = 1.$$

Wir kommen zum zweiten Problem, der Bestimmung von a und b. Wir setzen a und b als unbekannte Koeffizienten in der Partialbruchzerlegung an:

$$\frac{1}{(1-\phi z)(1-\hat{\phi}z)} = \frac{a}{1-\phi z} + \frac{b}{1-\hat{\phi}z}$$

Auf gemeinsamen Nenner gebracht haben wir $(a+b) - (a + b\hat{\phi} + b\phi)z = 1$, d. h. a und b müssen das Gleichungssystem

$$\begin{aligned} a + b &= 1 \\ \hat{\phi}a + \phi b &= 0 \end{aligned}$$

erfüllen. Auflösung ergibt $a = \frac{\phi}{\sqrt{5}}, b = -\frac{\hat{\phi}}{\sqrt{5}}$, und wir erhalten nach (50)

$$F_n = \frac{\phi}{\sqrt{5}}\phi^{n-1} - \frac{\hat{\phi}}{\sqrt{5}}\hat{\phi}^{n-1},$$

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right). \tag{51}$$

Da $|\frac{1-\sqrt{5}}{2}| < 1$ ist, erkennen wir, dass F_n die zu $\frac{1}{\sqrt{5}}\phi^n$ nächstgelegene ganze Zahl ist.

Der folgende allgemeine Satz besagt, dass unsere Schritte 1. bis 4. immer funktionieren.

Satz 4.3 *Es sei $q_1, \ldots, q_d$ eine feste Folge komplexer Zahlen, $d \geq 1, q_d \neq 0$*

$$q(z) = 1 + q_1 z + \ldots q_d z^d = (1 - \alpha_1 z)^{d_1} \ldots (1 - \alpha_k z)^{d_k},$$

wobei also die α_i's die verschiedenen Nullstellen von $q^R(z)$ sind mit den Vielfachheiten d_i, $i = 1, \ldots, k$. Für eine Zählfunktion $f : \mathbb{N}_0 \to \mathbb{C}$ sind die folgenden Bedingungen äquivalent:

(A1) *Rekursion der Länge d. Für alle $n \geq 0$ gilt*

$$f(n+d) + q_1 f(n+d-1) + \ldots + q_d f(n) = 0.$$

(A2) *Erzeugende Funktion.*

$$F(z) = \sum_{n \geq 0} f(n) z^n = \frac{p(z)}{q(z)},$$

wobei $p(z)$ ein Polynom vom Grad $< d$ ist.

(A3) *Partialbruchzulegung.*

$$F(z) = \sum_{n \geq 0} f(n) z^n = \sum_{i=1}^{k} \frac{g_i(z)}{(1 - \alpha_i z)^{d_i}}$$

für Polynome $g_i(z)$ vom Grad $< d_i$ mit $i = 1, \ldots, k$.

(A4) *Explizite Darstellung.*

$$f(n) = \sum_{i=1}^{k} p_i(n) \alpha_i^n,$$

wobei die $p_i(n)$ Polynome in n vom Grad $< d_i$ sind ($i = 1, \ldots k$).

Beweis: Wir definieren die Mengen V_1, V_2, V_3 und V_4 durch

$$V_i = \{ f : \mathbb{N}_0 \to \mathbb{C} : f \text{ erfüllt (A}i\text{)} \}, \quad i = 1, \ldots 4.$$

Jede dieser vier Mengen ist ein Vektorraum über $\mathbb{C}$, da Summe und skalares Vielfaches wieder die jeweilige Bedingung erfüllen. Als nächstes sehen wir, dass jeder dieser Vektorräume Dimension d hat. In (A1) können wir die Anfangswerte $f(0), \ldots, f(d-1)$ beliebig wählen, in (A2) die d Koeffizienten $p_0, p_1, \ldots, p_{d-1}$ von $p(z)$ und in (A3), (A4) jeweils d_i Koeffizienten von $g_i(z)$ bzw. $p_i(n)$ mit $\sum_{i=1}^{k} d_i = d$. Wenn wir also $V_i \subseteq V_j$ zeigen können, so folgt $V = V_j$.

Sei $f \in V_2$, dann ergibt Koeffizientenvergleich für z^{d+n} in $q(z) \sum_{n \geq 0} f(n) z^n = p(z)$ gerade die Rekursion (A1), d.h. $f \in V_1$ und somit $V_1 = V_2$.

Sei $f \in V_3$, auf gemeinsamen Nenner gebracht erhalten wir

$$\sum_{n \geq 0} f(n) z^n = \frac{\sum_{i=1}^{k} g_i(z) \prod_{j \neq i} (1 - \alpha_j z)^{d_j}}{\prod_{i=1}^{k} (1 - \alpha_i z)^{d_i}} = \frac{p(z)}{q(z)}$$

mit Grad $p(z) \leq \max(\text{Grad } g_i(z) + \sum_{j \neq i} d_j) < \sum_{i=1}^{k} d_i = d$, und wir erhalten $f \in V_2$, somit $V_1 = V_2 = V_3$.

Schließlich wollen wir $V_3 \subseteq V_4$ zeigen. Sei $f \in V_3$ und $F(z) = \sum_{i=1}^{k} \frac{g_i(z)}{(1 - \alpha_i z)^{d_i}}$. Betrachten wir einen Summanden $\frac{g_i(z)}{(1 - \alpha_i z)^{d_i}}$. Nach Beispiel (e) des vorigen Abschnittes haben wir

$$\frac{1}{(1 - \alpha_i z)^{d_i}} = \sum_{n \geq 0} \binom{d_i + n - 1}{n} \alpha_i^n z^n = \sum_{n \geq 0} \binom{d_i + n - 1}{d_i - 1} \alpha_i^n z^n.$$

Multiplikation mit $g_i(z) = g_0 + g_1 z + \ldots g_{d_i-1} z^{d_i-1}$ bedeutet Indexverschiebung, d. h. wir erhalten

$$\begin{aligned}\frac{g_i(z)}{(1-\alpha_i z)^{d_i}} &= \sum_{n\geq 0}\left(\sum_{j=0}^{d_i-1} g_j \binom{d_i+n-j-1}{d_i-1}\alpha_j^{n-j}\right) z^n \\ &= \sum_{n\geq 0}\left(\sum_{j=0}^{d_i-1} \alpha_i^{-j} g_j \binom{d_i+n-j-1}{d_i-1}\alpha_j^{n}\right) z^n\end{aligned}$$

Schreiben wir nun $p_i(n) = \sum_{j=0}^{d_i-1} \alpha_i^{-j} g_j \binom{n+d_i-j-1}{d_i-1}$, so ist $p_i(n)$ ein Polynom in n vom Grad $\leq d_i - 1$, also ist $f \in V_4$ und wir sind fertig. ∎

Betrachten wir als Beispiel die Rekursion

$$f(n+2) - 6f(n+1) + 9f(n) = 0$$

mit den Anfangswerten $f(0) = 0$, $f(1) = 1$ Hier ist $q(z) = 1 - 6z + 9z^2 = (1-3z)^2$, also die Lösung von der Form

$$f(n) = (a + bn)3^n.$$

Aus $0 = f(0) = a$ erhalten wir $a = 0$, und aus $1 = f(1) = (a+b)3$ ergibt sich $b = \frac{1}{3}$. Die Lösung ist somit $f(n) = n3^{n-1}$.

Wie berechnen wir die Polynome $g_i(z)$ oder $p_i(n)$? Besonders einfach wird die Sache, wenn die Nullstellen $\alpha_1 \ldots, \alpha_d$ von $q^R(z)$ alle verschieden sind, d. h. $d_i = 1$ für alle i und $k = d$ gilt. In diesem Fall sind die Polynome $g_i(z)$ vom Grad 0, also $g_j(z) = a_i$, $(i = 1, \ldots, d)$, und ebenso $p_i(n) = a_i$. Aus

$$\frac{p(z)}{q(z)} = \frac{\sum_{i=1}^d a_i \prod_{j\neq i}(1-\alpha_j z)}{\prod_{i=1}^d (1-a_i z)}$$

folgt $p(z) = \sum_{i=1}^d a_i \prod_{j\neq i}(1-\alpha_j z)$. Für $z = \frac{1}{a_i}$ erhalten wir daraus

$$p(\frac{1}{\alpha_i}) = a_i \prod_{j\neq i}(1 - \frac{\alpha_j}{\alpha_i}),$$

da in einem Summanden $a_h \prod_{j\neq h}(1-\frac{\alpha_j}{\alpha_i})$, von $p(z)$ für $h \neq i$ der Faktor $1 - \frac{\alpha_j}{\alpha_i} = 0$ auftritt. Daraus erhalten wir nun die Formel

$$a_i = \frac{p(\frac{1}{\alpha_i})}{\prod_{j\neq i}(1-\frac{a_j}{a_i})} \ (i = 1, \ldots, d). \tag{52}$$

Den Ausdruck (52) können wir noch weiter vereinfachen. Mit $q(z) = \prod_{i=1}^d (1-\alpha_i z)$ gilt für die Ableitung $q'(z) = -\sum_{i=1}^d \prod_{j\neq i}(1-\alpha_j z)\alpha_i$, und daher $q'(\frac{1}{\alpha_i}) = -\prod_{j\neq i}(1-\frac{a_j}{a_i})\alpha_i$. Eingesetzt in (52) ergibt dies

$$a_i = \frac{-\alpha_i p(\frac{1}{\alpha_i})}{q'(\frac{1}{\alpha_i})} \ (i = 1, \ldots d). \tag{53}$$

Zum Beispiel können wir die Rechnung für die Fibonacci-Zahlen abkürzen, ohne den Weg über die Partialbruchzerlegung zu gehen. Hier ist $p(z) = z, q(z) = 1-z-z^2$, , $q'(z) = -1-2z$, $\alpha_1 = \phi$, $\alpha_2 = \hat{\phi}$, also

$$a_i = \frac{-\alpha_i(\frac{1}{\alpha_i})}{-1-\frac{2}{a_i}} = \frac{\alpha_i}{a_i+2}.$$

Nun berechnet man sofort $\frac{\phi}{\phi+2} = \frac{1}{\sqrt{5}}$, $\frac{\hat{\phi}}{\hat{\phi}+2} = -\frac{1}{\sqrt{5}}$ und erhält wiederum (51).

Unsere Methode der erzeugenden Funktionen erweist sich auch bei simultanen Rekursionen als erfolgreich. Ein Problem in einem mathematischen Wettbewerb 1980 stellte folgende Frage:

Beispiel 4.4 *Schreibe die Zahl* $(\sqrt{2}+\sqrt{3})^{1980}$ *in Dezimaldarstellung. Was ist die letzte Stelle vor und die erste Stelle nach dem Komma?*

Das scheint erstens hoffnungslos, und zweitens, was hat das mit Rekursionen zu tun? Betrachten wir allgemein $(\sqrt{2}+\sqrt{3})^{2n}$. Wir erhalten $(\sqrt{2}+\sqrt{3})^0 = 1, (\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}, (\sqrt{2}+\sqrt{3})^4 = (5+2\sqrt{6})^2 = 49+20\sqrt{6}$. Sind alle Ausdrücke $(\sqrt{2}+\sqrt{3})^{2n}$ von der Form $a_n + b_n\sqrt{6}$? Klar mit Induktion:

$$\begin{aligned}(\sqrt{2}+\sqrt{3})^{2n} &= (\sqrt{2}+\sqrt{3})^{2n-2}(\sqrt{2}+\sqrt{3})^2 \\ &= (a_{n-1}+b_{n-1}\sqrt{6})(5+2\sqrt{6}) \\ &= (5a_{n-1}+12b_{n-1}) + (2a_{n-1}+5b_{n-1})\sqrt{6}.\end{aligned}$$

Wir erhalten also gleichzeitig eine Rekursion für die Folgen (a_n) und (b_n)

$$a_n = 5a_{n-1}+12b_{n-1} \tag{54}$$
$$b_n = 2a_{n-1}+5b_{n-1} \tag{55}$$

mit den Anfangswerten $a_0 = 1, b_0 = 0$.

Die Lösung dieser Rekursionen erfolgt mit unseren 4 Schritten:
Schritt 1.

$$\begin{aligned}a_n &= 5a_{n-1}+12b_{n-1}+[n=0] \ (\text{ da } a_0 = 1) \\ b_n &= 2a_{n-1}+5b_{n-1}.\end{aligned}$$

Schritt 2. Mit $A(z) = \sum_{n\geq 0} a_n z^n$, $B(z) = \sum_{n\geq 0} b_n z^n$ ergibt sich

$$\begin{aligned}A(z) &= 5zA(z)+12zB(z)+1 \\ B(z) &= 2zA(z)+5zB(z).\end{aligned}$$

Schritt 3. Wir lösen nach $A(z)$ auf. Aus der zweiten Gleichung haben wir $B(z) = \frac{2zA(z)}{1-5z}$, und eingesetzt in die erste ergibt dies

$$A(z) = 5zA(z) + \frac{24z^2A(z)}{1-5z} + 1$$

oder

$$A(z) = \frac{1-5z}{1-10z+z^2}.$$

Schritt 4. Hier ist $q(z) = q^R(z)$ und wir erhalten $q(z) = (1-(5+2\sqrt{6})z)(1-(5-2\sqrt{6})z)$. Da die beiden Nullstellen verschieden sind, können wir Formel (53) verwenden, und erhalten mühelos für die Koeffizienten von $A(z)$

$$a_n = \frac{1}{2}((5+2\sqrt{6})^n + (5-2\sqrt{6})^n). \tag{56}$$

Schön, jetzt kennen wir a_n (und b_n können wir natürlich analog berechnen), aber was sagt uns das über die Kommastellen in $(\sqrt{2}+\sqrt{3})^{2n}$ für $n = 990$? Nun, zunächst wissen wir $(5+2\sqrt{6})^n = (\sqrt{2}+\sqrt{3})^{2n} = a_n + b_n\sqrt{6}$, d. h. (56) ergibt $a_n = \frac{1}{2}(a_n + b_n\sqrt{6} + (5-2\sqrt{6})^n)$ oder

$$a_n = b_n\sqrt{6} + (5-2\sqrt{6})^n. \tag{57}$$

Bezeichnen wir mit $\{x\}$ den Anteil einer reellen Zahl nach dem Komma, also $x = \lfloor x \rfloor + \{x\}$, $0 \leq \{x\} < 1$. Da a_n ganzzahlig ist, folgt aus (57) $\{b_n\sqrt{6}\} + \{(5-2\sqrt{6}^n\}) = 1$. Nun geht $(5-2\sqrt{6})^n \to 0$ wegen wegen $5-2\sqrt{6} < 1$. Das heißt für große n, und sicherlich für $n = 990$, gilt $(5-2\sqrt{6})^n = 0,00\ldots$ und daher $\{b_n\sqrt{6}\} = 0,99\ldots$ Die erste Stelle nach dem Komma von $a_{990} + b_{990}\sqrt{6}$ ist demnach 9.

Sei nun A die Einerstelle von a^{990} und B diejenige von $b^{990}\sqrt{6}$ also $a_{990} = \ldots A$ und $b_{990}\sqrt{6} = \ldots B, 9\ldots$ Aus (57) folgt $A \equiv B + 1 \pmod{10}$, und somit ist die Einerstelle von $a_{990} + b_{990}\sqrt{6}$ gleich $A + B \equiv 2A - 1 \pmod{10}$. Für Leser, die mit dem modulo Rechnen nicht vertraut sind - in Abschnitt 12.1 (in Aigner) wird dies nachgeholt. Wir müssen also nur noch A bestimmen und dazu benutzen wir die ursprüngliche Rekursion (54). Die ersten Werte der Einerstelle $\pmod{10}$ sind

n	a_n	b_n
0	1	0
1	5	2
2	9	0
3	5	8
4	1	0
5	5	2

Die Einerstellen von a_n wiederholen sich also periodisch alle 4 Schritte. Insbesondere ist $990 \equiv 2 \pmod{4}$, also $A = 9$, und wir erhalten das Ergebnis $2 \cdot 9 - 1 \equiv 7 \pmod{10}$, also ist 7 die gesuchte letzte Ziffer vor dem Komma.

4.3 Erzeugende Funktionen vom Exponentialtyp

Für viele Zählfunktionen (a_n) ist es vorteilhaft, anstelle der üblichen erzeugenden Funktion die Funktion

$$\widetilde{A}(z) = \sum_{n\geq 0} \frac{a_n}{n!}$$

zu betrachten. Wir nennen $\widetilde{A}(z)$ die exponentielle erzeugende Funktion der Folge (a_n).

Multiplikation von zwei exponentiellen erzeugenden Funktionen $\widetilde{A}(z) = \sum_{n\geq 0} \frac{a_n}{n!} z^n, \widetilde{B}(z) = \sum_{n\geq 0} \frac{b_n}{n!} z^n$ ist einfach. Sei $\widetilde{C}(z) = \sum_{n\geq 0} \frac{c_n}{n!} z^n$ mit $\widetilde{C}(z) = \widetilde{A}(z)\widetilde{B}(z)$. Nach der Produktformel (48) in Abschnitt 4.1 erhalten wir

$$\frac{c_n}{n!} = \sum_{k=0}^{n} \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!},$$

also

$$c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}. \tag{58}$$

Wegen des Auftretens von $\binom{n}{k}$ heißt (58) die *Binomialkonvolution*. Sind also die Zählfunktionen $(a_n), (b_n)$ und (c_n) durch (58) verbunden, so können wir sofort $C(z) = A(z)B(z)$ schließen.

Testen wir dies an einem einfachen Beispiel. Für die Exponentialfunktion e^{az} gilt

$$e^{az} = \sum_{n\geq 0} \frac{a^n}{n!} z^n,$$

d.h. e^{az} ist die exponentielle erzeugende Funktion der geometrischen Folge $(a^0, a^1, \ldots)$ Aus $e^{az} = e^{(a+b)z}$ folgt mittels (58) sofort

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

d. h. der Binomialsatz ist nichts anderes als die binomiale Konvolution von Exponentialfunktionen.

Ein anderes Beispiel: In Abschnitt 2.1.3 haben wir $\sum_{n\geq 0} \binom{a}{n} z^n = (1+z)^a$ erhalten. Schreiben wir die linke Seite $\sum_{n\geq 0} \frac{a^{\underline{n}}}{n!}$, so stellen wir fest, dass $(1+z)^a$ die exponentielle erzeugende Funktion der Folge $(a^{\underline{n}})$ ist. Da $D(1+z)^a(1+z)^b = (1+z)^{a+b}$ gilt, erhalten wir mit Binomialkonvolution

$$(a+b)^{\underline{n}} = \sum_{k=0}^{n} \binom{n}{k} a^{\underline{k}} b^{\underline{n-k}}$$

oder

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k}$$

unsere wohlbekannte Vandermonde-Identität (14) aus Abschnitt 2.5.4.

Was ist die exponentielle erzeugende Funktion der Derangementzahlen D_n? Auf Seite 22 haben wir in (44) die Beziehung $n! = \sum_{k=0} n\binom{}{k} D_k$ gefunden. Die Folge $(n!)$ ist also die binomiale Konvolution der Folge (D_k) mit der konstanten Folge $(1, 1....)$, deren exponentielle erzeugende Funktion natürlich e^z z ist. Nach (58) folgt daher für $\hat{D}(z) = \sum_{n\geq 0} \frac{D_n}{n!} z^n$,

$$\hat{D}(z)e^z = \sum_{n\geq 0} \frac{n!}{n!} z^n = \sum_{n\geq 0} z^n = \frac{1}{1-z},$$

und wir schließen $\hat{D}(z) = \frac{e^{-z}}{1-z}$. Fassen wir dies als Gleichung zwischen gewöhnlichen erzeugenden Funktionen auf, so wissen wir aus Abschnitt 1, dass die rechte Seite die ersten n Glieder von e^{-z} aufsummiert. Also erhalten wir abermals unsere altbekannte Formel

$$\frac{D_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Ganz allgemein entspricht unsere Binomial-Inversionsformel (42) aus Abschnitt 3.3 der selbstverständlichen Gleichung

$$\hat{V}(z) = \hat{U}(z)e^z \Longleftrightarrow \hat{U}(z) = \hat{V}(z)e^{-z}$$

mit $\hat{U}(z) = \sum_{n\geq 0} \frac{u_n}{n!} z^n, \hat{V}(z) = \sum_{n\geq 0} \frac{v_n}{n!} z^n$.

Noch ein Beispiel, das die Prägnanz der Methode der erzeugenden Funktionen deutlich macht. Sei a_n die Anzahl der Abbildungen f von $\{1, \ldots, n\}$ nach $\{1, \ldots, n\}$ mit der Eigenschaft, dass $j \in$ Bild (f) auch alle $i < j$ in Bild (f) sind, $a_0 = 1$. Zum Beispiel erhalten wir $a_2 = 3$ mit den Abbildungen $1 \to 1, 2 \to 1; 1 \to 1; 2 \to 2; 1 \to 2; 2 \to 1$. Angenommen, f bildet genau k Elemente auf 1 ab, dann können diese Elemente auf $\binom{n}{k}$ Arten gewählt werden, und der Rest kann auf a_{n-k} Weisen auf $\{2, \ldots n\}$ abgebildet werden. Wir erhalten somit

$$a_n = \sum_{k=1}^{n} a_{n-k} \qquad 2a_n = \sum_{k=0}^{n} \binom{n}{k} a_{n-k} + [n = 0].$$

Für die exponentielle erzeugende Funktion ergibt dies

$$2\hat{A}(z) = e^z \hat{A}(z) + 1$$

also

$$\hat{A}(z) = \frac{1}{2 - e^z}$$

Durch Entwickeln der rechten Seite erhalten wir

$$\frac{1}{2-e^z} = \frac{1}{2} \cdot \frac{1}{1 - e^2/2} = \frac{1}{2} \sum_{k\geq 0} \left(\frac{e^z}{2}\right)^k = \sum_{k\geq 0} \frac{1}{2^{k+1}} \sum_{n\geq 0} \frac{k^n z^n}{n!}$$

und daraus mit Koeffizientenvergleich für z^n:

$$a_n = \sum_{k\geq 0} \frac{k!}{2^{k+1}}.$$

Wir haben also nicht nur eine kombinatorische Interpretation der Reihe $\sum_{k\geq 0} \frac{k^n}{2^{k+1}}$ gefunden, wir wissen auch, dass ihr Wert eine natürliche Zahl, nämlich a_n. Für $n = 2$ erhalten wir beispielsweise $\sum_{k\geq 0} \frac{k^2}{2^{k+1}} = 3$ und für $n = 3$, $\sum_{k\geq 0} \frac{k^3}{2^{k+1}} = 13$.

4.4 Partialbruchzerlegung

Im Folgenden wollen wir einen anderen Weg beschreiben, Quotienten von Polynomen (als Potenzreihen) zu berechnen. Der Schlüssel liegt in der Darstellung von $a(X)/b(X)$ als Partialbruch. Besitzt $b(X)$ eine Darstellung als $s(X)t(X)$, so gibt es Polynome $f(X)$, $g(X)$ mit

$$\frac{a(X)}{b(X)} = \frac{f(X)}{s(X)} + \frac{g(X)}{t(X)}.$$

So gilt beispielsweise

$$\frac{5-3X}{2-3X+X^2} = \frac{2}{1-X} + \frac{1}{2-X}.$$

Seien $a(X)$, $b(X)$ Polynome, so erhalten wir

$$a(X) = b(X)q(X) + r(X),$$

wobei entweder $r(X)$ das Nullpolynom ist oder der Grad von $r(X)$ kleiner als der von $b(X)$ ist. Das führt zu

$$\frac{a(X)}{b(X)} = q(X) + \frac{r(X)}{b(X)}.$$

Mithin muss lediglich eine Partialbruchzerlegung für $\frac{r(X)}{b(X)}$ gesucht werden.

Satz 4.5 *Es sei F ein Körper und $a(X), b(X)$ Polynome in $F[X]$ mit*

(i) *deg $a(X) <$ deg $b(X)$.*

(ii) *$b(X) = s(X)t(X)$, wobei $s(X)$ und $t(X)$ relativ prim sind.*

(iii) *$b_0 \neq 0$.*

Dann gibt es Polynome $f(X)$ und $g(X)$ so dass

$$deg\, f(X) < deg\, s(X), \quad deg\, g(X) < deg\, t(X),$$

und

$$\frac{a(X)}{b(X)} = \frac{f(X)}{s(X)} + \frac{g(X)}{t(X)},$$

wobei diese Gleichung in $F[[X]]$ gilt.

Beweis: Zunächst bemerken wir, dass $s(X)$ und $t(X)$ Inverse in $F[[X]]$ haben, da aus $s_0t_0 = b_0$ und der Bedingung $b_0 \neq 0$ folgt, dass $s_0 \neq 0$ und $t_0 \neq 0$ ist.

Da der größte gemeinsame Teiler von $s(X)$ und $t(X)$ gleich 1 ist, folgt

$$1 = \lambda(X)t(X) + \mu(X)s(X)$$

für geeignete Polynome $\lambda(X), \mu(X) \in F[x]$. Multipliziert man mit dem Polynom $a(X)$ und setzt $\overline{f}(X) = a(X)\lambda(X)$ bzw. $\overline{g}(X) = a(X)\mu(X)$, so erhält man

$$a(X) = \overline{f}(X)t(X) + \overline{g}(X)s(X).$$

Polynomdivision liefert

$$\overline{f}(X) = q(X)s(X) + f(X),$$

wobei der Grad von f kleiner als der von s ist. Setzt man diese Zerlegung nun ein, so folgt

$$a(X) = f(X)t(X) + g(X)s(X),$$

wobei $g(X) = \overline{g}(X) + q(X)t(X)$ gilt. Es bleibt zu zeigen, dass der Grad von $g(X)$ kleiner als der von $t(X)$ ist.

Nun gilt

$$deg\, a(X) < deg\, b(X), \quad deg\, f(X)t(X) < deg\, s(X)t(X) = deg\, b(X).$$

Wegen $g(X)s(X) = a(X) - f(X)t(X)$ folgt

$$deg\, g(X)s(X) = deg\, (a(X) - f(X)t(X)) < deg\, b(X) = deg\, s(X)t(X).$$

Also ist $deg\, g(X) < deg\, t(X)$ wie verlangt. Dividiert man die Gleichung $a(X) = f(X)t(X) + g(X)s(X)$ schließlich durch $b(X) = s(X)t(X)$, so erhält man die Behauptung. ∎

Es lässt sich leicht nachweisen, dass die Polynome $f(X)$ und $g(X)$ aus dem Satz 4.5 eindeutig festgelegt sind.

Hat nun ein Polynom $b(X)$ die folgende Zerlegung in irreduzible Polynome

$$b(X) = p_1(X)^{m_1} p_2(X)^{m_2} \cdots p_k(X)^{m_k},$$

so liefert wiederholte Anwendung von Satz 4.5

$$\frac{a(X)}{b(X)} = \frac{h_1(X)}{p_1(X)^{m_1}} + \frac{h_2(X)}{p_2(X)^{m_2}} + \cdots + \frac{h_k(X)}{p_k(X)^{m_k}},$$

wobei $deg\, h_i(X) < deg\, p_i(X)^{m_i}$ $(1 \le i \le k)$. Sind insbesondere die irreduziblen Faktoren linear, also

$$b(X) = \beta(\alpha_1 - X)^{m_1}(\alpha_2 - X)^{m_2} \cdots (\alpha_k - X)^{m_k},$$

so ergibt sich

$$\frac{a(X)}{b(X)} = \frac{h_1(X)}{(\alpha_1 - X)^{m_1}} + \frac{h_2(X)}{(\alpha_2 - X)^{m_2}} + \cdots + \frac{h_k(X)}{(\alpha_k - X)^{m_k}},$$

wobei $deg h_i(X) < m_i$, $1 \le i \le k$. Setzt man

$$h(X) = \gamma_m + \gamma_{m-1}(\alpha - X) + \cdots + \gamma_1(\alpha - X)^{m-1},$$

so erhält man

$$\frac{h(X)}{(\alpha - X)^m} = \frac{\gamma_1}{(\alpha - X)} + \frac{\gamma_2}{(\alpha - X)^2} + \cdots + \frac{\gamma_m}{(\alpha - X)^m}.$$

Beispiel 4.6 Man finde die Partialbruchzerlegung von

$$\frac{4 + X - X^2}{3 - 5X + X^2 + X^3}$$

Wir zerlegen den Nenner in Linearfaktoren:

$$\begin{aligned} 3 - 5X + X^2 + X^3 &= (1 - X)(3 - 2X - X^2) \\ &= (1 - X)(1 - X)(3 + X) \end{aligned}$$

Also lautet der Ansatz für die Partialbruchzerlegung

$$\frac{4 + X - X^2}{3 - 5X + X^2 + X^3} = \frac{A}{1 - X} + \frac{B}{(1 - X)^2} + \frac{C}{3 + X}.$$

Multipliziert man beide Seiten mit $(1 - X)^2(3 + X)$ und führt einen Koeffizientenvergleich durch, so erhält man das folgende Gleichungssystem

$$\begin{array}{rcrcrcl} 4 &=& 3A &+& 3B &+& C, \\ 1 &=& -2A &+& B &-& 2C, \\ -1 &=& -A & & &+& C, \end{array}$$

Die Lösung lautet: $A = \frac{1}{2}$, $B = 1$, $C = -\frac{1}{2}$.

4.5 Der binomische Lehrsatz für negative Exponenten

Betrachtet man $(1+X)^{-1}$ als Potenzreihe, so lässt sich folgende Darstellung gewinnen:

$$(1+X)^{-1} = 1 - X + X^2 - X^3 + \cdots.$$

Also macht es Sinn, $(1+X)^{-m}$ als formale Potenzreihe zu betrachten. Damit lässt sich der binomische Lehrsatz für negative Exponenten herleiten:

Satz 4.7 *Der Koeffizient von X^n in der Potenzreihe $(1+X)^{-m}$ ist*

$$(-1)^n \binom{m+n-1}{n}.$$

Beweis: Um das Minuszeichen zu vermeiden, betrachten wir $(1-X)^{-m}$. Aus

$$(1-X)^{-1} = 1 + X + X^2 + \cdots,$$

folgt, dass $(1-X)^{-m}$ Produkt von m Faktoren ist. Wir werden zeigen, dass der Koeffizient von X^n der Zahl der ungeordneten Selektionen mit Wiederholung entspricht.

Wir stellen uns vor, dass jeder Faktor einen Zeiger hat, der im Ausgangszustand beim Term 1 steht. Dann wählen wir eine ungeordnete Selektion mit Wiederholung vom Umfang n aus den m Faktoren. Bei jeder Auswahl eines Faktors bewegen wir den Zeiger um eine Position nach rechts. Ist also ein bestimmter Faktor i-mal angesprochen worden, so steht der Zeiger bei X^i. Daher erhalten wir für jeden der $\binom{m+n-1}{n}$ möglichen Auswahlen einen markierten Term, insgesamt also den Faktor X^n. Jede dieser Auswahlen trägt 1 zum Koeffizient von X^n bei. Deshalb beträgt der Koeffizient $\binom{m+n-1}{n}$. Ersetzt man noch X durch $-X$, so ist ein Korrekturfaktor $(-1)^n$ beizufügen. ∎

Im Falle von $(1+X)^{-2}$ folgt

$$(-1)^n \binom{2+n-1}{n} = (-1)^n \binom{n+1}{n} = (-1)^n (n+1),$$

somit lautet die Entwicklung von $(1+X)^{-2}$

$$1 - 2X + 3X^2 - 4X^3 + \cdots.$$

Der bekannte binomische Lehrsatz und Satz 4.7 lassen sich zu einer Formel zusammenfassen. Man definiert für $\alpha \in \mathbb{Z}$ und $n \in \mathbb{N}$

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-n+1)}{n!},$$

wobei $\binom{\alpha}{0} = 1$ gesetzt wird. Für den Fall, dass α positiv ist, erhält man aus einem früheren Lemma . Ist α eine negative Zahl, also $\alpha = -m$, so folgt

$$\begin{aligned}\binom{-m}{n} &= \frac{(-m)(-m-1)(-m-2)\cdots(-m-n+1)}{n!} \\ &= (-1)^n \frac{m(m+1)(m+2)\cdots(m+n-1)}{n!} \\ = (-1)^n \binom{m+n-1}{n}\end{aligned}$$

Dadurch lässt sich der binomische Lehrsatz wie folgt verallgemeinern

$$(1+X)^k = \binom{k}{0} + \binom{k}{1} X + \binom{k}{2} X^2 + \cdots + \binom{k}{n} X^n + \cdots.$$

Im Allgemeinen steht dann auf der rechten Seite eine Potenzreihe, ist jedoch k eine positive Zahl, so folgt

$$\binom{k}{n} = 0 \quad \text{falls} \quad n > k.$$

4.6 Homogene lineare Rekursionen

Beispiel 4.8 Der binomische Lehrsatz liefert ein nahe liegendes Beispiel:

$$(1+X)^k = \binom{k}{0} + \binom{k}{1}X + \binom{k}{2}X^2 + \cdots + \binom{k}{n}X^n + \cdots$$

ist eine erzeugende Funktion für die Folge

$$u_n = \binom{k}{n}.$$

Insbesondere für rekursiv definierte Folgen erweist sich die Methode, erzeugende Funktionen zu benutzen, als sehr schlagkräftig. Es sei $(u_n)_{n\in\mathbb{N}_0}$ eine Zahlenfolge mit $u_0 = 0$, $u_1 = 1$, $u_2 = 5$. Ferner gelte

$$u_{n+2} - 5u_{n+1} + 6u_n = 0.$$

Sei nun $U(X)$ die erzeugende Funktion von $(u_n)_{n\in\mathbb{N}}$. Setzt man die ersten Werte ein, so erhält man

$$\begin{aligned} U(X) &= u_0 + u_1X + u_2X^2 + u_3X^3 + \cdots \\ &= 0 + X + (5u_1 - 6u_0)X^2 + (5u_2 - 6u_1)X^3 + \cdots \\ &= X + 5(u_1X^2 + u_2X^3 + \cdots) - 6(u_0X^2 + u_1X^3 + \cdots). \end{aligned}$$

Somit ergibt sich

$$U(X) = X + 5XU(X) - 6X^2U(X),$$

also

$$U(X) = \frac{X}{1 - 5X + 6X^2}.$$

Nun lässt sich $1-5X+6X^2 = (1-2X)(1-3X)$ schreiben, was zur folgenden Partialbruchzerlegung führt:

$$U(X) = \frac{-1}{1-2X} + \frac{1}{1-3X}.$$

Da sich aber $(1-2X)^{-1}$ bzw. $(1-3X)^{-1}$ schnell entwickeln lassen, folgt

$$U(X) = -(1 + 2X + (2X)^2 + \cdots) + (1 + 3X + (3X)^2 + \cdots),$$

also $u_n = 3^n - 2^n$.

In Verallgemeinerung des letzten Beispiels gehen wir von folgenden linearen Gleichungen aus:

$$[HLR] \quad \begin{cases} u_0 = c, \quad u_1 = c_1, \quad \ldots \ u_{k-1} = c_{k-1}, \\ u_{n+k} + a_1u_{n+k-1} + \cdots + a_ku_n = 0 \quad (n \geq 0). \end{cases}$$

Satz 4.9 *Für das durch [HLR] gegebene System lautet die Lösungsfunktion (als erzeugende Funktion)*

$$U(X) = \frac{R(X)}{1 + a_1X + a_2X^2 + \cdots + a_kX^k},$$

wobei $R(X)$ ein Polynom vom Grade kleiner als k ist.

Beweis: Wir betrachten das Produkt

$$\begin{aligned} & (1 + a_1X + \cdots + a_kX^k)U(X) \\ = \ & (1 + a_1X + \cdots + a_kX^k) \cdot \\ & (u_0 + u_1X + \cdots + u_nX^n + \cdots). \end{aligned}$$

Der Koeffizient von X^{n+k} lautet

$$u_{n+k} + a_1 u_{n+k-1} + \cdots + a_k u_n \quad (n \geq 0).$$

Da aber (u_n) die Rekursion [HLR] erfüllt, sind die Koeffizienten u_{n+k} gleich Null. Die einzigen Koeffizienten, die nicht verschwinden, sind jene von $1, X, \ldots, X^{k-1}$, und daher ist das Produkt ein Polynom $R(X)$ vom Grad $< k$. Die nicht verschwindenden Koeffizienten von $R(X)$ lassen sich auch wie folgt gewinnen:

$$R(X) = u_0 + (u_1 + a_1 u_0)X + \cdots + (u_{k-1} + a_1 u_{k-2} + \cdots + a_{k-1} u_0)X^{k-1}.$$

Da die Werte von $u_0, u_1, \ldots, u_{k-1}$ durch [HLR] festgelegt sind, lässt sich $R(X)$ durch [HLR] spezifieren. ∎

Wir definieren die Hilfsgleichung für [HLR] als

$$T^k + a_1 T^{k-1} + \cdots + a_k = 0.$$

Deren eventuell im Körper vorhandene Wurzeln determinieren die erzeugende Funktion. Daher gehen wir ab sofort davon aus, dass der zugrunde liegende Körper $\mathbb{C}$ ist.

Seien nun $\alpha_1, \alpha_2, \ldots, \alpha_s$ die Wurzeln der Hilfsgleichung mit den Vielfachheiten $m_1, m_2, \ldots, m_s$. Dann können wir die Hilfsgleichung wie folgt schreiben:

$$(T - \alpha_1)^{m_1}(T - \alpha_2)^{m_2} \cdots (T - \alpha_s)^{m_s} = 0,$$

wobei $m_1 + m_2 + \cdots + m_s = k$. Ersetzt man nun T durch $1/X$, so folgt

$$U(X) = \frac{R(X)}{(1 - \alpha_1 X)^{m_1} \cdots (1 - \alpha_s X)^{m_s}}.$$

Satz 4.10 *Es sei $(u_n)_{n\in\mathbb{N}}$ eine Lösung von [HLR]; ferner habe die Hilfsgleichung die Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_s$ mit den Vielfachheiten $m_1, m_2, \ldots, m_s$. Dann gilt*

$$u_n = P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_s(n)\alpha_s^n.$$

Dabei ist $P_i(n)$ für $i = 1, 2, \ldots, s$ ein Term der Form

$$A_0 + A_1 n + \cdots + A_{m_i - 1} n^{m_i - 1}.$$

Mit anderen Worten: P_i ist eine Polynomfunktion in n vom Grade $\leq m_i - 1$.

Beweis: Nach früheren Ergebnissen lässt sich $U(X)$ schreiben als Summe von s Termen der Gestalt

$$\frac{\gamma_1}{1 - \alpha X} + \frac{\gamma_2}{(1 - \alpha X)^2} + \ldots + \frac{\gamma_m}{(1 - \alpha X)^m},$$

wobei in jedem solchen Term $\alpha = \alpha_i$ und $m = m_i$ ist. Wendet man die Binomialentwicklung an, so lautet der Koeffizient von X^n nun

$$\gamma_1 \binom{1 + n - 1}{n} \alpha^n + \gamma_2 \binom{2 + n - 1}{n} \alpha^n + \cdots + \gamma_m \binom{m + n - 1}{n} \alpha^n.$$

Wir vereinfachen, benutzen $\binom{n+l}{n} = \binom{n+l}{l}$ und können diese Terme in der Form $P(n)\alpha^n$ schreiben, wobei

$$P(n) = \gamma_1 \binom{n}{0} + \gamma_2 \binom{n+1}{1} + \cdots + \gamma_m \binom{n+m-1}{m-1}.$$

Wegen

$$\binom{n+l}{l} = \frac{(n+l)(n+l-1)\cdots(n+1)}{l(l-1)\cdots 1}$$

ist $\binom{n+l}{l}$ eine Polynomfunktion in n vom Grade l. Also ist $P(n)$ eine Polynomfunktion in n vom Grade höchstens $m - 1$. ∎

Beispiel 4.11 Diskussion von Rekursionen vom Fibonacci-Typ

$$a_n = A a_{n-1} + B a_{n-2}, \ (n \geq 2).$$

4.7 Rekursiv definierte Folgen als Objekte der Linearen Algebra

Die Analyse des letzten Abschnittes wollen wir noch einmal unter dem Licht der Linearen Algebra erörtern.

Wir betrachten erneut Folgen $(u_n)_{n\in\mathbb{N}_0}$, $u_n \in \mathbb{C}$, die der Rekursion

$$u_{n+k} + a_1 u_{n+k-1} + \cdots + a_k u_n = 0 \tag{59}$$

genügen. Wir verzichten jetzt allerdings auf die Angabe von Anfangsbedingungen. Ohne Schwierigkeiten weist man nach:

Lemma 4.12 *Die Menge L der Folgen (u_n), die* (59) *erfüllen, bildet im Folgenraum einen $\mathbb{C}$-Unterraum.*

Es ist nahe liegend, die Frage nach der Dimension zu stellen. Eine Antwort lässt sich dadurch geben, dass wir eine Basis von L beschreiben. Dabei fragen wir uns zunächst, ob eventuell geometrische Folgen in L liegen. Wir erhalten als Ergebnis:

Lemma 4.13 *Es sei $(u_n) = (\alpha^n)$ eine Folge. Diese Folge erfüllt* (59) *genau dann, wenn α eine Wurzel der Hilfsgleichung ist.*

Beweis: Man berechnet ohne weiteres, dass $(\alpha^n)_{n\in\mathbb{N}_0}$ genau dann (59) erfüllt, wenn

$$\alpha^{n+k} + a_1\alpha^{n+k-1} + \cdots + a_k\alpha^n = 0$$

genügt, was zu

$$\alpha^k + a_1\alpha^{k-1} + \cdots + a_{k-1}\alpha + a_k = 0$$

führt. ∎

Das letzte Lemma macht verständlich, warum in Satz 4.10 die geometrischen Folgen auftauchen. Schließlich weist man nach, dass für verschiedene Nullstellen (α_1^n), (α_2^n) die Folgen mit $n \in \mathbb{N}_0$ linear unabhängig sind.

Lemma 4.14 *Es seien $(\alpha_1^n)_{n\in\mathbb{N}}$, $(\alpha_2^n)_{n\in\mathbb{N}}$ geometrische Folgen mit $\alpha_1 \neq \alpha_2$. Dann sind diese Folgen linear unabhängig.*

Auf die Diskussion des Falls einer Vielfachheit einer Nullstelle wollen wir hier verzichten.

4.8 Der inhomogene Fall

Komplizierter wird die Situation, wenn ein inhomogener Störterm auftritt.

$$\begin{aligned} &u_0 = c, \quad u_1 = c_1, \ \ldots, \ u_{k-1} = c_{k-1}, \\ &u_{n+k} + a_1 u_{n+k-1} + \cdots + a_k u_n = f(n) \quad (n \geq 0). \end{aligned}$$

Dessen Form selbst bestimmt nun wieder den Ansatz. Es soll hier nicht auf die allgemeine Theorie eingegangen werden. Wir beschränken uns auf die Angabe eines Beispiels: Es seien

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+2} - u_{n+1} - 6u_n = n \quad (n \geq 0).$$

Es sei $U(X)$ die zugehörige erzeugende Funktion. Mit den üblichen Techniken erhalten wir

$$\begin{aligned} & (1 - X - 6X^2)(u_0 + u_1X + u_2X^2 + \cdots) \\ = \ & u_0 + (u_1 - u_0)X + (u_2 - u_1 - 6u_0)X^2 + \cdots + (u_{n+2} - u_{n+1} - 6u_n)X^{n+2} + \cdots \\ = \ & X + (X^3 + 2X^4 + \cdots + nX^{n+2} + \cdots) \\ = \ & X + X^3(1 - X)^{-2}. \end{aligned}$$

Wegen $1 - X - 6X^2 = (1 + 2X)(1 - 3X)$ gilt für die erzeugende Funktion $U(X)$ schließlich

$$(1 + 2X)(1 - 3X)U(X) = \frac{X - 2X^2 + 2X^3}{(1 - X)^2},$$

und somit

$$\begin{aligned} U(X) &= \frac{X - 2X^2 + 2X^3}{(1+2X)(1-3X)(1-X)^2} \\ &= \frac{A}{1+2X} + \frac{B}{1-3X} + \frac{C}{1-X} + \frac{D}{(1-X)^2} \end{aligned}$$

für gewisse noch zu ermittelnde Konstanten A, B, C, D. Ein lineares Gleichungssystem liefert dann

$$A = -\frac{2}{9}, \quad B = \frac{1}{4}, \quad C = \frac{5}{36}, \quad D = -\frac{1}{6}.$$

Das führt zur Lösung

$$u_n = \frac{1}{36}[(-2)^{n+3} + 3^{n+2} - 6n - 1].$$

5 Diskrete Strukturen und Geometrie

5.1 Designs

Im Folgenden werden wir uns kurz mit kombinatorischen Grundmustern beschäftigen, die im Grenzbereich von Kombinatorik, Statistik und Geometrie liegen. Ihr weiter gehendes Studium gehört in eine Spezialvorlesung, hier geht es uns insbesondere um das Vorstellen von Grundideen und das Aufzeigen kombinatorischer Zählprinzipien.

Wir stellen uns folgende Situation vor: Ein Hersteller möchte ein neu entwickeltes Produkt testen. Dabei stehen v unterschiedliche Ausführungen zur Diskussion. Dieser Test sollte dem Grundsatz genügen:

(i) Jeder Verbraucher sollte die gleiche Anzahl, nämlich k Ausführungen kennenlernen.

(ii) Jede Ausführung sollte von der gleichen Anzahl von Testpersonen, nämlich r, überprüft werden.

Ist $v = 8$, $k = 4$ und $r = 3$, so könnte ein möglicher Versuchsplan lauten:

$$1234,\ 5678,\ 1357,\ 2468,\ 1247,\ 3658,$$

wobei wir die unterschiedlichen Ausführungen mit den Ziffern 1 bis 8 bezeichnet haben.

Definition 5.1 *Es sei X eine v-Menge. Eine Menge $\mathcal{B}$ von k-Teilmengen von X heißt* Design *oder* Blockplan *mit den Parametern (v, k, r), wenn jedes $x \in X$ zu genau r Teilmengen in $\mathcal{B}$ gehört. Die Teilmengen bezeichnen wir vielfach als* Blöcke *des Design.*

Das obige Beispiel beschrieb schon eine konkrete Situation.

Ist $\mathcal{B}$ ein Design, denn zählen wir die Elemente der Menge

$$\{(x, B) \mid x \in X,\, x \in B,\, B \in \mathcal{B}\}$$

. Zweifache Abzählung liefert die Identität

$$r \cdot v = b \cdot k,$$

wobei $b = |\mathcal{B}$ gesetzt wurde. Somit folgt $b = \frac{rv}{k} \leq \binom{v}{k}$, denn $\binom{v}{k}$ ist die Zahl der k-Teilmengen von X. Die nächste Aussage geht noch einen Schritt weiter:

Satz 5.2 *Es gibt genau dann einen Blockplan mit den Parametern (v, k, r), wenn*

$$k \mid vr \quad \text{und} \quad \frac{vr}{k} \leq \binom{v}{k} \tag{60}$$

gelten.

Beweis: Die Notwendigkeit der Bedingung wurde gerade hergeleitet. Ferner beachte man, dass gilt

$$\frac{vr}{k} \leq \binom{v}{k} \Longleftrightarrow r \leq \binom{v-1}{k-1}.$$

Letzteres ist klar, da jedes x, das in einem $B \in \mathcal{B}$ auftritt, von $k-1$ von x verschiedenen Elementen aus X 'begleitet' wird.

Wir setzen die Gültigkeit der Parameterbedingung (60) voraus. Es sei $b = vr/k$ und $\mathcal{B}$ eine Menge von b verschiedenen k-Teilmengen einer v-Menge X. Wir definieren

$$S := \{(x, B) \mid x \in X,\ B \in \mathcal{B}, x \in B\}, \tag{61}$$

also ist

$$|\,S\,| = \sum_{x \in X} r_x(S) = \sum_{B \in \mathcal{B}} r_B(S) = bk = vr.$$

Gilt für alle $x \in X$ bereits $r_x(S) = r$, dann ist $\mathcal{B}$ schon ein Design. Andernfalls gibt es $x_1, x_2 \in X$ mit $r_{x_1}(S) > r > r_{x_2}(S)$. Wir definieren

$$\begin{aligned} \mathcal{B}_1 : &= \{B \in \mathcal{B} : x_1 \in B \text{ und } x_2 \notin B\}, \\ \mathcal{B}_2 : &= \{B \in \mathcal{B} : x_2 \in B \text{ und } x_1 \notin B\}. \end{aligned}$$

Für $B \in \mathcal{B}_1$ sei $B^* := (B \setminus \{x_1\}) \cup \{x_2\}$. Setzen wir $n := |\{B \in \mathcal{B} \mid x_1, x_2 \in B\}|$, so gilt $|\mathcal{B}_1| = r_{x_1} - n$ und $|\mathcal{B}_2| = r_{x_2} - n$ und es folgt $|\mathcal{B}_1| \geq |\mathcal{B}_2|$. Daher gibt es mindestens ein $B_0 \in \mathcal{B}_1$ mit $B_0^* \notin \mathcal{B}_2$. Für $\mathcal{B}' := (\mathcal{B} \setminus \{B_0\}) \cup \{B_0^*\}$ sei S' definiert analog wie (61) für $\mathcal{B}$. Dann gilt für alle $x_i \in X$, $2 < i \leq v$ auch $r_{x_i}(S') = r_{x_i}(S)$ und auch $r_{x_1}(S') = r_{x_1}(S) - 1$, $r_{x_2}(S') = r_{x_2}(S) + 1$. Also liegt $\mathcal{B}'$ 'näher' an einem Design als $\mathcal{B}$. Nach einer endlichen Anzahl von Schritten gewinnt man aus $\mathcal{B}$ ein Design. ∎

Wir bemerken, dass die zweite Bedingung zu

$$r \leq \binom{v-1}{k-1}$$

umgeschrieben werden kann. Auf diese Weise lässt sich auch einsehen, dass diese Bedingung notwendig ist: jedes Element x, das in einem Block auftritt, wird von $k-1$ der restlichen $v-1$ Objekte begleitet. Folglich kann x nicht mehr als $\binom{v-1}{k-1}$-mal auftreten.

Die Bedingung, dass jedes Element in der gleichen Anzahl von Blöcken auftritt, kann auf verschiedene Weisen verschärft werden. Man könnte etwa verlangen, dass jedes Paar in der gleichen Anzahl von Blöcken enthalten ist bzw. allgemeiner

Definition 5.3 *Es sei X eine v-Menge. Dann heißt eine Menge $\mathcal{B}$ von k-Teilmengen von X ein t-Design mit den Parametern (v, k, r_t), wenn für jede t-Teilmenge T von X die Zahl der Blöcke, die T enthalten, genau r_t beträgt.*

Die bisher betrachteten Designs sind im Sinne dieser Definition 1-Designs. Es wird sofort klar, dass die endlichen projektiven Ebenen als 2-Designs auftreten. Das nächste Beispiel zeigt ein 3-Design mit $v = 8$ und $k = 4$:

1235	4678
1346	2578
1457	2368
1568	2347
1267	3458
1378	2456
1248	3567

Es liegt auf der Hand, dass es eine mühsame Arbeit ist, im Einzelnen nachzuweisen, dass es sich um ein 3-Design handelt. Jede 3-Teilmenge tritt in genau einem der 14 Blöcken auf, etwa $\{2, 3, 8\}$ im Block 2368 und in keinem weiteren Block. Dieses Design ist allerdings kein 4-Design, weil etwa $\{1, 2, 3, 6\}$ nicht in einem Block auftritt.

Satz 5.4 *Ist $\mathcal{B}$ ein t-Design mit den Parametern (v, k, r_t), so ist $\mathcal{B}$ auch ein s-Design für alle $s = 1, 2, \ldots, t-1$.*

Beweis: Offenbar genügt es, die Behauptung für $s = t - 1$ zu zeigen.

Sei X die v-Menge der Objekte und $Y \subset X$ mit $\mid Y \mid = t - 1$. Wir definieren:

$$S = \{(x, B) \mid x \in X \setminus Y,\, B \in \mathcal{B}, \{x\} \cup Y \subseteq B\}.$$

Da x nicht in der $t-1$-Menge Y liegt, gibt es $v - (t-1)$ Möglichkeiten für x und zu jedem x wiederum r_t Möglichkeiten für B, da $\{x\} \cup Y$ eine t-Teilmenge von X ist, also $\mid S \mid = r_t \cdot (v - t + 1)$.

Auf der anderen Seite sei r_y die Zahl der Blöcke mit $Y \subset B$. Für jedes solche B ist jedes der $k - (t-1)$ Elemente von $B \setminus Y$ ein mögliches x. Also ist die Zahl der Paare (x, B) auch gleich $(k - (t-1)) \cdot r_y$. Gleichsetzung der beiden Terme liefert

$$r_y \cdot (k - (t-1)) = r_t \cdot (v - t + 1).$$

Da r_y nur von v, t, k abhängt, folgt die Behauptung. ∎

Der Beweis des letzten Satzes lässt sich noch weiter auswerten. Er liefert eine Formel für die Abhängigkeit von r_{t-1} von r_t, nämlich

$$r_{t-1} = r_t \cdot \frac{v-t+1}{k-t+1}.$$

Konkret im obigen Beispiel gilt mit $v = 8, k = 4$ und $r_3 = 1$ schließlich

$$r_2 = r_3 \cdot \frac{v-2}{k-2} = 3, \quad r_1 = r_2 \cdot \frac{v-1}{k-1} = 7.$$

Satz 5.5 (i) *Ist $\mathcal{B}$ ein t-Design mit den Parametern (v, k, r_t), dann gilt für das s-Design $\mathcal{B}$, $1 \le s \le t-1$*

$$r_s = r_t \frac{(v-s)(v-s-1)\cdots(v-t+1)}{(k-s)(k-s-1)\cdots(k-t+1)}.$$

(ii) *Gibt es ein t-Design mit den Parametern (v, k, r_t), dann gilt für jedes s mit $0 \le s \le t-1$ stets*

$$(k-s)(k-s-1)\cdots(k-t+1) \mid r_t(v-s)(v-s-1)\cdots(v-t+1).$$

Beweis: Aus dem Beweis von (5.4) folgt: $r_{t-1} = r_t \cdot \frac{v-(t-1)}{k-(t-1)}$. Wiederholte Anwendung liefert die Behauptung; beachte $r_1 = r_{t-(t-1)}$. ∎

Die Teilbarkeitsbedingung in (ii) hilft, gewisse Parametermengen auszuschließen. Ist etwa $v = 56$, $k = 11$ und $r_2 = 1$, so ergeben sich:

$$\begin{array}{lccc} (s=0): & 11 \times 10 & \mid & 56 \times 55 \\ (s=1): & 10 & \mid 55 & \end{array}.$$

Im Unterschied zu den 1-Designs sind diese Teilbarkeitsbedingungen nur notwendig, nicht jedoch hinreichend.

5.2 Zyklische Konstruktion von Designs

Es sei $K \subseteq \mathbb{Z}_m$ und $i \in \mathbb{Z}_m$ beliebig, dann bezeichnet $K + i$ jene Teilmenge von $\mathbb{Z}_m$, die durch Komplexaddition entsteht:

$$K + i = \{x + i \mid x \in K\}.$$

Lemma 5.6 *Es sei $m \in \mathbb{N}$ und $K \subseteq \mathbb{Z}_m$. Sind die m Teilmengen $K + i$, $i \in \mathbb{Z}_m$ paarweise verschieden, dann bilden diese Teilmengen Blöcke eines 1-Designs $\mathcal{B}$ mit den Parametern $v = m$, $k = |K|$ und $r = k$.*

Beweis: Um dies zu beweisen, beachte man, dass ein beliebiges Element $a \in \mathbb{Z}_m$ genau dann in $K + i$ auftritt, wenn $a = x + i$ für ein $x \in K$ gilt. Diese Aussage ist äquivalent zu $0 = x + (i - a)$, woraus folgt, dass 0 im Block $K + (i - a)$ liegt. Daher ist a genau dann in den Blöcken

$$K + i_1, K + i_2, \ldots, K + i_r,$$

enthalten, wenn

$$0 \in K + (i_1 - a), K + (i_2 - a), \ldots, K + (i_r - a)$$

liegt. Somit liegen 0 und jedes beliebige a in der gleichen Anzahl r von Blöcken. Nach Konstruktion ist $v = m$. Die Zahl der Blöcke b ist ebenfalls m, so dass wegen $bk = vr$ die Wiederholungszahl r gleich der Blockgröße k ist, also $r = k = |K|$, wie behauptet. ∎

Von Interesse ist die Situation, in der jeder Block gleichviele Elemente aus K enthält. Diese Beobachtung ist Anlass zur folgenden Definition.

Definition 5.7 *Eine Teilmenge $K \subseteq \mathbb{Z}_m$ heißt eine* Differenzmenge[29]*, wenn für beliebige $x \neq y \in K$ die Differenz $x - y$ jeden Wert $\neq 0$ in $\mathbb{Z}_m$ gleich oft annimmt.*

Beispiel 5.8 Man rechnet schnell nach, dass die Teilmenge $\{0, 2, 3, 4, 8\}$ aus $\mathbb{Z}_{11}$ eine Differenzmenge ist, wie eine entsprechende Tabelle zeigt:

	0	2	3	4	8
0	–	9	8	7	3
2	2	–	10	9	5
3	3	1	–	10	6
4	4	2	1	–	7
8	8	6	5	4	–

.

Satz 5.9 *Es sei $K \subseteq \mathbb{Z}_m$ eine Differenzmenge. Dann sind die Mengen $K + i$, mit $i \in \mathbb{Z}_m$ Blöcke eines 2-Designs mit den Parametern*

$$v = m, \quad k = |K|, \quad r_2 = k(k-1)/(m-1).$$

Beweis: Es seien $a, b \in \mathbb{Z}_m$. Da K eine Differenzmenge ist, hat die Gleichung

$$x - y = a - b$$

$k(k-1)/(m-1)$ Lösungen mit $x, y \in K$. Für jede Lösung (x, y) sei $i = a - x$. Dann ist

$$a = x + i, \quad b = a - (x - y) = y + i,$$

und a und b gehören beide zu $K + i$. Daher ist jede 2-Teilmenge $\{a, b\}$ aus $\mathbb{Z}_m$ enthalten in $r_2 = k(k-1)/(m-1)$ Blöcken $K + i$ und K folglich ein 2-Design. ∎

Es ist im Allgemeinen schwierig, für gegebene Werte m und k Differenzenmengen anzugeben, selbst wenn man die offensichtlich notwendige Bedingung, dass $m - 1$ die Zahl $k(k-1)$ zu teilen hat (r_2 ist dann eine ganze Zahl), voraussetzt. Die Konstruktion spezieller Differenzmengen ist eine eigenständige anspruchsvolle Disziplin.

5.3 Lateinische Quadrate

Ausgangssituation ist eine klassische Aufgabe der Unterhaltungsmathematik, die der Mathematiker Euler 1782 am Petersburger Hof zu lösen versuchte:

- *1. Vorgabe:* Man positioniere 36 Offiziere aus 6 verschiedenen Regimentern in einem 6×6 Quadrat, dass jedes Regiment genau einmal in jeder Zeile und in jeder Spalte vertreten ist.
- *2. Vorgabe:* Diese Offiziere sind insgesamt sechs verschiedenen Diensträngen zuzuordnen.

Ist es möglich, die Aufstellung auch so vorzunehmen, dass *zusätzlich* in jeder Zeile und in jeder Spalte jeder Dienstgrad genau einmal vertreten ist? Die Lösung blieb lange offen, Euler vermutete, daß das Problem keine positive Lösung besitzt.

Definition 5.10 *Es sei K eine n-Menge. Unter einem lateinischen Quadrat L der Ordnung n versteht man eine $n \times n$-Matrix, in der in jeder Zeile und jeder Spalte jedes Element aus K genau einmal vertreten ist.*

Ohne weiteres kann man $K = \{0, 1, \ldots, n-1\}$ annehmen. Allerdings kommt die Bezeichnung *lateinisch* daher, dass man im 18. Jahrhundert bei solchen Quadraten, die damals nur in der Unterhaltungsmathematik vorkamen, zur Belegung der Felder nicht Zahlen, sondern lateinische Buchstaben verwandte.

Die Bedeutung der Restklassenmengen $\mathbb{Z}_m$ unterstreicht der folgende offensichtliche Satz:

[29] Man beachte, dass es unterschiedliche Definitionen gibt; siehe z. B. Beutelspacher; Rosenbaum: Projektive Geometrie. Vieweg 1992.

Satz 5.11 *Für jedes $m \geq 2$ ist die folgende Matrix*

$$L(i,j) = i + j, \quad i,j \in \mathbb{Z}_m$$

ein lateinisches Quadrat.

Definition 5.12 *Zwei lateinische Quadrate L_1, L_2 heißen zueinander* orthogonal*, wenn es für jedes Paar $(k,k') \in \mathbb{Z}_m \times \mathbb{Z}_m$ genau eine Position (i,j) gibt mit*

$$L_1(i,j) = k, \quad L_2(i,j) = k'.$$

Eine Menge von m lateinischen Quadraten heißt paarweise orthogonal *(pairwise mutually orthogonal), wenn jedes Paar von lateinischen Quadraten orthogonal ist.*

Die Frage nach der maximalen Größe einer Menge von paarweise orthogonalen lateinischen Quadraten der Ordnung n kann als eine der tiefsten zentralen Fragen der Geometrie und Kombinatorik bezeichnet werden. Genau danach hatte man eigentlich Euler seinerzeit gefragt. Die Antwort, die zu Beginn dieses Jahrhunderts durch Tarry gegeben werden konnte, lautete: *Es gibt kein Paar orthogonaler lateinischer Quadrate der Ordnung 6.* Euler vermutete nun weiter, dass 6 (neben 2) wohl nicht die einzige *Ausnahmeordnung* sein könne und dass zu keiner geraden, nicht durch 4 teilbaren Ordnung orthogonale lateinische Quadrate existieren würden. Erst 1959/60 konnten Bose, Parker und Shrikhande diese Euler'sche Vermutung widerlegen; sie gaben sogar für jede gerade, nicht durch 4 teilbare Ordnung ≥ 10 ein Verfahren zur Konstruktion eines Paares orthogonaler lateinischer Quadrate an. Andererseits hatte schon Euler zeigen können, dass es zu jeder entweder ungeraden oder aber durch 4 teilbaren Ordnung ein solches Paar gibt. Somit sind tatsächlich 2 und 6 die einzigen Ordnungen, zu denen es keine orthogonalen lateinischen Quadrate gibt[30].

Satz 5.13 *Es sei p eine Primzahl und $t \in \mathbb{Z}_p$, $t \neq 0$. Dann definiert die Vorschrift*

$$L_t(i,j) = ti + j, \quad i,j \in \mathbb{Z}_p$$

ein lateinisches Quadrat. Für jedes Paar (t,u) mit $t \neq u$ sind die lateinischen Quadrate L_t und L_u zueinander orthogonal.

Beweis: ohne Beweis in der Vorlesung ∎

[30] vgl. insbesondere die Ausführungen in dem Buch von Pickert, G.: Einführung in die endliche Geometrie. 1974. Stuttgart: Klett.

6 Gruppen

6.1 Begriffliches

Wenngleich die nächste Begriffsbildung eigentlich als bekannt vorausgesetzt werden kann, erwähnen wir sie der Vollständigkeit halber. Historisch geht die formale Definition auf das Jahr 1882 zurück ([13] resp. [7], p. 13). Jedoch sind schon seit den Zeiten Euler's Argumentationen und Fragestellungen bekannt, die wir heute der Gruppentheorie zuordnen.

Definition 6.1 *Eine Menge G zusammen mit einer Verknüpfung $*$ heißt* Gruppe*, wenn $(G, *)$ die folgenden Eigenschaften hat:*

(i) (G1) *Für alle $x, y \in G$ gilt: $x * y \in G$.*

(G2) *Für alle $x, y, z \in G$ gilt: $(x * y) * z = x * (y * z)$.*

(G3) *Es gibt ein Element $e \in G$ mit $e * x = x * e = x$ für alle $x \in G$.*

(G4) *Für alle $x \in G$ gibt es ein $x' \in G$ mit $x * x' = x' * x = e$.*

(ii) *Gilt überdies*

$$x * y = y * x$$

für alle $x, y \in G$, so heißt $(G, *)$ eine abelsche[31] *oder* kommutative *Gruppe.*

(iii) *Ist G eine endliche Menge, so heißt $(G, *)$ eine endliche Gruppe; die Elementeanzahl von G wird als* Ordnung *bezeichnet, in Zeichen $|G|$. Andernfalls sprechen wir von einer* unendlichen Gruppe*.*

Offensichtlich wird in (G1) sichergestellt, dass $(G, *)$ ein *Verknüpfungsgebilde* ist. (G2) konstatiert das *Assoziativgesetz* für die Verknüpfung, während in (G3) die Existenz eines *neutralen Elements* gefordert wird. (G4) ist für die Existenz eines jeweiligen *inversen Elements* verantwortlich.

Im Folgenden werden wir als Verknüpfungszeichen meist $\cdot$ verwenden bzw. den Punkt ganz weglassen. Das zu x inverse Element schreibt sich dann als x^{-1}. In kommutativen Gruppen wählt man vielfach $+$ als Verknüpfungszeichen. Das neutrale Element (siehe (G3)) schreibt man dann als 0, das zu x inverse Element als $-x$.

Bevor wir nun Beispiele angeben, wollen wir eine scheinbare Offenheit unserer Definition ausräumen.

Lemma 6.2 *Es sei $(G, \cdot)$ eine Gruppe. Dann gelten:*

(i) *Es gibt genau ein Element e mit $e \cdot x = x \cdot e = x$ für alle $x \in G$.*

(ii) *Zu jedem $x \in G$ gibt es genau ein Element $x' \in G$ mit $x \cdot x' = x' \cdot x = e$.*

Beweis: elementares Nachrechnen ∎

[31] benannt nach dem dänischen Mathematiker *Niels Henrik Abel* - geboren 5. August 1802, gestorben am 6. April 1829) in Froland, Norwegen- war ein norwegischer Mathematiker.

Abel war der Sohn von Soren Georg Abel, einem Theologen und Philologen, und Ane Marie Simonson. Er hatte sechs Geschwister. Abel besuchte 1821 die Universität von Christiania (Oslo). Er arbeitete von 1825 - 1827 im Ausland, vorwiegend in Paris, Berlin und Göttingen. Nach seiner Rückkehr wurde er Dozent an der Universität und Ingenieurschule in Christiania.

Abel formulierte die Theorie des elliptischen Integrals um in die Theorie der elliptischen Funktionen, indem er deren inverse Funktionen benutzte. Auf diesem Gebiet arbeitete er mit Carl Gustav Jacob Jacobi zusammen.

1824 bewies er, dass die allgemeine Gleichung fünften Grades nicht durch eine Formel gelöst werden kann, die nur Wurzeln und arithmetische Grundoperationen verwendet. Abel war neben Galois, der Abels Untersuchungen zur Unlösbarkeit von Gleichungen (Satz von Abel-Ruffini) auf spezielle Gleichungen verallgemeinerte (sog. Galoistheorie), ein wichtiger Mitbegründer der Gruppentheorie. Abel starb 1829 an Lungentuberkulose.

Nach Abel sind die abelschen Gruppen und die abelschen Integrale benannt, auerdem vergibt die norwegische Akademie der Wissenschaften seit 2003 den Abel-Preis.

Beispiele 6.3 (i) die Menge der ganzen Zahlen $(\mathbb{Z}, +)$; die Menge der Restklassen $(\mathbb{Z}_n, +)$ bei Division durch m hinsichtlich der Addition resp. die Menge $(U(\mathbb{Z}_n), \cdot)$ der invertierbaren Restklassen hinsichtlich der Multiplikation.

(ii) die unmittelbar beschreibbaren Gruppen mit kleinen Elementeanzahlen, etwa V_4 als *Klein'sche Vierergruppe.*

(iii) die additiven bzw. multiplikativen Gruppen der Körper $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$.

(iv) die symmetrischen Gruppen $(S_n, \circ)$ der Permutationen endlicher Mengen.

(v) die geometrischen Symmetriegruppen $(D_n, \circ)$ der regelmäßigen n-Ecke, die so genannten *Diedergruppen.*

(vi) $\mathrm{GL}_n(F) = \{A \mid A \text{ ist eine } n \times n\text{-Matrix mit Einträgen aus } F \text{ und } \det A \neq 0\}$.

Wir geben nun weitere elementare Begriffsbildungen an:

Definition 6.4 *Es sei $(G, \cdot)$ eine Gruppe.*

(i) *Eine nichtleere Teilmenge $U \subseteq G$ heißt* Untergruppe*, falls $xy^{-1} \in U$ für alle $x, y \in U$ gilt, in Zeichen: $U \leq G$.*

(ii) *Es sei $x \in G$ und m die kleinste natürliche Zahl, für die $x^m = 1$ gilt. Dann heißt m die* Ordnung *des Elementes x und wir schreiben $|x|$. Gibt es kein solches m, so sagt man, dass x* unendliche Ordnung *habe.*

Lemma 6.5 *Es sei $(G, \cdot)$ eine endliche Gruppe und $g \in G$. Dann gilt:*

$$g^s = 1 \Longleftrightarrow |g| \mid s.$$

Beweis: offensichtlich ∎

6.2 Homomorphismen

Ähnlich wie in der Linearen Algebra lineare Abbildungen die zu Vektorräumen passenden Abbildungen sind, werden wir nun strukturverträgliche Abbildungen definieren und diskutieren.

Definition 6.6 *Es seien $(G, *), (H, *')$ Gruppen und $\varphi : G \longrightarrow H$ eine Abbildung. Die Abbildung φ heißt ein* Homomorphismus*, falls $\varphi(x * y) = \varphi(x) *' \varphi(y)$ für alle $x, y \in G$ gilt. Ist $G = H$, so spricht man auch von einem* Endomorphismus*. Ist φ eine bijektive Abbildung, so heißt φ ein* Isomorphismus*. Ist φ ein Isomorphismus und $G = H$, so spricht man von einem* Automorphismus*.*

Gruppen, zwischen denen ein Isomorphismus konstituiert werden kann, heißen auch *isomorph.* Ohne Beweis erwähnen wir:

Lemma 6.7 *Es sei $\varphi : G \longrightarrow H$ ein Isomorphismus der Gruppen $(G, *)$ und $(H, *')$. Dann ist auch φ^{-1} ein Isomorphismus.*

Man beachte, dass *nicht* in jeder Theorie die Umkehrung eines bijektiven Isomorphismus wieder ein Isomorphismus sein muss. So sind die Umkehrabbildungen von bijektiven, ordnungstreuen Abbildungen nicht notwendigerweise ordnungstreu.

6.3 Zyklische Gruppen

Ziel unserer Darlegungen ist es, einen möglichst großen Vorrat an Standardbeispielen von Gruppen zu präsentieren. Die einfachste Klasse und dennoch eine überall auftretende Klasse von Gruppen ist die Klasse der *zyklischen Gruppen*. Zyklische Gruppen werden einerseits durch ihre Eigenschaften charakterisiert und definiert, anderseits stellt sich die Frage, wie sie *realisiert* werden, m.a.W. welche Modelle sie besitzen. Beide Fragen werden wir beantworten.

Definition 6.8 *Eine Gruppe G heißt* zyklisch*, wenn ein Element $x \in G$ existiert, so dass $G = \{x^n \mid n \in \mathbb{Z}\}$. Wir schreiben $G = \langle x \rangle$.*

Es ergeben sich zwei Typen von Fällen. Einerseits kann das erzeugende Element x eine unendliche Ordnung besitzen, also $G = \{\ldots, x^{-2}, x^{-1}, x^0, x^1, x^2, \ldots\}$ und wir schreiben $G = C_\infty$. Eine Realisierung ist z.B. die additive Gruppe $(\mathbb{Z}, +) = \langle 1 \rangle$ und wie man sich überzeugt, ist jede zyklische Gruppe, deren Erzeuger unendliche Ordnung hat, isomorph zu $(\mathbb{Z}, +)$. Hat der Erzeuger die Ordnung m, also $C_n = \{x^i \mid i = 0, \ldots, n-1\}$, so ist jede andere zyklische Gruppe mit dieser Eigenschaft ebenfalls von diesem Isomorphietyp. Wie wir weiter unten noch sehen werden, lassen sich die zyklischen Gruppen C_n durch die Kongruenzengruppen $(\mathbb{Z}_n, +_n)$ realisieren. Dadurch sind schon *alle* zyklischen Gruppen gegeben - und wir wiederholen nochmals unsere Argumentation:

Satz 6.9 *Es sei G eine zyklische Gruppe. Dann ist G entweder zu $(C_\infty, \cdot)$ oder zu einem $(C_n, \cdot)$ für ein $n \in \mathbb{N}$ isomorph. Insbesondere sind alle zyklischen Gruppen kommutativ.*

Beweis: Es sei G eine zyklische Gruppe. Sind alle Potenzen von x untereinander verschieden, so liegt die Menge der Elemente $\{1, x, x^2, \ldots, x^n, \ldots\}$ sicher in G. Dann ist es nicht möglich, dass zwei Potenzen von x^{-1} übereinstimmen, wie man leicht nachrechnet. Gleichzeitig stimmt auch keine Potenz von x mit einer nichttrivialen von x^{-1} überein, mit anderen Worten:

$$G = \{\ldots, x^{-3}, x^{-2}, x^{-1}, 1, x^1, x^2, x^3, \ldots\}.$$

Offensichtlich beschreibt:

$$\phi : i \mapsto x^i$$

einen Isomorphismus von $(\mathbb{Z}, +)$ nach $(G, \cdot)$, d.h. $(G, \cdot)$ ist zur additiven Gruppe der ganzen Zahlen isomorph.

Wir betrachten nun den Fall einer zyklischen Gruppe $G = \langle x \rangle$, wobei die Potenzen von x nicht alle verschieden sind. Es lässt sich leicht begründen, dass auch als fragliche Exponenten auch positive ganze Zahlen in Frage kommen. Dann gibt es ein kleinstes $m < k$, $m, k \in \mathbb{N}$ mit $x^m = x^k$, also $x^{k-m} = 1$ für die natürliche Zahl $k - n$. O.B.d.A. gibt es eine kleinste natürliche Zahl $n \in \mathbb{N}$ mit $x^n = 1$. Dann ist

$$G = \{1, x, x^2, \ldots, x^{n-1}\},$$

und diese Menge ist abgeschlossen gegenüber der Multiplikation und der Inversenbildung. Das Rechnen in G gehorcht, wie man leicht sieht, der modulo-n Addition, d.h. $(G, \cdot) \cong (\mathbb{Z}_n, +)$. ∎

6.4 Kongruenzen

Wir schließen noch einmal an die Charakterisierung der zyklischen Gruppen an und beleuchten entsprechende Aspekte von einer anderen Seite, nämlich aus dem Kontext des Rechnens mit Kongruenzen. Im Folgenden sind, wenn nichts anderes gesagt wird, die auftretenden Elemente ganze Zahlen.

Definition 6.10 *Es seien $x_1, x_2 \in \mathbb{Z}$, $m \in \mathbb{N}$. Wir sagen, dass x_1* kongruent zu x_2 modulo m *ist, in Zeichen*

$$x_1 \equiv x_2 \pmod{m}$$

falls m die Zahl $x_1 - x_2$ teilt.

Man zeigt durch direktes Nachrechnen, dass diese Relation eine Äquivalenzrelation ist. Die von x erzeugte Äquivalenzklasse $\{x' \in \mathbb{Z} \mid x \equiv x' \pmod m\}$ bezeichnen wir mit $[x]_m$. Diese Äquivalenzrelation ist auch mit den Verknüpfungen in $\mathbb{Z}$ verträglich; in solchen Fällen spricht man auch von einer *Kongruenzrelation*. Wiederum durch elementares Nachrechnen rechtfertigt man den nächsten Satz:

Proposition 6.11 *Es sei $m \in \mathbb{N}$ und $x_1,\ x_2,\ y_1,\ y_2 \in \mathbb{Z}$ mit*

$$x_1 \equiv x_2 \pmod m, \quad y_1 \equiv y_2 \pmod m.$$

Dann gelten:

(i) $x_1 + y_1 \equiv x_2 + y_2 \pmod m$

(ii) $x_1 y_1 \equiv x_2 y_2 \pmod m$.

Auf diesen elementaren wie fundamentalen Regeln beruhen Quersummenkriterien. Aufgrund von Proposition 6.11 liefert die Addition- resp. Multiplikationsverknüpfung wiederum eine volle Äquivalenzklasse. Nun kann man auf diesen Äquivalenzklassen Komplexoperationen definieren, nämlich

$$\begin{aligned} [x]_m +_m [y]_m &= \{x' + y' \mid x' \in [x]_m,\ y' \in [y]_m\} \\ [x]_m \cdot_m [y]_m &= \{x' \cdot y' \mid x' \in [x]_m,\ y' \in [y]_m\} \end{aligned}$$

Die Menge aller Äquivalenz- oder auch Resteklassen *modulo m* bezeichnen[32] wir mit $\mathbb{Z}_m$.

6.4.1 Die Gruppen und Ringe $\mathbb{Z}_m$

Dieses Rechnen mit den Äquivalenzklassen genügt ähnlichen Grundsätzen wie das Rechnen in $\mathbb{Z}$[33], nämlich

Proposition 6.12 *Es seien $a, b, c \in \mathbb{Z}_m$, $1 = [1]_m$ und $0 = [0]_m$. Dann gelten:*

(i) $a +_m b \in \mathbb{Z}_m$.

(ii) $a +_m b = b +_m a$.

(iii) $(a +_m b) +_m c = a +_m (b +_m c)$.

(iv) $a +_m 0 = a$.

(v) *Jedes Element aus $\mathbb{Z}_m$ lässt sich als endliche Summe von 1 darstellen. Ferner ist jede m-fache Summe eines beliebigen Elements gleich $0 \in \mathbb{Z}_m$.*

Mit anderen Worten: $(\mathbb{Z}_m, +_m)$ ist eine zyklische Gruppe der Ordnung m.

Wir können allerdings auch noch mehr aussagen:

Proposition 6.13 *Mit den bekannten Verknüpfungsdefinitionen ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring.*

Die eine Restklasse erzeugenden Elemente werden auch als *Repräsentanten* der Restklasse bezeichnet. Offensichtlich bilden die Zahlen $0, 1, \ldots, m-1$ ein volles *Repräsentantensystem*.

Im Folgenden werden wir die Indizes bei den Verknüpfungen weglassen.

Hinweis: Manchmal ist es günstiger, anstelle der Klassen mit diesen ausgezeichneten Repräsentanten zu rechnen. Für die *Einfachheit der Objekte* (z.B. die Zahlen 0 bis $m-1$) muss man dann mit einer *nicht mehr so glatten Verknüpfungsvorschrift* bezahlen (z.B. Fallunterscheidungen). Da das Rechnen mit den Repräsentanten im Falle $m = 12$ dem Rechnen auf der Uhr entspricht, ist in der didaktischen Literatur auch von der so genannten *Uhrenarithmetik* die Rede. Mathematisch sind beide Betrachtungsweisen gleichwertig. Wir werden daher zwischen beiden möglichen Repräsentationsformen hin- und her schalten.

[32] Hier ist zu beachten, dass wir die Bezeichnung $\mathbb{Z}$ eigentlich schon vergeben haben, nämlich für die einer zyklischer Gruppe der Ordnung m. Diese ist aber bis auf Isomorphie einzig - und man überlegt sich schnell, dass die hier diskutierte Restklassenaddition genau dieses Merkmal aufweist.

[33] M.a.W.: Jedes Element $a \in \mathbb{Z}_m$ ist eine Klasse $[x]_m$ für ein geeignetes $x \in \mathbb{Z}$.

6.4.2 Invertierbare Elemente

Definition 6.14 *Ein Element $r \in \mathbb{Z}_m$ heißt* invertierbar*, falls es ein $x \in \mathbb{Z}_m$ mit $rx = 1 \in \mathbb{Z}_m$ gibt. Man bezeichnet auch x als das* Inverse *von r, und wir schreiben $x = r^{-1}$. Für die Menge der invertierbaren Elemente von $\mathbb{Z}_m$ schreiben wir $U(\mathbb{Z}_m)$. Die Elemente von $U(\mathbb{Z}_m)$ werden auch* Einheiten *von $\mathbb{Z}_m$ genannt.*

Der folgende Satz kennzeichnet die invertierbaren Elemente in $\mathbb{Z}_m$ durch Eigenschaften ihrer Repräsentanten.

Proposition 6.15 *Das Element $r \in \mathbb{Z}_m$ ist genau dann invertierbar, wenn r, m als Elemente von $\mathbb{Z}$ relativ prim sind, d.h. $ggT(r, m) = 1$.*

Beweis: Zunächst rechtfertigt man die folgende Aussage:

$$\mathrm{ggT}(r, m) = 1 \Longleftrightarrow \mathrm{ggT}(r + km, m) = 1 \text{ für beliebiges } k \in \mathbb{N}.$$

Es seien r, m relativ prim. Dann gibt es $x, y \in \mathbb{Z}$ mit $xr + ym = 1$, was $[x]_m \cdot [r]_m = [1]_m$ nach sich zieht, also ist $[x]_m$ invertierbar in $\mathbb{Z}_m$.

Sei umgekehrt $[x]_m[r]_m = 1$, also $rx = 1 - km$ für ein $k \in \mathbb{Z}$. Dann ist $rx + km = 1$, also ist der $\mathrm{ggT}(r, m)$ ein Teiler von 1, was die Behauptung beweist. ∎

Wir erinnern an die Definition der Euler'schen ϕ-Funktion:

$$\phi(m) = |\{x \in \mathbb{N} \mid \mathrm{ggT}(m, x) = 1\}|.$$

Sie bestimmt offenbar die Anzahl der invertierbaren Elemente von $\mathbb{Z}$, d.h. es gibt genau $\phi(m)$ verschiedene Einheiten in $\mathbb{Z}_m$. Die nächste Aussage ist, wenn auch elementar, eine klassische Aussage der elementaren Zahlentheorie, die jedoch auch als gruppentheoretische Aussage verstanden werden kann.

Offensichtlich ist mit zwei Elementen aus $U(\mathbb{Z}_m)$ auch das Produkt in $U(\mathbb{Z}_m)$; ist ferner $x \in U(\mathbb{Z}_m)$, so auch das Element $x^{-1} \in U(\mathbb{Z}_m)$. Setzt man

$$yU(\mathbb{Z}_m) = \{z \in \mathbb{Z}_m \mid z = yx \text{ für ein } x \in U(\mathbb{Z}_m)\},$$

so ergibt sich für $y \in U(\mathbb{Z}_m)$ über die genannten Beobachtungen $yU(\mathbb{Z}_m) = U(\mathbb{Z}_m)$.

Wir halten fest:

Lemma 6.16 *$(U(\mathbb{Z}_m), \cdot)$ ist eine abelsche Gruppe mit $\phi(m)$ Elementen.*

Korollar 6.17 *Ist $y \in \mathbb{Z}_m$ invertierbar, so gilt in $\mathbb{Z}_m$: $y^{\phi(m)} = 1$.*

Beweis: Es sei u das Produkt aller Elemente aus $U(\mathbb{Z}_m)$, etwa $u = x_1 x_2 \cdots x_k$, wobei $k = \phi(m)$ gilt. Nun ist $yU(\mathbb{Z}_m) = U(\mathbb{Z}_m)$, also sind die Mengen $\{x_1, \ldots, x_k\} = \{yx_1, \ldots, yx_k\}$ gleich. Auf der anderen Seite ist

$$\begin{aligned} u = x_1 x_2 \cdots x_k &= (yx_1)(yx_2) \cdots (yx_k) \\ &= y^k u, \end{aligned}$$

woraus die Behauptung folgt. ∎

Man beachte, dass eine zu (6.17) gleichwertige Darstellung lautet:

$$\mathrm{ggT}(y, m) = 1 \Longrightarrow y^{\phi(m)} \equiv 1 \pmod{m}. \tag{62}$$

Die Aussage (62) ist in der Literatur auch als *Euler'scher Satz* bekannt. Im Falle dass $m = p$ prim ist, spricht man die nächste Aussage als *kleinen Fermat'schen Satz* an:

$$p \not| y \Longrightarrow y^{p-1} \equiv 1 \pmod{p}. \tag{63}$$

Unter besonderen Zusatzeigenschaften lassen sich zyklische Gruppen weiter zerlegen. Dazu benötigen wir eine weitere Begriffsbildung, die im Prinzip aus der Linearen Algebra bekannt ist.

Definition 6.18 *Es seien $(A, *_1)$, $(B, *_2)$ Gruppen. Unter dem direkten Produkt der Gruppen A und B versteht man das kartesische Produkt $A \times B$ versehen mit der Verknüpfung $* = (*_1, *_2)$.*

Es bedarf keiner großen Überlegungen, dass $(A \times B, *)$ wiederum eine Gruppe ist. So liegt es nun nahe, direkte Produkte von zyklischen Gruppen zu bilden. Wir beschreiten den umgekehrten Weg und überlegen uns, wann zyklische Gruppen wiederum direkte Produkte von kleineren zyklischen Gruppen sind. Dass dies nicht immer der Fall ist, zeigt das Beispiel der beiden nicht isomorphen Gruppen der Ordnung 4, nämlich $\mathbb{Z}_4$ resp. $\mathbb{Z}_2 \times \mathbb{Z}_2$ (Klein'sche Vierergruppe).

Proposition 6.19 *Es seien $m, n \in \mathbb{N}$ relativ prim. Dann gilt*

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}.$$

Beweis: Es seien x, y die jeweiligen Erzeuger von $\mathbb{Z}_m$ resp. $\mathbb{Z}_n$, deren Ordnungen relativ prim sind. Sei nun $z = (x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Seine Ordnung sei r. Dann ist wegen $z^r = (x^r, y^r) = (1, 1)$ die Zahl r ein Vielfaches von m und n und zwar aus Definitionsgründen das kleinste gemeinsame Vielfache dieser Zahlen. Andererseits folgt

$$r = \mathrm{kgV}(m, n) = \frac{mn}{\mathrm{ggT}(m, n)} = mn,$$

da m, n relativ prim sind. Da nun $\mathbb{Z}_m \times \mathbb{Z}_n$ insgesamt mn Elemente besitzt, und es ein Element z der Ordnung mn enthält, folgt aus Anzahlgründen, dass $\mathbb{Z}_m \times \mathbb{Z}_n$ isomorph zu $\mathbb{Z}_{mn}$ sein muss. ∎

6.5 Definierende Relationen

Die Darstellungen der zyklischen Gruppen in dieser Form sind die einfachsten Beispiele für eine Repräsentation einer Gruppe über *definierende Relationen* und *Erzeuger*.

Allgemeiner: wird eine Gruppe G durch eine Menge S erzeugt, die eine Menge von Relationen $R_1, R_2, \ldots R_m$ genügen, wobei R_i eine Gleichung in den Elementen $S \cup \{e\}$ ist, dann sprechen wir von einer *Präsentation* von G und schreiben

$$G = \langle S \mid R_1, R_2, \ldots R_m \rangle.$$

Beispielsweise lässt sich die Diedergruppe $\mathbb{D}_n$ durch

$$\langle r, f \mid r^n = 1,\ f^2 = 1,\ rf = fr^{-1} \rangle$$

repräsentieren.

Dieses Prinzip lässt sich auch modifizieren. Betrachtet man eine Menge S, deren Elemente wir als *Alphabet* resp. *Buchstaben* bezeichnen wollen, so sollen zulässige Wörter als Buchstabenfolgen (einschließlich des leeren Wortes) verstanden werden, wobei wir beliebige ganzzahlige Exponenten (an jedem Buchstaben) zulassen. Zwei Wörter verknüpft man, in dem man sie hintereinander schreibt.

Sind überdies Relationen $R_1, R_2, \ldots, R_m$ vorgegeben, so bewirken diese Relationen mögliche Verkürzungen der Wörter. Auf diese Weise lässt sich eine Gruppe konstruieren. Bestehen zwischen den Buchstaben nur triviale Relationen, so bezeichnet man die dabei entstehende Gruppe als *freie Gruppe* mit den Erzeugern S. Mit anderen Worten: $(\mathbb{Z}, +) = (C_\infty, \cdot)$ ist somit die freie Gruppe mit einem Erzeuger.

Beispiel 6.20 (i) *Die Diedergruppen $\mathbb{D}_n$ haben die folgende Darstellung:*

$$\mathbb{D}_n = < r, f \,|\, r^n = 1, f^2 = 1, rfr^{-1} = f > .$$

(ii) *Die (unendliche) Diedergruppe $\mathbb{D}_\infty$ wird definiert durch*

$$\mathbb{D}_\infty = < r, f \,|\, f^2 = 1, rfr^{-1} = f >;$$

sie ist universelles Element in der Klasse der Diedergruppen.

(iii) *Die achtelementige sog. Quarternionengruppe*

$$Q_4 =< r, a \,|\, r^2 = a^2 = (ra)^2, a^4 = 1 >$$

Sie ist unter den nichtkommutativen Gruppen die kleinste Gruppe, deren sämtliche Untergruppen Normalteiler sind. Darüberhinaus sind alle echten Untergruppen von Q_4 abelsch.

6.6 Untergruppen

Bereits oben hatten wir die Definition einer Untergruppe angegeben. In der nächsten Definition legen wir einige weiterführende Begriffsbildungen fest.

Definition 6.21 *Es sei $(G, \cdot)$ eine Gruppe und $H \leq G$ eine Untergruppe.*

(i) *Unter dem* Zentrum *einer Gruppe G, in Zeichen: $Z(G)$, verstehen wir die Menge $\{z \in G \mid zg = gz$ für alle $g \in G\}$.*

(ii) *Die Menge $Hg = \{x \mid \exists h \in H : x = hg\}$ heißt* Linksnebenklasse[34] *von g bezüglich H. Analog definiert man eine Rechtsnebenklasse.*

(iii) *Eine Untergruppe $H \leq G$, deren Linksnebenklassen jeweils in einer Rechtsnebenklasse enthalten sind, heißt* Normalteiler*, in Zeichen: $H \triangleleft G$.*

Offensichtlich ist das Zentrum einer Gruppe wieder eine Untergruppe, wie man leicht nachrechnet.

Beispiel 6.22 *Im Folgenden wollen wir einige Begriffsbildungen an der Diedergruppe $\mathbb{D}_4$ verdeutlichen. Diese Diedergruppe genügt den Relationen*

$$\mathbb{D}_4 = \langle r, f | r^4 = 1 = f^2,\ rf = fr^3 \rangle.$$

(i) *Das Zentrum $Z(G)$ ergibt sich als die von r^2 erzeugte Untergruppe P der Ordnung 2.*

(ii) *Betrachtet man die von f erzeugte Untergruppe $T = \{1, f\}$, so rechnet man nach, dass die von dem Element r erzeugten Links- resp. Rechtsnebenklassen nicht übereinstimmen.*

(iii) *Natürlich ist $Z(G)$ ein Normalteiler; desgleichen auch $\{1, r, r^2, r^3\}$.*

Offensichtlich ist das Zentrum einer Gruppe wieder eine Untergruppe, wie man leicht nachrechnet.

Beachte, dass je zwei verschiedene Nebenklassen disjunkt sein müssen. Schließlich gilt:

$$aH = bH \Longleftrightarrow b^{-1}a \in H.$$

Ferner haben alle (endlichen) Nebenklassen gleich viele Elemente. Bezeichnet man die Anzahl der Linksnebenklassen als *Index* der Untergruppe H, in Zeichen: $[G : H]$, so gilt offenbar die folgende Identität:

$$[G : 1] = [G : H][H : 1].$$

Man beachte, dass $[G : 1] = |G|$ resp. $[H : 1] = |H|$ nichts anderes als die Gruppenordnungen von G bzw. H sind. Die dahinter stehende elementare Aussage wird vielfach als *Satz von Lagrange*[35] bezeichnet und liefert ein notwendiges Kriterium für die Existenz von Untergruppen. Dieses Kriterium ist keinesfalls hinreichend. Es gibt Gruppen, wobei die Gruppenordnung Teiler enthält, die nicht als Untergruppenordnung auftreten.

[34] Die Notation, was man unter einer Links- resp. Rechtsnebenklasse versteht, ist nicht immer einheitlich. Wir orientieren uns an dem in Ringtheorie relativ unstrittigen Begriff von Links- resp. Rechtsidealen.

[35] Joseph Louis Lagrange; franzsischer Mathematiker (1736 - 1813); Stichworte zu seinem mathematischen Werk: analytische Mechanik, Wahrscheinlichkeitsrechnung, Numerik (Lagrange-Interpolationsformel, Analysis (Lagrange-Restglied).

Proposition 6.23 *Es sei G Gruppe und $|G| = n$, $H \leq G$ eine Untergruppe mit $|H| = m$. Dann ist m ein Teiler von n.*

Beweis: Die Untergruppe H induziert eine Partition auf der Gruppe G, wobei sämtliche Komponenten gleichmächtig sind. Der Rest folgt aus der Endlichkeit. ∎

Da jedes Element g einer endlichen Gruppe eine zyklische Gruppe erzeugt, folgt mit Proposition 6.23 sofort:

Korollar 6.24 *Es sei G eine Gruppe mit $|G| = n$ und $g \in G$. Dann gelten:*

(i) *Die Ordnung von g teilt n.*

(ii) $g^n = 1$.

Das Korollar zeigt, dass die *Ordnung eines Elementes g* nichts anderes ist als die *Gruppenordnung* der von g erzeugten Untergruppe. Wir verweisen auf eine elementare Konsequenz:

Lemma 6.25 *Eine Gruppe G von Primzahlordnung p ist zyklisch, d.h. $(G, \cdot) \cong (\mathbb{Z}_p, +)$.*

Die folgende Charakterisierung für *Normalteiler* lässt sich schnell gewinnen:

Lemma 6.26 *Es sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann sind die folgenden Aussagen äquivalent:*

(a) $gH = Hg$ *für alle* $g \in G$.

(b) $gHg^{-1} \subseteq H$ *für alle* $g \in G$.

(c) $gHg^{-1} = H$ *für alle* $g \in G$.

Beweis: (a) $\Rightarrow$ (b) ist offensichtlich.

(b) $\Rightarrow$ (c) Es bleibt nachzuweisen: $H \subseteq gHg^{-1}$. Sei $x \in H$, also $x = g(g^{-1}xg)g^{-1}$, was wegen $g^{-1}xg \in H$ die Behauptung beweist.

(c) $\Rightarrow$ (a) ist offensichtlich. ∎

Die nächste Aussage zeigt die zentrale Bedeutung von *Normalteilern* auf.

Lemma 6.27 *Es sei $\varphi : G \longrightarrow G'$ ein Homomorphismus der Gruppen G und G'; dabei e' das neutrale Element von G'. Dann ist*

$$Kern(\varphi) = \{g \in G \mid \varphi(g) = e'\}$$

ein Normalteiler von G. Diese Menge heißt Kern *von φ.*

Beweis: straightforward ∎

Wir erwähnen an dieser Stelle ein später oft benutztes elementares Ergebnis.

Lemma 6.28 *Es sei $\varphi : G \longrightarrow G'$ ein Homomorphismus der Gruppen G und G' und e das neutrale Element von G. Dann sind die folgenden Aussagen äquivalent:*

(a) φ *ist injektiv.*

(b) $\mathrm{Kern}(\varphi) = \{e\}$.

Beweis: (a) $\Rightarrow$ (b) Sei e' das neutrale Element von G' und $g \in \mathrm{Kern}(\varphi)$, also $\varphi(g) = e'$. Dann folgt wegen $\varphi(e) = e'$ und aus der Injektivität $g = e$.

(b) $\Rightarrow$ (a) Es sei $\varphi(g_1) = \varphi(g_2)$, also $\varphi(g_1 g_2^{-1}) = e'$ und somit $g_1 g_2^{-1} \in \mathrm{Kern}(\varphi) = \{e\}$. Folglich ist $g_1 g_2^{-1} = e$, d. h. $g_1 = g_2$ und der Homomorphismus φ ist injektiv. ∎

Es erhebt sich die Frage, ob Normalteiler immer etwas mit Homomorphismen zu tun haben. Darauf werden wir im übernächsten Abschnitt eine Antwort geben.

6.7 Eine ergänzende Charakterisierung von zyklischen Gruppen

Im nächsten Satz wird erneut die Bedeutung der Euler'schen ϕ-Funktion offenbar und eine kleine Anwendung der Möbius-Inversionsformel aufgezeigt.

Satz 6.29 *Es sei G eine endliche Gruppe der Ordnung $n \geq 2$. Dann sind die folgenden Aussagen äquivalent:*

(a) *G ist eine zyklische Gruppe.*

(b) *Für jeden Teiler d der Gruppenordnung n von G ist die Zahl der Elemente $x \in G$ mit $x^d = 1$ gleich d.*

(c) *Für jeden Teiler d der Gruppenordnung n von G ist die Zahl der Elemente $x \in G$, die die Ordnung d haben, gleich $\phi(d)$.*

Beweis: (a) $\Rightarrow$ (b) Es sei G eine zyklische Gruppe der Ordnung n, die vom Element g erzeugt werde. Sei nun d ein Teiler von n, etwa $dk = n$ für eine natürliche Zahl k. Die Elemente

$$1, g^k, g^{2k}, \ldots, g^{(d-1)k}$$

sind, weil die jeweiligen Exponenten $< n$ erfüllen, sämtlich verschieden, und jedes Element erfüllt die Gleichung $x^d = 1$, denn

$$(g^{ik})^d = (g^{kd})^i = (g^n)^i = 1^i = 1.$$

Somit haben wir bereits d Elemente gefunden, die die Gleichung $x^d = 1$ erfüllen.

Es bleibt zu zeigen, dass es keine andere Lösungen gibt. Sei y ein Element von G mit $y^d = 1$. Da G von g erzeugt ist, gilt $y = g^f$ für ein $f \geq 0$, also

$$g^{fd} = (g^f)^d = y^d = 1.$$

Die Ordnung von g ist n, und wegen Lemma 6.5 muss fd ein Vielfaches von n sein, etwa ln. Daher gilt

$$fd = ln = l(dk),$$

also $f = lk$ und $y = g^f = g^{lk}$, weswegen y von dem ursprünglich betrachteten Typ ist.

(b) $\Rightarrow$ (c) Wir nehmen an, dass (b) gilt, also für jeden Teiler d der Gruppenordnung $|G| = n$ gibt es genau d Elemente $x \in G$ mit $x^d = 1$. Ist x ein Element von G mit der Ordnung $|x| = c$. Genau dann wenn c ein Teiler von d ist, gilt $x^d = 1$ (verwende Lemma 6.5). Mit $\alpha(c)$ bezeichnen wir die Anzahl der Elemente in G mit der Ordnung c. Nach Voraussetzung muss daher gelten:

$$d = \sum_{c|d} \alpha(c).$$

Diese Formel erinnert uns an ein Ergebnis im Zusammenhang mit der Euler'schen ϕ-Funktion, nämlich (vgl. Proposition 1.17):

$$d = \sum_{c|d} \phi(c).$$

Um $\phi(d) = \alpha(d)$ zu rechtfertigen, was unsere Aussage beweisen würde, benutzen wir die Möbius-Inversionsformel (vgl. 3.11) und es ergibt sich

$$\alpha(d) = \sum_{c|d} \mu(c)\frac{d}{c} \quad \text{resp.} \quad \phi(d) = \sum_{c|d} \mu(c)\frac{d}{c},$$

woraus die Behauptung $\alpha(d) = \phi(d)$ folgt.

(c) $\Rightarrow$ (a) Wenn wir von (c) ausgehen, wissen wir insbesondere, dass die Anzahl der Elemente mit Ordnung n gleich $\phi(n)$ ist. Nun ist $\phi(n) \geq 1$, da 1 immer relativ prim zu n ist. Folglich enthält G wenigstens ein Element der Ordnung n. Aus $|G| = n$ folgt, dass G zyklisch ist. ∎

Wir können nun dieses Ergebnis benutzen, um alle Untergruppen H einer zyklischen Gruppe G der Ordnung n zu bestimmen. Nach der Aussage des Satzes von Lagrange wissen wir, dass $|H| = d$ für einen Teiler d von n gilt. Mit Korollar 6.24(ii) genügt jedes der d Elemente der Gleichung $x^d = 1$. Wir haben aber gezeigt, dass G genau d Elemente enthält, die $x^d = 1$ erfüllen. Also konstituieren diese Elemente gerade die Untergruppe H. Wir haben damit gezeigt:

Korollar 6.30 *Eine zyklische Gruppe der Ordnung n hat für jeden Teiler d von n genau eine Untergruppe der Ordnung d, und diese Untergruppen sind wieder zyklisch.*

6.8 Faktorgruppen und Homomorphiesatz

Wir verweisen insbesondere die Darstellung in [8].

Satz 6.31 *Sei G eine Gruppe, N ein Normalteiler von G, G/N die Menge der rechten Nebenklassen von G bzgl. N und $\rho : G \longrightarrow G/N$, $a \mapsto aN$. Dann gibt es genau eine (innere) Verknüpfung $*$ von G/N, so dass gilt:*

(i) *$(G/N, *)$ ist eine Gruppe.*

(ii) *Die Abbildung ρ ist ein Homomorphismus von G in $(G/N, *)$.*

ρ ist dann sogar ein Epimorphismus, es gilt $Kern(\rho) = N$, N ist das neutrale Element von $(G/N, *)$ und $a^{-1}N$ das Inverse von aN.

Beweis: Dass die Verknüpfung eindeutig ist, lässt sich wie folgt einsehen: Ist $(G/N, *)$ eine Gruppe und ρ ein Homomorphismus von G in $(G/N, *)$, so gilt für alle $a, b \in G$:

$$aN * bN = \rho(a) * \rho(b) = \rho(ab) = (ab)N.$$

Es gibt eine Verknüpfung $*$ von G/N mit $aN * bN = (ab)N$ für alle $a, b \in G$:

Dazu ist zu zeigen, dass aus $a_1N = aN$ und $b_1N = bN$ stets $(a_1b_1)N = (ab)N$, d.h. $(a_1b_1)^{-1}(ab) \in N$ folgt.

Wegen $a_1N = aN$ gibt es ein $n \in N$ mit $a = a_1n$ und wegen $b_1N = bN = Nb$ ein $m \in N$ mit $nb = b_1m$. Damit erhält man $(a_1b_1)^{-1}(ab) = b_1^{-1}a_1^{-1}ab = b_1^{-1}a_1^{-1}a_1nb = b_1^{-1}b_1m = m \in N$.

Dass $(G/N, *)$ eine Gruppe mit neutralem Element $N = eN$ ist (e sei das neutrale Element von G) und $a^{-1}N$ das Inverse von aN ist, folgt unmittelbar aus der Definition der Verknüpfung. Ebenso folgt, dass ρ ein Epimorphismus ist. Ferner gilt: $a \in \text{Kern}(\rho) \Leftrightarrow aN = N \Leftrightarrow a \in N$, also $\text{Kern}(\rho) = N$. ∎

Definition 6.32 *Sei G eine Gruppe und N ein Normalteiler von G. Die im vorangegangenen Satz konstruierte Gruppe G/N heißt die* Faktorgruppe *von G* modulo *N. Der Epimorphismus $\rho : G \longrightarrow G/N$, $a \mapsto aN$, heißt der* kanonische Epimorphismus *von G auf G/N.*

Sei G eine Gruppe und H eine Teilmenge von G. Wir bemerken: Dann ist H genau dann Normalteiler von G, wenn es eine Gruppe G' und einen Homomorphismus $\varphi : G \longrightarrow G'$ gibt mit $\text{Kern}(\varphi) = H$. Dass der Kern eines Gruppenhomomorphismus ein Normalteiler ist, wurde schon oben bewiesen. Der Rest folgt unmittelbar aus Satz 6.31.

Sei $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus, N ein Normalteiler von G und $\rho : G \longrightarrow G/N$ der kanonische Epimorphismus. Es soll zunächst untersucht werden, wann es einen Gruppenhomomorphismus $\overline{\varphi} : G/N \longrightarrow G'$ gibt, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \rho\downarrow & \nearrow & \overline{\varphi} \\ G/N & & \end{array} .$$

Notwendig für die Existenz eines derartigen Homomorphismus ist die Bedingung $N \subseteq \text{Kern}(\varphi)$, denn aus $\overline{\varphi} \circ \rho = \varphi$ folgt $\varphi(n) = \overline{\varphi}(\rho(n)) = \overline{\varphi}(N)$ für alle $n \in N$, so dass $\varphi(n)$ für jedes $n \in N$ gleich dem neutralen Element von G' ist. Dabei ist N das neutrale Element von G/N und $\overline{\varphi}$ ein Gruppenhomomorphismus.

Satz 6.33 *Sei $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus, N ein Normalteiler von G mit $N \subseteq Kern(\varphi)$ und $\rho : G \longrightarrow G/N$ der kanonische Epimorphismus. Dann gibt es genau einen Gruppenhomomorphismus*

$$\overline{\varphi} : G/N \longrightarrow G' \text{ mit } \quad \overline{\varphi} \circ \rho = \varphi.$$

Mit φ ist auch $\overline{\varphi}$ ein Epimorphismus, und es gilt $Kern(\overline{\varphi}) = Kern(\varphi)/N$.

Beweis: (1) Es gibt höchstens ein solches $\overline{\varphi}$, denn aus $\overline{\varphi} \circ \rho = \varphi$ folgt für jedes $a \in G : \overline{\varphi}(aN) = \overline{\varphi}(\rho(a)) = \varphi(a)$.

(2) Es gibt eine Abbildung $\overline{\varphi} : G/N \longrightarrow G'$ mit $\overline{\varphi}(aN) = \varphi(a)$ für alle $a \in G$, denn aus $bN = aN$ folgt $b^{-1}a \in N$, also $e' = \varphi(b^{-1}a) = \varphi(b)^{-1}\varphi(a)$ und daher $\varphi(b) = \varphi(a)$ wegen $N \subseteq \text{Kern}(\varphi)$ (e' sei dabei das neutrale Element von G').

(3) Die Abbildung $\overline{\varphi} : G/N \longrightarrow G'$ mit $\overline{\varphi}(aN) = \varphi(a)$ für alle $a \in G$ ist ein Gruppenhomomorphismus, denn für alle $a, b \in G$ gilt $\overline{\varphi}((aN)(bN)) = \overline{\varphi}((ab)N) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aN)\overline{\varphi}(bN)$.

(4) Sei φ surjektiv. Dann gibt es zu jedem $a' \in G'$ ein $a \in G$ mit $a' = \varphi(a) = \overline{\varphi}(\rho(a))$; $\overline{\varphi}$ ist also ebenfalls surjektiv.

(5) Für jedes $a \in G$ gilt: $aN \in \text{Kern}(\overline{\varphi}) \Leftrightarrow \varphi(a) = e' \Leftrightarrow a \in \text{Kern}(\varphi) \Leftrightarrow aN \in \text{Kern}(\varphi)/N$, denn aus $aN \in \text{Kern}(\varphi)/N$ folgt, dass es ein $b \in \text{Kern}(\varphi)$ mit $aN = bN$, also mit $ab^{-1} \in N \subseteq \text{Kern}(\varphi)$ gibt, so dass man $a \in \text{Kern}(\varphi)$ erhält. ∎

Satz 6.34 *Es sei $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus der Gruppen G und G'. Dann ist durch*

$$\overline{\varphi}(a\, Kern(\varphi)) := \varphi(a) \quad \text{für alle } a \in G$$

ein Monomorphismus

$$\overline{\varphi} : G/Kern(\varphi) \longrightarrow G'$$

erklärt. Die Gruppen $G/Kern(\varphi)$ und $\varphi(G)$ sind also isomorph.

Beweis: Dass es genau einen Gruppenhomomorphismus $\overline{\varphi}$ mit der angegebenen Eigenschaft gibt, folgt aus 6.33. Wegen 6.33 gilt auch $\text{Kern}(\overline{\varphi}) = \text{Kern}(\varphi)/\text{Kern}(\varphi) = \{\text{Kern}(\varphi)\}$. Im $\text{Kern}(\overline{\varphi})$ liegt somit lediglich das neutrale Element von $G/\text{Kern}(\varphi)$, so dass $\overline{\varphi}$ daher injektiv ist. ∎

6.9 Endliche abelsche Gruppen

Die nächste Aussage[36], die wir bis auf weiteres nur in der kommutativen Situation benötigen, bezeichnet man als *Satz von Cauchy*[37].

[36] Die folgenden Ausführungen lehnen sich an Darstellungen in [8] an.

[37] Augustin Louis Cauchy - geboren 21. August 1789 in Paris, gestorben 23. Mai 1857 in Sceaux - war ein französischer Mathematiker.

Als ein Pionier der Analysis entwickelte er die von Gottfried Wilhelm Leibniz und Sir Isaac Newton aufgestellten Grundlagen weiter und formulierte sie als Theorie, wobei er die fundamentalen Aussagen auch formal bewies. Insbesondere in der Funktionentheorie stammen viele zentrale Sätze von ihm. Seine fast 800 Publikationen decken im Großen und Ganzen die komplette Bandbreite der damaligen Mathematik ab.

Nach dem Tode Leonhard Eulers hatten viele den Eindruck, dass die Mathematik fast vollständig erforscht und keine wesentlichen Probleme mehr übrig seien. Es waren insbesondere Carl Friedrich Gauß und Cauchy, die diesen Eindruck relativieren konnten.

Stichworte zu seinem mathematischen Werk: Cauchy-Kriterium, Beiträge zur Funktionentheorie, Theorie der Differentialgleichungen, Geometrie, Algebra, Zahlentheorie und Mechanik.

Satz 6.35 *Es sei G eine endliche abelsche Gruppe und p eine Primzahl, die ein Teiler der Gruppenordnung ist. Dann gibt es ein $a \in G$ mit der Ordnung p.*

Beweis: Es sei p prim und ein Teiler von $|G|$. Es genügt zu zeigen, dass es ein $a \in G$ und ein $m \in \mathbb{N}$ gibt, so dass das Element a die Ordnung pm hat, also $pm \cdot a = 0 = p \cdot ma$, woraus sich unmittelbar ein Element der Ordnung p, nämlich $ma \in G$ ergibt. Dann hat nämlich das Element ma die Ordnung p.

Die Aussage des Satzes beweisen wir über die Ordnung von G in Abhängigkeit von der jeweiligen Primzahl p. Da eine Gruppe der Ordnung p stets isomorph zu $(\mathbb{Z}_p, +)$ ist und somit ein Element der Ordnung p besitzt, ist der Induktionsanfang also gesichert.

Es sei G eine endliche abelsche Gruppe mit einer Ordnung $> p$ und die Aussage richtig für jede Gruppe, deren Ordnung kleiner als die von G ist. Es sei p eine Primzahl, die $|G|$ teilt, und $b \neq 1$ ein Element in G. Ist die Gruppenordnung k von b durch p teilbar, so sind wir aufgrund unserer Vorbemerkung fertig.

Andernfalls bilden wir die von b erzeugte Untergruppe $H = \langle b \rangle$, deren Ordnung ebenfalls nicht durch p teilbar ist. Da G abelsch ist, ist $H = \langle b \rangle$ ein Normalteiler von G und auch die Gruppe G/H ist abelsch. Wegen $p \nmid |H|$ ist p ein Teiler der Ordnung der Faktorgruppe G/H, deren Ordnung kleiner als die von G ist. Insofern gibt es eine Nebenklasse $c + H$, die als Gruppenelement von G/H eine durch p teilbare Ordnung hat. Ist daher $\rho : G \to G/H$ der kanonische Epimorphismus und wählt man $a \in G$, dass $\rho(a) = c + H$ gilt, so ist $pa \in H$, also $k(pa) = 0$, das heißt ka ist das gesuchte Element. ∎

Damit ergibt sich die nächste Aussage, die uns im Spezialfall von zyklischen Gruppen (vgl. Lemma 6.19) schon begegnet ist:

Lemma 6.36 *Es sei G eine endliche abelsche Gruppe. Gilt $|\,G\,| = mn$ mit teilerfremden natürlichen Zahlen m und n, so sind*

$$G_m := \{a \in G \mid ma = 0\} \quad \textit{und} \quad G_n := \{a \in G \mid na = 0\}$$

Untergruppen von G und es gilt:

(i) $G \cong G_m \times G_n$.

(ii) $|\,G_m\,| = m$, $|\,G_n\,| = n$.

Beweis: (i) Nach dem Satz von Cauchy gibt es in G zu jedem Primteiler, nämlich m resp. n, Elemente, die diese Ordnung aufweisen. Somit sind die Mengen G_m und G_n nicht leer. Da G abelsch ist, sind G_m und G_n Untergruppen von G. Die Abgeschlossenheit hinsichtlich der Addition ist sofort evident. Was die Existenz eines inversen Elements von a mit $ma = 0$ anbetrifft, so beachte: $a + (m-1)a = 0$, folglich ist $(m-1)a$ das Inverse des Elementes a, mithin ergibt sich $m(m-1)a = (m-1)ma = (m-1)0 = 0$.

Außerdem gilt $G_m \cap G_n = \{0\}$, denn aus $ma = na = 0$ folgt $0 = (km + ln)a = 1a = a$, weil m und n relativ zu einander sind.

Ein entsprechendes Argument wenden wir nochmals an: Sei also $1 = km + ln$ und es ergibt sich

$$1 \cdot G = (km + ln) \cdot G = km \cdot G + ln \cdot G \subseteq mG + nG \subseteq G_n + G_m \subseteq G.$$

Damit ist

$$G = G_m \oplus G_n = \{x + y \mid x \in G_m,\, y \in G_n\}$$

nachgewiesen.

Andererseits können keine zwei verschiedenen Summenbildungen auf ein und dasselbe Element von G hinauslaufen. Ein Isomorphismus zwischen $G_m + G_n$ und $G_m \times G_n$ liegt auf der Hand, mit

anderen Worten: die interne direkte Summe $G_m + G_n$ ist isomorph zum äußeren direkten Produkt $G_m \times G_n$ und insgesamt gleich G.

(ii) Aus Anzahlgründen folgt die Behauptung. ∎

Wir formulieren nun den *Hauptsatz für endliche abelsche Gruppen*, wobei wir die Gruppe (weiterhin) additiv repräsentieren wollen.

Satz 6.37 *Es sei G eine endliche abelsche Gruppe. Für jeden Primteiler p von $|\,G\,|$ bezeichne*

$$S(p) = \{a \in G \mid \exists\, l \in \mathbb{N} : p^l a = 0\}.$$

Dann gelten:

(i) *$S(p)$ ist eine Untergruppe von G.*

(ii) *Diese Untergruppe hat p^k Elemente, falls p^k die maximale Primzahlpotenz ist, die $|\,G\,|$ teilt.*

(iii) *Sind $p_1, p_2, \ldots, p_r$ die verschiedenen Primfaktoren von $|\,G\,|$, so gilt:*

$$G \cong S(p_1) \times \ldots \times S(p_r).$$

Wir halten folgende Begriffsbildung separat fest:

Definition 6.38 *Eine Gruppe heißt* p-Gruppe*, wenn die Elementeordnungen Potenzen einer Primzahl p sind.*

Der obige Satz besagt, dass $S(p)$ eine p-Gruppe ist. Nach dem Satz von Cauchy hat $S(p)$ eine Primzahlpotenzordnung. $S(p)$ ist nach (ii) überdies eine maximale p-Gruppe.

Beweis: (i) Offensichtlich ist $S(p)$ nicht leer, ja nach Lemma 6.35 auch nicht trivial. Mehr noch, $S(p)$ ist eine Untergruppe, denn $p^r x = p^s y = 0$ und $r \geq s$ impliziert $p^r(x - y) = 0$. Also folgt aus $x, y \in S(p)$ stets $x - y \in S(p)$.

(ii) Um die zweite Aussage zu beweisen, nehmen wir an, dass $S(p)$ weniger als p^k Elemente besitzt. Die Ordnung der Faktorgruppe $G/S(p)$ ist daher durch p teilbar, $G/S(p)$ enthält also ein Element $x + S(p)$ der Ordnung p. Es ergibt sich: $px \in S(p)$, d.h. $p^i x = 0$, was $x \in S(p)$ nach sich zieht. Widerspruch.

(iii) Wir führen den Beweis über vollständige Induktion nach r. Für $r = 1$ ist alles klar. Sei also $r > 1$ und $|\,G\,| = p_1^{k_1} \cdots p_r^{k_r}$. Da $m = p_1^{k_1} \ldots p_{r-1}^{k_{r-1}}$ und $n = p_r^{k_r}$ teilerfremd sind, ist $G \simeq G_m \times G_n$ nach Lemma 6.36, wobei $G_m = \{a \in G \mid ma = 0\}$ und $G_n = \{a \in G \mid na = 0\}$ gesetzt war. Wir bezeichnen mit H wechselweise G_m oder G_n. Sei nun p ein Primfaktor von $|H|$ und $a \in G$ mit $p^l = 0$, dann ist nach Definition von G_m resp. G_n offensichtlich $a \in H$, wir halten $|\,H\,|$

$$S(p) = \{a \in G \mid \exists l \in \mathbb{N} : p^l a = 0\} \subseteq H.$$

Die Induktionsannahme liefert

$$G_m = S(p_1) \times \cdots \times S(p_{r-1}) \quad \text{und} \quad G_n = S(p_r),$$

und hieraus folgt die Behauptung. ∎

Will man alle endlichen abelschen Gruppen klassifizieren, so genügt es nach Satz 6.37, dies für alle endlichen abelschen p-Gruppen zu tun. Dies geschieht durch den folgenden

Satz 6.39 *Sei G eine endliche abelsche p-Gruppe. Dann gibt es eindeutig bestimmte natürliche Zahlen*

$$1 \leq l_1 \leq l_2 \leq \cdots \leq l_n$$

und zyklische p-Untergruppen $G_1, \ldots, G_n$ von G mit $|\,G_i\,| = p^{l_i}$ für $i = 1, \ldots, n$, so dass

$$G \cong G_1 \times \ldots \times G_n.$$

Der Beweis ist elementar und technisch, überdies liefert er uns keine neuen Einsichten, so dass in den einschlägigen Fachtexten nachgelesen werden kann.

Es sei p^n die Ordnung einer p-Gruppe $S(p)$. Hier kommen also die (ungeordneten) Zahlpartitionen des Exponenten n ins Spiel.

Beispiele 6.40 *Gesucht sind alle abelsche Gruppen der Ordnung* $72 = 2^3 \cdot 3^3$. *Für* $S(2)$ *ergeben sich folgende Alternativen:* $S(2) \cong \mathbb{Z}_8$ *oder* $S(2) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ *oder* $S(2) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$*; hingegen gilt für* $S(3) \cong \mathbb{Z}_9$ *resp.* $S(3) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. *Die jeweiligen Alternativen lassen sich miteinander kombinieren.*

7 Permutationsgruppen

7.1 G-Mengen

Wie vorher bezeichnet $\mathbb{N}_n$ die Menge der n ersten natürlichen Zahlen. Auf $\mathbb{N}_n$ operiert die Menge S_n aller Permutationen in natürlicher Weise. Diesen Ansatz werden wir jetzt verallgemeinern, was uns zum Begriff der G-Menge[38] führt.

Dass nicht notwendigerweise immer die volle Permutationsgruppe von Interesse ist, zeigt das nachfolgende Beispiel; zunächst jedoch eine weitere Definition:

Definition 7.1 *Unter einem* Graphen $\mathcal{G}$ *verstehen wir eine endliche Menge V, den so genannten Ecken (vertices) und einer Menge E von 2-Teilmengen von V, den Kanten (edges) von $\mathcal{G}$. Wir schreiben: $\mathcal{G} = (V, E)$.*

Von Interesse sind nun Gruppen G, die als Automorphismen auf dem Graphen operieren, mit anderen Worten: die *Automorphismen-Gruppe* von $\mathcal{G}$.

Beispiel 7.2 Es sei $\mathcal{G}$ ein Quadrat, dessen Ecken wir im Uhrzeigersinn mit $1, 2, 3, 4$ bezeichnen. Man erhält insgesamt acht Permutationen:

Identität	id
Drehung im Uhrzeigersinn um 90^0	(1234)
Drehung im Uhrzeigersinn um 180^0	(13)(24)
Drehung im Uhrzeigersinn um 270^0	(1432)
Spiegelung an der Diagonalen 13	(24)
Spiegelung an der Diagonalen 24	(13)
Spiegelung an der Mittelsenkrechten von 12	(12)(34)
Spiegelung an der Mittelsenkrechten von 14	(14)(23)

Das legt folgende Definition nahe:

Definition 7.3 *Es sei G eine Gruppe und X eine nichtleere Menge. Die Menge X heißt eine G-Menge, falls eine Abbildung $\kappa : G \times X \longrightarrow X$ existiert (das Bild von $\kappa(g, x)$ schreiben wir als gx), so dass für alle $g_1, g_2 \in G$, $x \in X$ gilt:*

$$(g_1 g_2)x = g_1(g_2 x) \quad \text{und} \quad ex = x.$$

Abkürzend setzen wir: $(G, X; \kappa)$

Wir merken an, dass die Begriffsbildung einer G-Menge vielfach schon unter der schwächeren Voraussetzung, dass G ein Monoid ist, tragfähig ist.

Wir sagen auch, dass G auf X *operiert*. Jedes $g \in G$ induziert dann eine Abbildung $\sigma_g : X \longrightarrow X$ vermöge

$$\sigma_g(x) = gx$$

für alle $x \in X$. Überdies gilt nach Definition

$$\sigma_{g_1 g_2} = \sigma_{g_1} \sigma_{g_2}$$

für alle $g_1, g_2 \in G$. Da G als Gruppe vorausgesetzt war, existiert mit σ_a auch $\sigma_{a^{-1}}$, somit ist die Abbildung $a \mapsto \sigma_a$ ein Homomorphismus von G in die Gruppe aller Permutationen von X. Man sagt dann auch, dass G als Gruppe von Permutationen dargestellt wird. Hier liegt die Grundidee der *Darstellungstheorie*, nämlich Gruppenelemente als Homomorphismen von Vektorräumen darzustellen.

Wir verdeutlichen dieses Konzept mit mehreren Beispielen:

Beispiel 7.4 Es sei G eine Gruppe und X eine Menge.

[38] vgl. insbesondere [9], S. 19ff

(i) Wir setzen $X = G$ und $\kappa : (a, x) \mapsto axa^{-1}$. Bei der Aktion handelt es sich um das *Konjugieren*. Offensichtlich ist $(G, G; \kappa)$ eine G-Menge. Die durch Konjugieren induzierten Abbildungen σ_g sind sogar Gruppenisomorphismen von G.

(ii) Sei nun $X = \mathcal{P}(G)$ die Menge der Teilmengen von G und $A \in \mathcal{P}(G)$ eine solche Menge. Dann ist auch $aAa^{-1} \in \mathcal{P}(G)$. Ist überdies A eine Untergruppe, so ist auch aAa^{-1} wiederum eine solche. Ist A ein Normalteiler von G, so bleibt A unter allen σ_g fest.

(iii) Wir setzen wieder $X = G$ und definieren für jedes $a \in G$ die Translation $\sigma_a(x) = ax$. Dann ist $(G, G; \kappa)$ eine G-Menge. Man beachte, dass σ_a zwar eine bijektive Abbildung von X ist, nicht jedoch ein Gruppenhomomorphismus.

Sei nun X eine Menge, auf der eine Gruppe G von Permutationen operiert. Wir setzen

$$x \sim y \Longleftrightarrow gx = y \text{ für ein } g \in G.$$

Beachte, dass $\sim$ eine Äquivalenzrelation ist. Die Komponenten dieser Partition heißen *Bahnen* oder auch *Orbits*, es sind also jene Mengen, die unter der Wirkung von G nicht unterschieden werden können.

Die Mengen $Gx = \{y \in X \mid y = gx \text{ für ein } g \in G\}$ sind die von x erzeugten Orbits. Umgekehrt beschreiben wir mit

$$G(x \to y) = \{g \in G \mid gx = y\}$$

die Menge aller Gruppenelemente, die x in y überführen. Insbesondere ist im Falle $x = y$ offensichtlich $G(x \to x)$ die Menge aller Permutationen, unter denen x festbleibt.

Es stellt sich die Frage nach der Anzahl der Elemente in einem Orbit. Zuvor eine Definition:

Definition 7.5 *Es sei $(G, X; \kappa)$ eine G-Menge. Dann heißt die Menge*

$$G(x \to x) = \{g \in G \mid gx = x\}$$

auch Stabilisator *von x, kurz G_x. Gelegentlich findet man auch die Bezeichnung* Isotropiegruppe.

Offenbar ist G_x eine Untergruppe von G.

Lemma 7.6 *Es sei $(G, X; \kappa)$ eine G-Menge. Dann gelten:*

(i) *Der Stabilisator G_x ist eine Untergruppe.*

(ii) *Sei $h \in G(x \to y)$. Dann ist*

$$G(x \to y) = hG_x$$

die Rechtsnebenklasse von G_x in Bezug auf h.

Beweis: (i) ist klar.

(ii) Liegt a in der Rechtsnebenklasse hG_x, so gilt $a = hb$ für ein $b \in G_x$. Also ist

$$a(x) = hb(x) = h(x) = y$$

und daher gehört a zu der Menge $G(x \to y)$. Ist umgekehrt c in $G(x \to y)$, dann ergibt sich

$$h^{-1}c(x) = h^{-1}(y) = x,$$

d.h. $h^{-1}c = d$ ist im Stabilisator von G_x enthalten. Mit anderen Worten: $c = hd \in hG_x$. ∎

Im Falle, dass die G-Aktion auf $X = G$ das Konjugieren ist, ist $G_x = \{g \in G \mid gx = xg\}$.

Definition 7.7 *Es sei G eine Gruppe und $x \in G$. Die Menge aller Elemente g, die mit x kommutieren, heißt* Zentralisator *von x; kurz: $G_x = \{g \in G \mid gx = xg\}$. Ist $G_x = G$, so gehört das Element zum Zentrum $Z(G)$ der Gruppe, wobei wir*

$$Z(G) = \{g \in G \mid gx = xg \text{ für alle } x \in G\}$$

als Zentrum *bezeichnen.*

7.2 Genaueres über Orbits

In diesem Abschnitt soll die fundamentale Beziehung zwischen der Größe eines Orbits und der Untergruppenordnung eines Stabilisators G_x hergestellt werden.

Satz 7.8 *Es sei $(G, X; \kappa)$ eine G-Menge, wobei X als endlich vorausgesetzt wird. Ferner sei $x \in X$ beliebig. Dann gilt:*

$$|\,Gx\,| \cdot |\,G_x\,| = |\,G\,|,$$

mit anderen Worten: die Anzahl der Elemente eines Orbits entspricht dem Index des Stabilisators.

Beweis: Wir fixieren das Element x und betrachten nun

$$S = \{(g, y) \mid \exists g \in G : gx = y\}.$$

Wir werden nun auf zwei Weisen die Menge S im kartesischen Produkt $G \times X$ abzählen, indem wir die Einträgeanzahl $r_g(S)$ in den Zeilen und die Einträgeanzahl $c_y(S)$ in den Spalten benutzen. Nach Definition gibt es genau ein $y \in X$ mit $gx = y$ für jedes $g \in G$. Mit anderen Worten: in jeder Zeile steht genau ein Eintrag, also ist $r_g(S) = 1$ für jedes $g \in G$.

Die Zahl $c_y(S)$ ist die Anzahl der Gruppenelemente g mit $gx = y$, also gleich $|\,G(x \to y)\,|$. Ist also y im Orbit Gx, so gilt

$$c_y(S) = |\,G(x \to y)\,| = |\,G_x\,|,$$

ansonsten ist $c_y(S) = 0$.

Getrenntes Aufaddieren der Spalten resp. Zeilen führt zu der Gleichung

$$\sum_{y \in X} c_y(S) = \sum_{g \in G} r_g(S),$$

die wir auswerten müssen. Die rechte Seite liefert als Summe den Wert $|G|$, da ja in jeder Zeile genau einmal ein Eintrag auftritt.

Nun in den Spalten, die in der Bahn von x liegen, also Spalten, die einen Eintrag aus Gx haben, können Einträge gefunden werden. Bildet ein Gruppenelement g das Element x auf y ab, so auch alle von rechts mit G_x multiplizierten Elemente. Fazit:

$$|Gx| \cdot |G_x| = |G|.$$

■

Als Konsequenz aus Satz 7.8 ergibt sich für den Fall, dass die Aktion einer G-Menge als Konjugieren auf der Gruppe G selbst verstanden wird (vgl. Beispiel 7.2 (i)):

$$|G_x| \cdot (\text{ Zahl der Konjugierten von } x) = |\,G\,|.$$

Daraus folgt:

Korollar 7.9 *Die Zahl der Konjugierten eines Elements ist ein Teiler der Gruppenordnung.*

Wendet man die Argumentation auf das Eingangsbeispiel 7.2 an, so ergibt sich:

Beispiel 7.10 Wegen $id : 1 \to 1$ resp. $(1234) : 1 \to 2$ resp. $(13)(24) : 1 \to 3$ und $(1432) : 1 \to 4$ folgt $G1 = \{1, 2, 3, 4\}$, also ist das Orbit die gesamte Menge X und $|\,G1\,| = 4$. Der Stabilisator von 1 ist ferner $G_1 = \{\mathrm{id}, (24)\}$, und daher $|\,G1\,| \cdot |\,G_1\,| = 4 \cdot 2 = 8$, wie erwartet, da als Gruppe G die Diedergruppe $\mathbb{D}_4$ operiert.

Kennt man also die Größe einer Bahn wie auch den Stabilisator, so lässt sich die Gruppenordnung berechnen.

Wir wollen uns nun dem Problem zuwenden, die Anzahl der Bahnen unter einer Aktion einer Permutationsgruppe G auf eine Menge X zu berechnen. Jede Bahn ist eine Teilmenge von X, deren Elemente unter der Aktion ununterscheidbar sind. Wir benutzen noch folgende Abkürzung:

$$F(g) = \{x \in X \mid gx = x\}.$$

$F(g)$ ist die *Fixmenge* unter der Wirkung von $g \in G$. Der nächste Satz besagt nun, dass die Anzahl der Bahnen gleich der durchschnittlichen Größe der Fixmengen $F(g)$ ist.

Satz 7.11 *Es sei $(G, X; \kappa)$ eine endliche G-Menge. Die Zahl der Orbits von G auf X beträgt*

$$\frac{1}{|\,G\,|} \sum_{g \in G} |\,F(g)\,|.$$

Beweis: Wiederum benutzen wir die Methode, Paare eines kartesischen Produktes auf verschiedene Weise abzuzählen. Es sei

$$E = \{(g, x) \in G \times X \mid gx = x\}.$$

Dann ist die Elementezahl $r_g(E)$ einer Zeile gleich der Anzahl solcher Elemente x, die unter g festbleiben, also gleich $|\,F(g)\,|$. In der Spalte mit Eingang x stehen jene Elemente von G, die x festlassen, also $c_x(E) = |\,G_x\,|$. Mithin gilt:

$$\sum_{g \in G} |\,F(g)\,| = \sum_{x \in X} |\,G_x\,|. \tag{64}$$

Angenommen, es gibt t Orbits und z sei ein beliebiges Element aus X. Mit Satz 7.8 folgt nun unmittelbar aus $Gx = Gz$, dass die zugehörigen Stabilisatoren $|\,G_x\,|, |\,G_z\,|$ gleich sind. Folglich stehen auf der rechten Seite von (64) $|\,Gz\,|$ Terme, die gleich $|\,G_z\,|$ sind, nämlich jene, die durch jedes $x \in Gz$ aus der zugehörigen Bahn induziert werden. Der Gesamtbeitrag dieser Terme beträgt

$$|\,Gz\,| \cdot |\,G_z\,| = |\,G\,|$$

aufgrund von Satz 7.8. Mit anderen Worten: der Beitrag von Seiten eines Orbits beträgt $|\,G\,|$. Somit steht auf der rechten Seite $t|\,G\,|$ und wir erhalten schließlich

$$t = \frac{1}{|\,G\,|} \sum_{g \in G} |\,F(g)\,|,$$

wobei t die Zahl der Orbits bezeichnet. ∎

7.3 Die Klassengleichung

In diesem letzten Abschnitt wollen wir weitere Folgerungen aus den Anzahlbedingungen ziehen.

Satz 7.12 *Es sei $(G, G; \kappa)$ eine G-Menge, wobei κ als Translation operiert, d.h.*

$$\kappa(a, x) = \sigma_a(x) = ax.$$

Dann ist der Homomorphismus $a \mapsto \sigma_a$ von G in die Gruppe der Permutationen der Menge G injektiv.

Beweis: straightforward ∎

Aus diesem Satz folgt nun unmittelbar der *Satz von Cayley*[39].

[39] Arthur Cayley (1821 - 1895)

Korollar 7.13 *Jede endliche Gruppe ist zu einer Untergruppe einer symmetrischen Gruppe S_n isomorph.*

Dieser Darstellungssatz ist nicht in jedem Fall aufschlussreich, da beispielsweise im endlichen Fall n-elementige Gruppe in der 'riesigen' Gruppe S_n realisiert wird, die $n!$ Elemente besitzt. Unter Zusatzbedingungen kann allerdings die Einbettung 'günstiger' gewählt werden, d. h. G in eine symmetrische Gruppe $S_{n'}$ eingebettet werden.

Gehen wir noch einmal zurück zur Konjugation einer endlichen Gruppe G als Aktion auf sich selbst. Die Bahnen entsprechen dabei den Konjugationsklassen und bilden eine Partition von G. Da jedes Element von $Z(G)$ zu sich konjugiert ist, gibt es $|\,Z(G)\,|$ Klassen mit je einem Element. Die weiteren Klassen mögen jeweils n_i Elemente beinhalten, wobei, wie oben bemerkt, jedes n_i Teiler von $|\,G\,|$ ist.

Satz 7.14 (Klassengleichung) *Unter den obigen Bezeichnungen gilt für eine endliche Gruppe G*

$$|\,G\,| = |\,Z(G)\,| + (n_1 + n_2 + \cdots n_c). \tag{65}$$

Diese Gleichung heißt *Klassengleichung* von G. Die Tatsache, dass jeder Term n_i ein Teiler von $|\,G\,|$ ist, hat eine bemerkenswerte Konsequenz.

Satz 7.15 *Ist G eine endliche p-Gruppe, dann ist das Zentrum $Z(G)$ nicht trivial.*

Beweis: In der Klassengleichung für G gilt $|\,G\,| = p^r$. Nun ist jedes n_i ein Teiler von p^r. Wegen $n_i \neq 1$ ist $n_i = p^{e_i}$ mit geeignetem $e_i \geq 1$. Aus Teilbarkeitsgründen muss p auch $|Z(G)|$ teilen, d. h. $|Z(G)| > 1$. ∎

8 Ringe, Körper, Polynome

8.1 Begriffliches zur Ringtheorie

Im ersten Kapitel hatten wir ausführlich die algebraischen Eigenschaften einer intuitiv verstandenen Menge $\mathbb{Z}$ der ganzen Zahlen diskutiert. In gleicher Weise könnte man Strukturmerkmale anderer Mengen von Objekten, etwa von Polynomen, näher beleuchten. Diese Beobachtungen liefern die Basis einer axiomatischen Definition der Struktur *Ring*, wobei wir diese Begriffsbildung (vgl. Kapitel 1) noch einmal in Erinnerung bringen.

Definition 8.1 *Ein Ring $(R, +, \cdot)$ ist eine Menge mit zwei binären Verknüpfungen $+$ und $\cdot$, die wir Addition und Multiplikation nennen. Im Hinblick auf diese Verknüpfungen sind die folgenden Eigenschaften erfüllt:*

R1 *$(R, +)$ ist eine abelsche Gruppe.*

R2 *Die Multiplikation $\cdot$ ist eine (innere) Verknüpfung und erfüllt das Assoziativgesetz. Das Element $1 \neq 0$ ist das neutrale Element bzgl. der Multiplikation, also $1a = a1 = a$ für alle $a \in R$, m.a.W. $(R, \cdot)$ ist ein Monoid.*

R3 *Es gelten die Distributivgesetze, d.h. für alle $a, b, c \in R$ ist*

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c). \end{aligned}$$

Wir halten fest, dass die von uns betrachteten Ringe ein neutrales Element der Multiplikation besitzen. Die Kommutativität der Multiplikation wird nicht vorausgesetzt, andernfalls spricht man von einem *kommutativen* Ring. Allerdings sind die hier diskutierten Ringe bis auf Widerruf kommutativ.

Beispiele 8.2 (i) Wir verweisen auf den Ring $\mathbb{Z}$ sowie die in Kapitel 1 erwähnten Beispiele.

(ii) Jeder (kommutative) Körper ist ein (kommutativer) Ring.

(iii) Von Interesse sind die elementar konstruierbaren Restklassenringe $\mathbb{Z}_n$ mit $n \in \mathbb{N}$.

(iv) Die Gaußschen Zahlen $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ bilden einen Ring. Die Gaußschen Zahlen sind die Punkte eines quadratischen Gitters in der komplexen Zahlenebene. Beachte: $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

(v) Wir können analog zu dem Ring der Gaußschen Zahlen einen Unterring $\mathbb{Z}[\alpha]$ zu jeder komplexen Zahl α bilden. Diesen Unterring $\mathbb{Z}[\alpha]$ definieren wir als den kleinsten Unterring von $\mathbb{C}$, der α enthält, und wir nennen ihn *den von α erzeugten Unterring.*

(vi) $K[X]$ steht für den Ring der formalen Polynome in X mit Elementen aus K als Koeffizienten, wobei wir K als kommutativen Körper voraussetzen. Dieser Prozess lässt sich iterieren: $K[X, Y] = K[X][Y]$. Hier sind ausschließlich die konstanten Polynome $\neq 0$ Einheiten.

(vii) Die Menge $\mathcal{R}$ der stetigen reellwertigen Funktionen in einer reellen Variablen bildet einen Ring mit der Addition und Multiplikation von Funktionen:

$$[f + g](x) = f(x) + g(x) \text{ und } [fg](x) = f(x)g(x).$$

(viii) Der Ring $\mathbb{R}^{n \times n}$ aller $n \times n$-Matrizen mit reellen Einträgen ist ein wichtiges Beispiel für einen Ring, der nicht kommutativ ist.

Von Interesse sind insbesondere bei einem ersten Zugang *nullteilerfreie Ringe*:

Definition 8.3 *Ein kommutativer Ring R heißt* Integritätsbereich*, wenn $ab = 0$ stets $a = 0$ oder $b = 0$ nach sich zieht.*

Mit anderen Worten: ein (kommutativer) Ring R ist genau dann ein Integritätsbereich, wenn für ihn die *Kürzungsregel* gilt:

$$\text{Ist } ab = ac \text{ und } a \neq 0, \text{ so ist } b = c. \tag{66}$$

Diese Bedingung (66) ist *notwendig* für die Einbettung von R einen (größeren) Körper, jedoch nicht hinreichend. Erfüllt jedoch ein Ring nicht diese Kürzungsregel, so besitzt er *Nullteiler*.

Man beachte, dass $\mathbb{Z}_n$ Nullteiler besitzt, wenn die Zahl n eine zusammengesetzte Zahl ist. Ist beispielsweise $n = xy$ mit $x, y \notin \{1, -1\}$, so gilt in $\mathbb{Z}_n$ stets $[x]_n \cdot [y]_n = 0$.

Nicht notwendig jedes Element eines Ringes R besitzt allerdings bezüglich der Multiplikation ein inverses Element. Was wir bereits bei den Ringen $(\mathbb{Z}_n, +, \cdot)$ formuliert haben, lässt sich allgemeiner betrachten:

Definition 8.4 *Ein Element x heißt* invertierbar *oder* Einheit in R, *falls*

$$ux = xu = 1$$

für ein geeignetes $u \in R$ gilt. Die Menge der Einheiten eines Ringes R bezeichnen wir mit $U(R)$.

Das Element x schreibt man dann auch als u^{-1}.

Ohne Schwierigkeiten weist man nach:

Lemma 8.5 *Die Menge der Einheiten eines Ringes $(R, +, \cdot)$ bildet bezüglich der Multiplikation eine Gruppe $(U(R), \cdot)$.*

Beispiele 8.6 (i) $U(\mathbb{Z}) = \{1, -1\}$

(ii $U(\mathbb{Z}_n) = \{[a]_n \in \mathbb{Z}_m \mid ggT(a, n) = 1\}$. *Daher ist $\mathbb{Z}_n$ - in Erweiterung unserer obigen Beobachtung - genau dann nullteilerfrei bzw. ein Körper, wenn n prim ist.*

Eine Reihe weiterer Begriffe ist ebenfalls einzuführen:

Definition 8.7 *Es sei $(R, +, \cdot)$ ein Ring.*

(i) *Eine Untergruppe $(I, +) \leq (R, +)$ heißt* Linksideal, *falls $R \cdot I \subseteq I$. Entsprechend wird* Rechtsideal *definiert.*

(ii) *Eine Untergruppe $(I, +) \leq (R, +)$ heißt* zweiseitiges Ideal, *falls I Links- und Rechtsideal zugleich ist.*

(iii) *Ist R ein kommutativer Ring und I ein Ideal $\neq R$, so heißt I ein Primideal, falls $x, y \in R \backslash I$ stets $xy \in R \backslash I$ impliziert.*

Wir erwähnen ferner:

Lemma 8.8 (i) *Im kommutativen Ring $\mathbb{Z}$ der ganzen Zahlen wird jedes Ideal von einem Element erzeugt, d. h. $\mathbb{Z}$ ist ein* Hauptidealring.

(ii) *Genau die Primzahlen erzeugen in $\mathbb{Z}$ Primideale.*

Beweis: (i) Die Aussage lässt sich direkt herleiten: Für ein beliebiges Ideal $I \neq (0)$ finden wir ein minimales Element $q \in \mathbb{N} \cap I$. Für ein beliebiges Element $a \in I$ liefert Proposition 1.7 die Zerlegung $a = bq + r$ mit $0 \leq r < b$. Aufgrund der Minimalität von q folgt $r = 0$, also ist a ein Vielfaches von q, mithin $I = \mathbb{Z}q = (q)$. ∎

8.2 Ringhomomorphismen und Faktorringe

Die entsprechenden Begriffsbildungen für Abbildungen, d. h. *Homomorphismen, Endomorphismen, Isomorphismen* und *Automorphismen* sind sinngemäß aus der Gruppentheorie (vgl. Abschnitt 6.2) übertragbar:

Definition 8.9 *Es seien R, R' Ringe und $\varphi : R \longrightarrow R'$. Dann heißt φ ein* Ringhomomorphismus*, falls das folgende gilt:*

(i) $\varphi : (R, +) \longrightarrow (R', +)$ *ist ein Gruppenhomomorphismus.*

(ii) $\varphi(xy) = \varphi(x) \cdot \varphi(y)$.

(iii) $\varphi(1) = 1 \in R'$.

Ist φ bijektiv, so spricht man von einem Isomorphismus.[40]

Was für Gruppen Normalteiler sind, übernimmt die Begriffsbildung zweiseitiges Ideal für Ringe. Es sei $I \neq R$ ein Ideal in R. Setzt man

$$a \sim b \Longleftrightarrow a - b \in I$$

so wird dadurch in R eine Äquivalenzrelation definiert. Seien $a + I$, $b + I$ Äquivalenzklassen, so sind die Definitionen

$$(a + I) + (b + I) = (a + b) + I$$

bzw.

$$(a + I) \cdot (b + I) = ab + I$$

repräsentantenunabhängig und definieren auf der Faktorstruktur R/I einen Ring. Wiederum gibt es einen kanonischen Epimorphismus $\rho : R \longrightarrow R/I$. Auf Beweise soll hier verzichtet werden. Entsprechend beweist man einen Homomorphiesatz, den wir hier in einer eingeschränkten Form zitieren; sein Beweis ergibt sich unmittelbar durch Nachrechnen.

Satz 8.10 *Es sei I ein Ideal eines Ringes R.*

(a) *Es gibt eine eindeutig bestimmte Ringstruktur auf der Menge der Nebenklassen $\overline{R} = R/I$, so dass die kanonische Abbildung $\rho : R \to \overline{R}$, die das Element r auf das Element $\overline{r} = r + I$ abbildet, ein Homomorphismus ist.*

(b) *Der Kern von ρ ist gerade I.*

8.3 Integritätsbereiche und Quotientenkörper

Im Folgenden werden alle Ringe als kommutativ vorausgesetzt. Von besonderem Interesse sind in der klassischen Ringtheorie die Integritätsbereiche:

Lemma 8.11 *Es sei R ein Integritätsbereich. Dann ist auch der Polynomring $R[X]$ ein Integritätsbereich.*

Lemma 8.12 *Ein Integritätsbereich mit endlich vielen Elementen ist ein Körper.*

Satz 8.13 *Es sei R ein Integritätsbereich. Dann gibt es eine Einbettung von R in einen Körper, das heißt, es gibt einen injektiven Ringhomomorphismus $\iota : R \to K$, wobei K ein Körper ist.*

[40] Injektive Ringhomomorphismen werden auch als Monomorphismen bezeichnet. Die kategorientheoretische Definition eines Epimorphismus bedingt jedoch, daß Ringepimorphismen nicht surjektiv sein müssen. Für Detailfragen konsultiere der Leser die einschlägigen Fachtexte.

Beweis: (vgl. ([2], S. 422) Wir verstehen als Bruch das Symbol a/b, wobei $a, b \in R$ gilt und $b \neq 0$ vorausgesetzt werden. Auf der Menge der Brüche führt man folgende Äquivalenzrelation ein:

$$a_1/b_2 \sim a_2/b_2 \Leftrightarrow a_1 b_2 = a_2 b_1.$$

Diese Relation ist reflexiv, symmetrisch und transitiv. Der zu konstruierende Körper K ist die Menge von Äquivalenzklassen von Brüchen. Wie bei rationalen Zahlen verwenden wir folgende Sprechweise: Wir nennen zwei Brüche a_1/b_1 und a_2/b_2 gleich in K, wenn sie äquivalent sind, $a_1/b_1 = a_2/b_2$ in K bedeutet also $a_1 b_2 = a_2 b_1$. Addition und Multiplikation von Brüchen wird wie bei rationalen Zahlen definiert:

$$(a/b)(c/d) = ac/bd \text{ und } a/b + c/d = (ad + bc)/bd.$$

Dabei ist nachzurechnen, dass diese Verknüpfungen auf Äquivalenzklassen wohldefiniert sind. Man muss also zeigen, dass man äquivalente Ergebnisse erhält, wenn man a/b und c/d durch äquivalente Brüche ersetzt. Außerdem muss man die Körperaxiome nachprüfen. All diese Rechnungen lassen wir als Übungen. ∎

Der auf diese Weise konstruierte Körper, dessen relative Eindeutigkeit man beweisen kann, heißt Quotientenkörper $Q(R) = K$ des Integritätsbereiches R.

Beispiele 8.14 (i) $Q(\mathbb{Z}) = \mathbb{Q}$.

(ii) *Der Quotientenkörper $Q(K[X])$ ist der Körper der rationalen Funktionen $K(X)$, also jener Funktionen, die sich als Quotienten von (ganzen) rationalen Funktionen*[41] *darstellen.*

(iii) *$Q(\mathbb{Z}[i] = \mathbb{Q}(i)$, also die komplexen Zahlen mit rationalem Real- und Imaginäranteilen.*

8.4 Körper

Bereits unter den Faktorringen von $\mathbb{Z}$ hatten wir Ringe kennengelernt, in denen die Einheitengruppe maximal ist in dem Sinne, dass alle Elemente $\neq 0$ invertierbar sind. Dies führt zu der eigentlich bekannten Begriffsbildung *Körper*, die wir hier der Vollständigkeit halber zitieren.

Definition 8.15 *Ein Ring R , in dem jedes Element $\neq 0$ invertierbar ist, heißt R ein Körper. Ist zusätzlich die Multiplikation kommutativ, so heißt R kommutativer Körper.*

Gelegentlich bezeichnet man Körper, für die die Kommutativität der Multiplikation nicht notwendigerweise gefordert wird, als *Schiefkörper*. Manchmal versteht man allerdings unter Schiefkörpern ausdrücklich nichtkommutative Körper.

Beispiel 8.16

(i) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}, \mathbb{H}$ sind Körper. Den Körpern $\mathbb{C}$ und $\mathbb{H}$ unterliegt ein gleiches Bauprinzip: sie sind Divisionsalgebren über den reellen Zahlen $\mathbb{R}$, nämlich der Dimension 2 und 4. Die von Hamilton[42] nachweislich am 16. Oktober 1843 entdeckten Quarternionen stellen eine vierdimensionale Algebra dar, wobei die Elemente $1, i, j, k$ Basis sind und den Vertauschungsregeln

[41] In der Analysis sind dies genau jene Funktionen, die an Unstetigkeiten lediglich Pole aufweisen.

[42] Sir William Rowan Hamilton (geb. 4. August 1805 in Dublin; gest. 2. September 1865 bei Dunsink) war ein irisch-englischer Mathematiker und Physiker. Hamilton studierte in Dublin Mathematik und wurde bereits 1827 Professor für Astronomie sowie königlicher Astronom (Royal Astronomer) für Irland.

In frühen Jahren beschäftigte sich Hamilton mit Strahlensystemen und der geometrischen Optik. Mit nur 18 Jahren entdeckte er das für die Physik wichtige Hamiltonsche Extremalprinzip, das besagt, dass jede Bewegung eines mechanischen Systems derart verläuft, dass die Wirkung stationär ist.

$$\delta S = \delta \int L(q, \dot{q}, t) dt = 0$$

Mit Hilfe der Variationsrechnung folgen aus dem Hamiltonschen Prinzip die Euler-Lagrange-Gleichungen als notwendige Bedingung.

Später beschäftigte er sich mit Quaternionen (hyperkomplexen Zahlen), die heutzutage Anwendung in der Computergrafik finden.

$ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$ genügen. Dieses Konstruktionsprinzip lässt sich nicht auf höhere Dimensionen verallgemeinern, wie in den sechziger Jahren des vergangenen Jahrhunderts durch BOTT und MILNOR gezeigt worden ist. M.a.W. die einzigen Divisionsalgebren über den reellen Zahlen, die selbst wieder Körper sind, existieren nur für die Dimensionen 2 und 4. Für die Dimension 8 existieren noch die so genannten *Cayley-Zahlen*[43], die jedoch nicht mehr das Assoziativgesetz der Multiplikation erfüllen.

(ii) Jeder Restklassenring $\mathbb{Z}_p$ der ganzen Zahl mit p Primzahl ist ein Körper.

(iii) Es sei $\mathbb{C}$ die Menge der Matrizen der Form

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

über $\mathbb{R}$. Dann ist $\mathbb{C}$ wiederum ein Körper.

Es sei F ein Körper und 1 das neutrale Element der Multiplikation. Die Menge $P = \{n \cdot 1 \mid n \in \mathbb{Z}\}$, also die Menge beliebiger Summen der 1, ist offensichtlich ein Ring. Dabei können zwei Situationen auftreten:

Fall 1: Es gibt ein kleinstes $p \in \mathbb{N}$ mit $p \cdot 1 = 0$. Dieses Element p muss eine Primzahl sein, andernfalls gäbe es natürliche Zahlen p_1, p_2, beide von 1 verschieden und $p_1 p_2 = p$. Daraus folgt aber $(p_1 \cdot 1) \cdot (p_2 \cdot 1) = 0$. Da F keine Nullteiler besitzt, erhielten wir $p_1 \cdot 1 = 0$ bzw. $p_2 \cdot 1 = 0$, ein Widerspruch zur Minimalität von p. Also ist $P \cong \mathbb{Z}_p$ und P somit der kleinste, in F enthaltene Körper.

Fall 2: Es gibt kein p mit $p \cdot 1 = 0$, folglich ist P ein zu $\mathbb{Z}$ isomorpher Ring. Da aber P in einem Körper liegt, folgt, dass jedes Element $\neq 0$ aus P invertierbar ist. Mithin liegt im Körper F ein zum Körper $\mathbb{Q}$ isomorpher Körper, der in diesem Fall wiederum der kleinste Teilkörper in F ist.

Die in beiden Fällen beschriebenen Körper heißen *Primkörper* des Körpers F. Die Zahl p im Fall 1 heißt *Charakteristik* von F, im zweiten Fall sagt man, dass die Charakteristik 0 betrage.

Damit haben wir nun folgendes bewiesen:

Proposition 8.17 *Es sei F ein Körper. Dann gibt es einen kleinsten Körper $K \subseteq F$, der von dem neutralen Element 1 der Multiplikation erzeugt wird. Dieser Primkörper ist entweder zu $\mathbb{Q}$ oder zu $\mathbb{Z}_p$ isomorph, wobei im letzten Fall p eine Primzahl p ist.*

Der Beweis wurde bereits oben erbracht. Somit existiert in Gestalt von $\mathbb{Z}_p$ zu jeder Primzahl p eine Körper mit p Elementen. Die weitergehende Frage ist die Frage nach generellen Parametern für endliche Körper.

8.5 Polynome

Die zur Rede stehende Begriffsbildung ist nicht neu, sie soll aber der Vollständigkeit halber erörtert werden.

Es sei R ein kommutativer Ring. Sind $a_0, \ldots, a_n$ Elemente des Ringes R, so nennt man einen formalen Ausdruck

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n$$

ein *Polynom*. Die Elemente $a_0, \ldots, a_n$ heißen *Koeffizienten* von $f(X)$, der Ring R *Koeffizientenring* und X heißt eine *Unbestimmte*. Ist $a_n \neq 0$, so heißt die natürliche Zahl $n \in \mathbb{N}$ der *Grad* des Polynoms und a_n *Leitkoeffizient* von $f(X)$. Ein Polynom $f(X)$ heißt *normiert* (*monic* in der englischen Literatur), falls der Leitkoeffizient 1 oder lediglich eine Einheit aus R ist.

Eine wesentliche Eigenschaft von Polynomen ist es, dass man die Unbestimmte durch alles, was 'sinnvoll' ist, substituieren kann.

Man muss aus grundsätzlichen Überlegungen allerdings das Polynom $f(X)$ von der durch $f(X)$ gemäß $x \to f(x)$ induzierten Polynomfunktion unterscheiden, da unterschiedliche Polynome gegebenenfalls zur gleichen Funktion auf R führen können.

[43] vgl. ([10], Seite 792)

Es ist naheliegend, auf der Menge der Polynome eine Addition, nämlich die komponentenweise Addition der Koeffizienten, und eine Multiplikation, nämlich das hinlänglich bekannte Faltungsprodukt, einzuführen. Wir erhalten als Ergebnis:

Lemma 8.18 *$(R[X], +, \cdot)$ ist ein Ring.*

In erster Näherung verhalten sich Polynome (über Körpern) wie ganze Zahlen. Den schon von $\mathbb{Z}$ her bekannten Divisionsalgorithmus findet man wieder für Polynome.

Satz 8.19 *Es sei F ein kommutativer Körper und $F[X]$ der zugehörige Polynomring. Ferner seien $a(X), b(X) \in F[X]$ mit $b(X) \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q(X), r(X) \in F[X]$ mit*

$$a(X) = b(X)q(X) + r(X),$$

wobei entweder $r(X) = 0$ ist oder der Grad von $r(X)$ kleiner als der Grad von $b(X)$ ist.

Beweis: Es sei das Polynom $b(X)$ gegeben. Wir beweisen die Aussage per Induktion über den Grad von $a(X)$. Ist der Grad von $a(X)$ kleiner als der Grad von $b(X)$, so sind wir fertig.

Sei nun der Grad von $a(X)$ größer oder gleich dem Grad von $b(X)$. Nach Induktionsannahme dürfen wir die Aussage des Satzes als richtig für Polynome mit kleinerem Grad als jenen von $a(X)$ voraussetzen. Seien

$$a(X) = a_{d+k}X^{d+k} + \cdot + a_0, \quad b(X) = b_dX^d + \cdots + b_0,$$

wobei $a_{d+k} \neq 0$, $b_d \neq 0$ mit $k \geq 0$ gelten. Setze

$$\overline{a}(X) = a(X) - a_{d+k}b_d^{-1}X^k b(X).$$

Der Koeffizient von X^{d+k} in $\overline{a}(X)$ beträgt

$$a_{d+k} - (a_{d+k}b_d^{-1})b_d = 0,$$

und somit ist der Grad von $\overline{a}(X)$ kleiner als der Grad von $a(X)$. Folglich gibt es Polynome $\overline{q}(X)$ und $r(X)$ mit

$$\overline{a}(X) = b(X)\overline{q}(X) + r(X),$$

wobei entweder der Grad von $r(X)$ kleiner dem Grad von $b(X)$ ist oder $r(X) = 0$ gilt. Setzt man nun

$$q(X) = \overline{q}(X) + a_{d+k}b_k^{-1}X^k,$$

dann folgt

$$a(X) = b(X)q(X) + r(X)$$

wie verlangt war.

Es bleibt noch zu zeigen, dass $q(X)$ und $r(X)$ eindeutig festgelegt sind.

Sei

$$a(X) = b(X)q_1(X) + r_1(X) = b(X)q_2(X) + r_2(X),$$

wobei entweder der Grad von $r_i(X)$ kleiner dem Grad von $b(X)$ ist oder $r_i(X) = 0$ folgt. Dann ergibt sich

$$b(X)(q_1(X) - q_2(X)) = r_2(X) - r_1(X).$$

Nun hat das Polynom auf der linken Seite entweder Grad größer oder gleich Grad von $b(X)$ oder ist gleich Null, während auf der rechten Seite ein Polynom mit Grad kleiner als Grad $b(X)$ steht, woraus $r_2(X) = r_1(X)$ und somit $q_1(X) = q_2(X)$ folgt. ∎

Ähnlich wie für ganze Zahlen aus $\mathbb{Z}$ lässt sich über die Eigenschaft 'Division mit Rest' ein größter gemeinsamer Teiler $\mathrm{ggT}(f(X), g(X))$ für Polynome $f(X), g(X) \in F[X]$ einführen. Auf die nahe liegende formale Definition (vgl. Definition 1.10) verzichten wir hier.

Satz 8.20 *Es sei F ein kommutativer Körper und $F[X]$ der Polynomring über F. Dann gelten:*

(i) *Für je zwei Polynome $a(X), b(X)$ existiert ein größter gemeinsamer Teiler $d(X)$.*

(ii) *Es gibt Polynome $\lambda(X), \mu(X)$ in $F[X]$ so dass gilt:*

$$d(X) = \lambda(X)a(X) + \mu(X)b(X).$$

Dass dieser größte gemeinsame Teiler für beliebige Polynome $a(X), b(X)$ existiert, folgt aus einer sukzessiven Anwendung des Divisionsalgorithmus.

Beweis:

$$\begin{aligned} a(X) &= b(X)q_0(X) + r_0(X) \\ b(X) &= r_0(X)q_1(X) + r_1(X) \\ r_0(X) &= r_1(X)q_2(X) + r_2(X) \\ \dots &= \dots \\ r_{n-2}(X) &= r_{n-1}(X)q_n(X) + r_n(X) \\ r_{n-1}(X) &= r_n(X)q_{n+1}(X). \end{aligned}$$

Wir beobachten, dass dieser Algorithmus abbricht, da mit jedem Schritt sich der Grad des Restpolynoms verringert. Auf der anderen Seite gilt

$$ggT(a(X), b(X)) = ggT(b(X), r_0(X))$$

und so weiter, so dass $r_n(X) = \mathrm{ggT}(a(X), b(X))$ folgt.

(ii) Umgekehrt lässt sich diese Kette zu einer Summendarstellung des größten gemeinsamen Teilers arrangieren. ∎

Mit den obigen Ergebnissen läßt sich auch die folgende Aussage schnell beweisen:

Lemma 8.21 *Es sei $F[X]$ der Polynomring in einer Unbestimmten über dem (kommutativen) Körper F und $I \leq F[X]$ ein Ideal. Dann wird I von einem Element erzeugt, als R ist ein Hauptidealring.*

Beweis: Wir skizzieren nur die Grundidee. Ist $I \neq (0)$, so gibt es in I ein Polynom minimalen Grades, etwa $b(X)$. Für jedes $a(X) \in I$ gibt es eine Zerlegung im Sinne einer Division mit Rest von folgender Form: $a(X) = b(X)q(X) + r(X)$, wobei $r(X)$ einen kleineren Grad als $b(X)$ haben muss. Wegen $r(X) \in I$ folgt $r(X) = 0$. ∎

8.6 Faktorisierung von Polynomen

Die weitere Entwicklung der Theorie erfolgt zunächst analog wie in $\mathbb{Z}$. Hier müssen wir auf eine weitere Eigenschaft von $\mathbb{Z}$ verallgemeinernd aufmerksam machen:

$$ab = 0 \text{ impliziert } a = 0 \text{ oder } b = 0.$$

Ringe mit einer solchen Eigenschaft nennt man bekanntlich *nullteilerfrei* bzw. im kommutativen Fall spricht man von *Integritätsringen*.

Die folgenden Definitionen beschreiben weitere ringtheoretische Eigenschaften, die wir zwar nur auf Polynome anwenden werden, die aber allgemeiner eingestuft werden müssen.

Definition 8.22 *Es sei R ein nullteilerfreier kommutativer Ring.*

(i) *Elemente $a, b \in R$ heißen* assoziiert, *wenn es eine Einheit $u \in U(R)$ mit $a = bu$ gibt. Sind a und b assoziiert, so schreibt man $a \sim b$.*

(ii) *Ein Element $0 \neq p \in R \backslash U(R)$ heißt* Primelement *von R, wenn gilt: $p \mid a \cdot b$ impliziert $p \mid a$ oder $p \mid b$.*

(iii) *Ein Element* $0 \neq p \in R \backslash U(R)$ *heißt* irreduzibel *in* R*, wenn gilt:* $p = ab$ *impliziert* $a \in U(R)$ *oder* $b \in U(R)$*.*

(iv) *Ein Element von* R *heißt* reduzibel*, wenn es nicht irreduzibel ist.*

Bemerkung 8.23 *In einem Integritätsbereich ist jedes Primelement irreduzibel.*

Beweis: Es seien $a, b \in R$ mit $p = ab$ gegeben. Da p ein Primelement ist, folgt $p \mid a$ oder $p \mid b$. Sei o.B.d.A. $p \mid a$, also gibt es ein $c \in R$ mit $pc = a$, woraus sich $p = ab = pcb$, also $cb = 1$ ergibt. Daher ist $b \in U(R)$ und p irreduzibel. ∎

Die Umkehrung gilt nicht notwendigerweise.

Beispiel 8.24 Es sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ Unterring der komplexen Zahlen. Das Element $\alpha = 2 + \sqrt{-5}$ ist irreduzibel, aber es ist kein Primelement: $3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, also gilt $\alpha \mid 3^2$, jedoch nicht $\alpha \mid 3$.

Proposition 8.25 *Es sei* R *ein nullteilerfreier Hauptidealring. Dann sind die folgenden Aussagen äquivalent:*

(a) p *ist ein irreduzibles Element.*

(b) p *ist ein Primelement.*

Beweis: Nach Bemerkung 8.23 ist jedes Primelement irreduzibel. Daher bleibt nur die Implikation $(a) \Rightarrow (b)$. Es sei nun umgekehrt p ein irreduzibles Element. Das von p erzeugte Ideal ist maximal, d.h. es gibt kein $m \in R$ mit $(p) \subset (m) \subset R$: Jedes Ideal M, das (p) enthält, lässt sich darstellen als $M = (m)$. Aus $p \in (m)$ folgt nun $p = rm$ für ein $r \in R$, also ist r oder m eine Einheit. Mit anderen Worten: (p) ist maximales Ideal.

Sei nun $p \mid ab$, also $ab \in pR$, d.h. es gibt ein Element r mit $pr = ab$. Teilt nun p das Element a, so ist der Nachweis der Primteilereigenschaft erbracht. Andernfalls müssen $p \nmid a$ unterstellen, so dass das irreduzible Element p mit dem Element a nur den größten gemeinsamen Teiler 1 haben kann. Das Element 1 lässt sich also linear durch p und a darstellen, genauer $1 = xp + ya$. Das Element $b = xp + yab$ ist dann aber durch p teilbar, weil die rechte Summe p als Teiler erhält. Mithin ist p ein Primelement. ∎

Satz 8.26 *Es sei* F *ein Körper und* $F[X]$ *der Polynomring in der Unbestimmten* X *über* F*. Dann ist jedes nicht konstante Polynom* $f(X) \in F[X]$ *Produkt von irreduziblen Polynomen. Jede Darstellung ist bis auf Einheiten und die Reihenfolge eindeutig.*

Beweis: Wir verfahren nach dem gleichen Muster wie die Begründung der entsprechenden Aussage für $\mathbb{Z}$, nämlich Satz 1.20. Dies ist nicht verwunderlich, weil auch $F[X]$ ein Hauptidealring ist. Es sei also $r \in F[X]$ gegeben. Ist r irreduzibel, so sind wir fertig, andernfalls kann r als $r_{i_1} s_{i_1}$ geschrieben werden, wobei weder r_{i_1} noch s_{i_1} Einheiten sind. Entsprechend argumentiert man weiter, so dass lediglich zu zeigen bleibt, dass dieser Prozess abbricht. Insgesamt erhält man eine aufsteigende Kette von Idealen $(r) \subset (r_{i_1}) \subset (r_{i_2}) \subset \ldots$. Da die Vereinigung einer aufsteigenden Kette von Idealen wieder ein Ideal ist, das wegen Lemma 8.21 ein Hauptideal ist, folgt, dass der Prozess nach endlich vielen Schritten abbricht.

Die Eindeutigkeit der Darstellung beweist man durch vollständige Induktion über die Anzahl der irreduziblen Faktoren in einer Zerlegung von r, wobei man sich der Primteilereigenschaft von irreduziblen Elementen bedient. ∎

Damit stellt sich die naheliegende Frage, wie man irreduzible Polynome erkennen kann. Natürlich sind alle linearen Polynome $\in F[X]$ irreduzibel, was sich über den Grad erklärt. Schwieriger wird die Frage für Polynome vom Grade größer oder gleich 2. Der nächste Satz gibt Auskunft, wenn ein nicht-lineares Polynom auf keinen Fall irreduzibel ist, nämlich wenn es eine Nullstelle aus F aufweist. Genau dann lässt sich ein Linearfaktor abspalten:

Satz 8.27 *Es sei F ein kommutativer Körper und $f(X) \in F[X]$. Dann ist $X - \alpha$ genau dann ein Teiler von $f(X)$, wenn $f(\alpha) = 0$ für ein $\alpha \in F$ gilt.*

Beweis: Angenommen, $X - \alpha$ ist ein Teiler von $f(X)$, also gilt in $F[X]$ nun

$$f(X) = (X - \alpha)g(X).$$

Setzt man nun in beide Seiten ein, so ergibt sich

$$f(\alpha) = (\alpha - \alpha)g(\alpha) = 0g(\alpha) = 0.$$

Umgekehrt, sei nun $f(\alpha) = 0$ in F. Nach Satz 8.19 gibt es Polynome $q(X)$ und $r(X)$ in $F[X]$ mit

$$f(X) = (X - \alpha)q(X) + r(X),$$

wobei entweder der Grad von $r(X)$ kleiner als der Grad von $X - \alpha$ ist oder $r(X) = 0$ gilt. Wertet man nun diesen Ansatz jeweils bei α aus, unter Beachtung von $f(\alpha) = 0$, so folgt

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

Ist nun der Grad von $r(X)$ kleiner als der von $X - \alpha$, dann muss $r(X)$ eine Konstante sein, also $r = 0$. Daraus folgt schließlich die Behauptung. ∎

Die letzte Aussage heißt auch *Faktorisierungssatz*. Essenz ist die Beobachtung, dass α genau dann eine *Wurzel* (Nullstelle) eines Polynoms $f(X)$ ist, wenn $f(\alpha) = 0$ gilt.

Ohne ins Detail zu gehen merken wir an, dass dieser Satz auch eine Version in Polynomringen über nicht notwendig kommutativen Körpern zulässt. Hier muss man dann so genannte Linkseingesetzte $f_L(\alpha) = \sum_{i=0}^{n} \alpha^i a_i$ bzw. Rechtseingesetzte $f_R(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$ unterscheiden. Der euklidische Algorithmus greift auch in diesem Kontext.

Satz 8.28 *Es sei F ein kommutativer Körper und $f(X)$ ein Polynom vom Grad $n \geq 1$ in $F[X]$. Dann hat die Gleichung $f(x) = 0$ höchstens n Lösungen oder Wurzeln in F.*

Beweis: folgt unter Anwendung von 8.27 und vollständiger Induktion. ∎

Wir beschließen diesen Abschnitt mit folgender wichtiger Beobachtung, die wir zum Teil oben bemerkt hatten:

Satz 8.29 *Es sei F ein kommutativer Körper und $f(X)$ ein irreduzibles Polynom aus $F[X]$. Dann ist $(f(X))$ ein maximales Primideal in $F[X]$. Der Restklassenring $F' = F[X]/(f(X))$ ist ein Körper, der eine Körpererweiterung von F darstellt.*

Beweis: Zunächst ist $F[X]$ nach 8.21 ein Hauptidealring. Nach Proposition 8.25 erzeugen irreduzible Elemente maximale Ideale. Maximale Ideale sind grundsätzlich Primideale, was wir hier allerdings nicht bewiesen haben. Insofern argumentieren wir direkt. Sind $a(X), b(X)$ Polynome und nimmt an, dass $a(X)b(X) \in (f(X))$ gilt, so teilt $f(X)$das Produkt $a(X)b(X)$. Da $f(X)$ als irreduzibles Element auch ein Primelement ist, muss $f[X]$ einen der beiden Faktoren teilen, der dann im Ideal $(f(X))$ liegt. Somit ist $(f(X))$ ein Primideal, also $F[X]/(f(X))$ ein nullteilerfreier Ring, d.h. ein Integritätsbereich. Darüberhinaus ist jedes Element $\neq 0$ invertierbar: Sei $g(X]) + (f((X))$ ein solches. Dann sind o.B.d.A. die Polynome $f(X)$ und $g(X)$ relativ prim, also existieren Polynome $\lambda(X)$ und $\mu(X)$ mit $1 = \lambda(X)f(X) + \mu(X)g(X)$. Modulo $(f(X))$ gilt daher $(\mu(X) + (f(X)))(g(X) + (f(X))) = 1$. Damit ist $F[X]/(f(X))$ ein Körper. ∎

Beispiele 8.30 Über dem Ring $\mathbb{R}$ sind die einzigen irreduziblen Polynome die vom Grad 2 oder lineare Terme. Über $\mathbb{Z}_2$ ist z. B. das Polynom $f(X) = X^2 + X + 1$ irreduzibel.

Es stellen sich naheliegend die folgenden Fragen:

- Gibt es über jedem Körper F und zu jedem Grad ein entsprechendes Polynom $f(X)$, das irreduzibel ist?
- Wie beweist man die Irreduzibilität eines Polynomes?

Darauf wird im nächsten Semester eingegangen werden.

Doch was ist die Philosophie dieser Erweiterung? Sie ist zunächst einmal *algebraisch* orientiert, die Erweiterung von F zu dem größeren Körper bedient sich algebraischer Hilfsmittel. F' stellt neue Elemente bereit, die als Restklassen von Idealen geschaffen werden. In der Körpertheorie diskutiert man allerdings auch andere Körpererweiterungen, z.B. transzendene Körpererweiterungen, die erst später vorgestellt werden sollen.

Der Erweiterungskörper F' enthält auch F, wenn man die Elemente von F über die Polynomrestklassen von Polynomen versteht, die nur aus einem konstanten Anteil bestehen.

Doch wie kommen neue Elemente hinzu? Über den algebraischen Erweiterungsprozess, durch das Arbeiten mit Polynomen anstelle des Umgehens mit Koeffizienten! Dabei ist insbesondere die Restklasse $X + (f(X))$ von Bedeutung. Sie verhält sich so wie eine in F nicht vorhandene Nullstelle des Polynoms $f(X)$. Wertet man also das Polynom $f(X)$ über F' aus, so ist definitionsgemäß das neue Element eine Nullstelle aus F' von $f(X)$. Insofern verhelfen uns auch die Körpererweiterungen zu neuen Nullstellen, die vorher nicht vorhanden waren.

In gewisser Weise sind diese Erweiterungen mehrdeutig, unterscheiden sich aber nicht, weil sie isomorph sind. Das über $\mathbb{Q}$ irreduzible Polynom X^2-2 induziert nach F' Nullstellen X und $-X$, die wir uns sowohl als $\sqrt{2}$ wie auch als $-\sqrt{2}$ vorstellen dürfen. Mit anderen Worten: $\sqrt{2}$ und $-\sqrt{2}$ sind algebraisch nicht zu unterscheiden oder positiv registriert: F' besitzt einen F-Automorphismus der Ordnung 2, also einen Automorphismus, der F fest lässt und X nach $-X$ transportiert. Mit dieser 'Unschärfe' beschäftigt sich die Galois-Theorie genauer, indem sie aus der Struktur der Gruppe aller F-Automorphismen Informationen gewinnt, die auch als Eigenschaft des eigentlich über F nicht zerfallenden Polynoms $f(X)$ gedeutet werden können.

9 Endliche Körper und einige Anwendungen

9.1 Ein endlicher Körper mit 9 Elementen

Über dem Körper $\mathbb{Z}_3$ betrachten wir den Polynomring modulo X^2+1. Wie man durch Einsetzen leicht erkennt, ist dieses Polynom irreduzibel, induziert also einen Erweiterungskörper F_9 von $\mathbb{Z}_3$. Wir beschreiben die Elemente dieses Erweiterungskörpers F_9 mit

$$\{0,1,2,X,X+1,X+2,2X,2X+1,2X+2\}.$$

Die Addition erfolgt in F_9 gemäß

	0	1	2	X	X+1	X+2	2X	2X+ 1	2X+2
0	0	1	2	X	X+1	X+2	2X	2X+1	2X+2
1	1	2	0	X+1	X+2	X	2X+1	2X+2	2X
2	2	0	1	X+2	X	X+1	2X+2	2X+1	2X
X	X	X+1	X+2	2X	2X+1	2X+2	0	1	2
X+1	X+1	X+2	X	2X+1	2X+2	2X	1	2	0
X+2	X+2	X	X+1	2X+2	2X	2X+1	2	0	1
2X	2X	2X+1	2X+2	0	1	2	X	X+1	X+2
2X+1	2X+1	2X+2	2X	1	2	0	X+1	X+2	X
2X+2	2X+2	2X	2X+1	2	0	1	X+2	X	X+1

Die folgende Tabelle benennt die jeweiligen inversen Elemente:

1	2	X	X+1	X+2	2X	2X+1	2X+2
1	2	2X	X+2	X+1	X	2X+2	2X+1

Man rechnet schnell nach, dass die multiplikative Gruppe von $2X+1$ erzeugt wird, denn $(2X+1)^2 = X$, $(2X+1)^3 = X+1$, $(2X+1)^4 = 2$, $(2X+1)^5 = X+2\,(2X+1)^6 = 2X$, $(2X+1)^7 = 2X+2$, $(2X+1)^8 = 1$.

9.2 Die Ordnung eines endlichen Körpers

Im letzten Abschnitt hatten wir bereits die *Charakteristik* eines Körpers eingeführt. Im Falle eines endlichen Körpers gewinnt man mit dieser Charakteristik noch weitergehende Einsichten:

Satz 9.1 *Es sei F ein endlicher Körper der Charakteristik p. Dann ist die additive Gruppe isomorph zu $(\mathbb{Z}_p)^r$. Insbesondere gilt: $|\,F\,| = p^r$ für ein $r \geq 1$.*

Beweis: Der Körper F habe $\mathbb{Z}_p$ als Primkörper. Dann ist, wie man sich leicht überlegt, F ein $\mathbb{Z}_p$-Vektorraum. Der Rest folgt ohne Schwierigkeiten. ∎

9.3 Zur Konstruktion endlicher Körper

Wir knüpfen an die Beobachtung an, dass Faktorringe von Polynomringen über Körpern nach irreduziblen Polynomen wiederum Körper liefern.

Satz 9.2 *Es sei $k(X)$ ein irreduzibles Polynom vom Grad r über dem endlichen Körper $\mathbb{Z}_p[X]$ und $I = (k(X))$ das zugehörige Hauptideal im Polynomring $\mathbb{Z}_p[X]$. Dann ist der Restklassenring $\mathbb{Z}_p[X]/(k(X))$ ein kommutativer Körper F der Ordnung p^r.*

Beweis: Nach einem früheren Satz erzeugt ein irreduzibles Element ein Primideal, das maximal ist, folglich ist der Restklassenring ein Körper. Der Rest folgt aus Anzahlgründen. ∎

Damit stellt sich die Frage, inwieweit für beliebiges $\mathbb{Z}_p$ und vorgegebenes $r \in \mathbb{N}$ ein irreduzibles Polynom vom Grad r in $\mathbb{Z}_p[X]$ existiert.

9.4 Der Satz vom primitiven Element

Im vorigen Unterabschnitt hatten wir gezeigt, dass die additive Gruppe eines Körpers F mit p^r Elementen zur direkten Summe $(\mathbb{Z}_p)^r$ isomorph ist. Die multiplikative Gruppe von F hat die Ordnung $p^r - 1 = q - 1$ und besitzt eine relativ einfache Gestalt[44].

Satz 9.3 *Es sei F ein endlicher (kommutativer) Körper mit $q = p^r$ Elementen, wobei p eine Primzahl ist. Dann ist die multiplikative Gruppe $F \setminus \{0\}$ zyklisch und somit kommutativ.*

Beweis: Da die multiplikative Gruppe $q - 1 = p^r - 1$ Elemente hat, gilt $f^{q-1} = 1$ für jedes $f \neq 0, f \in F$. Also hat die Gleichung $X^{q-1} - 1 = 0$ genau $q - 1$ Wurzeln (oder Nullstellen) aus F. Wir werden nachweisen, dass F^* die Eigenschaften von Satz 6.29 erfüllt, über den zyklische Gruppen charakterisiert werden. Genauer: Wir beweisen, dass es für jeden Teiler d von $q - 1$ genau d Elemente f gibt, die $f^d = 1$ erfüllen.

Es sei nun $dk = q - 1$. Man rechnet schnell nach, dass die folgende algebraische Identität gilt:

$$X^{q-1} - 1 = (X^d - 1)(X^{d(k-1)} + X^{d(k-2)} + \cdots + X^d + 1) = (X^d - 1)g(X),$$

wobei $g(X)$ den zweiten Faktor bezeichnet. Da $g(X)$ vom Grad $d(k-1)$ ist, hat $g(X) = 0$ höchstens $d(k-1)$ Wurzeln in F. Ferner hat $X^d - 1$ höchstens d Wurzeln in F. Da aber in Gestalt der Elemente aus F^* insgesamt $q - 1 = d(k-1) + d$ Nullstellen existieren, müssen die Abschätzungen scharf sein, d. h. es gibt genau d Elemente aus F^* mit $f^d = 1$, was zu beweisen war. ∎

Definition 9.4 *Einen Erzeuger der multiplikativen Gruppe F^* des Körpers F bezeichnet man als* primitives Element*.*

Damit lautet das obige Ergebnis:

Korollar 9.5 *Jeder endliche Körper besitzt ein primitives Element.*

So elegant der Beweis auch war, er ist nicht konstruktiv. Es können ja insgesamt $\phi(q-1)$ primitive Elemente vorliegen.

Eine Folgerung aus diesem Satz scheint naheliegend, obgleich wir sie noch nicht mit den Mitteln der Vorlesung unmittelbar beweisen können. Bei der Behandlung von Zerfällungskörpern wird dieses Ergebnis ein Nebenprodukt sein.

Satz 9.6 *Alle endlichen Körper mit der Elementeanzahl p^r, p prim , $r \in \mathbb{N}$ sind zueinander isomorph.*

Dass diese Aussage jeweils für die additive wie multiplikative Gruppe separat gilt, ist offensichtlich. Trivial ist allerdings nicht, daß eine bijektive Abbildung gefunden werden kann, die beides zugleich bewerkstelligt.

Beispiel 9.7 Man finde ein primitives Element in $\mathbb{Z}_{41}$.

Lösung: Wir beginnen unsere Suche bei 2. Ist 2 primitiv, so müßten wir alle Elemente erhalten. Es ergibt sich:

n :	1	2	3	4	5	6	7	8	9	10
2^n :	2	4	8	16	32	23	5	10	20	40
n :	11	12	13	14	15	16	17	18	19	20
2^n :	39	37	33	25	9	18	36	31	21	1

[44] Diese tieferliegende Erkenntnis, dass nämlich die multiplikative Gruppe eines endlichen Körpers *kommutativ* ist, geht auf J.H.M. Wedderburn (1905) zurück: A theorem on finite algebras. *Trans. Amer. Math. Soc.* **6** (1905), 349 - 352.

Mithin ist die Ordnung von 2 nur 20, nicht jedoch 40, d.h. 2 ist kein primitives Element. Wir könnten nun bei 3 beginnen, man beachte aber, dass 9 mit 2^{15} module 41 übereinstimmt, daraus folgt

$$3^8 = 9^4 \bmod 41 = 2^{60} \bmod 41 = (2^{20})^3 \bmod 41 = 1 \bmod 41,$$

die Ordnung von 3 ist also lediglich 8. Auch sind die Elemente 4 und 5 Potenzen von 2 und daher ihre Ordnungen Teiler von 20. Die Ordnung des Elementes 6 hingegen errechnet sich als das kgV der Ordnungen von 2 und 3, und daher ist 6 ein primitives Element des gegebenen Rings.

Es gibt nun Tabellen, in denen primitive Elemente vorgehalten werden. Erzeugt ein Polynom $k(X)$ vom Grad r in $\mathbb{Z}_p[X]$ den Körper mit F mit p^r Elementen, so ist möglicherweise X ein geeignetes primitives Element. In diesem Fall sagen wir, dass $k(X)$ ein *primitives irreduzibles Polynom* heißt.

Satz 9.8 *Für jede Primzahl p und jede natürliche Zahl $n \geq 1$ gibt es ein normiertes primitives Polynom $f(X) \in \mathbb{Z}_p[X]$ vom Grad n.*

Auf den etwas länglichen Beweis verzichten wir an dieser Stelle, er folgt aus allgemeineren Überlegungen und wird in der Vorlesung Algebra II geliefert.

9.5 Endliche Körper und lateinische Quadrate

Endliche Körper ermöglichen es, in diskreten Strukturen zu 'rechnen'. Ausgangssituation ist eine klassische Aufgabe der Unterhaltungsmathematik, die der Mathematiker Euler 1782 am Petersburger Hof zu lösen versuchte:

- *1. Vorgabe:* Man positioniere 36 Offiziere aus 6 verschiedenen Regimentern in einem 6×6 Quadrat, dass jedes Regiment genau einmal in jeder Zeile und in jeder Spalte vertreten ist.
- *2. Vorgabe:* Diese Offiziere sind insgesamt sechs verschiedenen Diensträngen zuzuordnen.

Ist es möglich, die Aufstellung auch so vorzunehmen, dass *zusätzlich* in jeder Zeile und in jeder Spalte jeder Dienstgrad genau einmal vertreten ist? Die Lösung blieb lange offen, Euler vermutete, daß das Problem keine positive Lösung besitzt.

Definition 9.9 *Es sei K eine n-Menge. Unter einem lateinischen Quadrat L der Ordnung n versteht man eine $n \times n$-Matrix, in der in jeder Zeile und jeder Spalte jedes Element aus K genau einmal vertreten ist.*

Ohne weiteres kann man $K = \{0, 1, \ldots, n-1\}$ annehmen. Allerdings kommt die Bezeichnung *lateinisch* daher, dass man im 18. Jahrhundert bei solchen Quadraten, die damals nur in der Unterhaltungsmathematik vorkamen, zur Belegung der Felder nicht Zahlen, sondern lateinische Buchstaben verwandte.

Die Bedeutung der Restklassenmengen $\mathbb{Z}_m$ unterstreicht der folgende offensichtliche Satz:

Satz 9.10 *Für jedes $m \geq 2$ ist die folgende Matrix*

$$L(i, j) = i + j, \quad i, j \in \mathbb{Z}_m$$

ein lateinisches Quadrat.

Definition 9.11 *Zwei lateinische Quadrate L_1, L_2 heißen zueinander* orthogonal*, wenn es für jedes Paar $(k, k') \in \mathbb{Z}_m \times \mathbb{Z}_m$ genau eine Position (i, j) gibt mit*

$$L_1(i, j) = k, \quad L_2(i, j) = k'.$$

Eine Menge von m lateinischen Quadraten heißt paarweise orthogonal *(pairwise mutually orthogonal), wenn jedes Paar von lateinischen Quadraten orthogonal ist.*

Die Frage nach der maximalen Größe einer Menge von paarweise orthogonalen lateinischen Quadraten der Ordnung n kann als eine der tiefsten zentralen Fragen der Geometrie und Kombinatorik bezeichnet werden. Genau danach hatte man eigentlich Euler seinerzeit gefragt. Die Antwort, die zu Beginn dieses Jahrhunderts durch Tarry gegeben werden konnte, lautete: *Es gibt kein Paar orthogonaler lateinischer Quadrate der Ordnung 6.* Euler vermutete nun weiter, dass 6 (neben 2) wohl nicht die einzige *Ausnahmeordnung* sein könne und dass zu keiner geraden, nicht durch 4 teilbaren Ordnung orthogonale lateinische Quadrate existieren würden. Erst 1959/60 konnten Bose, Parker und Shrikhande diese Euler'sche Vermutung widerlegen; sie gaben sogar für jede gerade, nicht durch 4 teilbare Ordnung ≥ 10 ein Verfahren zur Konstruktion eines Paares orthogonaler lateinischer Quadrate an. Andererseits hatte schon Euler zeigen können, dass es zu jeder entweder ungeraden oder aber durch 4 teilbaren Ordnung ein solches Paar gibt. Somit sind tatsächlich 2 und 6 die einzigen Ordnungen, zu denen es keine orthogonalen lateinischen Quadrate gibt[45].

Satz 9.12 *Es sei p eine Primzahl und $t \in \mathbb{Z}_p$, $t \neq 0$. Dann definiert die Vorschrift*

$$L_t(i,j) = ti + j, \quad i,j \in \mathbb{Z}_p$$

ein lateinisches Quadrat. Für jedes Paar (t,u) mit $t \neq u$ sind die lateinischen Quadrate L_t und L_u zueinander orthogonal.

Beweis: ohne Beweis in der Vorlesung ∎

Der nachfolgende Satz ist ein Beispiel dafür, wie man kombinatorische Strukturen algebraisch generieren kann.

Satz 9.13 *Es sei q eine Primzahlpotenz. Dann gibt es $q-1$ paarweise orthogonale lateinische Quadrate der Ordnung q.*

Beweis: Zunächst konstatieren wir, dass es einen Körper F der Ordnung q gibt. Für jedes der $q-1$ Elemente $t \in F^*$ definieren wir eine $q \times q$ Matrix durch die Einträge

$$L_t(i,j) = ti + j \quad i,j \in F_q.$$

Man rechnet ohne weiteres nach, dass jedes L_t ein lateinisches Quadrat ist: aus $L_t(i,j) = L_t(i,j')$ folgt $ti+j = ti+j'$ und durch elementare algebraische Umformungen $j = j'$. Entsprechend verfährt man mit den Spalteneinträgen.

Seien nun L_u und L_t verschiedene lateinische Quadrate. Wir nehmen nun an, dass in den Positionen (i_1,j_1) und (i_2,j_2) gleiche Einträge stehen, d. h.

$$ti_1 + j_1 = k, \quad ui_1 + j_1 = k',$$

bzw.

$$ti_2 + j_2 = k, \quad ui_2 + j_2 = k'.$$

Dann folgt

$$t(i_1 - i_2) = j_2 - j_1, \quad u(i_1 - i_2) = j_2 - j_1.$$

Ist nun $i_1 = i_2$, dann folgt auch $j_1 = j_2$ und die beiden Positionen stimmen überein. Andernfalls ist $i_1 - i_2 \neq 0$ und besitzt somit ein Inverses in F und es folgt

$$t = u = (i_1 - i_2)^{-1}(j_2 - j_1),$$

also $L_t = L_u$. Somit gibt es insgesamt $q-1$ paarweise orthogonale lateinische Quadrate. ∎

[45] vgl. insbesondere die Ausführungen in dem Buch von Pickert, G.: Einführung in die endliche Geometrie. 1974. Stuttgart: Klett.

9.6 Endliche Körper und Designs

Satz 9.14 *Es sei F ein endlicher Körper der Ordnung q. Dann gibt es ein 2-Design mit den Parametern*

$$v = q^2, \;\; k = q, \;\; r_2 = 1.$$

Dieses 2-Design ist eine affine Ebene.

Beweis: Als 2-Design betrachte man die affine Ebene über dem Körper F. Punkte sind die Paare (x, y) mit $x, y \in F$. Als Geraden wählen wir die Punktmengen $\{(x, y) \mid ax + by = c,\ x, y \in F\}$, wobei $a, b, c \in F$ gilt und $(a, b) \neq (0, 0)$ erfüllt ist. Die weitere Rechnung soll hier nicht angegeben werden. ∎

Ohne Schwierigkeiten lässt sich herleiten:

Lemma 9.15 *Es sei $\mathcal{A}$ ein 2-Design wie oben konstruiert über dem Körper F mit q Elementen. Dann gelten:*

(i) *Auf jeder Geraden liegen q Punkte.*

(ii) *Durch jeden Punkt gehen $q + 1$ Geraden.*

(iii) *Es gibt insgesamt $q^2 + q$ Geraden.*

Beweis: straightforward ∎

Diese affine Ebene lässt sich eindeutig zu einer projektiven Ebene erweitern:

Satz 9.16 *Für jede Primzahlpotenz q gibt es ein 2-Design mit den Parametern*

$$v = q^2 + q + 1, \;\; k = q + 1, \;\; r_2 = 1.$$

Dieses 2-Design hat die zusätzliche Eigenschaft, dass je zwei Blöcke genau einen Punkt gemeinsam haben.

Für Details verweisen wir auf die Übungen.

9.7 Quadrate in endlichen Körpern

Wir beschäftigen uns mit der Frage, welche Elemente eines endlichen Körpers F Quadrate sind. Nun besitzt die multiplikative Gruppe von F ein primitives Element α, d. h.

$$F^* = \{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{q-1}\}.$$

Offensichtlich sind die geraden Potenzen $\alpha^{2m} = (\alpha^m)^2$ Quadrate. Die Frage, ob auch ungerade Potenzen, Quadratwurzeln besitzen, hängt von q ab.

Angenommen eine ungerade Potenz von α habe eine Quadratwurzel, etwa $\alpha^{2m+1} = \beta^2$. Da β selbst eine Potenz von α ist, folgt $\beta = \alpha^k$ und schließlich

$$\alpha^{2(m-k)+1} = \alpha^{2m+1}\alpha^{-2k} = \alpha^{2m+1}(\beta^2)^{-1} = 1.$$

Die Ordnung von $\alpha \in F^*$ beträgt $q - 1$, also ist $2(m - k) + 1$ ein Vielfaches von $q - 1$. Ist jedoch q ungerade, so ist $q - 1$ gerade, was zu einem Widerspruch führt. Somit sind genau die geraden Potenzen eines primitiven Elementes Quadrate für den Fall, dass q ungerade ist. Ist q ungerade, so ist q auch Potenz einer ungeraden Primzahl.

Es sei nun weiterhin q ungerade. Die Menge der Quadrate bezeichnen wir mit $\mathcal{Q}$, d.h.

$$\mathcal{Q} = \{\alpha^2, \alpha^4, \ldots, \alpha^{q-1}\}.$$

Diese Menge hat insgesamt $\frac{1}{2}(q - 1)$ Elemente.

Satz 9.17 *Es sei q eine ungerade Primzahlpotenz. Ist $q \equiv 1 (mod\ 4)$, dann ist -1 Quadrat in F; ist $q \equiv 3 (mod\ 4)$, dann hat -1 keine Quadratwurzel in F.*

Beweis: Zunächst zeigen wir, dass

$$\alpha^{\frac{1}{2}(q-1)} = -1$$

gilt, wobei α ein primitives Element von F ist. Beachte, dass die Gleichung $x^2 = 1$ genau die Lösungen $\{-1, 1\}$ hat. Auf der anderen Seite erfüllen α^{q-1} und $\alpha^{\frac{1}{2}(q-1)}$ die Gleichung $x^2 = 1$ und deshalb sind sie 1 bzw. -1.

Nach den vorigen Überlegungen ist $\alpha^{1/2(q-1)}$ ein Quadrat genau dann, wenn $\frac{1}{2}(q-1)$ gerade ist, also

$$\frac{1}{2}(q-1) = 2m$$

erfüllt ist, was $q = 4m + 1$ nach sich zieht. ∎

Satz 9.18 *Ist q eine Primzahlpotenz der Form $4n+3$ und F ein endlicher Körper mit q Elementen, dann ist die Menge $\mathcal{Q}$ der Quadrate $\neq 0$ in F eine Differenzmenge mit den Parametern $(4n+3, 2n+1, n)$. Mit anderen Worten: jedes Element $\neq 0$ in F lässt sich als Differenz von Quadraten auf n verschiedene Weisen darstellen.*

Beweis: Sei z ein (festes) Quadrat in F, etwa $z = \zeta^2$ mit $\zeta \neq 0$. Es gibt μ Möglichkeiten, z als Differenz von Quadraten darzustellen, etwa

$$z = u^2 - v^2.$$

Wir zeigen nun, dass jedes andere Element $w \in F$ auf gleichviel Weisen als Differenz von Quadraten darstellbar ist.

Ist w ein Quadrat, etwa $w = \omega^2$, dann gilt

$$w = (\omega\zeta^{-1})^2\zeta^2 = \beta^2 z \quad (\beta = \omega\zeta^{-1} \in F).$$

Also gibt es für jede Darstellung von z als Differenz der Quadrate u und v einen entsprechenden Ausdruck für $w = (\beta u)^2 - (\beta v)^2$.

Ist nun w kein Quadrat, so ist w eine ungerade Potenz eines primitiven Elements. Da auch -1 kein Quadrat ist, ist auch -1 eine ungerade Potenz des gleichen primitiven Elements und $-w = (-1)w$ ist eine gerade Potenz dieses primitiven Elementes. Also ist $-w$ ein Quadrat, etwa $-w = \theta^2$, und es folgt

$$w = -\theta^2 = -(\theta\zeta^{-1})^2\zeta^2 = \gamma^2(-z) \quad (\gamma = \theta\zeta^{-1} \in F).$$

Wiederum folgt, dass für jede Darstellung von z als Differenz von Quadraten eine entsprechende Darstellung von w induziert wird:

$$w = (\gamma v)^2 - (\gamma u)^2.$$

Daher hat jedes Element $\neq 0$ die gleiche Anzahl μ von Darstellung als Differenz von Quadraten.

Nun ist $|\mathcal{Q}| = \frac{1}{2}(q-1) = 2n + 1$ und daher ist die Gesamtzahl der Differenzen von verschiedenen Quadraten $2n(2n+1)$. Da auf diese Weise insgesamt $q-1 = 4n+2$ verschiedene Werte $\neq 0$ auftreten, jedes Element aber μ-fach ist, folgt aus

$$2n(2n+1) = \mu(4n+2)$$

schließlich $\mu = n$, was zu beweisen war. ∎

Ist p eine Primzahl der Form $4n + 3$, so folgt aus dem Satz, dass die Menge $\mathcal{Q}$ der Quadrate $\neq 0$ in $\mathbb{Z}_p$ eine Differenzmenge mit den Parametern $(4n + 3, 2n + 1, n)$ ist, wodurch wir ein früheres

Ergebnis für $p = 23$ verallgemeinert haben. Mit Satz[46] 9.19 ergibt sich, dass die Mengen $\mathcal{Q} + i$, mit $(i \in \mathbb{Z}_p)$ Blöcke in einem 2-Design mit denselben Parametern sind.

[46]

Satz 9.19 *Es sei $K \subseteq \mathbb{Z}_m$ eine Differenzmenge. Dann sind die Mengen $K + i$, mit $i \in \mathbb{Z}_m$ Blöcke eines 2-Designs mit den Parametern*

$$v = m, \quad k = |K|, \quad r_2 = k(k-1)/(m-1).$$

Index