ELEMENTARE ZAHLENTHEORIE

KATHARINA HÜBNER

Inhaltsverzeichnis

Date: 13. November 2025.

1. Zahlen

1.1. **Die natürlichen Zahlen.** Die natürlichen Zahlen bilden das fundamentale Forschungsobjekt, das wir in der Zahlentheorie verstehen wollen. Sie heißen „natürlich", weil sie wahrscheinlich die naheliegendste Konstruktion in der Welt der Zahlen sind. Schon als kleine Kinder lernen wir zählen: eins, zwei, drei... Und dadurch, dass man zählt, also der drei die vier folgen lässt und der sieben die acht, hat man die natürlichen Zahlen im Grunde genommen schon definiert. Um sie in der Mathematik, genauer in der Zahlentheorie, zu nutzen, wollen wir herausarbeiten was dieses Zählen formal bedeutet. Genauer gesagt formulieren wir in den *Peanoaxiomen*, die Annahme, dass es möglich ist zu zählen.

Peanoaxiome. *Es gibt eine Menge* $\mathbb{N}$*, die Menge der* natürlichen Zahlen *zusammen mit einem Element* $1 \in \mathbb{N}$ *(genannt* Eins*) und einer Abbildung*

$$N : \mathbb{N} \to \mathbb{N},$$

(die einer Zahl $n \in \mathbb{N}$ *ihren* Nachfolger $N(n)$ *zuordnet) mit den folgenden Eigenschaften:*

(i) 1 *ist kein Nachfolger, also* $N(n) \neq 1$ *für alle* $n \in \mathbb{N}$*,*
(ii) die Abbildung N *ist injektiv,*
(iii) vollständige Induktion*: Jede Teilmenge* $M \subseteq \mathbb{N}$*, für die gilt:*
- $1 \in M$*,*
- *aus* $m \in M$ *folgt* $N(m) \in M$*,*

ist bereits ganz $\mathbb{N}$*.*

Die Abbildung $N : \mathbb{N} \to \mathbb{N}$ aus den Peanoaxiomen modelliert das Zählen. Wir fangen mit der Eins an, die nach Annahme existiert. Die Zwei ist dann per Definition der Nachfolger $N(1)$ der 1, drei ist der Nachfolger von zwei, und so fort.

Ausgehend von den Peanoaxiomen können wir die Addition und die Multiplikation natürlicher Zahlen definieren: Wir beginnen mit der Addition. Um zu lernen wie mit der vollständigen Induktion formal zu argumentieren ist, sehen wir uns den Beweis im Detail an. Die Abbildung N_m im folgenden Lemma soll letztendlich die Abbildung $n \mapsto m + n$ werden. Das sollte man im Hinterkopf behalten um die Intuition nicht zu verlieren.

Lemma 1.1. *Für jedes* $m \in \mathbb{N}$ *gibt es eine eindeutige Abbildung*

$$N_m : \mathbb{N} \longrightarrow \mathbb{N}$$

mit den folgenden Eigenschaften

(i) $N_m(1) = N(m)$*,*
(ii) $N_m(N(n)) = N(N_m(n))$ *für alle* $n \in \mathbb{N}$*.*

Beweis. Sei $M \subseteq \mathbb{N}$ die Menge aller natürlichen Zahlen, für die eine eindeutige Abbildung N_m mit den geforderten Eigenschaften (i) und (ii) existiert. Wir wollen zunächst

zeigen, dass $1 \in M$. Es erfüllt $N_1 := N$ die gewünschten Eigenschaften tautologischerweise. Wir müssen uns aber noch davon überzeugen, dass N die einzige Abbildung ist, die das tut. Sei

$$\varphi : \mathbb{N} \to \mathbb{N}$$

eine weitere Abbildung, die die Eigenschaften erfüllt. Wir betrachten die Menge $A \subseteq \mathbb{N}$ aller natürlicher Zahlen n, für die gilt $\varphi(n) = N(n)$. Für $n = 1$ haben wir

$$\varphi(1) = N(1)$$

nach Eigenschaft (i). Ist $n \in A$, so gilt

$$\varphi(N(n)) = N(\varphi(n)) = N(N(n)).$$

Die erste Gleichheit folgt aus (ii) für φ und die zweite aus der Tatsache, dass $n \in A$, also $\varphi(n) = N(n)$. Daraus folgt, dass $N(n) \in A$. Nach vollständiger Induktion erhalten wir $A = \mathbb{N}$ und somit $\varphi = N$. Damit haben wir gezeigt, dass $1 \in M$.

Für $m \in M$ wollen wir nun zeigen, das $N(m) \in M$. Wir definieren

$$\begin{aligned} N_{N(m)} : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto N_m(N(n)). \end{aligned}$$

Dann gilt

$$N_{N(m)}(1) = N_m(N(1)) = N(N_m(1)) = N(N(m))$$

und für $n \in \mathbb{N}$

$$N_{N(m)}(N(n)) = N_m(N(N(n))) = N(N_m(N(n))) = N(N_{N(m)}(n)),$$

also gibt es auch für $N(m)$ die geforderte Abbildung. Wir müssen noch zeigen, dass sie eindeutig ist. Sei dazu $\varphi : \mathbb{N} \to \mathbb{N}$ eine weitere Abbildung mit den geforderten Eigenschaften. Sei $A \subseteq \mathbb{N}$ die Menge aller natürlichen Zahlen n, so dass $\varphi(n) = N_m(n)$. Dann ist $1 \in A$ wegen $N_m(1) = N(m) = \varphi(m)$. Für $n \in N$ ist außerdem

$$N_m(N(n)) = N(N_m(n)) = N(\varphi(n)) = \varphi(N(n)),$$

weshalb auch $N(n) \in A$ gilt. Nach vollständiger Induktion folgern wir, dass $A = \mathbb{N}$. Daher gilt $N_m = \varphi$ und die Abbildung ist eindeutig.

Wir haben also gezeigt, dass es eine eindeutige Abbildung $N_{N(m)}$ mit den gewünschten Eigenschaften gibt. Das bedeutet, dass auch $N(m)$ in $\mathbb{N}$ enthalten ist. Nach dem Prinzip der vollständigen Induktion folgt daraus $M = \mathbb{N}$. Die Abbildung N_m ist also für alle $m \in \mathbb{N}$ eindeutig definiert. □

Um tatsächlich von der „Addition" zu sprechen, müssen wir noch zeigen, dass die Abbildung N_m aus Lemma 1.1 die üblichen Rechenregeln der Addition erfüllt.

Lemma 1.2. *Die Abbildung N_m hat die folgenden Eigenschaften für alle $m, n, k \in \mathbb{N}$:*

- $N_m(n) = N_n(m)$ *(Kommutativgesetz),*
- $N_k(N_m(n)) = N_m(N_k(n))$ *(Assoziativgesetz).*

Beweis. Übungsaufgabe. □

Wir erinnern uns daran, dass wir uns unter der Abbildung N_m die Vorschrift $n \mapsto m+n$ vorstellen. Nachdem wir Lemma 1.2 bewiesen haben, bekommen wir die Rechtfertigung dafür tatsächlich $m+n$ zu schreiben, da die Addition die altbekannten Regeln erfüllt und tatsächlich das tut, was wir von ihr erwarten.

Definition 1.3. Wir definieren die Addition

$$\begin{aligned}\mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N},\\ (m,n) &\longmapsto m+n := N_m(n).\end{aligned}$$

Mit dieser neuen Notation nehmen die Rechenregeln aus Lemma 1.2 die vertraute Form an:

- $m+n = n+m$ (Kommutativgesetz),
- $(m+n)+k = m+(n+k)$ (Assoziativgesetz).

Lemma 1.4. *Für jedes $m \in \mathbb{N}$ ist die Abbildung N_m injektiv. Das heißt, es gilt die Kürzungsregel*

$$n+m = k+m \qquad \Rightarrow \qquad n = k.$$

Beweis. Das folgt mit vollständiger Induktion aus der Injektivität von N. □

Mit der gleichen Herangehensweise können wir die Multiplikation definieren. Ebenso wie bei der Addition konstruieren wir zuerst für jede natürliche Zahl $m \in \mathbb{N}$ eine Abbildung M_m, unter der wir uns die Multiplikation mit m, also $n \mapsto mn$ vorstellen. Da wir die Addition schon definiert haben, können wir darin schon die etwas intuitiveren Notationen $N(n) = n+1$ und $N_m(n) = m+n$ verwenden.

Lemma 1.5. *Für jedes $m \in \mathbb{N}$ gibt es eine eindeutige Abbildung*

$$M_m : \mathbb{N} \longrightarrow \mathbb{N}$$

mit den folgenden Eigenschaften

- $M_m(1) = m$,
- $M_m(n+1) = M_m(n) + m$ *für alle* $n \in \mathbb{N}$.

Beweis. Übungsaufgabe. □

Wir können nun auch die Rechenregeln, die die Multiplikation betreffen, beweisen:

Lemma 1.6. *Die Abbildung M_m hat folgende Eigenschaften für $m,n,k \in \mathbb{N}$:*

- $M_m(n) = M_n(m)$ *(Kommutativgesetz),*
- $M_k(M_m(n)) = M_m(M_k(n))$ *(Assoziativgesetz),*
- $M_k(m+n) = M_k(m) + M_k(n)$ *(Distributivgesetz),*
- M_m *ist injektiv (Kürzungsregel).*

Definition 1.7. Wir definieren die Multiplikation

$$\begin{aligned}\mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N},\\ (m,n) &\longmapsto m \cdot n := mn := M_m(n).\end{aligned}$$

Das Kommutativ-, Assoziativ- und das Distributivgesetz nehmen mit dieser Definition die vertraute Form an und wir können ab jetzt wie gewohnt mit den natürlichen Zahlen rechnen. Auch gibt es für die Multiplikation eine Kürzungsregel, das heißt aus $mn = kn$ folgt $m = k$. Was uns noch fehlt ist die Möglichkeit natürliche Zahlen zu vergleichen, also zu sagen welche größer oder kleiner ist. Mithilfe der Addition ist dies aber nun ein leichtes:

Definition 1.8. Seien $m,n \in \mathbb{N}$ wir sagen, dass m kleiner als n ist (oder äquivalent n größer als m), falls es $k \in \mathbb{N}$ gibt mit $n = m+k$. In dem Fall schreiben wir $m < n$ oder $n > m$. Ist m kleiner oder gleich n, schreiben wir $m \leq n$ oder $n \geq m$.

Der Vergleich „$\leq$" definiert eine sogenannte Ordnungsrelation auf $\mathbb{N}$. Das bedeutet, dass die Eigenschaften aus dem folgenden Lemma erfüllt sind:

Lemma 1.9. *Es gilt für $m, n, k, \ell \in \mathbb{N}$:*

(i) aus $m \leq n$ und $n \leq m$ folgt $m = n$,
(ii) aus $m \leq n$ und $n \leq k$ folgt $m \leq k$ (Transitivität),
(iii) aus $m \leq n$ und $k \leq \ell$ folgt $m + k \leq n + \ell$.

Beweis. (ii) und (iii) folgen direkt mit den Rechenregeln der Addition. Um (i) zu zeigen nehmen wir an, dass $m \neq n$. Dann gibt es $k, k' \in \mathbb{N}$ mit

$$m + k = n, \qquad n + k' = m.$$

Daraus folgt

$$n = m + k = n + (k + k').$$

Damit wir die Kürzungsregel anwenden können, addieren wir noch auf beiden Seiten die Eins:

$$n + 1 = n + (k + k' + 1).$$

Nun folgt aus Lemma 1.4, dass $1 = k + k' + 1$. Aber 1 ist nach Peanoaxiomen kein Nachfolger einer natürlichen Zahl. Das führt zum Widerspruch, weshalb unsere Annahme $m \neq n$ falsch ist. □

Wir beenden diesen Abschnitt mit einem wichtigen Prinzip die natürlichen Zahlen betreffend.

Satz 1.10. *Jede nichtleere Teilmenge $A \subseteq \mathbb{N}$ hat ein kleinstes Element.*

Beweis. Angenommen $A \subseteq \mathbb{N}$ habe kein kleinstes Element. Wir definieren

$$M := \{m \in \mathbb{N} \mid n \notin A \ \forall n \leq m\}.$$

Dann ist $1 \in M$, denn andernfalls wäre 1 ein kleinstes Element von A. Für $m \in M$ ist auch $m + 1 \in M$, denn sonst wäre $m + 1$ ein kleinstes Element von A. Nach vollständiger Induktion ist $M = \mathbb{N}$. Daraus folgt aber, dass A die leere Menge ist. □

Dieses Prinzip können wir (in einem sehr einfachen Fall, wenn nämlich die Menge A endlich ist) anwenden um folgende Beobachtung zu machen:

Korollar 1.11. *Für $m, n \in \mathbb{N}$ gilt entweder $m \leq n$ oder $m > n$.*

Beweis. Die Menge $\{m, n\}$ hat nach Satz 1.10 ein kleinstes Element. Ist dieses gleich m, so erhalten wir $m \leq n$ und ist es gleich n, dann $n \leq m$. Im letzten Fall haben wir entweder $n = m$, dann gilt aber auch $m \leq n$ oder $m > n$. □

1.2. **Die ganzen Zahlen.** Aus den natürlichen Zahlen können wir die ganzen Zahlen $\mathbb{Z}$ konstruieren indem wir Differenzen bilden. Wir wollen also grob gesprochen Zahlen der Form $m - n$ für $n, m \in \mathbb{N}$ betrachten. So wäre beispielsweise $-1 = 3 - 2$ und $-2 = 5 - 7$. Diese Darstellungen sind allerdings nicht eindeutig bestimmt, da etwa $2 - 3 = 3 - 4$. Wir bekommen diesen Umstand in den Griff indem wir eine Äquivalenzrelation auf den Paaren (m, n) definieren:

Lemma 1.12. *Die Vorschrift*

$$(m, n) \sim (m', n') \qquad \Leftrightarrow \qquad m + n' = m' + n$$

definiert eine Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$.

Beweis. Übungsaufgabe. □

Definition 1.13. Wir definieren die *ganzen Zahlen* als

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim$$

Auf $\mathbb{Z}$ können wir nun durch

$$(m, n) + (m', n') := (m + m', n + n')$$

eine Addition definieren und durch

$$(m, n) \cdot (m', n') := (mm' + nn', mn' + nm')$$

eine Multiplikation, die die übrigen Rechenregeln erfüllen (Kommutativgesetz, Assoziativgesetz, Distributivgesetz). Natürlich müssten wir auch überprüfen, dass diese Definitionen unabhängig von der Wahl von Repräsentanten ist, also kompatibel mit der Äquivalenzrelation. Durch

$$\begin{aligned} \mathbb{N} &\longrightarrow \mathbb{Z} \\ n &\longmapsto (n, 0) \end{aligned}$$

erhalten wir eine Einbettung der natürlichen in die ganzen Zahlen, die mit Addition und Multiplikation vertauscht. Wir benutzen die Notationen $0 := (1, 1)$, $1 := (1, 0)$ und für $n \in \mathbb{N}$ schreiben wir (ein bisschen schlampig) $n := (n, 0)$ und $-n := (0, n)$. Für eine beliebige ganze Zahl (m, n) setzen wir $-(m, n) := (n, m)$. Es ist nicht schwierig nachzuweisen, dass $(\mathbb{Z}, +)$ die Struktur einer abelschen Gruppe trägt, wir wollen diesen Begriff jedoch an dieser Stelle nicht diskutieren. Ab jetzt betrachten wir die natürlichen Zahlen als Teilmenge der ganzen Zahlen. Wir machen noch folgende Beobachtung:

Lemma 1.14. *Sei $n \in \mathbb{Z}$. Dann ist entweder $n = 0$, $n \in \mathbb{N}$ oder $-n \in \mathbb{N}$.*

Beweis. Die Zahl n wird durch ein Paar (n_1, n_2) natürlicher Zahlen repräsentiert. Nach Korollar 1.11 gilt entweder $n_2 \leq n_1$ oder $n_2 > n_1$. Im ersten Fall ist entweder $n_1 = n_2$ und dann ist $(n_1, n_2) = 0$ oder es gibt $m \in \mathbb{N}$ mit $n_1 = n_2 + m$ und dann können wir den Repräsentanten folgendermaßen ändern:

$$(n_1, n_2) = (n_2 + m, n_2) \sim (m, 0)$$

und das liegt in $\mathbb{N}$. Andernfalls gibt es $m \in \mathbb{N}$ mit $n_2 = n_1 + m$ und

$$-(n_1, n_2) = (n_2, n_1) = (n_1 + m, n_1) = (m, 0) \in \mathbb{N}.$$

□

1.3. **Teilbarkeit.**

Definition 1.15. Seien a, b ganze Zahlen. Dann *teilt a die Zahl b*, wenn es $m \in \mathbb{Z}$ gibt, so dass

$$b = ma.$$

In diesem Fall schreiben wir $a|b$ und sagen auch, dass a ein *Teiler* von b ist und b ein *Vielfaches* von a.

Für die Teilbarkeit gelten die folgenden Rechenregeln:

Proposition 1.16. *Seien $a, b, c, d, x, y \in \mathbb{Z}$. Dann gilt:*

(i) aus $d|a$ folgt $d|ab$,
(ii) aus $d|c$ und $c|a$ folgt $d|a$,

(iii) *aus $d|a$ und $d|b$ folgt $d|xa + yb$,*
(iv) *aus $d|c$ folgt $c = 0$ oder $|d| \leq |c|$,*
(v) *aus $d|c$ und $c|d$ folgt $c = \pm d$.*

Hierbei haben wir in (iv) den Absolutbetrag benutzt, der wie üblich definiert ist durch:

$$|n| = \begin{cases} n & \text{falls } n \in \mathbb{N} \\ -n & \text{sonst.} \end{cases}$$

Beweis. (i), (ii) und (iii) folgen direkt aus den Definitionen. Für (v) braucht man noch zusätzlich die Kürzungsregel für die Multiplikation. Wir beweisen (iv): Nehmen wir an $d|c$ und $c \neq 0$. Dann ist auch $d \neq 0$. Wenn wir c und/oder d durch $-c$ beziehungsweise $-d$ ersetzen, ändert das weder die Teilbarkeitsrelation, noch die Beträge. Wir können somit annehmen, dass $c, d \in \mathbb{N}$. Nach Annahme gibt es $a \in \mathbb{N}$ mit $c = ad$. Ist $a = 1$, gilt $c = d$ und wir sind fertig. Falls $a > 1$, schreiben wir

$$c = (a-1)d + d.$$

Dann ist $a - 1 \neq 0$, also $(a-1)d \in \mathbb{N}$. Nach Definition der Ordnungsrelation ist dann $d \leq c$. □

Definition 1.17. Der *größte gemeinsame Teiler* zweier ganzer Zahlen m und n (nicht beide Null) ist die größte natürliche Zahl g, die Teiler sowohl von m als auch von n ist. Wir schreiben in dem Fall

$$g = \mathrm{ggT}(m, n).$$

Man beachte, dass diese Definition sinnvoll ist, in dem Sinne, dass es immer eine größte natürliche Zahl gibt, die m und n teilt. Das wird durch Proposition 1.16 (iv) sichergestellt.

Definition 1.18. Das *kleinste gemeinsame Vielfache* zweier ganzer Zahlen $m \neq 0$ und $n \neq 0$ ist die größte natürliche Zahl k, die Vielfaches sowohl von m als auch von n ist.

Dass diese Definition sinnvoll ist folgt aus Satz 1.10. Danach hat nämlich die Menge aller Vielfachen von m und n, die in $\mathbb{N}$ liegen, ein kleinstes Element.

Um den kleinsten gemeinsamen Teiler zu finden, kann man den euklidischen Algorithmus benutzen. Dieser arbeitet mit wiederholter Division mit Rest.

Proposition 1.19 (Division mit Rest)**.** *Seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Dann gibt es eindeutig bestimmte Zahlen $r, q \in \mathbb{Z}$ mit $r \in \{0, \ldots, |b| - 1\}$ derart, dass*

$$a = r + qb.$$

Beweis. Wir betrachten die Menge

$$M = \{a - qb \mid q \in \mathbb{Z}\} \cap \big(\mathbb{N} \cup \{0\}\big).$$

Enthält sie die Null, so ist b ein Teiler von a und wir erhalten die gewünschte Gleichung mit $r = 0$. Andernfalls haben wir $M \subseteq \mathbb{N}$ und nach Satz 1.10 hat M ein kleinstes Element r. Dann muss $r \leq |b| - 1$ gelten. Andernfalls wäre $r - b \in M$, was im Widerspruch zur Minimalität von r steht. Damit haben wir die gewünschten Zahlen r und q gefunden.

Um die Eindeutigkeit zu zeigen nehmen wir an, dass wir $r_1, r_2 \in \{0, \ldots, |b| - 1\}$ und q_1, q_2 vorliegen haben mit

$$r_1 + q_1 b = r_2 + q_2 b \quad \Leftrightarrow \quad r_2 - r_1 = (q_1 - q_2)b.$$

Nach Annahme ist $r_2 - r_1 \in \{-|b|+1, \ldots, |b|-1\}$ und nach obiger Gleichung außerdem durch b teilbar. Nach Proposition 1.16 (iv) ist damit die einzige Möglichkeit $r_2 - r_1 = 0$, also $r_1 = r_2$. Aus der Kürzungsregel für die Multiplikation folgt dann $q_1 = q_2$. □

Wir sind nun bereit für den *euklidischen Algorithmus*. Dabei geht man wie folgt vor. Gegeben seien zwei natürliche Zahlen m und n.

- Zu Beginn setzen wir $x_0 := m$ und $x_1 := n$.
- Nehmen wir an für ein $i \in \mathbb{N}$ seien $x_0, x_1, x_2, \ldots, x_{i-1}$ bereits konstruiert. Durch Division mit Rest können wir schreiben

$$x_{i-2} = x_i + x_{i-1}a_i \tag{1}$$

  für nichtnegative ganze Zahlen x_i und a_i mit $x_i < x_{i-1}$.

Schauen wir uns die Definition des Algorithmus an, so springen folgende Beobachtungen ins Auge:

- Ist k ein Teiler von x_i und x_{i-1}, so teilt k alle weiteren x_j. Insbesondere folgt daraus
$$\mathrm{ggT}(x_i, x_{i-1}) = \mathrm{ggT}(m, n).$$
- Wegen der Bedingung $x_i < x_{i-1}$ gelangt man nach endlich vielen Schritten zu einem $i \in \mathbb{N}$ mit $x_i = 0$.

Wir schauen uns nun die Stelle i_0 an, für die gilt $x_{i_0+1} = 0$, aber $x_i > 0$ für $i \leq i_0$:

$$\begin{aligned} x_{i_0-2} &= x_{i_0} + x_{i_0-1}a_{i_0}, \\ x_{i_0-1} &= x_{i_0}a_{i_0+1} \end{aligned}$$

und $x_{i_0} > 0$. Wir behaupten, dass $g := x_{i_0}$ der größte gemeinsame Teiler von m und n ist. Wegen $x_{i_0-1} = x_{i_0}a_{i_0+1}$, ist g ein Teiler von x_{i_0-1} und x_{i_0}. Deshalb teilt g alle x_i's, insbesondere m und n. Gäbe es einen größeren Teiler g' von m und n, so müsste g' auch $x_{i_0} = g$ teilen, was im Widerspruch zu $g' > g$ steht.

Der euklidische Algorithmus liefert zusammen mit dem größten gemeinsamen Teiler g auch noch einen äußerst nützlichen Zusammenhang zwischen m, n und g:

Lemma 1.20. *Seien m und n zwei ganze Zahlen (nicht beide Null) mit größtem gemeinsamen Teiler g. Dann gibt es ganze Zahlen a und b, so dass*

$$g = am + bn.$$

Beweis. Falls eine oder beide der ganzen Zahlen m und n negativ sind, ersetzen wir sie durch $-m$ beziehungsweise $-n$. Dadurch können wir annehmen, dass $m, n \in \mathbb{N}$ und müssen am Ende nur eventuell a durch $-a$ und/oder b durch $-b$ ersetzen. Wir betrachten die natürlichen Zahlen x_i, die wie oben durch den euklidischen Algorithmus bestimmt werden. Wenn wir die definierenden Gleichungen (1) etwas umstellen, erhalten wir

$$\begin{aligned} x_2 &= x_0 - x_1a_2 \\ x_3 &= x_1 - x_2a_3 \\ &\vdots \\ x_{i_0-1} &= x_{i_0-3} - x_{i_0-2}a_{i_0-1}, \\ x_{i_0} &= x_{i_0-2} - x_{i_0-1}a_{i_0}. \end{aligned}$$

Außerdem wissen wir, dass $g = x_{i_0}$. Diese Gleichungen können wir nun sukzessive ineinander einsetzen:

$$\begin{aligned} g = x_{i_0} &= x_{i_0-2} - x_{i_0-1}a_{i_0} \\ &= x_{i_0-2}(1 + a_{i_0-1}) - x_{i_0-3}a_{i_0}. \\ &\vdots \end{aligned}$$

Wir erhalten eine Gleichung der Form

$$g = x_{i_0} = ax_0 + bx_1 = am + bn$$

für ganze Zahlen a, b. □

2. Primzahlen

Die grundlegenden Bausteine in der Zahlentheorie sind die Primzahlen. Jede natürliche Zahl kann durch Primfaktorzerlegung eindeutig als Produkt von Primzahlen geschrieben werden. Wir werden im Laufe der Vorlesung sehen, dass sie auch in vielen weiteren Aspekten eine wichtige Rolle spielen.

2.1. **Primfaktorzerlegung.** Wir wollen uns den Umstand, dass man jede natürliche Zahl eindeutig in ihre Primfaktoren zerlegen kann, genauer anschauen. Insbesondere wollen wir einen formalen Beweis dafür geben. Zunächst definieren wir die wichtigsten Objekte dieser Vorlesung:

Definition 2.1. Eine *Primzahl* ist eine natürliche Zahl $p > 1$, deren einzige positive Teiler 1 und p selbst sind.

Nun könnte man sich fragen, warum die 1 keine Primzahl sein soll. Schließlich erfüllt sie die definierende Eigenschaft auch. Strukturell ist aber die Natur der 1 sehr anders geartet als die der Primzahlen. Zusammen mit der -1 bildet sie die *Einheiten* der ganzen Zahlen $\mathbb{Z}$, das heißt, man kann durch 1 und -1 auch teilen. Will man nun eine ganze Zahl $n \in \mathbb{Z}$ in ihre Primfaktoren zerlegen, so ermittelt man welche Primzahlen n teilen und mit welcher Potenz. Die Frage aber, mit welcher Potenz die 1 in der Primfaktorzerlegung vorkommt, ist sinnbefreit. Sie kommt in jeder beliebigen Potenz vor, weil sie eine Einheit ist.

Der erste Schritt zur Primfaktorzerlegung besteht darin einen Primteiler zu finden. Wir erinnern uns, dass ein *Teiler* einer ganzen Zahl n eine ganze Zahl k ist, so dass $a \in \mathbb{Z}$ existiert mit $ak = n$. Ist a darüber hinaus eine Prinzahl, so nennen wir a einen *Primteiler* von n.

Lemma 2.2. *Sei $n > 1$ eine natürlich Zahl. Dann hat n einen Primteiler.*

Beweis. Wir argumentieren per Induktion über n. Für $n = 2$ ist 2 ein Primteiler. Nehmen wir nun an, dass alle natürlichen Zahlen k mit $1 < k < n$ einen Primteiler besitzen. Wir wollen uns davon überzeugen, dass dann auch n einen Primteiler besitzt. Ist n eine Primzahl, so ist n selbst ein Primteiler von n. Andernfalls hat n einen Teiler k mit $1 < k < n$. Nach Induktionsannahme besitzt k einen Primteiler p. Dann ist p aber auch ein Primteiler von n. □

Mithilfe von Lemma 1.20 können wir eine äquivalente Charakterisierung von Primzahlen geben, die nützlich sein wird, wenn wir die Eindeutigkeit der Primfaktorzerlegung beweisen werden.

Proposition 2.3. *Eine natürliche Zahl $p > 1$ ist eine Primzahl genau dann, wenn für alle ganzen Zahlen m und n, so dass p das Produkt mn teilt, schon $p|m$ oder $p|n$ gilt.*

Beweis. Angenommen p erfüllt die Eigenschaft aus der Aussage des Lemmas. Wir wollen zeigen, dass p prim ist. Sei $m \in \mathbb{N}$ ein Teiler von p, das heißt, es gibt eine natürliche Zahl n, so dass $p = mn$. Insbesondere teilt p das Produkt mn. Nach Annahme gibt es nun zwei Fälle: $p|m$ oder $p|n$. Im ersten Fall gibt es $a \in \mathbb{N}$, so dass $m = ap$. Daraus folgt

$$p = mn = anp,$$

Da $p \neq 0$, folgt aus der Kürzungsregel für die Multiplikation, dass $an = 1$. Daher muss $a = n = 1$ gelten und somit $m = p$. Im zweiten Fall argumentiert man genauso und erhält $m = 1$ (und $n = p$). Die einzigen Teiler von p sind also 1 und p.

Für die umgekehrte Implikation nehmen wir an, p sei eine Primzahl. Seien $m, n \in \mathbb{N}$, so das p das Produkt mn teilt. Der größte gemeinsame Teiler von p und m ist ein Teiler von p, also entweder gleich p oder gleich 1, weil p eine Primzahl ist. Im ersten Fall ist p ein Teiler von m und wir sind fertig. Im zweiten Fall finden wir nach Lemma 1.20 ganze Zahlen a und b, so dass

$$1 = am + bp.$$

Damit können wir zeigen, dass p ein Teiler von n ist:

$$n = n \cdot 1 = n(am + bp) = a(nm) + bp.$$

Offensichtlich teilt p den Summanden bp. Nach Annahme teilt p aber auch (nm) und somit teilt p die ganze Summe. Daraus folg $p|n$. □

Proposition 2.4 (eindeutige Primfaktorzerlegung)**.** *Jede natürliche Zahl m besitzt eine bis auf Permutation der Primzahlen eindeutige Primfaktorzerlegung*

$$m = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$$

für $k \in \mathbb{N} \cup \{0\}$, paarweise verschiedene Primzahlen $p_1, \ldots, p_k$ und natürliche Zahlen $r_1, \ldots, r_k$. (Für $k = 0$ betrachten wir das leere Produkt, das ist per Definition gleich 1).

Beweis. Wir führen den Beweis per Induktion über m. Für $m = 1$ ist nichts zu zeigen. Nehmen wir also an, dass jede natürliche Zahl kleiner m eine eindeutige Primfaktorzerlegung hat. Wir zeigen zunächst die Existenz einer Primfaktorzerlegung. Mithilfe von Lemma 2.2 finden wir eine Primzahl p, die m teilt. Das heißt

$$m = pn$$

für eine natürliche Zahl $n < m$. Nach Induktionsannahme hat n eine Primfaktorzerlegung

$$n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$$

Ist p verschieden von den Primzahlen $p_1, \ldots, p_k$, so ist

$$m = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k} p$$

eine Primfaktorzerlegung von m. Ist $p = p_i$ für ein $i \in \{1, \ldots, k\}$ so ist

$$m = p_1^{r_1} \cdot \ldots \cdot p_i^{i+1} \cdot \ldots \cdot p_k^{r_k}$$

eine Primfaktorzerlegung.

Wir müssen noch zeigen, dass Primfaktorzerlegungen eindeutig sind. Seien

$$p_1^{r_1} \cdot \ldots \cdot p_k^{r_k} = m = q_1^{s_1} \cdot \vdots \cdot q_h^{s_h}$$

zwei Primfaktorzerlegungen. Dann teilt p_1 das Produkt

$$q_1^{s_1} \cdot \ldots \cdot q_h^{s_h}.$$

Nach mehrmaliger Anwendung von Proposition 2.3 folgt daraus, dass p_1 eine der Primzahlen q_i teilt. Nach Umsortieren können wir annehmen, das $i = 1$, also $p_1|q_1$. Es muss dann $p_1 = q_1$ gelten, da q_1 als Primzahl nur die Teiler 1 und q_1 hat und $p_1 > 1$ ist.

Wir behaupten, dass auch die Exponenten r_1 und s_1 gleich sein müssen. Je nachdem ob $r_1 \geq s_1$ oder $r_1 \leq s_1$ können wir daher auf beiden Seiten einen Faktor $p1^{s_1} = q_1^{s_1}$ beziehungsweise $p_1^{r_1} = q_1^{r_1}$ kürzen. Ohne Beschränkung der Allgemeinheit nehmen wir an $r_1 \geq s_1$. Dann erhalten wir

$$p_1^{r_1 - s_1} p_2^{r_2} \cdots p_k^{r_k} = m/p_1^{s_1} = q_2^{s_2} \cdots q_h^{s_h}.$$

Ist $h = 1$, so ist das Produkt auf der rechten Seite leer, also gleich 1. Daraus folgt, dass auf der linken Seite insbesondere $r_1 = r_2$ gelten muss, da ansonsten p_1 die 1 teilen würde. Ist $h \geq 2$ und wäre $r_1 > s_1$, könnten wir das obige Argument nochmal führen um zu folgern, dass $p_1 = q_i$ für ein $i \in \{2, \ldots, h\}$. Aber da $p_1 = q_1$ und die Primzahlen q_i paarweise verschieden sind, ist dies nicht möglich. Es gilt also $r_1 = s_1$ und wir haben folgende Gleichheit von Primfaktorzerlegungen

$$p_2^{r_2} \cdots p_k^{r_k} = m/p_1^{r_1} = q_2^{s_2} \cdots q_h^{s_h}.$$

Da $m/p_1^{r_1} < m$, ist die obige Primfaktorzerlegung eindeutig nach Induktionsannahme. Es gilt also (nach Umsortieren):

$$\begin{aligned} k &= h \\ r_i &= s_i \quad \forall\ i = 2, \ldots, k \\ p_i &= q_i \quad \forall\ i = 2, \ldots, k. \end{aligned}$$

Somit ist auch die Primfaktorzerlegung von m eindeutig. □

2.2. **Unendlich viele Primzahlen.** Dass es unendlich viele Primzahlen gibt, ist schon seit mehr als 2000 Jahren bekannt. Der berühmteste Beweis dafür stammt von Euklid:

Satz 2.5. *Es gibt unendlich viele Primzahlen.*

Beweis. Nehmen wir an, es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_r$. Wir betrachten die natürliche Zahl

$$n = p_1 \cdot \ldots \cdot p_r + 1.$$

Nach Lemma 2.2 hat n einen Primteiler p. Nach Annahme ist p identisch mit einer der Primzahlen $p_1, \ldots, p_r$. Daher teilt p sowohl das Produkt $p_1 \cdot \ldots \cdot p_r$ als auch n. Dann muss p aber auch $1 = n - p_1 \cdot \ldots \cdot p_r$ teilen, was unmöglich ist. □

Im Laufe der Jahrhunderte wurden viele weitere Beweise dafür gefunden, dass es unendlich viele Primzahlen gibt. Sie benutzen auf den ersten Blick sehr unterschiedliche Techniken. Oft jedoch ist darin die eindeutige Primfaktorzerlegung versteckt. Wir schauen uns im Folgenden einige von ihnen an und machen uns klar wo die Primfaktorzerlegung eingeht.

Beweis von Euler. Wir nehmen wieder an, es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_r$. Dann berechnen wir das endliche Produkt

$$\prod_{i=1}^{r} \frac{1}{1 - 1/p_i}.$$

Die einzelnen Faktoren sind die Grenzwerte der geometrischen Reihe zu $1/p_i$:

$$\sum_{m=1}^{\infty} \left(\frac{1}{p_i}\right)^m = 1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \ldots = \frac{1}{1 - 1/p_i}.$$

Setzen wir das in das Produkt ein und multiplizieren aus, erhalten wir

$$\prod_{i=1}^{r} \frac{1}{1-1/p_i} = \prod_{i=1}^{r} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \ldots\right) \tag{2}$$

$$= \sum_{m_1=1}^{\infty} \cdots \sum_{m_r=1}^{\infty} \frac{1}{p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}}. \tag{3}$$

Nach Proposition 2.4 hat jede natürliche Zahl eine eindeutige Primfaktorzerlegung. Da $p_1, \ldots, p_r$ alle Primzahlen umfasst, können wir also jede natürliche Zahl n eindeutig in der Form

$$n = p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$$

mit $m_i \in \mathbb{N} \cup \{0\}$ schreiben. In der Summe in (2) über alle $(m_1, \ldots, m_r) \in (\mathbb{N} \cup \{0\})^r$ durchläuft $p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$ daher gerade alle natürlichen Zahlen. Das Produkt ist also gleich der harmonischen Reihe:

$$\prod_{i=1}^{r} \frac{1}{1-1/p_i} = \sum_{n=1}^{\infty} \frac{1}{n}. \tag{4}$$

Wir wissen aber aus der Analysis, dass die harmonische Reihe divergiert, was nicht sein kann, da das Produkt auf der linken Seite endlich ist. □

In Eulers Beweis taucht schon eine Andeutung zu Zetafunktionen auf, die wir später behandeln werden. Die Riemannsche Zetafunktion ist für eine komplexe Zahl s mit Realteil $\Re(s) > 1$ definiert als

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Die Bedingung an den Realteil von s wird gebraucht um zu zeigen, dass die Reihe konvergiert: Wir schreiben $s = s_1 + is_2$ mit $s_1, s_2 \in \mathbb{R}$ und $s_1 > 1$. Dann haben wir folgende Abschätzung

$$\left|\frac{1}{n^s}\right| = \frac{1}{|\exp(s \log n)|} = \frac{1}{|\exp(s_1 \log n + is_2 \log n)|} = \frac{1}{\exp(s_1 \log n)} = \frac{1}{n^{s_1}}.$$

Für $s_1 > 1$ konvergiert die Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n^{s_1}}$$

und liefert eine Majorante für $\zeta(s)$. Die Formel (4) ergibt keinen Sinn (wir haben gezeigt, dass sie einen Widerspruch produziert). Wenn wir aber nun auf der rechten Seite über $1/n^s$ für $\Re(s) > 1$ summieren und auf linken Seite das Produkt über alle (unendlich viele) Primzahlen mit entsprechend modifizierten Faktoren nehmen, so erhalten wir mit der gleichen Rechnung die Produktformel

$$\prod_{p \text{ prim}} \frac{1}{1-p^{-s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Da das Produkt nun über unendlich viele Primzahlen läuft, muss man sich beim Beweis allerdings noch zusätzlich Gedanken über Konvergenz machen.

Wir schauen uns nun noch einen weiteren Beweis für die Unendlichkeit der Menge der Primzahlen an, der mit Topologie arbeitet. Er stammt von Fürstenberg aus dem Jahr 1955.

Beweis von Fürstenberg. Wir definieren auf den ganzen Zahlen wie folgt eine Topologie. Für $a, m \in \mathbb{Z}$ betrachen wir die Teilmengen

$$B_m(a) := a + m\mathbb{Z} = \{a + mb \mid b \in \mathbb{Z}\}.$$

Wir nennen diese Teilmenge einen Ball. Tatsächlich kann man mit einer geeigneten Metrik $B_m(a)$ interpretieren als Ball um a vom Radius $1/m$. Das heißt, je größer m, desto kleiner der Ball. Man kann zeigen, dass der Schnitt von $B_m(a)$ und $B_n(b)$ genau dann nicht leer ist, wenn $\mathrm{ggT}(m, n)|(a - b)$ und in diesem Fall

$$B_m(a) \cap B_n(b) = B_k(c),$$

wobei $k = \mathrm{kgV}(m, n)$ und $c \in \mathbb{Z}$, so dass $c \cdot \mathrm{ggT}(m, n) = a - b$. Dafür braucht man den chinesischen Restsatz, den wir später beweisen werden.

Insbesondere folgt, dass der Schnitt zweier Bälle entweder leer oder wieder ein Ball ist. Daher bilden die Bälle die Basis einer Topologie. Darin ist eine Teilmenge $U \subseteq \mathbb{Z}$ genau dann offen, wenn es für jedes $a \in U$ ein $m \in \mathbb{Z}$ gibt mit $B_m(a) \subseteq U$. Da die Bälle unendliche Kardinalität haben, ist jede nichtleere offene Teilmenge von $\mathbb{Z}$ unendlich. Die Bälle sind per Konstruktion offen. Wir wollen uns nun davon überzeugen, dass sie auch abgeschlossen sind. Für $m \in \mathbb{Z}$ folgt

$$\mathbb{Z} = \bigcup_{a=0}^{|m|-1} B_m(a)$$

aus der Division durch m mit Rest (Proposition 1.19). Aus der Eindeutigkeit der Division mit Rest folgt, dass die Bälle $B_m(a)$ disjunkt sind. Jeden Ball $B_m(b)$ kann man mithilfe der Division mit Rest mit $B_m(a)$ für ein $a \in \{0, \ldots, |m| - 1\}$ identifizieren. Dieser ist das Komplement der offenen Bälle $B_m(a')$ für $a' \neq a$ (und $a' \in \{0, \ldots, |m| - 1\}$), also abgeschlossen.

Nehmen wir nun an es gäbe es nur endlich viele Primzahlen $p_1, \ldots, p_r$. Wir behaupten, dass dann

$$\mathbb{Z} \setminus \bigcup_{i=1}^{r} B_{p_i}(0) = \{1, -1\}.$$

Hierzu machen wir die Beobachtung,dass $B_{p_i}(0)$ genau aus den Zahlen besteht, die durch p_i teilbar sind. Da jede ganze Zahl außer ± 1 einen Primteiler hat (Lemma 2.2), folgt die obige Identität. Andererseits wissen wir, dass die Bälle $B_{p_i}(0)$ abgeschlossen sind, also muss $\{1, -1\}$ offen sein. Aber alle nichtleeren offenen Mengen sind unendlich, Widerspruch. □

2.3. **Primzahlzwillinge.** Wir wissen nun, dass es unendlich viele Primzahlen gibt. Jetzt könnte man sich fragen, wie diese verteilt sind. Intuitiv gibt es anteilig immer weniger Primzahlen, je größer die Zahlen werden, oder anders ausgedrückt, der Abstand zwischen den Primzahlen wird immer größer. Tatsächlich kann man auch beweisen, dass die

Lücken zwischen den Primzahlen beliebig groß werden können: Wir schreiben dafür alle Primzahlen in aufsteigender Ordnung in eine Liste:

$$p_1 < p_2 < p_3 < p_4 < \dots,$$

also

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \dots$$

Proposition 2.6. *Es gibt beliebig lange Lücken in der Folge der Primzahlen $(p_i)_{i\in\mathbb{N}}$, das heißt*

$$\limsup_{i\in\mathbb{N}}(p_{i+1} - p_i) = \infty.$$

Beweis. Wir zeigen, dass es für jede natürliche Zahl $n \geq 2$ eine Primzahl p_i gibt, so dass

$$p_{i+1} - p_i \geq n.$$

Daraus folgt das Resultat, da dann die Folge $(p_{i+1} - p_i)_{i\in\mathbb{N}}$ nicht beschränkt sein kann.

Wir überzeugen uns zunächst davon, dass es keine Primzahlen im Intervall $[n!+2, n!+n]$ gibt. Wir haben für $k \in \{2, \dots, n\}$ die Faktorisierung

$$n! + k = k\left(\frac{n!}{k} + 1\right) = k(1 \cdot 2 \cdot \ldots \cdot (k-1) \cdot (k+1) \cdot \ldots (n-1) \cdot n + 1).$$

Also teilt k die Zahl $n! + k$. Aber k ist weder gleich 1 noch gleich $n! + k$. Deshalb kann $n! + k$ keine Primzahl sein.

Sei nun p_i die größte Primzahl kleiner oder gleich $n! + 1$. Da alle Zahlen im Intervall $[n! + 2, n! + n]$ keine Primzahlen sind, ist p_{i+1} größer oder gleich $n! + n + 1$. Für die Differenz gilt also

$$p_{i+1} - p_i \geq (n! + n + 1) - (n! + 1) = n.$$

□

Es ist jedoch eine offene Frage, ob auch beliebig kleine Lücken unendlich oft vorkommen. Die Differenz zwischen 3 und 2 ist 1. Für alle weiteren Primzahlen ist die Differenz aber mindestens 2, da alle Primzahlen größer 2 ungerade sind. Zwei Primzahlen, deren Differenz gleich 2 ist, nennt man *Primzahlzwillinge*. Das wären also

$$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (41,43),\ (71,73), \dots$$

Man vermutet, dass es unendlich viele solcher Primzahlzwillinge gibt. Bewiesen ist das allerdings nicht. Mit dem Computer kann man nach Primzahlzwillingen suchen. Die bis jetzt größten bekannten Primzahlzwillinge sind

$$2996863034895 \cdot 2^{1290000} \pm 1.$$

Das sind sehr große Zahlen, die Suche ist sehr aufwändig und bringt uns natürlich nicht weiter bei der Suche eines Beweises. Man kann die Vermutung, dass es unendlich viele Primzahlzwillinge gibt, umformulieren zu der Vermutung, dass

$$\liminf_{i\in\mathbb{N}}(p_{i+1} - p_i) = 2.$$

Ein erster Schritt wäre zu zeigen, dass der lim inf überhaupt endlich ist. Das ist tatsächlich schon gelungen und es wurde auch eine obere Schranke gefunden:

Satz 2.7 (Maynard, Tao 2013)**.** *Es gibt unendlich viele $i \in \mathbb{N}$ mit $p_{i+1} - p_i \leq 600$, also*

$$\liminf_{i\in\mathbb{N}}(p_{i+1} - p_i) \leq 600.$$

Von 600 zu 2 ist es allerdings noch ein langer Weg und scheint auch mit heutigen Methoden nicht erreichbar zu sein.

3. Kongruenzen

3.1. **Restklassenringe.** Seien $a, b, m \in \mathbb{Z}$ Wir sagen, dass a *kongruent zu* b *modulo* m ist, geschrieben

$$a \equiv b \mod m,$$

falls $m|(b-a)$. Anders ausgedrückt ist das genau dann der Fall, wenn es $k \in \mathbb{Z}$ gibt mit

$$b = a + km.$$

Lemma 3.1. *Die Relation auf Z*

$$a \sim b \quad \Leftrightarrow \quad a \equiv b \mod m$$

ist eine Äquivalenzrelation.

Wir definieren

$$\mathbb{Z}/m\mathbb{Z} := \mathbb{Z}/\sim$$

als die Menge der Äquivalenzklassen. Diese Äquivalenzklassen werden auch als *Restklassen* modulo m bezeichnet. Wir schreiben

$$[a]_m = \{a + km \mid k \in \mathbb{Z}\}$$

für die Restklasse von a modulo m. Wenn es keine Verwechslungsgefahr gibt, sparen wir uns das m in der Notation und schreiben nur $[a]$.

Lemma 3.2. *Durch*

$$[a] + [b] := [a + b]$$
$$[a] \cdot [b] := [ab]$$

werden wohldefinierte Operationen $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *definiert, die das Kommutativ-, Assoziativ-, und Distributivgesetz erfüllen. Außerdem gibt es für jedes* $[a] \in \mathbb{Z}/m\mathbb{Z}$ *ein additives Inverses* $-[a]$*, das heißt es gilt*

$$[a] + (-[a]) = 0 = [0].$$

Beweis. Seien $a, b \in \mathbb{Z}$. Wir müssen zeigen, dass $[a + b]$ und $[ab]$ nicht von der Wahl der Repräsentanten a und b abhängen. Wir wählen also andere Repräsentanten $a' \equiv a \mod m$ und $b' \equiv b \mod m$. Das bedeutet, dass es $k, n \in \mathbb{Z}$ gibt mit

$$a' = a + km, \qquad b' = b + nm.$$

Dann gilt

$$a' + b' = a + km + b + nm = a + b + (k + n)m \equiv a + b \mod m$$

und

$$a'b' = (a + km)(b + nm) = ab + (an + bk + knm)m \equiv ab \mod m.$$

Kommutativ-, Assoziativ-, und Distributivgesetz folgen direkt aus den jeweiligen Gesetzen auf $\mathbb{Z}$. Das additive Inverse zu $[a]$ ist $[-a]$, denn

$$[a] + [-a] = [a - a] = [0] = 0.$$

□

Beim Betrachten von Lemma 3.2 scheinen auf $\mathbb{Z}/m\mathbb{Z}$ die gleichen Rechenregeln zu gelten wie auf $\mathbb{Z}$. Präzise kann man das formulieren durch die Feststellung, dass sowohl $\mathbb{Z}$ als auch $\mathbb{Z}/m\mathbb{Z}$ *kommutative Ringe* sind. Wenn wir uns die Multiplikation anschauen, entdecken wir aber neue Phänomene, die für $\mathbb{Z}$ nicht auftreten:

- $[2]_6 \cdot [3]_6 = [6]_6 = [0]_6$, aber $[2]_6, [3]_6 \neq 0$. Das heißt, $\mathbb{Z}/6\mathbb{Z}$ hat *Nullteiler*.
- Es gilt $[1]_8^2 = [3]_8^2 = [5]_8^2 = [7]_8^2 = 1$. Das heißt, die quadratische Gleichung $x^2 = 1$ hat in $\mathbb{Z}/8\mathbb{Z}$ vier Lösungen. In $\mathbb{Z}$ haben quadratische Gleichungen maximal zwei Lösungen.

Wir wollen im folgenden das Phänomen der Nullteiler genauer untersuchen. Damit keine Missverständnisse entstehen definieren wir, was wir unter einem Nullteiler verstehen:

Definition 3.3. Ein *Nullteiler* in einem kommutativen Ring R ist ein Element $a \in R$, so dass es $b \in R$ gibt mit $b \neq 0$, so dass $ab = 0$. Ist 0 der einzige Nullteiler, so heißt der Ring *nullteilerfrei*.

Wegen der Kürzungsregel für die Multiplikation ist $\mathbb{Z}$ nullteilerfrei. Die Ringe $\mathbb{Z}/m\mathbb{Z}$ haben jedoch im Allgemeinen nichttriviale Nullteiler.

Lemma 3.4. *$[a]$ ist genau dann ein Nullteiler von $\mathbb{Z}/m\mathbb{Z}$, wenn $\mathrm{ggT}(a, m) \neq 1$. Insbesondere ist $\mathbb{Z}/m\mathbb{Z}$ genau dann nullteilerfrei, wenn m eine Primzahl ist.*

Beweis. Wir nehmen an, dass $g := \mathrm{ggT}(a, m) \neq 1, m$ und wollen zeigen, dass $[a]$ ein Nullteiler ist. Dann gibt es $r, s \in \mathbb{Z}$ mit

$$a = rg, \qquad m = sg.$$

Da $g \neq m$, haben wir $[a] \neq 0$. Da $g \neq 1$, haben wir $[s] \neq 0$. Für das Produkt gilt

$$[a][s] = [as] = [rgs] = [rm] = 0,$$

also ist $[a]$ ein Nullteiler.

Für die Rückrichtung nehmen wir an, dass $[a]$ ein Nullteiler ist. Dann ist a nicht durch m teilbar und es gibt $b \in \mathbb{Z}$ so dass $[a][b] = 0$ und $[b] \neq 0$. Per Definition bedeutet das, dass b nicht durch m teilbar ist und es $r \in \mathbb{Z}$ gibt mit

$$ab = rm.$$

Wir können nun die Primfaktorzerlegungen auf beiden Seiten vergleichen. Sei

$$m = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$$

die Primfaktorzerlegung von m.Das heißt, es gibt eine Addition, durch die $\mathbb{Z}$ beziehungsweise $\mathbb{Z}/m\mathbb{Z}$ eine abelsche Gruppe wird und eine kommutative Multiplikation, die

Da m nicht b teilt, muss es ein $i \in \{1, \ldots, k\}$ geben, so dass p_i in der Primfaktorzerlegung von b in niedrigerer Potenz vorkommt als $p_i^{r_i}$. Dann muss p_i aber a teilen damit die Primfaktorzerlegung auf beiden Seiten die gleiche ist. Somit ist p_i ein Teiler von a und von m und der größte gemeinsame Teiler g von m und a ist nicht 1. Außerdem ist $g \neq m$, da wir $[a] \neq 0$ angenommen haben. □

Definition 3.5. Für einen kommutativen Ring R definieren wir

$$R^\times := \{a \in R \mid \exists b \in R \text{ mit } ab = 1\}.$$

Ausgestattet mit der Multiplikation ist $R^\times$ eine abelsche Gruppe, genannt die *Einheitengruppe*, oder kurz *Einheiten*.

Lemma 3.6. *Es gilt*

(i) $\mathbb{Z}^\times = \{1, -1\}$,

(ii) $(\mathbb{Z}/m\mathbb{Z})^\times := \{[a] \in \mathbb{Z}/m\mathbb{Z} \mid \mathrm{ggT}(a, m) = 1\}$.

Beweis. Um (i) zu zeigen betrachten wir $a, b \in \mathbb{Z}$ mit $ab = 1$. Insbesondere gilt $a|1$ und daraus folgt nach Proposition 1.16 (iv), dass $|a| \leq 1$. Das ist nur erfüllt für $a = \pm 1$ oder $a = 0$, aber $0 \cdot b = 0$, also $a \neq 0$. Umgekehrt sind 1 und -1 Einheiten, da $1 \cdot 1 = 1$ und $(-1)(-1) = 1$.

Für (ii) betrachten wir $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$, so dass $[a][b] = 1$ und wollen zeigen, dass $\mathrm{ggT}(a, m) = 1$. Es gibt also $r \in \mathbb{Z}$ mit

$$ab = 1 + rm.$$

Dann muss aber $\mathrm{ggT}(a, m) = 1$ sein, da jeder gemeinsame Teiler von a und m auch $1 = ab - rm$ teilt. Andersherum wollen wir zeigen, dass für $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$ das Element $[a]$ eine Einheit ist. Nach Lemma 1.20 gibt es $b, c \in \mathbb{Z}$ mit

$$ab + mc = 1.$$

Es gilt folglich

$$[a][b] = 1$$

und $[a]$ ist eine Einheit. □

Kombinieren wir die Informationen aus Lemma 3.4 und Lemma 3.6, so erkennen wir, dass die Elemente von $\mathbb{Z}/m\mathbb{Z}$ entweder Nullteiler oder Einheiten sind. Das ist nicht in jedem Ring der Fall. In $\mathbb{Z}$ ist nur die 0 ein Nullteiler und nur 1 und -1 sind Einheiten. Alle anderen Elemente sind weder Nullteiler noch Einheiten.

Schauen wir uns insbesondere $\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p an. Nach Lemma 3.4 ist $\mathbb{Z}/p\mathbb{Z}$ nullteilerfrei und somit sind nach Lemma 3.6 alle Elemente ungleich Null Einheiten. Das bedeutet gerade, dass $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist.

Definition 3.7. Wir schreiben

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$

für den Körper mit p Elementen.

3.2. **Der Chinesische Restsatz.** Wir wollen in diesem Abschnitt Fragestellungen von folgendem Typ lösen: Gibt es eine natürliche Zahl, die kongruent 2 modulo 5 und kongruent 3 modulo 7 ist? Hier wäre 17 eine Lösung. Aber auch 52 erfüllt die beiden Kongruenzen. Es gibt also mehrere Lösungen und es stellt sich die Frage, ob man alle beschreiben kann. Andererseits gibt es auch derartige Aufgabenstellungen, die keine Lösung haben. Beispielsweise gibt es keine natürliche Zahl, die 3 modulo 6 und 4 modulo 15 ist. Das liegt daran, dass alle Zahlen kongruent 3 modulo 6 durch 3 teilbar sein müssen. Es gibt aber keine Zahl, die kongruent 4 modulo 15 ist und durch 3 teilbar.

Wir wollen das Problem nun systematisch angehen. Das Resultat, das die Lösung solcher Kongruenzgleichungen beschreibt, heißt *Chinesischer Restsatz*. Um ihn zu formulieren und zu beweisen müssen dafür aber noch etwas Vorarbeit leisten.

Lemma 3.8. *Seien m und n natürliche Zahlen, so dass m ein Teiler von n ist. Dann wird durch die Zuordnung*

$$[a]_n \mapsto [a]_m$$

eine wohldefinierte Abbildung

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

definiert, die mit Addition und Multiplikation vertauscht, also ein Ringhomomorphismus ist.

Beweis. Wir müssen uns davon überzeugen, dass aus $[a]_n = [b]_n$ folgt, dass $[a]_m = [b]_m$. Es gebe also $k \in \mathbb{Z}$, so dass

$$b = a + kn.$$

Da m ein Teiler von n ist, können wir n in der Form mr für $r \in \mathbb{Z}$ schreiben. Dann erhalten wir

$$b = a + (kr)m$$

und somit $[a]_m = [b]_m$. Die Verträglichkeit mit Addition und Multiplikation ist klar. □

Der kritische Punkt in dem Lemma ist die Beobachtung, dass wenn m ein Teiler von n ist, folgende Implikation für die Kongruenzen gilt:

$$a \equiv b \mod n \qquad \Rightarrow \qquad a \equiv b \mod m.$$

Beispielsweise folgt also aus $a \equiv 2 \mod 15$, dass $a \equiv 2 \mod 3$.

Im chinesischen Restsatz tauchen Produkte von Restklassenringen auf. Wir wollen uns noch kurz daran erinnnern wie das Produkt von Ringen gebildet wird: Seien R und S zwei Ringe. Das Produkt $R \times S$ (als Mengen) besteht aus den Paaren (r, s) für $r \in R$ und $s \in S$. Darauf definieren wir die Addition und Multiplikation komponentenweise:

$$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) := (r_1 r_2, s_1 s_2).$$

Man rechnet leicht nach, dass die üblichen Rechenregeln erfüllt sind, das Produkt $R \times S$ also tatsächlich ein Ring ist. Sein Nullelement ist $(0, 0)$ und sein Einselement $(1, 1)$.

Das Produkt $R \times S$ zweier Ringe hat immer nichttriviale Nullteiler. Es gilt nämlich

$$(0, 1) \cdot (1, 0) = (0, 0),$$

also sind $(0, 1)$ und $(1, 0)$ Nullteiler.

Satz 3.9 (Chinesischer Restsatz)**.** *Seien $m_1, \ldots, m_r$ teilerfremde natürliche Zahlen und sei $m := m_1 \cdot \ldots \cdot m_r$ deren Produkt Dann ist der Ringhomomorphismus*

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z} \tag{5}$$

$$[a]_m \longmapsto ([a]_{m_1}, \ldots, [a]_{m_r}) \tag{6}$$

ein Isomorphismus.

Bevor wir den Satz beweisen machen wir uns klar, was er in der Sprache der Kongruenzen bedeutet. Die Surjektivität der Abbildung sagt uns, dass wir für gegebene ganze Zahlen $a_1, \ldots, a_r$ eine ganze Zahl a finden, so dass

$$a \equiv a_i \mod m_i \quad \forall i = 1, \ldots, r.$$

Die Injektivität übersetzt sich dann dazu, dass a eindeutig ist modulo m. Die Teilerfremdheit der m_i ist notwendig, wie das Beispiel am Anfang gezeigt hat: Es gibt keine ganze Zahl, die kongruent 3 modulo 6 und 4 modulo 15 ist.

Beweis. Wir müssen zeigen, dass die Abbildung (5) bijektiv ist. Sowohl $\mathbb{Z}/m\mathbb{Z}$ als auch $\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$ haben die Kardinalität $m = m_1 \cdot \ldots \cdot m_r$. Deshalb reicht es die Injektivität der Abbildung zu zeigen. Seien also $a, b \in Z$, so dass

$$([a]_{m_1}, \ldots, [a]_{m_r}) = ([b]_{m_1}, \ldots, [b]_{m_r}).$$

Anders ausgedrückt gilt

$$[a-b]_{m_i} = 0, \quad \text{für alle } i = 1, \dots, r.$$

Daher ist $a - b$ durch alle m_i teilbar. Da $m_1, \dots, m_r$ teilerfremd sind, folgt daraus, dass auch m ein Teiler von $a - b$ ist. Das bedeutet aber gerade, dass $[a]_m = [b]_m$. □

Sei m eine natürliche Zahl mit Primfaktorzerlegung $m = p_1^{r_1} \dots p_k^{r_k}$. Dann folgt aus dem chinesischen Restsatz insbesondere

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_k}.$$

Korollar 3.10 (Chinesischer Restsatz für Einheiten)**.** *Seien $m_1, \dots, m_r$ teilerfremde natürliche Zahlen und $m := m_1 \cdot \dots \cdot m_r$ ihr Produkt. Die Zuordnung*

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z}) &\longrightarrow (\mathbb{Z}/m_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/m_r\mathbb{Z}) \\ [a]_m &\longmapsto ([a]_{m_1}, \dots, [a]_{m_r})\end{aligned}$$

definiert definiert einen Isomorphismus (abelscher Gruppen).

Beweis. Die Aussage folgt, indem man auf beiden Seiten des Ringhomomorphismus (5) aus dem chinesischen Restsatz die Einheitengruppe bildet und benutzt, dass für zwei Ringe R und S gilt $(R \times S)^\times = R^\times \times S^\times$. Alternativ kann man sich auch erinnern, dass die Einheiten in $\mathbb{Z}/m\mathbb{Z}$ gerade aus den Restklassen $[a]_m$ bestehen, für die a teilerfremd zu m ist. Dann benutzt man den chinesischen Restsatz und die Beobachtung, dass a genau dann teilerfremd zu m ist, wenn a teilerfremd zu allen m_i ist. □

3.3. **Die Eulersche φ-Funktion.** Grob gesprochen misst die eulersche φ-Funktion für eine natürliche Zahl n den Anteil der ganze Zahlen, die teilerfremd zu n sind. Sie ist formal folgendermaßen definiert:

Definition 3.11. Die Abbildung

$$\begin{aligned}\varphi : \mathbb{N} &\longrightarrow \mathbb{C} \\ n &\longmapsto \#\{m \in \{0, \dots, n-1\} \mid \mathrm{ggT}(m, n) = 1\}\end{aligned}$$

heißt *eulersche φ-Funktion.*

Selbstverständlich nimmt φ nur Werte in $\mathbb{N}$ ein und wir hätten sie gleich als Funktion $\mathbb{N} \to \mathbb{N}$ definieren können. Allerdings werden wir uns später mit *zahlentheoretischen Funktionen* beschäftigen. Dies sind per Definition Funktionen $\mathbb{N} \to \mathbb{C}$ und φ ist eine davon. Das ist der Grund, warum wir als Ziel $\mathbb{C}$ gewählt haben.

Lemma 3.12. *Für $n \geq 2$ gilt*

$$\varphi(n) = \#\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

Beweis. Die Menge $\{0, \dots, n-1\}$ ist ein Repräsentantensystem für die Restklassen in $\mathbb{Z}/n\mathbb{Z}$, also

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \dots, [0]_{n-1}\}$$

und $[m]_n \neq [k]_n$ für alle $k, m \in \{0, \dots, n-1\}$. Aus Lemma 3.6 wissen wir, dass $[m]_n$ genau dann eine Einheit ist, wenn $\mathrm{ggT}(m, n) = 1$. □

Proposition 3.13. *Für teilerfremde natürliche Zahlen m, n gilt*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Beweis. Aus dem chinesischen Restsatz für Einheiten (Korollar 3.10) wissen wir, dass

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times .$$

Berechnet man auf beiden Seiten die Kardinalität, erhält man die Aussage. □

Sind m und n *nicht* teilerfremd, so ist $\varphi(mn) \neq \varphi(m)\varphi(n)$. Beispielsweise ist $\varphi(3) = 2$, aber $\varphi(9) = 6 \neq 2 \cdot 2$. Es ist nicht möglich für φ eine explizite Formel im herkömmlichen Sinne anzugeben. Wir können φ aber in Abhängigkeit von der Primfaktorzerlegung beschreiben:

Proposition 3.14. *Sei n eine natürliche Zahl mit Primfaktorzerlegung $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$. Dann gilt*

$$\varphi(n) = p_1^{r_1-1}(p_1 - 1) \cdot \ldots \cdot p_k^{r_k-1}(p_k - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Beweis. Übungsaufgabe. □

Der folgende Satz ist eine Verallgemeinerung des *kleinen Fermatschen Satzes*, den wir danach noch als Spezialfall festhalten.

Satz 3.15 (Euler)**.** *Seien $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ teilerfremd. Dann gilt*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Beweis. Wir betrachten die Multiplikation mit a:

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ [b]_n &\longmapsto [ab]_n.\end{aligned}$$

Da $[a]_n$ invertierbar ist, ist dieser Homomorphismus ein Isomorphismus. Wir berechnen nun

$$[a]_n^{\varphi(n)} \cdot \prod_{[k]_n \in (\mathbb{Z}/n\mathbb{Z})^\times} [k]_n = \prod_{[k]_n \in (\mathbb{Z}/n\mathbb{Z})^\times} [ak]_n = \prod_{[k]_n \in (\mathbb{Z}/n\mathbb{Z})^\times} [k]_n.$$

Im ersten Schritt haben wir benutzt, dass $\varphi(n)$ gleich der Anzahl der Faktoren ist, wir also je einen Faktor $[a]_n$ für jedes $[k]_n$ haben. Im zweiten Schritt nutzen wir aus, dass Multiplikation mit $[a]_n$ einen Isomorphismus auf $(\mathbb{Z}/n\mathbb{Z})^\times$ definiert. Kürzen wir auf beiden Seiten das Produkt $\prod[k]_n$, erhalten wir das Resultat. □

Korollar 3.16 (kleiner Fermat)**.** *Für jede Primzahl p und jede ganze Zahl a gilt*

$$a^p \equiv a \mod p.$$

Beweis. Ist a durch p teilbar, sind sowohl a als auch a^p kongruent 0 modulo p. Ist p kein Teiler von a, sind a und p teilerfremd und es gilt nach Satz 3.15

$$a^{p-1} = a^{\varphi(p)} \equiv 1 \mod p.$$

Multiplizieren wir beide Seiten mit a, erhalten wir das Resultat. □

Abschließend wollen wir noch eine Eigenschaft der eulerschen φ-Funktion beweisen, die Einblicke liefert wie die φ-Funktion einer natürlichen Zahl mit der ihrer Teiler zusammenhängt.

Proposition 3.17. *Für eine natürliche Zahl n gilt*

$$\sum_{\substack{d|n\\ d>0}} \varphi(d) = n.$$

Beweis. Wir sortieren die Restklassen in $\mathbb{Z}/n\mathbb{Z}$ nach ihrem größten gemeinsamen Teiler mit n und erhalten eine disjunkte Vereinigung

$$\mathbb{Z}/n\mathbb{Z} = \coprod_{d|n} \{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = d\}. \tag{7}$$

Für jeden Teiler $d < n$ von n setzen wir $n_d := n/d$ und betrachten wir die Abbildung

$$\begin{aligned} \pi_d : (\mathbb{Z}/n_d\mathbb{Z})^\times &\to \mathbb{Z}/n\mathbb{Z} \\ [a]_{n_d} &\mapsto [da]_n. \end{aligned}$$

Diese ist wohldefiniert, denn falls $[a]_{n_d} = [b]_{n_d}$ gibt es $k \in \mathbb{N}$ mit $b = a + kn_d$ und daraus folgt

$$db = da + kn_d d = kn.$$

Außerdem ist π_d injektiv aus folgendem Grund. Seien $a, b \in \mathbb{Z}$ mit $[da]_n = [db]_n$. Dann gibt es $k \in \mathbb{Z}$ mit

$$db = da + kn = da + kn_d d.$$

Da $d \neq 0$, können wir d kürzen und erhalten $b = a + kn_d$, also $[a]_{n_d} = [b]_{n_d}$.

Wir behaupten nun, dass das Bild von π_d gerade gleich $\{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = d\}$ ist. Für jedes $[a]_{n_d} (\in \mathbb{Z}/n_d\mathbb{Z})^\times$ ist $[da]_n$ in dieser Menge enthalten, denn a ist teilerfremd zu n_d und daraus folgt

$$\mathrm{ggT}(da, n) = \mathrm{ggT}(da, dn_d) = d.$$

Andererseits liegt jedes Element $[a]_n$ mit $\mathrm{ggT}(a,n) = d$ im Bild, weil a durch d teilbar ist und $\mathrm{ggT}(a/d, n_d) = 1$.

Zusammenfassend haben wir gezeigt, dass π_d eine Bijektion von $\mathbb{Z}/n_d\mathbb{Z})^\times$ auf $\{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = d\}$ induziert. Insbesondere gilt daher

$$\varphi(n_d) = \#\left(\mathbb{Z}/n_d\mathbb{Z}\right)^\times = \#\{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = d\}.$$

Den Fall $d = n$, also $n_d = 1$ haben wir noch nicht behandelt. Dieser ist aber offensichtlich:

$$\varphi(1) = 1 = \#\{[n]_n\} = \#\{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = n\}.$$

Nun können wir in der Zerlegung (7) von $\mathbb{Z}/n\mathbb{Z}$ auf beiden Seiten die Kardinalität berechnen und erhalten

$$n = \sum_{\substack{d|n\\ d>0}} \varphi(d).$$

□

4. Zahlentheoretische Funktionen

Eine *zahlentheoretische Funktion* oder auch *arithmetische Funktion* ist eine Abbildung $\mathbb{N} \to \mathbb{C}$.

4.1. Multiplikative zahlentheoretische Funktionen.

Definition 4.1. Sei $\psi : \mathbb{N} \to \mathbb{C}$ eine zahlentheoretische Funktion.

(i) ψ ist *multiplikativ*, falls $\psi(1) = 1$ und für *teilerfremde* natürliche Zahlen m und n gilt
$$\psi(mn) = \psi(m)\psi(n).$$
(ii) ψ ist *vollständig multiplikativ*, falls $\psi(1) = 1$ und für *alle* natürlichen Zahlen m und n gilt
$$\psi(mn) = \psi(m)\psi(n).$$

Die Bedingung $\psi(1) = 1$ dient nur dazu die konstante Funktion $\psi(n) = 0$ auszuschließen. Gibt es $n \in \mathbb{N}$ mit $\psi(n) \neq 0$, so folgt aus
$$\psi(1)\psi(n) = \psi(1 \cdot n) = \psi(n)$$
durch Kürzen von $\psi(n)$, dass $\psi(1) = 1$.

Beispiele 4.2. (i) Die konstante Funktion $n \mapsto 1$ ist eine vollständig multiplikative zahlentheoretische Funktion. Wir bezeichnen sie mit 1.
(ii) Für jede natürliche Zahl k ist $n \mapsto n^k$ vollständig multiplikativ. Insbesondere ist die Identität $n \mapsto n$ vollständig multiplikativ. Wir bezeichnen sie mit I^k. Für $k = 1$ schreiben wir auch $I^1 = I$. Auch für $k = 0$ ist die Definition sinnvoll und wir haben $I^0 = 1$.
(iii) Die Funktion $\delta : \mathbb{N} \to \mathbb{C}$ mit
$$\delta(n) := \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$
ist vollständig multiplikativ.
(iv) Die eulersche φ-Funktion ist multiplikativ (nach Proposition 3.13), aber nicht vollständig multiplikativ.

Man könnte sagen, dass die interessanten zahlentheoretischen Funktionen die sind, die multiplikativ, aber nicht vollständig multiplikativ sind. Wir wollen uns einige davon anschauen, die im weiteren Verlauf immer wieder auftauchen werden.

Beispiel 4.3 (Die Möbiussche μ-Funktion)**.** Sie ist folgendermaßen definiert:
$$\mu(n) := \begin{cases} 1 & n = 1, \\ (-1)^r & n = p_1 \cdots p_r \text{ mit } p_i \neq p_j, \\ 0 & n \text{ nicht quadratfrei.} \end{cases}$$
Wenn man im zweiten Fall auch $r = 0$ zulässt, also das leere Produkt, bekommt man auch automatisch $\mu(1) = 1$. Der dritte Fall bedeutet explizit, dass es eine natürliche Zahl $b > 1$ gibt, so dass b^2 die Zahl n teilt. Für Primzahlpotenzen p^r mit $r \in \mathbb{N}$ gilt demnach
$$\mu(p^r) = \begin{cases} -1 & r = 1 \\ 0 & r > 1 \end{cases}$$
Die Multiplikativität der Möbiusschen μ-Funktion folgt direkt aus den Definitionen.

Beispiel 4.4 (Die Teilerfunktion)**.** Sie ist folgendermaßen definiert:

$$\sigma_0(n) := \#\{d \in \mathbb{N} \mid d|n\}.$$

Für Primpotenzen gilt

$$\sigma_0(p^r) = r + 1$$

Um einzusehen, dass σ_0 multiplikativ ist, müssen wir die Teiler eines Produkts mn teilerfremder natürliche Zahlen m und m verstehen. Die relevante Erkenntnis ist in Lemma 4.5 festgehalten. Wenn d das Produkt mn teilt, bekommen wir also eine eindeutige Zerlegung $d = d_m d_n$ mit $d_m|m$ und $d_n|n$. Diese Konstruktion liefert eine Umkehrabbildung zu

$$\begin{aligned}\{d_m \in \mathbb{N} \mid d_m|m\} \times \{d_n \in \mathbb{N} \mid d_n|n\} &\longrightarrow \{d \in \mathbb{N} \mid d|mn\}\\ (d_m, d_n) &\longmapsto d_m d_n,\end{aligned}$$

welche daher bijektiv ist. Nehmen wir auf beiden Seiten die Kardinalität, erhalten wir die Multiplikativität der Teilerfunktion σ_0.

Lemma 4.5. *Seien m und n teilerfremde natürliche Zahlen. Dann hat jeder Teiler d von mn eine eindeutige Zerlegung*

$$d = d_m d_n$$

für einen Teiler d_m von m und einen Teiler d_n von n.

Beweis. Seien

$$m = p_1^{k_1} \cdots p_r^{k_r} \qquad \text{und} \qquad n = q_1^{m_1} \cdots q_s^{m_s}$$

die Primfaktorzerlegungen von m und n. Dann sind wegen der Teilerfremdheit von m und n die Primzahlen p_i und q_j paarweise verschieden und die Primfaktorzerlegung von mn ist

$$mn = p_1^{k_1} \cdots p_r^{k_r} \cdot q_1^{m_1} \cdots q_s^{m_s}.$$

Jeder Teiler d von mn hat somit die Form

$$d = p_1^{k_1'} \cdots p_r^{k_r'} \cdot q_1^{m_1'} \cdots q_s^{m_s'}.$$

mit $k_i' \leq k_i$ und $m_j' \leq m_j$. So bekommen wir die gewünschte eindeutige Zerlegung in

$$d_m = p_1^{k_1'} \cdots p_r^{k_r'} \qquad \text{und} \qquad d_n = q_1^{m_1'} \cdots q_s^{m_s'}.$$

□

Beispiel 4.6 (Die Teilersummenfunktion)**.** Sie ist folgendermaßen definiert:

$$\sigma_1(n) := \sum_{d|n} d.$$

Für Primpotenzen gilt

$$\sigma_1(p^r) := \sum_{k=0}^{r} p^k = 1 + p + p^2 + \ldots + p^r = \frac{p^{r+1} - 1}{p - 1}.$$

Auch die Teilersummenfunktion ist multiplikativ. Das ist eine Übungsaufgabe. Allgemeiner ist für jedes $k \in \mathbb{N}$ die *Teilerpotenzsummenfunktion*

$$\sigma_k(n) = \sum_{d|n} d^k$$

multiplikativ. Die Teilerfunktion σ_0 und die Teilersummenfunktion σ_1 bilden die Spezialfälle $k = 0$ und $k = 1$.

4.2. **Mersennesche Primzahlen und vollkommene Zahlen.** Eine gängige Methode neue Primzahlen zu erzeugen stammt von Marin Mersenne, einem Minoritenpater, der sich im 17. Jahrhundert mit Mathematik befasste. Hierbei betrachtet man für eine Primzahl p die Zahl

$$M_p := 2^p - 1.$$

Dies ist nicht immer eine Primzahl, aber die Chancen stehen nicht schlecht auf diese Weise eine große Primzahl zu erzeugen. Zum Beipiel gilt

$$\begin{aligned} M_2 &= 3, \\ M_3 &= 7, \\ M_5 &= 31, \\ M_7 &= 127, \end{aligned}$$

aber $M_11 = 2047$ ist keine Primzahl, sondern gleich dem Produkt $23 \cdot 89$. Ist n keine Primzahl, so ist $M_n = 2^n - 1$ nach folgendem Lemma nie eine Primzahl. Wenn man auf der Suche nach Primzahlen ist, sollte man also nur M_p für Primzahlen p betrachten.

Lemma 4.7. *Ist m ein Teiler von n so ist M_m ein Teiler von M_n.*

Beweis. Übungsaufgabe. □

Primzahlen der Form $2^p - 1$ für eine Primzahl p heißen *Mersenne*-Primzahlen. Bis heute sind 51 Mersenne-Primzahlen bekannt. Man vermutet jedoch, dass es unendlich viele davon gibt.

Definition 4.8. Eine natürliche Zahl n heißt *vollkommen*, wenn sie $\sigma_1(n) = 2n$ erfüllt, wobei σ_1 die Teilersummenfunktion ist. In anderen Worten bedeutet das

$$n = \sum_{\substack{d \neq n \\ d|n}} d.$$

Der Faktor 2 ist in dieser Beschreibung nicht mehr vorhanden, weil wir nur über Teiler d von n summieren, die ungleich n sind. In $\sigma_1(n)$ ist aber auch der Summand n enthalten.

Man vermutet, dass es keine ungeraden vollkommenen Zahlen gibt, weiß aber nur, dass es keine gibt, die kleiner als 10^{1500} sind.

Satz 4.9. *Seien m und u natürliche Zahlen, wobei u ungerade ist, also $2 \nmid u$. Dann ist $n := 2^m u$ genau dann eine vollkommene Zahl, wenn*

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

gilt mit einer Primzahl $M_{m+1} = 2^{m+1} - 1$. In diesem Fall muss auch $m + 1$ eine Primzahl sein.

Beweis. Wir nehmen an $u = 2^{m+1} - 1$ mit einer Primzahl $m+1$. Um $\sigma_1(n)$ zu berechnen, untersuchen wir die Teiler von 2^m und von M_{m+1}. Die Teiler von 2^m sind von der Form

2^k für $k \in \{0, \ldots, m\}$ und die Teiler von M_{m+1} sind 1 und M_{m+1} selbst. Daraus folgt

$$\begin{aligned}\sigma_1(n) &= \sigma_1(2^m)\sigma_1(M_{m+1}) \\ &= (1 + 2 + 4 + \ldots + 2^m)(1 + M_{m+1}) \\ &= \frac{2^{m+1} - 1}{2 - 1}(1 + 2^{m+1} - 1) \\ &= 2^{m+1}(2^{m+1} - 1) \\ &= 2n.\end{aligned}$$

Nehmen wir nun an, n sei vollkommen. Wie oben haben wir

$$\sigma_1(2^m) = 2^{m+1} - 1.$$

Daraus können wir den Wert bei n berechnen:

$$2^{m+1}u = 2n = \sigma_1(n) = (2^{m+1} - 1)\sigma_1(u). \tag{8}$$

Da 2^{m+1} und $2^{m+1} - 1$ teilerfremd sind, folgt daraus $(2^{m+1} - 1)|u$. Es gibt also $k \in \mathbb{N}$ mit

$$u = (2^{m+1} - 1)k$$

Kürzen wir in (8) auf beiden Seiten den Faktor $2^{m+1} - 1$, erhalten wir

$$2^{m+1}k = \sigma_1(u). \tag{9}$$

Wir wollen zunächst zeigen, dass $k = 1$. Wäre $k > 1$, so hätte u mindestens die Teiler

$$1,\ k,\ (2^{m+1} - 1),\ (2^{m+1} - 1)k = u.$$

Somit gilt für die Teilersummenfunktion

$$\sigma_1(u) \geq (1 + k + (2^{m+1} - 1) + (2^{m+1} - 1)k) = 2^{m+1}(k + 1).$$

Kombinieren wir das mit Gleichung (9), erhalten wir

$$2^{m+1}k \geq 2^{m+1}(k + 1),$$

was zum Widerspruch führt.

Nun müssen wir noch zeigen, dass $u = 2^{m+1} - 1$ eine Primzahl ist. Da $k = 1$, wird aus (9) die Gleichheit

$$\sigma_1(u) = 2^{m+1} = (2^{m+1} - 1) + 1 = u + 1.$$

Das kann aber nur gelten, wenn u eine Primzahl ist, da es sonst außer 1 und u weitere Teiler gäbe.

Die letzte Aussage, dass auch $m+1$ eine Primzahl sein muss, folgt aus Lemma 4.7. □

4.3. **Faltung.**

Definition 4.10. Seien f und g zahlentheoretische Funktionen. Wir definieren ihre *Faltung* durch

$$(f * g)(n) := \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Die Faltung operiert auf den multiplikativen zahlentheoretischen Funktionen, das heißt, die Faltung zweier multiplikativer Funktionen ist wieder multiplikativ. Das ist Inhalt des nächsten Lemmas:

Lemma 4.11. *Die Faltung $(f * g)$ zweier multiplikativer zahlentheoretischer Funktionen f und g ist eine multiplikative zahlentheoretische Funktion.*

Beweis. Seien m und n teilerfremde natürliche Zahlen. Jeder Teiler d von mn hat eine eindeutige Zerlegung

$$d = d_m d_n$$

in einen Teiler d_m von m und einen Teiler d_n von n. Somit können wir die Summe in der Definition der Faltung folgendermaßen aufspalten:

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d) g\left(\frac{n}{d}\right) \\
&= \sum_{d_m|m} \sum_{d_n|n} f(d_m d_n) g\left(\frac{mn}{d_m d_n}\right) \\
&= \sum_{d_m|m} \sum_{d_n|n} f(d_m) f(d_n) g\left(\frac{m}{d_m}\right) g\left(\frac{n}{d_n}\right) \\
&= \left(\sum_{d_m|m} f(d_m) g\left(\frac{m}{d_m}\right)\right) \left(\sum_{d_n|n} f(d_n) g\left(\frac{n}{d_n}\right)\right) \\
&= f(m) g(n).
\end{aligned}$$

□

Es gilt sogar noch mehr und das macht die Faltung zu einem sehr nützlichen Werkzeug:

Proposition 4.12. *Die Faltung definiert auf der Menge der zahlentheoretischen Funktionen die Struktur einer abelschen Gruppe mit neutralem Element*

$$\delta(n) := \begin{cases} 1 & n = 1 \\ 0 & n > 1. \end{cases}$$

Die multiplikativen zahlentheoretischen Funktionen bilden eine Untergruppe.[1]

Beweis. Wir müssen die folgenden Aussagen zeigen:

(i) $f * \delta = f$ für alle f,
(ii) $(f * g) * h = f * (g * h)$ für alle f, g, h,
(iii) $f * g = g * f$ für alle f, g,
(iv) für jedes f gibt es ein Inverses $\check{f}$ mit $f * \check{f} = \delta$.

Hierbei sind f, g und h jeweils zahlentheoretische Funktionen. (i). Es gilt

$$(f * \delta)(n) = \sum_{d|n} f(d) \delta\left(\frac{n}{d}\right).$$

Nach Definition ist $\delta\left(\frac{n}{n}\right) = \delta(1) = 1$ und 0 für alle anderen Teiler d von n. Daraus folgt

$$(f * \delta)(n) = f(n).$$

[1]Tatsächlich bilden die zahlentheoretischen Funktionen zusammen mit der punktweisen Addition $(f + g)(n) = f(n) + g(n)$ und der Faltung als Multiplikation sogar einen kommutativen Ring, allerdings ist die Summe zweier multiplikativer Funktionen nicht notwendig multiplikativ. Diese bilden nur eine Gruppe.

(ii). Wir haben

$$\begin{aligned}((f*g)*h)(n) &= \sum_{d|n}(f*g)(d)h\left(\frac{n}{d}\right)\\ &= \sum_{d|n}\sum_{r|d} f(r)g\left(\frac{d}{r}\right)h\left(\frac{n}{d}\right)\\ &= \sum_{\substack{r,s,t|n\\ rst=n}} f(r)g(s)h(t)\end{aligned}$$

und

$$\begin{aligned}(f*(g*h))(n) &= \sum_{r|n} f(r)(g*h)\left(\frac{n}{r}\right)\\ &= \sum_{r|n}\sum_{s|n/r} f(r)g(s)h\left(\frac{n/r}{s}\right)\\ &= \sum_{\substack{r,s,t|n\\ rst=n}} f(r)g(s)h(t),\end{aligned}$$

also gilt das Assoziativgesetz.

(iii). Das Kommutativgesetz ist klar, da

$$(f*g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{\substack{d,d'|n\\ dd'=n}} f(d)g(d') = \sum_{d'|n} f\left(\frac{n}{d'}\right)g(d') = (g*f)(n),$$

indem wir die Summanden einmal mit d und einmal mit $d' = n/d$ indizieren.

(iv). Es bleibt die Inverse $\check{f}$ zu einer zahlentheoretischen Funktion f zu konstruieren. Dafür gibt es keine explizite Formel. Wir konstruieren $\check{f}$ per Induktion über n. Wir fangen an, indem wir

$$\check{f}(1) := 1$$

setzen. Sei nun $n > 1$. Wir nehmen an, dass $\check{f}(m)$ für $m < n$ bereits definiert ist, so dass für alle $m < n$ gilt

$$\sum_{d|m} f(d)\check{f}\left(\frac{m}{d}\right) = \delta(m) = \begin{cases}1 & m = 1\\ 0 & m > 1.\end{cases}$$

Wir wollen, dass

$$0 = \delta(n) = \sum_{d|n} f(d)\check{f}\left(\frac{n}{d}\right).$$

Daher definieren wir

$$\check{f}(n) := -\sum_{\substack{d|n\\ d>1}} f(d)\check{f}\left(\frac{n}{d}\right).$$

In der Definition tauchen nur Werte $\check{f}(m)$ für $m < n$ auf, für die wir das schon definiert haben. Deshalb dürfen wir die Definition so hinschreiben. Außerdem gilt nun

$$\sum_{d|m} f(d)\check{f}\left(\frac{m}{d}\right) = \delta(m)$$

nicht nur für $m < n$, sondern auch für $m = n$ und wir haben den Induktionsschritt beendet.

Bisher haben wir gezeigt, dass die zahlentheoretischen Funktionen mit der Faltungsoperation eine abelsche Gruppe bilden. Es gilt noch zu zeigen, dass die multiplikativen zahlentheoretischen Funktionen eine Untergruppe davon bilden.

Sind aber f und g multiplikativ, so ist auch $f * g$ multiplikativ nach Lemma 4.11. Es fehlt nur noch, dass Inverse multiplikativer Funktionen ebenfalls multiplikativ sind.

Durch die obige induktive Definition des Inversen erhalten wir eine zahlentheoretische Funktion $\check{f} : \mathbb{N} \to \mathbb{C}$. Wir müssen uns allerdings noch davon überzeugen, dass $\check{f}$ multiplikativ ist, wenn f multiplikativ ist. Das machen wir induktiv über die beiden teilerfremden Faktoren m und n gleichzeitig. Für $m = n = 1$ ist das trivial:

$$\check{f}(1 \cdot 1) = \check{f}(1) = 1 = 1 \cdot 1 = \check{f}(1)\check{f}(1).$$

Seien nun m und n nicht beide gleich 1. Nehmen wir an die Multiplikativität gilt für alle teilerfremden Zahlen $m' \leq m$ und $n' \leq n$ mit $m'n' < mn$. Dann gilt unter Anwendung von Lemma 4.5

$$\begin{aligned}\check{f}(mn) &= -\sum_{\substack{d|mn \\ d>1}} f(d)\check{f}\left(\frac{mn}{d}\right) \\ &= -\sum_{\substack{d_m|m, d_n|n \\ d_m>1 \text{ oder } d_n>1}} f(d_m d_n)\check{f}\left(\frac{mn}{d_m d_n}\right)\end{aligned}$$

Weil nie gleichzeitig $d_m = 1$ und $d_n = 1$ gilt, ist $(mn)/(d_m d_n) = (m/d_m)(n/d_n) < mn$. Nach Induktionsannahme wissen wir schon, dass für diese Kombinationen $\check{f}$ multiplikativ ist. Außerdem ist f für alle Werte multiplikativ. Damit können wir die obige Rechnung fortsetzen:

$$\begin{aligned}\check{f}(mn) &= -\sum_{\substack{d_m|m, d_n|n \\ d_m>1 \text{ oder } d_n>1}} f(d_m)f(d_n)\check{f}\left(\frac{m}{d_m}\right)\check{f}\left(\frac{n}{d_n}\right) \\ &= -\sum_{d_m|m, d_n|n} f(d_m)f(d_n)\check{f}\left(\frac{m}{d_m}\right)\check{f}\left(\frac{n}{d_n}\right) + f(1)f(1)\check{f}(m)\check{f}(n) \\ &= -\left(\sum_{d_m|m} f(d_m)\check{f}\left(\frac{m}{d_m}\right)\right)\left(\sum_{d_n|n} f(d_n)\check{f}\left(\frac{n}{d_n}\right)\right) + \check{f}(m)\check{f}(n) \\ &= -(f * \check{f})(m)(f * \check{f})(n) + \check{f}(m)\check{f}(n) \\ &= -\delta(m)\delta(n) + \check{f}(m)\check{f}(n) \\ &= -\delta(mn) + \check{f}(m)\check{f}(n).\end{aligned}$$

Weil m und n nicht beide gleich 1 sind, ist $mn > 1$ und somit $\delta(mn) = 0$. Daraus folgt

$$\check{f}(mn) = \check{f}(m)\check{f}(n).$$

□

Wir wollen nun die Faltung für einige multiplikative Funktionen, die wir kennen, berechnen.

Beispiele 4.13. (i) Wegen Proposition 3.17 ist

$$(\varphi * 1)(n) = \sum_{d|n} \varphi(d) \cdot 1 = \sum_{d|n} \varphi(d) = n,$$

also

$$\varphi * 1 = I.$$

(ii) Es gilt

$$(1 * 1)(n) = \sum_{d|n} 1 \cdot 1 = \sigma_0(n),$$

also

$$1 * 1 = \sigma_0$$

(iii) Allgemeiner gilt

$$(I^k * 1)(n) = \sum_{d|n} n^k \cdot 1 = \sigma_k(n),$$

also

$$I^k * 1 = \sigma_k.$$

Die Faltung mit 1 hat einen eigenen Namen:

Definition 4.14. Für eine zahlentheoretische Funktion f heißt $F := f * 1$ die *summatorische Funktion* von f. Explizit gilt

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

Aus den obigen Beispielen kennen wir also die summatorischen Funktionen von φ, 1 und I^k. Als nächstes berechnen wir die summatorische Funktion der Möbiusschen μ-Funktion:

Lemma 4.15.

$$\mu * 1 = \delta.$$

Beweis. Wir wissen schon, dass beide Seiten multiplikativ sind. Es reicht also, die Gleichheit für Potenzen p^r einer Primzahl mit $r \geq 1$ zu testen. Es gilt

$$(\mu * 1)(p^r) = \sum_{d|p^r} \mu(d) = \sum_{k=0}^{r} \mu(p^k) = 1 + (-1) + 0 + \ldots + 0 = 0 = \delta(p^r).$$

□

Korollar 4.16 (Möbiussche Umkehrformel)**.** *Für die summatorische Funktion F einer zahlentheoretischen Funktion f gilt*

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

Beweis. Auf der rechten Seite der Gleichung steht die Faltung $F * \mu$ ausgewertet bei n. Per Definition ist F die Faltung $f * 1$. Einsetzen ergibt mithilfe von Lemma 4.15

$$F * \mu = f * 1 * \mu = f * \delta = f.$$

□

Wenden wir die Möbiussche Umkehrformel auf die Eulersche φ-Funktion und ihre summatorische Funktion I an, erhalten wir

$$\varphi(n) = \sum_{d|n} d \cdot \mu\left(\frac{n}{d}\right).$$

Für eine Primpotenz $n = p^r$ können wir das berechnen:

$$\begin{aligned}\varphi(p^r) &= \sum_{k=0}^{r} p^k \mu(p^{r-k}) \\ &= p^r\mu(1) + p^{r-1}\mu(p) + 0 \\ &= p^r - p^{r-1} \\ &= p^{r-1}(p-1).\end{aligned}$$

Wir erhalten somit die explizite Formel für die Eulersche φ-Funktion aus Proposition 3.14 zurück.

4.4. **Formale Potenzreihen.** Für einen Körper K betrachten wir die *formalen Potenzreihen*

$$K[\![T]\!] := \left\{ \sum_{i=0}^{\infty} a_i T^i \mid a_i \in K \right\}.$$

Wir können diese Definition für einen beliebigen Körper K hinschreiben, weil wir bei formalen Potenzreihen keine Konvergenzbedingung haben. Somit können wir aber im Allgemeinen auch keine „Funktionswerte" berechnen indem wir für T ein Element von K einsetzen. Unendliche Summen sind nur definiert, wenn es in K einen Begriff von Konvergenz gibt, also beispielsweise in $\mathbb{R}$ oder in $\mathbb{C}$. Aber selbst dann muss man darauf achten, dass die Reihe auch konvergiert. Für allgemeine formale Potenzreihen kann es vorkommen, dass die Reihe für keinen einzigen Wert von T konvergiert außer für $T = 0$ (Einsetzen von $T = 0$ liefert immer den 0-Koeffizienten). Aber Konvergenz interessiert uns an dieser Stelle nicht.

Die formalen Potenzreihen bilden einen Ring mit der üblichen Addition und Multiplikation: Für

$$f = \sum_{i=0}^{\infty} a_i T^i \qquad \text{und} \qquad g = \sum_{i=0}^{\infty} b_i T^i$$

in $K[\![T]\!]$ gilt

$$\begin{aligned}(f+g)(T) &:= \sum_{i=0}^{\infty} (a_i + b_i) T^i \\ (fg)(T) &:= \sum_{i=0}^{\infty} \sum_{k=0}^{i} a_i b_{i-k} T^i\end{aligned}$$

Die Einheiten werden wir im folgenden Lemma untersuchen.

Lemma 4.17. *Für jeden Körper K gilt*

$$\begin{aligned}(K[\![T]\!])^\times &= \left\{ \sum_{i=0}^{\infty} a_i T^i \mid a_0 \neq 0 \right\} \\ &= \{ f \in K[\![T]\!] \mid f(0) \neq 0 \}.\end{aligned}$$

Beweis. Falls $f \in K[\![T]\!]$ eine Einheit ist, gibt es $g \in K[\![T]\!]$, mit $fg = 1$. Dann gilt

$$1 = f(0)g(0).$$

Insbesondere muss $f(0)$ ungleich Null sein.

Für die Rückrichtung betrachten wir ein Element

$$f = \sum_{i=0}^{\infty} a_i T^i$$

von $K[\![T]\!]$ mit $f(0) = a_0 \neq 0$ und konstruieren induktiv ein Inverses

$$g = \sum_{i=0}^{\infty} b_i T^i.$$

Dass g invers zu f ist, bedeutet, dass $fg = 1$, also

$$\sum_{k=0}^{i} a_k b_{i-k} = \begin{cases} 1 & i = 0 \\ 0 & i > 0. \end{cases}$$

Da $a_0 \neq 0$ können wir dieses Element in K invertieren und definieren

$$b_0 := \frac{1}{a_0}.$$

Wir betrachten nun $i > 1$ und nehmen an, dass für $j < i$ die Elemente b_j bereits definiert sind, so dass gilt

$$\sum_{k=0}^{j} a_k b_{j-k} = \begin{cases} 1 & j = 0 \\ 0 & j > 0. \end{cases} \tag{10}$$

Dann setzen wir

$$b_i := -\frac{\sum_{k=0}^{i-1} a_k b_{i-k}}{a_0}.$$

Hierbei haben wir wieder ausgenutzt, dass $a_0 \neq 0$. Die Definition von b_i haben wir gerade so gewählt, dass die Gleichung Eq. (10) auch für $j = i$ gilt ohne für $j < i$ etwas zu ändern. Somit können wir die Koeffizienten b_j induktiv so konstruieren, dass $g = \sum_i b_i T^i$ invers zu f ist. Folglich ist f eine Einheit. □

Beispiel 4.18. Für ein lineares Polynom $a - bT$ mit $a \neq 0$ können wir das Inverse mithilfe der Formel für die geometrische Reihe bestimmen:

$$\frac{1}{a - bT} = \frac{1}{a} \cdot \frac{1}{1 - (b/a)T} = \frac{1}{a} \sum_{i=0}^{\infty} \left(\frac{b}{a} T\right)^i.$$

Streng genommen muss man sich hier Gedanken machen ob man die Formel für die geometrische Reihe anwenden darf. Die wurde ja eigentlich bewiesen im Falle, dass die geometrische Reihe konvergiert. Aber das angenehme an formalen Potenzreihen ist, dass wir gar keine Konvergenzbedingung haben und einfach durch Ausmultiplizieren überprüfen können, dass

$$(1 - cT) \sum_{i=0}^{\infty} c^i T^i = 1.$$

für alle $c \in K$.

Wir wollen nun multiplikativen Funktionen formale Potenzreihen über den komplexen Zahlen zuordnen, genauer gesagt eine Potenzreihe für jede Primzahl p.

Definition 4.19. Sei f eine multiplikative zahlentheoretische Funktion und p eine Primzahl. Dann definieren wir die formale Potenzreihe

$$\lambda_p(f,T) : \sum_{r=0}^{\infty} f(p^r)T^r \in \mathbb{C}[\![T]\!].$$

Da $f(1) = 1$, ist der konstante Koeffizient gleich 1, wir haben also

$$\lambda_p(f,T) \in 1 + T\mathbb{C}[\![T]\!].$$

Insbesondere ist $\lambda_p(f,T)$ invertierbar.

Lemma 4.20. *Sei f vollständig multiplikativ. Sei p eine Primzahl und $a_p := f(p)$. Dann gilt*

$$\lambda_p(f,T) = \frac{1}{1-a_pT}.$$

Beweis. Wegen der vollständigen Multiplikativität von f gilt

$$f(p^r) = f(p)^r = a_p^r$$

Wir nutzen nun die Formel für die geometrische Reihe um $\lambda_p(f,T)$ zu berechnen:

$$\lambda_p(f,T) = \sum_{r=0}^{\infty} f(p^r)T^r = \sum_{r=0}^{\infty} a_p^r T^r = \frac{1}{1-a_pT}.$$

□

Wir können nun die Potenzreihen zu den vollständig multiplikativen zahlentheoretischen Funktionen, die wir kennen hinschreiben:

Beispiel 4.21. (i) $\lambda_p(\delta,T) = 1$ für alle Primzahlen p, da $\delta(p) = 0$,
(ii) $\lambda_p(1,T) = \dfrac{1}{1-T}$,
(iii) $\lambda_p(I^k,T) = \dfrac{1}{1-p^kT}$.

Wir berechnen nun die Potenzreihe für die Möbiussche μ-Funktion:

Lemma 4.22. *Für jede Primzahl p gilt*

$$\lambda_p(\mu,T) = 1 - T.$$

Beweis. Das folgt sofort aus

$$\mu(p^r) = \begin{cases} 1 & r = 0 \\ -1 & r = 1 \\ 0 & r > 1. \end{cases}$$

□

Wir sehen hier, dass die Potenzreihen der Möbiusschen μ-Funktion sehr anders aussieht als die einer *vollständig* multiplikativen Funktion. Sie ist ein lineares Polynom, wohingegen die Potenzreihen der vollständig multiplikativen Funktionen Inverse von linearen Polynomen sind. Dies ist kein Zufall, da die Potenzreihen kompatibel mit der Faltung sind:

Proposition 4.23. *Für multiplikative zahlentheoretische Funktionen f und g und eine Primzahl p gilt*

$$\lambda_p(f * g, T) = \lambda_p(f, T)\lambda_p(g, T).$$

Beweis. Werten wir die Faltung $f * g$ an einer Primzahlpotenz p^r aus, erhalten wir

$$(f * g)(p^r) = \sum_{d|p^r} f(d)g\left(\frac{p^r}{d}\right) = \sum_{s=0}^{r} f(p^s)g(p^{r-s}).$$

Damit können wir die Potenzreihe zu $f * g$ berechnen:

$$\begin{aligned}
\lambda_p(f * g, T) &= \sum_{r=0}^{\infty} (f * g)(p^r)T^r \\
&= \sum_{r=0}^{\infty} \sum_{s=0}^{r} f(p^s)g(p^{r-s})T^r \\
&= \sum_{r=0}^{\infty} \sum_{\substack{s,t\geq 0 \\ s+t=r}} f(p^s)g(p^t)T^{s+t} \\
&= \sum_{s,t=0}^{\infty} f(p^s)g(p^t)T^{s+t} \\
&= \left(\sum_{s=0}^{\infty} f(p^s)T^s\right)\left(\sum_{t=0}^{\infty} g(p^t)T^t\right) \\
&= \lambda_p(f, T)\lambda_p(g, T).
\end{aligned}$$

□

Mithilfe von Proposition 4.23 ist es nun ein leichtes die zugehörigen Potenzreihen für weitere multiplikative Funktionen auszurechnen:

Lemma 4.24. *Sei p eine Primzahl. Dann gilt*

(i) $\lambda_p(\varphi, T) = \frac{1-T}{1-pT}$,

(ii) $\lambda_p(\sigma_k, T) = \frac{1}{(1-T)(1-p^kT)}$,

Beweis. (i). Da $\varphi = \mu * I$, können wir nach Proposition 4.23 die Potenzreihen von φ aus denen von μ und I berechnen. Da $\lambda_p(\mu, T) = 1 - T$ und $\lambda_p(I) = 1/(1 - pT)$, erhalten wir

$$\lambda_p(\varphi, T) = \lambda_p(\mu, T)\lambda_p(I, T) = \frac{1 - T}{1 - pT}.$$

(ii). Es gilt $\sigma_k = 1 * I^k$. Folglich haben wir

$$\lambda_p(\sigma_k, T) = \lambda_p(1, T)\lambda_p(I^k, T) = \frac{1}{(1 - T)(1 - p^kT)}.$$

□

Nun erinnern wir uns daran, dass für jede Primzahl p und jede multiplikative zahlentheoretische Funktion f die Potenzreihe $\lambda_p(f,T)$ in $1+T\mathbb{C}[\![T]\!]$ enthalten ist. Da $(fg)(0)=f(0)g(0)$ ist

$$1+T\mathbb{C}[\![T]\!]=\{f\in\mathbb{C}[\![T]\!]\mid f(0)\neq 0\}$$

abgeschlossen unter Multiplikation und somit eine Untergruppe von $\mathbb{C}[\![T]\!]^\times$. Wir erhalten also für jede Primzahl p einen Homomorphismus abelscher Gruppen

$$\lambda_p:\{\mathrm{MZF}\longrightarrow 1+T\mathbb{C}[\![T]\!],$$

wobei MZF die abelsche Gruppe der multiplikativen zahlentheoretischen Funktionen bezeichnet. Sei P die Menge aller Primzahlen. Dann können wir die Homomorphismen λ_p zu einem einzigen Homomorphismus

$$\begin{aligned}\lambda:\mathrm{MZF}&\longrightarrow (1+T\mathbb{C}[\![T]\!])^P\\ f&\longmapsto (\lambda_p(f,T))_{p\in P}\end{aligned}$$

zusammenfassen.

Proposition 4.25. *Der Homomorphismus λ ist ein Isomorphismus.*

Beweis. Da eine multiplikative zahlentheoretische Funktion f eindeutig durch ihre Werte an Primpotenzen p^r festgelegt ist und $f(p^r)$ gerade der r-te Koeffizient von $\lambda_p(f,T)$ ist, ist λ injektiv. Für die Surjektivität sei ein Element $(Q_p)_{p\in P}$ ein Element von $(1+T\mathbb{C}[\![T]\!])^P$. Das heißt jedes Q_p ist eine Potenzreihe der Form

$$Q_p=1+a_{p,1}T+a_{p,2}T^2+\dots$$

mit $a_{p,i}\in\mathbb{C}$. Wir können nun eine zahlentheoretische Funktion definieren durch

$$f(n)=f(p_1^{k_1}\cdot\ldots\cdot p_r^{k_r})=a_{p_1,k_1}\cdot\ldots\cdot a_{p_r,k_r},$$

wobei $n=p_1^{k_1}\cdot\ldots\cdot p_r^{k_r}$ die Primfaktorzerlegung von n ist. Es ist mithilfe der eindeutigen Primfaktorzerlegung nicht schwierig zu überprüfen, dass f multiplikativ ist. Außerdem gilt

$$\lambda_p(f,T)=1+f(p)T+f(p^2)T^2+\ldots=1+a_{p,1}T+a_{p,2}T^2+\ldots=Q_p(T).$$

□

5. Endliche Körper

Das Ziel dieses Kapitels ist es die endlichen Körper besser zu verstehen. Dafür müssen wir allerdings einige Grundlagen schaffen, weshalb einige Abschnitte auf den ersten Blick nichts mit endlichen Körpern zu tun haben.

5.1. **Die Ordnung einer endlichen Gruppe.** Für später brauchen wir einige Resultate über die Ordnung einer endlichen Gruppe oder eines Elements einer endlichen Gruppe. Wir schreiben die Gruppen in diesem Abschnitt multiplikativ. Für ein Element g einer Gruppe G bezeichnen wir mit $\langle g\rangle$ die Untergruppe von G, die von g erzeugt wird. Sie besteht aus allen Elementen der Form g^k für $k\in\mathbb{Z}$. Für $G=\mathbb{Z}$ und $m\in\mathbb{Z}$ haben wir (Achtung hier additive Schreibweise):

$$\langle m\rangle=m\mathbb{Z}=\{mk\mid k\in\mathbb{Z}\}.$$

Lemma 5.1. *Jede Untergruppe von $\mathbb{Z}$ ist von der Form $m\mathbb{Z}$ für ein $m\in\mathbb{Z}$.*

Beweis. Sei $H \subseteq \mathbb{Z}$ eine Untergruppe. Falls $H = \{0\}$, ist $H = 0\mathbb{Z}$ und die Aussage gilt. Andernfalls ist $H \cap \mathbb{N}$ eine nichtleere Teilmenge von $\mathbb{N}$, welche nach Satz 1.10 ein kleinstes Element m besitzt. Wir behaupten, dass

$$H = m\mathbb{Z}.$$

Es ist klar, dass $m\mathbb{Z} \subseteq H$, da $m \in H$ und H eine Untergruppe ist. Sei $h \in H$. Division mit Rest (Proposition 1.19) gibt uns $a \in \mathbb{Z}$ und $r \in \{0, \dots, m-1\}$ mit

$$h = r + am.$$

Da h und am in H enthalten sind, muss auch r ein Element von H sein. Wäre $r > 0$, also $f \in H \cap \mathbb{N}$, so führte das zum Widerspruch zur Minimalität von m. Deshalb muss $r = 0$ gelten und somit

$$h = am \in m\mathbb{Z}.$$

□

Definition 5.2. Eine Gruppe G heißt *zyklisch*, falls es ein Element $g \in G$ gibt mit $\langle g \rangle >= G$.

Beispielsweise ist $\mathbb{Z}$ zyklisch mit Erzeuger 1 und alle $\mathbb{Z}/m\mathbb{Z}$ sind zyklisch mit Erzeuger $[1]_m$ (als additive Gruppen). Aber $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist nicht zyklisch, denn

$$\begin{aligned}
\langle([0]_2, [0]_2)\rangle &= \{([0]_2, [0]_2)\},\\
\langle([0]_2, [1]_2)\rangle &= \{([0]_2, [1]_2), ([0]_2, [0]_2)\},\\
\langle([1]_2, [0]_2)\rangle &= \{([1]_2, [0]_2), ([0]_2, [0]_2)\},\\
\langle([1]_2, [1]_2)\rangle &= \{([1]_2, [1]_2), ([0]_2, [0]_2)\}.
\end{aligned}$$

Definition 5.3. Sei G eine endliche Gruppe.

- Die *Ordnung* von G ist die Kardinalität von G, also die Anzahl der Elemente.
- Für ein Element $g \in G$ definieren wir die Ordnung $\mathrm{ord}g$ von g als die Ordnung von $\langle g \rangle$.

Man kann unter anderem an den Ordnungen der Elemente von G ablesen, ob G zyklisch ist. Das ist genau dann der Fall, wenn es ein Element $g \in G$ gibt mit $\mathrm{ord}g = G$. Im obigen Beispiel von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ haben alle nichttrivialen Elemente die Ordnung 2, aber die ganze Gruppe hat die Ordnung 4.

Hier bemerken wir nocheinmal, dass für teilerfremde ganze Zahlen m und n nach dem chinesischen Restsatz gilt

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}.$$

Die Gruppe $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ist folglich zyklisch. Das Beispiel von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ illustriert, dass die Teilerfremdheit von m und n eine notwendige Bedingung ist.

Lemma 5.4. *Für ein Element g einer endlichen Gruppe G gilt*

$$\langle g \rangle = \{1, g, g^2, \dots, g^{\mathrm{ord}g-1}\}$$

Außerdem ist $g^k = 1$ genau dann, wenn $\mathrm{ord}g | m$ und somit

$$\mathrm{ord}g = \min\{k \in \mathbb{N} | g^k = 1\}.$$

Beweis. Wir betrachten den Homomorphismus

$$\begin{aligned}\varphi_g : \mathbb{Z} &\longrightarrow G,\\ k &\longmapsto g^k.\end{aligned}$$

Das Bild von φ_g ist per Definition $\langle g\rangle$. Der Kern ist eine Untergruppe von $\mathbb{Z}$ und folglich nach Lemma 5.1 ismorph zu $m\mathbb{Z}$ für ein $m \in \mathbb{Z}$. Wir erhalten einen Isomorphismus

$$\begin{aligned}\mathbb{Z}/m\mathbb{Z} &\longrightarrow \langle g\rangle\\ [k]_m &\longmapsto \varphi_g(k) = g^k.\end{aligned}$$

Insbesondere ist $g^k = 1$ genau dann, wenn $m|k$ und

$$\mathrm{ord} g = m = \min\{k \in \mathbb{N} | g^k = 1\}.$$

Wählen wir für die Elemente von $\mathbb{Z}/m\mathbb{Z}$ die Repräsentanten $0, 1, \ldots, m-1$, so sehen wir, dass

$$\langle g\rangle = \{1, g, g^2, \ldots, g^{m-1}\}.$$

□

Lemma 5.5. *Sei H eine Untergruppe einer endlichen Gruppe G. Dann ist $|H|$ ein Teiler von $|G|$. Insbesondere teilt für jedes Element $g \in G$ die Ordnung* ord$g$ *von g die Ordnung $|G|$.*

Beweis. Wir definieren auf G folgende Äquivalenzrelation:

$$g \sim g' \qquad \Leftrightarrow \qquad g'g^{-1} \in H.$$

Die Äquivalenzklassen sind die Linksnebenklassen

$$gH = \{gh \mid h \in H\}.$$

Sei $g_1, \ldots, g_r$ ein Repräsentantensystem für die Linksnebenklassen. Wir erhalten eine Zerlegung von G in disjunkte Teilmengen:

$$G = \coprod_{i=1}^{r} g_i H.$$

Alle Nebenklassen gH haben die Kardinalität $|H|$. Daher gilt

$$|G| = r|H|$$

und insbesondere ist $|H|$ ein Teiler von $|G|$. □

Korollar 5.6. *Für ein Element g einer endlichen Gruppe G gilt*

$$g^{|G|} = 1.$$

Beweis. Nach Lemma 5.5 ist ord$g$ ein Teiler von $|G|$. Daraus folgt die Aussage, da nach Lemma 5.4 für jedes Vielfache k von ord$g$ gilt $g^k = 1$. □

5.2. **Der Polynomring über einem Körper.** Wir stellen einige Resultate über den Polynomring $K[T]$ zusammen, die wir in den folgenden Abschnitten brauchen werden. Wir erinnern uns zunächst an die Definition

$$K[T] = \left\{ \sum_{i=0}^{n} a_i T^i \mid n \in \mathbb{N} \cup \{0\},\ a_i \in K \right\}.$$

Das ist ein Ring mit der üblichen Addition und Multiplikation. Für ein Polynom $f \neq 0$ definieren wir den *Grad* $\deg f$ als die größte (ganze) Zahl n, so dass $a_n \neq 0$. Außerdem setzen wir $\deg(0) := -\infty$. Hierbei ist „$-\infty$" rein formal aufzufassen als ein Element, das kleiner als alle ganzen Zahlen ist. Außerdem definieren wir

$$-\infty - \infty := -\infty \qquad \text{und} \qquad -\infty + m = -\infty \quad \forall m \in \mathbb{Z}.$$

Für ein nichttriviales Polynom f vom Grad n nennen wir den Koeffizienten von T^n den *Leitkoeffizienten* von f. Ein Polynom heißt *normiert*, falls sein Leitkoeffizient gleich 1 ist.

Beispiel 5.7. Wir betrachten das Polynom

$$f = 3T^2 + 4T - 1 \in \mathbb{Q}[T].$$

Dann hat f den Grad 2 und den Leitkoeffizienten 3.

Lemma 5.8. *Für zwei Polynome f und g in $K[T]$ gilt*

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

Beweis. Sei $n = \deg f$ und $g = \deg g$. Sind f und g nichttrivial, können wir sie folgendermaßen schreiben

$$f = \sum_{i=0}^{n} a_i T^i \qquad \text{und} \qquad g = \sum_{j=0}^{m} a_j T^j$$

mit $a_n \neq 0$ und $b_m \neq 0$. Das Produkt ist dann gegeben durch

$$fg = a_n b_m T^{m+n} + (a_n b_{m-1} + a_{n-1} b_m) T^{m+n-1} + \ldots (a_1 b_0 + a_0 b_1) T + a_0 b_0.$$

Daraus sieht man, dass der Leitkoeffizient des Produktes gleich $a_n b_m$ ist, insbesondere ungleich Null. Also folgt

$$\deg(fg) = m + n = \deg(f) + \deg(g).$$

Falls f oder g gleich Null ist, ist auch $fg = 0$ und auf beiden Seiten der Gradgleichung steht $-\infty$. Also ist die Gleichung auch in diesem Fall richtig. □

Lemma 5.9. *Der Polynomring $K[T]$ ist nullteilerfrei.*

Beweis. Seien f und g Polynome über K mit $fg = 0$. Nach Lemma 5.8 gilt

$$-\infty = \deg(0) = \deg(fg) = \deg(f) + \deg(g).$$

Das kann nur erfüllt sein, wenn entweder $\deg(f) = -\infty$ oder $\deg(g) = -\infty$ oder in anderen Worten $f = 0$ oder $g = 0$. □

Jedes Element a des Körpers K kann als konstantes Polynom aufgefasst werden. Solche Polynome nennen wir *Konstanten*.

Lemma 5.10. *Die Einheiten des Polynomrings sind die nichttrivialen Konstanten:*

$$K[T]^\times = K^\times.$$

Beweis. Dass alle Elemente von $K^\times$ Einheiten im Polynomring sind, ist klar. Sei $f \in K[T]^\times$. Wir wollen zeigen, dass f konstant und nicht Null ist. Als Einheit hat f ein Inverses g mit $fg = 1$. Dann gilt

$$0 = \deg(1) = \deg(fg) = \deg f + \deg g.$$

Da $\deg(f)$ und $\deg(g)$ Elemente von $\mathbb{N} \cup \{0, -\infty\}$ sind, kann dies nur gelten, falls

$$\deg f = \deg g = 0.$$

Das bedeutet, dass sowohl f als auch g nichttriviale Konstanten sind. □

Der Polynomring verhält sich in vielen Dingen analog zu $\mathbb{Z}$. Insbesondere kann man auch in $K[T]$ so etwas wie Primzahlen definieren. Diese Rolle wird von den irreduziblen Polynomen eingenommen.

Definition 5.11. Ein Polynom $f \in K[T]$ heißt *irreduzibel*, falls es nicht konstant ist und in jeder Faktorisierung

$$f = gh$$

eines der Polynome g und h konstant ist.

Ist f nicht irreduzibel, so heißt es *reduzibel*.

Die Bedingung, dass ein irreduzibles Polynom nicht konstant sein soll, stellt sicher, dass es keine Einheit ist. Das ist analog zu der Forderung, dass eine Primzahl nicht gleich Eins sein soll. Genau genommen sind die *normierten* irreduziblen Polynome das Gegenstück zu den Primzahlen, denn Primzahlen sind auch in dem Sinne normiert, dass sie positiv sind. Für jede Primzahl p hat auch $-p$ nur die Teiler ± 1 und $\pm p$. Gewissermaßen sollten p und $-p$ als äquivalent betrachtet werden, da sie sich nur um die Einheit -1 unterscheiden. Genauso sollten irreduzible Polynome f und g als äquivalent betrachtet werden, wenn sie sich nur durch eine Einheit unterscheiden, also $g = af$ für $a \in K^\times$.

Um die Bedingung der Irreduzibilität auf die gleiche Form zu bringen wie die Primzahlbedingung, brauchen wir auch für den Polynomring einen Begriff von Teilbarkeit. Wir können das ganz allgemein für jeden Ring definieren:

Definition 5.12. Sei R ein Ring und $a, b \in R$. Dann sagen wir, dass a ein Teiler von b ist, falls es $c \in R$ gibt mit $b = ac$.

Es gelten für die Teilbarkeit in einem allgemeinen Ring R ähnliche Rechenregeln wie in $\mathbb{Z}$ (siehe :

Lemma 5.13. *Seien $a, b, c, d, x, y \in R$. Dann gilt:*

(i) aus $d|a$ folgt $d|ab$,
(ii) aus $d|c$ und $c|a$ folgt $d|a$,
(iii) aus $d|a$ und $d|b$ folgt $d|xa + yb$,

Die beiden Regeln (iv) und (v) aus Proposition 1.16 gelten nicht für jeden Ring R. Hier braucht man zusätzliche Annahmen, die allerdings für den Polynomring erfüllt sind:

Lemma 5.14. *Seien R ein nullteilerfreier Ring und $c, d \in R \setminus \{0\}$ zwei Elemente. Dann folgt aus $d|c$ und $c|d$, dass es eine Einheit $a \in R^\times$ gibt mit $c = ad$.*

Beweis. Nach Annahme gibt es $a, b \in R$ mit

$$c = ad \qquad \text{und} \qquad d = bc.$$

Daraus folgt

$$c = ad = abc.$$

Umstellen ergibt

$$0 = c(ab - 1).$$

Weil R nullteilerfrei ist und $c \neq 0$, folgt daraus

$$ab = 1,$$

das heißt a ist eine Einheit. □

Lemma 5.15. *Seien f und g Polynome in $K[T]$ mit $f|g$. Dann gilt* $\deg(f) \leq \deg(g)$.

Beweis. Nach Annahme gibt es $h \in K[T]$ mit

$$g = fh.$$

Daraus folgt mit Lemma 5.8

$$\deg(g) = \deg(f) + \deg(h) \geq \deg(f).$$

□

Proposition 5.16. *Im Polynomring $K[T]$ gibt es Polynomdivision. Das heißt für Elemente $f, g \in K[T]$ mit $g \neq 0$ gibt es eindeutig bestimmte $r, h \in K[T]$ mit $r = 0$ oder* $\deg(r) < \deg(g)$, *so dass*

$$f = r + gh.$$

Beweis. Ist $f = 0$ oder $\deg f < \deg g$, sind wir fertig mit $r = f$ und $h = 0$. Andernfalls setzen wir $n = \deg f$ und $m = \deg h$. Sei a_n der Leitkoeffizient von f und b_m der Leitkoeffizient von g. Das Polynom

$$f' := f - T^{n-m}\frac{a_n}{b_m}g$$

hat Grad $\deg(f') < n = \deg(f)$, da sich der Leitkoeffizient gerade wegkürzt. Induktiv können wir annehmen, dass es $r, h' \in K[T]$ gibt mit $r = 0$ oder $\deg(f) < \deg(g)$, so dass

$$f' = r + gh',$$

also

$$f = f' + T^{n-m}\frac{a_n}{b_m}g = r + g(h' + T^{n-m}\frac{a_n}{b_m}).$$

Somit haben wir r und $h := h' + T^{n-m}\frac{a_n}{b_m}$ mit den geforderten Eigenschaften gefunden.

Um die Eindeutigkeit zu zeigen, betrachten wir r' und h' in $K[T]$ mit $\deg(r') < \deg(g)$, so dass

$$f = r + gh = r' + gh'.$$

Daraus folgt

$$r - r' = g(h' - h).$$

Wir können nun Lemma 5.8 anwenden, um die Grade zu vergleichen:

$$\deg(g) > \deg(r - r') = \deg(g) + \deg(h' - h).$$

Diese Ungleichung kann nur stimmen, wenn $\deg(h' - h)$ negativ ist, also $\deg(h' - h) = 0$. Hieraus folgt $h' = h$ und somit auch $r' = r$. □

Bemerkung 5.17. Vergleichen wir die Aussage von Lemma 5.15 mit Proposition 1.16 (iv) und Proposition 5.16 mit Proposition 1.19, so fällt auf, dass hier die Gradfunktion an die Stelle der Betragsfunktion tritt. Man kann diese Beobachtung formalisieren, was zur Definition eines *euklidischen Rings* führt. Das ist ein kommutativer, nullteilerfreier Ring R, der eine *Bewertungsfunktion*

$$g : R \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$$

besitzt mit folgenden Eigenschaften:

(i) für $x, y \in R$ gilt $g(xy) \geq g(x)$

(ii) Division mit Rest: für $x, y \in R$ mit $x \neq 0$ gibt es $r, z \in R$ mit $r = 0$ oder $g(r) < g(x)$, so dass

$$y = r + zx.$$

Die ganzen Zahlen bilden einen euklidischen Ring mit der Betragsfunktion und der Polynomring $K[T]$ ist euklidisch mit der Gradfunktion. Die folgende Diskussion über irreduzible Polynome und eindeutige Primfaktorzerlegung könnten wir auch ganz allgemein für irreduzible Elemente in einem euklidischen Ring führen.

Mithilfe der Polynomdivision können wir den euklidschen Algorithmus auch im Polynomring durchführen und so den größten gemeinsamen Teiler zweier Polynome f und g bestimmen. Dieser ist definiert als das normierte Polynom mit maximalem Grad, das sowohl f als auch g teilt. Um ihn zu bestimmen definieren wir $a_0 = f$, $a_1 = g$ und a_2 mit $\deg(a_2) < \deg(a_1)$ über die Polynomdivision:

$$a_0 = a_2 + b_2 a_1$$

mit $b_2 \in K[T]$. Wir fahren fort und definieren induktiv a_n aus a_{n-1} und a_{n-2} durch

$$a_{n-2} = a_n + b_n a_{n-1}$$

mit $\deg(a_n) < \deg(a_{n-1})$ und $b_n \in K[T]$. Irgendwann erreichen wir den Punkt, an dem $\deg a_{n_0+1} = -\infty$, also $a_{n_0+1} = 0$. Dann ist die Normierung von a_{n_0} der größte gemeinsame Teiler.

Durch sukzessives Einsetzen erhalten wir genauso wie in $\mathbb{Z}$:

Proposition 5.18. *Seien f und g Polynome, nicht beide Null, mit größtem gemeinsamen Teiler g. Dann gibt es $a, b \in K[T]$ mit*

$$g = af + bg.$$

Dieses Resultat hilft uns eine andere Charakterisierung von irreduziblen Polynomen zu finden:

Proposition 5.19. *Sei $p \in K[T]$ normiert. Dann ist p genau dann irreduzibel, wenn für alle Polynome $f, g \in K[T]$ gilt:*

$$p|fg \qquad \Rightarrow \qquad p|f \quad \text{oder} \quad p|g.$$

Beweis. Angenommen p erfüllt die Bedingung aus der Proposition und $p = fg$ für $f, g \in K[T]$. Dann teilt p entweder f oder g. Ohne Beschränkung der Allgemeinheit können wir annehmen p teilt f, also $f = ph$ für $h \in K[T]$. Daraus folgt

$$p = fg = pgh,$$

woraus wegen der Nullteilerfreiheit von $K[T]$ (Lemma 5.9) folgt

$$1 = gh.$$

Das heißt, g ist eine Einheit.

Für die Rückrichtung nehmen wir an p ist irreduzibel und $f, g \in K[T]$ mit $p|fg$. Falls $p \nmid f$, ist $\mathrm{ggT}(p, f)$ ein Teiler von p, der nicht p selbst multipliziert mit einer Konstante ist. Also ist $\mathrm{ggT}(p, f) = 1$. Aus Proposition 5.18 bekommen wir $a, b \in K[T]$ mit

$$1 = af + bp.$$

Dann ist

$$g = 1 \cdot g = (af + bp)g = a(fg) + (bg)p.$$

Beide Summanden sind durch p teilbar, folglich gilt $p|g$. □

Mit den gleichen Argumenten wie in $\mathbb{Z}$ können wir nun eine eindeutige Primfaktorzerlegung konstruieren:

Satz 5.20 (eindeutige Primfaktorzerlegung für Polynome)**.** *Jedes nichttriviale Polynom $f \in K[T]$ besitzt eine bis auf Vertauschung der Faktoren eindeutige Primfaktorzerlegung*

$$f = aQ_1^{k_r} \cdot \ldots \cdot Q_r^{k_r}$$

mit normierten irreduziblen Polynomen $Q_1, \ldots, Q_r$, natürlichen Zahlen k_r und einer Konstante $a \in K^\times$.

Beweis. Übungsaufgabe, es geht genauso wie für Proposition 2.4. □

Lemma 5.21. *Sei $f \in K[T]$ ein Polynom mit einer Nullstelle $a \in K$. Dann gibt es $g \in K[T]$ mit*

$$f = (T - a)g.$$

Beweis. Polynomdivision (Proposition 5.16) gibt uns $r, g \in K[T]$ mit $\deg(r) < \deg(T - a) = 1$, so dass

$$f = r + (T - a)g.$$

Einsetzen von a ergibt

$$0 = f(a) = r(a) + 0$$

Wegen $\deg(r) < 1$ ist r konstant, also $r = 0$. □

Das Resultat, das wir später brauchen werden ist folgendes:

Satz 5.22. *Sei $f \in K[T]$ ein nichttriviales Polynom vom Grad n. Dann hat f höchstens n Nullstellen.*

Beweis. Die Aussage gilt für konstante nichttriviale Polynome, welche gar keine Nullstellen haben. Induktiv nehmen wir an, dass die Aussage für Polynome vom Grad kleiner n richtig ist. Falls f keine Nullstelle besitzt, sind wir fertig. Ansonsten nehmen wir eine Nullstelle a und können somit f nach Lemma 5.21 faktorisieren als

$$f = (T - a)g$$

für ein Polynom $g \in K[T]$, das nach Lemma 5.8 den Grad $n-1$ hat. Daher hat g höchstens $n - 1$ Nullstellen. Daraus folgt, dass f höchstens n Nullstellen hat, da jede Nullstelle von f entweder eine Nullstelle von g ist oder eine von $T - a$, d.h. gleich a. □

5.3. **Die multiplikative Gruppe eines Körpers.** Wir untersuchen in diesem Abschnitt für einen Körper K seine multiplikative Gruppe

$$K^\times = \{x \in K \mid \exists y \in K : \ xy = 1\} = K \setminus \{0\}.$$

Wir interessieren uns besonders für die multiplikative Gruppe eines endlichen Körpers, oder allgemeiner für endliche Untergruppen von $K^\times$. Zum Beispiel hat $\mathbb{R}^\times$ die endliche Untergruppe $\{1, -1\}$ und für jedes $n \in \mathbb{N}$ hat $\mathbb{C}$ die endliche Untergruppe

$$\mu_n := \{e^{2\pi ik/n} \mid k \in \mathbb{Z}\}.$$

Zur Vorbereitung brauchen wir ein Lemma über die Restklassenringe $\mathbb{Z}/m\mathbb{Z}$.

Lemma 5.23. *Seien $m, k \in \mathbb{Z}$. Dann gilt für das Element $[k]_m$ von $\mathbb{Z}/m\mathbb{Z}$:*

$$\mathrm{ord}[k]_m = \frac{m}{\mathrm{ggT}(k, m)}.$$

Beweis. Wir schreiben d für die Ordnung $\mathrm{ord}[k]_m$. Dann ist d die kleinste natürliche Zahl, für die gilt

$$[kd]_m = 0.$$

Explizit bedeutet das, dass es $r \in \mathbb{Z}$ gibt mit

$$kd = rm.$$

und d ist minimal mit dieser Eigenschaft. Anders ausgedrückt ist kd das kleinste gemeinsame Vielfache von k und m. Das kann man auch mithilfe des größten gemeinsamen Teilers ausdrücken:

$$kd = \mathrm{kgV}(k, m) = \frac{km}{\mathrm{ggT}(k, m)}.$$

Daraus folgt

$$d = \frac{m}{\mathrm{ggT}(k, m)}.$$

□

Satz 5.24. *Sei K ein Körper und $G \subseteq K^\times$ eine endliche Untergruppe. Dann ist G zyklisch.*

Beweis. Für einen Teiler d von $n := |G|$ definieren wir die Teilmenge

$$G_d := \{g \in G \mid \mathrm{ord} g = d\}.$$

Wir behaupten

$$|G_d| = \begin{cases} 0 & G_d = \varnothing \\ \varphi(d) & G_d \neq \varnothing. \end{cases}$$

Um die Behauptung zu zeigen, nehmen wir an, dass es ein Element $g \in G_d$ gibt. Wir haben eine Inklusion

$$\langle g \rangle = \{1, g, \ldots, g^{d-1}\} \subseteq \{h \in G \mid h^d = 1\}.$$

Die linke Gruppe hat die Kardinalität d und die rechte Gruppe hat Kardinalität höchstens d, da die Elemente von G auch Elemente von K sind und das Polynom $T^d - 1$ nach Satz 5.22 höchstens d Nullstellen besitzt. Das kann nur erfüllt sein, wenn beide Untergruppen identisch sind mit Kardinalität d. Genauer gesagt sind haben wir wie im Beweis von Lemma 5.4 einen Isomorphismus

$$\mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} \langle 1, g, \ldots, g^{d-1} \rangle = \{g \in G \mid g^d = 1\},$$

der $k \in \mathbb{Z}/k\mathbb{Z}$ auf g^k schickt. Außerdem gilt

$$G_d \subseteq \{g \in G \mid g^d = 1\}.$$

Wir wissen aus Lemma 5.23, dass die Elemente der Ordnung d in $\mathbb{Z}/d\mathbb{Z}$ gerade die Restklassen $[k]_d$ sind mit $\mathrm{ggT}(k,d) = 1$. Daraus folgt

$$|G_d| = \varphi(d),$$

was die Behauptung zeigt.

Wir betrachten nun die disjunkte Zerlegung

$$\{g \in G \mid g^n = 1\} = \coprod_{d|n} G_d.$$

Für die Kardinalitäten bedeutet das

$$n = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n.$$

Hierbei haben wir für die mittlere Ungleichung benutzt, dass $|G_d|$ entweder gleich $\varphi(d)$ oder Null ist Die rechte Gleichheit ist die Aussage von Proposition 3.17. Wir folgern daraus, dass die mittlere Ungleichheit tatsächlich eine Gleichheit ist. Dann muss aber $|G_d| = \varphi(d)$ für alle Teiler d von n gelten, insbesondere für $d = n$. Das bedeutet, dass G_n nicht leer ist und jedes Element $g \in G_n$ hat Ordnung n und erzeugt daher die Gruppe G. □

5.4. **Die Charakteristik eines Körpers.** Wir wollen nun die Ergebnisse der letzten Abschnitte auf endliche Körper anwenden. Zunächst gehen wir aber der Frage nach welche endlichen Körper es überhaupt gibt.

Lemma 5.25. *Sei K ein Körper. Dann ist der Ringhomomorphismus*

$$\begin{aligned} \iota : \mathbb{Z} &\longrightarrow K \\ m &\longmapsto m := \underbrace{1 + \ldots + 1}_{m \text{ mal}} \end{aligned}$$

entweder injektiv oder es gibt eine Primzahl p, so dass

$$\ker(\iota) = p\mathbb{Z}.$$

Beweis. Der Kern von ι ist eine Untergruppe von $\mathbb{Z}$, also von der Form $m\mathbb{Z}$ für ein $m \in \mathbb{Z}$ (siehe Lemma 5.1). Fall $m = 0$ ist, ist ι injektiv. Andernfalls betrachten wir den induzierten injektiven Homomorphismus

$$\mathbb{Z}/m\mathbb{Z} \hookrightarrow K.$$

Dadurch wird $\mathbb{Z}/m\mathbb{Z}$ ein Teilring von K. Da K als Körper nullteilerfrei ist, muss das auch für den Teilring $\mathbb{Z}/m\mathbb{Z}$ gelten. Nach Lemma 3.4 muss dann m eine Primzahl sein. □

In der Notation von Lemma 5.25 ist entweder $\ker(\iota) = 0$ oder $\ker(\iota) = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p. Im ersten Fall sagen wir, dass K *Charakteristik* 0 hat und im zweiten Fall *Charakteristik* p. Beispielsweise haben $\mathbb{Q}$,$\mathbb{R}$ und $\mathbb{C}$ Charakteristik Null und

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

hat Charakteristik p.

Korollar 5.26. *Ein Körper K enthält entweder $\mathbb{Q}$ oder einen endlichen Körper $\mathbb{F}_p$ für eine Primzahl p (und genau einen davon).*

Beweis. Wir behandeln zuerst den Fall, dass $\iota : \mathbb{Z} \to K$ aus Lemma 5.25 injektiv ist. Dafür überzeugen wir uns davon, dass sich ι fortsetzen lässt zu einem Homomorphismus

$$\begin{aligned} \iota_{\mathbb{Q}} : \mathbb{Q} &\longrightarrow K \\ \frac{m}{n} &\longmapsto \frac{\iota(m)}{\iota(n)}, \end{aligned}$$

wobei für ein Element von $\mathbb{Q}$ eine Darstellung m/n gewählt wird mit $m, n \in \mathbb{Z}$, $n \neq 0$. Weil ι injektiv ist, ist $\iota(n) \neq 0$ und im Nenner steht nicht Null. Wir müssen uns noch davon überzeugen, dass $\iota(m)/\iota(n)$ unabhängig von der Darstellung als Bruch m/n ist: Für eine ander Darstellung m'/n' gibt es $k \in \mathbb{Z}$ mit $m' = km$ und $n' = kn$ und somit

$$\frac{\iota(m')}{\iota(n')} = \frac{\iota(k)\iota(m)}{\iota(k)\iota(n)} = \frac{\iota(m)}{\iota(n)}.$$

Außerdem ist es nicht schwierig nachzuprüfen, dass ι_Q ein Ringhomomorphismus ist, also verträglich ist mit Addition und Multiplikation. Der Homomorphismus $\iota_Q : \mathbb{Q} \to K$ ist wieder injektiv, da allgemein jeder Ringhomomorphismus von einem Körper in einen anderen Ring (mit 1) injektiv ist. Hier kann man das aber auch direkt sehen.

Falls ι nicht injektiv ist, gibt es nach Lemma 5.25 eine Primzahl p, so dass $\ker(\iota) = p\mathbb{Z}$. Dann erhalten wir einen injektiven Ringhomomorphismus

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow K.$$

□

Wir nennen $\mathbb{Q}$ beziehungsweise $\mathbb{F}_p$ den *Grundkörper* von K, falls $\mathbb{Q} \subseteq K$ beziehungsweise $\mathbb{F}_p \subseteq K$. Ein Körper der Charakteristik 0 enthält demnach $\mathbb{Q}$ und ist insbesondere immer unendlich. Einen endlicher Körper hat Charakteristik p für eine Primzahl p und enthält $\mathbb{F}_p$. Es gibt aber auch unendliche Körper der Charakteristik p. Ein Beispiel bildet der Körper der rationalen Funktionen über $\mathbb{F}_p$:

$$\mathbb{F}_p(T) := \{\frac{f(T)}{g(T)} \mid f(T), g(T) \in \mathbb{F}_p[T],\ g(T) \neq 0\}.$$

Proposition 5.27. *Sei K ein endlicher Körper der Charakteristik p. Dann gibt es $r \in \mathbb{N}$, so dass*

$$|K| = p^r.$$

Insbesondere ist die multiplikative Gruppe von K zyklisch der Ordnund $p^r - 1$

Beweis. Aus Korollar 5.26 wissen wir, dass

$$\mathbb{F}_p \subseteq K.$$

Dadurch bekommt K die Struktur eines $\mathbb{F}_p$-Vektorraums. Die Addition ist durch die Addition von K gegeben und die skalare Multiplikation mit $\mathbb{F}_p$ wird durch die Multiplikation von K induziert. Da K endlich ist, muss die Dimension von K über $\mathbb{F}_p$ endlich sein. Wir bezeichnen sie mit r. Dann gilt

$$|K| = |\mathbb{F}_p|^r = p^r.$$

Wir wissen aus Satz 5.24, dass $K^\times$ zyklisch ist. Außerdem ist $K^\times = K \setminus \{0\}$, also hat $K^\times$ die Kardinalität $p^r - 1$. □

5.5. **Konstruktion von Körpererweiterungen.** Tatsächlich gibt es für jede natürliche Zahl bis auf Isomorphie genau einen Körper mit p^r Elementen. Um das zu zeigen müssen wir aber ein bisschen ausholen. Wir haben in Kapitel 3 die Restklassenringe $\mathbb{Z}/m\mathbb{Z}$ untersucht. Diese Konstruktion kann man in weit größerer Allgemeinheit durchführen für einen Ring R und ein Ideal $I \subseteq R$.

Definition 5.28. Ein *Ideal* in einem Ring R ist eine Untergruppe $I \subseteq R$ (bezüglich der Addition), so dass für alle $r \in R$ und $a \in I$ gilt $ra \in I$. Ein *Hauptideal* ist ein Ideal der Form aR für ein $a \in R$.

Hier muss man sich noch klarmachen, dass für jedes $a \in R$ die Menge

$$aR = \{ar \mid r \in R\}$$

ein Ideal ist. Das folgt aber direkt aus den Definitionen. In jedem Ring ist $\{0\}$ und R selbst ein Ideal. Das Ideal R wird von jeder Einheit erzeugt. Insbesondere sind daher in einem Körper K die einzigen Ideale $\{0\}$ und K selbst

Für $a \in R$ sagen wir auch, dass aR das Ideal ist, das von a erzeugt wird und schreiben oft (a). Auch für mehrere Elemente $a_1, \dots, a_n$ können wir das Ideal betrachten, das von $a_1, \dots, a_n$ erzeugt wird, d.h. das kleinste Ideal, das $a_1, \dots, a_n$ enthält. Wir verwenden dafür die Notation $(a_1, \dots, a_n)$.

In $\mathbb{Z}$ haben wir in Lemma 5.1 gezeigt, dass jede Untergruppe von der Form $m\mathbb{Z}$ ist für ein $m \in \mathbb{Z}$. Da Ideale insbesondere Untergruppen sind, ist also jedes Ideal von der Form $m\mathbb{Z}$. Anders ausgedrückt ist $\mathbb{Z}$ ein *Hauptidealring*, also ein Ring, in dem jedes Ideal ein Hauptideal ist. Das ist der Fall für jeden euklidischen Ring, also auch für den Polynomring $K[T]$:

Lemma 5.29. *Der Polynomring $K[T]$ ist ein Hauptidealring.*

Beweis. Für ein Ideal $I \subseteq K[T]$ wählen wir ein Polynom $f \in I \setminus \{0\}$ von minimalem Grad. Für jedes andere Element $g \in I$ finden wir durch Polynomdivision (Proposition 5.16) $r, h \in K[T]$ mit $\deg r < \deg f$, so dass

$$g = r + fh.$$

Wegen der Minimalität von $\deg f$ muss $r = 0$ gelten und somit $g \in fK[T] = (f)$. Also folgt $I = (f)$. □

Der obige Beweis ist genau der gleiche wie für $\mathbb{Z}$ nur mit dem Grad statt der Bewertung. Man kann den gleichen Beweis auch ganz allgemein für euklidische Ringe führen.

Beispiel 5.30. Ein Beispiel für einen Ring, der *kein* Hauptidealring ist, ist $K[S,T]$, der Polynomring in zwei Variablen über einem Körper K. Um uns davon zu überzeugen, werden wir zeigen, dass (S,T) kein Hauptideal ist. Wenn (S,T) ein Hauptideal wäre, gäbe es ein Polynom $f(S,T) \in K[S,T]$ mit

$$(S,T) = (f).$$

Da $S, T \in (S,T)$, finden wir g und h in $K[S,T]$ mit

$$S = gf \qquad \text{und} \qquad T = hf.$$

Wir haben in $K[S,T]$ den Grad $\deg_S$ in S und den Grad $\deg_T$ in T (so dass beispielsweise $\deg_S(S^2T^3 - T^2 + S - 1) = 2$ und $\deg_T(S^2T^3 - T^2 + S - 1) = 3$). Diese beiden Grade sind additiv für Produkte von Polynomen (das folgt für $\deg_T$, indem man $K[S,T]$ als

Unterring von $K(S)[T]$ betrachtet und Lemma 5.8 auf den Körper $K(S)$ anwendet und genauso für $\deg_S$). Daraus folgt

$$0 = \deg_T(S) = \deg_T(gf) = \deg_T(g) + \deg_T(f)$$

und

$$0 = \deg_S(T) = \deg_S(hf) = \deg_S(g) + \deg_S(f).$$

Diese beiden Gleichungen können nur erfüllt sein, wenn alle beteiligten Grade Null sind, insbesondere

$$\deg_T(f) = \deg_S(f) = 0$$

Dann ist aber f eine Konstante und somit $(f) = K[S,T]$. Aber $(S,T) \neq K[S,T]$, da jedes Polynom $g \in (S,T)$ von der Form

$$g(S,T) = Sg_S(S,T) + Tg_T(S,T)$$

ist für zwei Polynome g_S und g_T in $K[S,T]$. Aber das konstante Polynom 1 ist nicht von dieser Form, wie man wieder mit einer Gradüberlegung sehen kann: Jeder Summand in

$$Sg_S(S,T) + Tg_T(S,T),$$

hat entweder $\deg_S \geq 1$ oder $\deg_T \geq 1$. Also ist $Sg_S(S,T) + Tg_T(S,T)$ entweder gleich Null oder $\deg_S(Sg_S(S,T) + Tg_T(S,T)) \geq 1$ oder $\deg_T(Sg_S(S,T) + Tg_T(S,T)) \geq 1$. Aber $\deg_S(1) = \deg_T(1) = 0$, womit obige Überlegung nicht vereinbar ist.

Genauso wie wir für das Ideal $m\mathbb{Z} \subseteq \mathbb{Z}$ den Restklassenring $\mathbb{Z}/m\mathbb{Z}$ konstruieren können, können wir das für ein allgemeines Ideal I eines Rings R: Wir betrachten auf R die Äquivalenzrelation

$$r_1 \sim r_2 \qquad \Leftrightarrow \qquad r_1 - r_2 \in I$$

und definieren R/I als die Menge der Äquivalenzklassen. Für $r_1 \sim r_2$ schreiben wir auch

$$r_1 \equiv r_2 \mod I.$$

und falls $I = (f)$ ein Hauptideal ist,

$$r_1 \equiv r_2 \mod f.$$

Für die Äquivalenzklasse eines Polynoms $g \in K[T]$ schreiben wir $[g]_I$ oder $[g]_f$, falls $I = (f)$. Wenn es keinen Grund zur Verwirrung gibt, schreiben wir auch oft nur $[g]$. Diese Notation ist kompatibel mit der, die wir schon für die Restklassenringe $\mathbb{Z}/m\mathbb{Z}$ eingeführt haben.

Lemma 5.31. *Sei I ein Ideal in einem Ring R. Dann wird R/I mit der induzierten Addition und Multiplikation von R ein Ring.*

Beweis. Übungsaufgabe. □

Wir nennen R/I den *Restklassenring* von R modulo I. Mithilfe des Konzepts der Restklassenringe können wir Ideale in Zusammenhang bringen mit Kernen von Ringhomomorphismen:

Lemma 5.32. *Der Kern eines Ringhomomorphismus $\varphi : R \to R'$ ist ein Ideal von R. Umgekehrt gibt es für jedes Ideal I eines Rings R einen Ringhomomorphismus $\varphi : R \to R'$, dessen Kern gerade I ist.*

Beweis. Wir wollen zeigen, dass der Kern eines Ringhomomorphismus $\varphi : R \to R'$ ein Ideal ist. Seien dazu a und b in $\ker(\varphi)$. Dann gilt

$$\varphi(a-b) = \varphi(a) - \varphi(b) = 0,$$

also $a - b \in \ker(\varphi)$. Das heißt, $\ker(\varphi)$ ist eine (additive) Untergruppe von R. Für $a \in \ker(\varphi)$ und $r \in R$ haben wir

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0,$$

also auch $ra \in \ker(\varphi)$. Somit ist $\ker(\varphi)$ ein Ideal.

Starten wir mit einem Ideal I eines Rings R, so können wir die kanonische Projektion auf den Restklassenring betrachten:

$$\begin{aligned} \varphi : R &\longrightarrow R/I \\ r &\longmapsto [r]_I. \end{aligned}$$

Dann gilt

$$\ker(\varphi) = I,$$

denn die Elemente im Kern sind per Definition die Elemente $r \in R$, die kongruent 0 mod I sind, also in I liegen. □

Wir interessieren uns besonders für die Restklassenringe von $K[T]$. Weil $K[T]$ nach Lemma 5.29 ein Hauptidealring ist, haben all diese die Form $K[T]/(f)$ für ein Polynom $f \in K[T]$, das wir ohne das Ideal (f) zu ändern normiert wählen können. Ist f linear, also $f(T) = T - a$ für eine Konstante $a \in K$, so ist $(f) = (T - a)$ der Kern des Einsetzungshomomorphismus

$$\begin{aligned} \varphi_a : K[T] &\twoheadrightarrow K \\ g &\mapsto g(a). \end{aligned}$$

Es ist klar, dass f im Kern liegt, da $f(a) = a - a = 0$. Für ein Element $g \in \ker(\varphi_a)$ ist a eine Nullstelle von g. Nach Lemma 5.21 gibt es daher ein Polynom $h \in K[T]$, so dass

$$g(T) = (T - a)h(T),$$

also $g \in (T - a)$. Folglich definiert φ_a einen Isomorphismus von $K[T]/(T - a)$ nach K.

Wir wollen nun die Struktur von $K[T]/(f)$ für Polynome f von höherem Grad untersuchen. Die Abbildung

$$\begin{aligned} K &\longrightarrow K[T]/(f) \\ a &\longmapsto [a]_f \end{aligned}$$

definiert einen Ringhomomorphismus, der automatisch injektiv ist. Das liegt daran, dass der Kern ein Ideal von K ist, also entweder $\{0\}$ oder ganz K. Da f nicht konstant ist, ist $[1]_f \neq [0]_f$, also kann der Kern nicht ganz K sein. Wir betrachten im Folgenden K als Unterring von $K[T]/(f)$. Dadurch bekommt $K[T]/(f)$ die Struktur eines K-Vektorraums mit der skalaren Multiplikation

$$a \cdot [g] := [ag] = [a][g]$$

für $a \in K$ und $g \in K[T]/(f)$.

Lemma 5.33. *Für ein nichttriviales Polynom $f \in K[T]$ vom Grad n ist $K[T]/(f)$ ein n-dimensionaler K-Vektorraum. Genauer ist eine Basis gegeben durch*

$$[1], [T], \ldots, [T^{n-1}].$$

Beweis. Sei $n = \deg f$. Für jedes $g \in K[T]$ finden wir durch Polynomdivision r und h in $K[T]$ mit $\deg r < n$, so dass

$$g = r + fh.$$

Es ist also

$$g \equiv r \mod (f).$$

Folglich finden wir für jede Restklasse in $K[T]/(f)$ einen Vertreter $r \in K[T]$ mit $\deg(r) < n$. Dieses Polynom r ist von der Form

$$r(T) = a_0 + a_1 T + \ldots + a_{n-1} T^{n-1}$$

für $a_i \in K[T]$. Daher gilt für die entsprechende Restklasse

$$[r] = a_0[1] + a_1[T] + \ldots a_{n-1}[T^{n-1}].$$

Wir haben somit gezeigt, dass $[1]$, $[T], \ldots, [T^{n-1}]$ ein Erzeugendensystem von $K[T]/(f)$ über K bilden.

Es bleibt zu zeigen, dass dieses Erzeugendensystem minimal ist, d.h. linear unabhängig. Seien $a_0, \ldots, a_{n-1} \in K$, so dass

$$a_0[1] + a_1[T] + \ldots + a_{n-1}[T^{n-1}] = [0].$$

Per Definition der Äquivalenzrelation bedeutet das, dass es ein Polynom $g \in K[T]$ gibt mit

$$a_0 + a_1 T + \ldots a_{n-1} T^{n-1} = g(T) f(T).$$

Vergleichen wir die Grade mithilfe von Lemma 5.8, erhalten wir

$$n - 1 \geq \deg(a_0 + a_1 T + \ldots a_{n-1} T^{n-1}) = \deg(gf) = \deg(g) + \deg(f) = \deg(g) + n.$$

Das kann nur stimmen, wenn $\deg(g)$ negativ ist, also $g = 0$. Dann ist aber auch

$$a_0 + a_1 T + \ldots a_{n-1} T^{n-1} = 0,$$

mit anderen Worten $a_i = 0$ für $i = 0, \ldots, n-1$. Damit ist $[1], [T], \ldots, [T^{n-1}]$ ein linear unabhängiges Erzeugendensystem, also eine Basis von $K[T]/(f)$. □

Wir wollen nun eine Version des chinesischen Restsatzes für Polynomringe beweisen. Dazu überlegen wir uns zunächst, dass für Ideale $J \subseteq I$ eines Rings R der Homomorphismus

$$R/J \longrightarrow R/I$$
$$[a]_J \longmapsto [a]_I$$

wohldefiniert ist. Das liegt daran, dass für $a, b \in R$ mit $[a]_J = [b]_J$ gilt

$$a - b \in J \subseteq I,$$

also $[a]_I = [b]_J$.

Im Polynomring $K[T]$ ist ein Ideal (f) genau dann in einem Ideal (g) enthalten, wenn $f \in (g)$. Per Definition bedeutet das, dass es $h \in K[T]$ gibt mit $f = gh$. Zusammenfassend gilt

$$(f) \subseteq (g) \qquad \Leftrightarrow \qquad g | h.$$

Insbesondere bekommen wir für $f, g \in K[T]$ Homomorphismen

$$K[T]/(fg) \to K[T]/(f) \qquad \text{und} \qquad K[T]/(fg) \to K[T]/(g),$$

die zusammengenommen einen Homomorphismus

$$K[T]/(fg) \longrightarrow K[T]/(f) \times K[T]/(g)$$

induzieren.

Proposition 5.34 (Chinesischer Restsatz für Polynomringe)**.** *Seien f und g teilerfremde Polynome in $K[T]$. Dann ist der Ringhomomorphismus*

$$\varphi : K[T]/(fg) \longrightarrow K[T]/(f) \times K[T]/(g)$$
$$[h]_{fg} \longmapsto ([h]_f, [h]_g)$$

ein Isomorphismus.

Beweis. Zunächst machen wir die Beobachtung, dass φ ein Homomorphismus von K-Vektorräumen ist. Beide Seiten haben die gleiche Dimension, denn nach Lemma 5.33 gilt

$$\dim_K (K[T]/(fg)) = \deg(fg) = \deg(f) + \deg(g)$$

und

$$\dim_K (K[T]/(f) \times K[T]/(g)) = \dim_K (K[T]/(f)) + \dim_K (K[T]/(g)) = \deg(f) + \deg(g).$$

Deshalb genügt es, die Injektivität von φ zu zeigen.

Sei $h \in \ker(\varphi)$. Dann gilt

$$[h]_f = 0 \qquad \text{und} \qquad [h]_g = 0.$$

Laut Definition der Äquivalenzrelation gibt es daher Polynome a und b in $K[T]$, so dass

$$fa = h = gb,$$

also $f|h$ und $g|h$. Da f und g teilerfremd sind, folgt daraus $fg|h$ (das sieht man mit der eindeutigen Primfaktorzerlegung aus Satz 5.20). Das heißt aber nichts anderes als $[h]_{fg} = 0$. Somit ist $\ker(\varphi) = 0$ und φ ist injektiv. □

Proposition 5.35. *Der Restklassenring $K[T]/(f)$ ist genau dann ein Körper, wenn f irreduzibel ist.*

Beweis. Wenn f reduzibel ist, gibt es nichtkonstante Polynome $g, h \in K[T]$ mit

$$f = gh.$$

Daraus folgt

$$\deg(g) < \deg(f) \qquad \text{und} \qquad \deg(h) < \deg(f).$$

Dann kann aber weder $f|g$ noch $f|h$ gelten, weswegen

$$[g]_f \neq 0 \qquad \text{und} \qquad [h]_f \neq 0.$$

Aber

$$[g]_f[h]_f = [gh]_f = [f]_f = 0,$$

also sind $[g]_f$ und $[h]_f$ nichttriviale Nullteiler in $K[T]/(f)$. Da Körper nullteilerfrei sind, kann $K[T]/(f)$ kein Körper sein.

Nehmen wir nun an, dass f irreduzibel ist. Um zu zeigen, dass $K[T]/(f)$ ein Körper ist, müssen wir für jede nichttriviale Restklasse $[h]_f$ eine Inverse finden. Sei $g = \mathrm{ggT}(f, h)$. Das ist ein Teiler von f. Da f irreduzibel ist, ist g entweder eine Konstante oder $g = af$ für eine Konstante a. Der zweite Fall tritt nicht ein, da $[g]_f \neq 0$. Also ist $g = 1$ (g ist per Definition normiert). Aus Proposition 5.18 erhalten wir Polynome $a, b \in K[T]$ mit

$$1 = af + bh.$$

Dann gilt

$$[b]_f[h]_f = [bh]_f = [1 - af]_f = [1]_f.$$

Das bedeutet, dass $[b]_f$ invers zu $[h]_f$ ist. □

Für $K = \mathbb{F}_p$ und ein irreduzibles Polynom $f \in \mathbb{F}_p[T]$ vom Grad r ist $\mathbb{F}_p[T]/(f)$ folglich ein Körper mit p^r Elementen. Wir haben allerdings noch nicht gezeigt, dass es für jede natürliche Zahl $r \in \mathbb{N}$ ein irreduzibles Polynom in $\mathbb{F}_p[T]$ vom Grad r gibt. Um dieser Frage nachzugehen, untersuchen wir für eine Primzahl p die zahlentheoretische Funktion

$$\begin{aligned} h_p : \mathbb{N} &\longrightarrow \mathbb{C}, \\ m &\longmapsto \#\{f \in \mathbb{F}_p[T] \text{ normiert, irreduzibel, } \deg(f) = m\} \end{aligned}$$

Proposition 5.36. *Sei p eine Primzahl und m eine natürliche Zahl. Dann gilt*

$$h_p(m) = \frac{1}{m} \sum_{d|m} p^d \mu(\frac{m}{d}),$$

wobei μ die Möbiusfunktion ist.

Beweis. Übungsaufgabe. □

Korollar 5.37. *Für jede natürliche Zahl m gibt es ein irreduzibles Polynom $f \in \mathbb{F}_p[T]$ vom Grad m.*

Beweis. Wir müssen zeigen, dass $h_p(m) > 0$. Dafür benutzen wir die explizite Formel für $h_p(m)$ aus Proposition 5.36:

$$h_p(m) = \frac{1}{m} \sum_{d|m} p^d \mu\left(\frac{m}{d}\right).$$

Der Vorfaktor $\frac{1}{m}$ spielt für die Frage der Positivität keine Rolle. Wir haben $\mu\left(\frac{m}{m}\right) = 1$ und $\mu\left(\frac{m}{d}\right) \geq -1$ für alle Teiler d von m mit $d < n$. Also erhalten wir

$$mh_p(m) = p^m + \sum_{\substack{d|m \\ d<m}} p^d \mu\left(\frac{m}{d}\right) \geq p^m - \sum_{\substack{d|m \\ d<m}} p^d \geq p^m - \sum_{d=0}^{m-1} p^d = p^m - \frac{p^m - 1}{p-1} > 0.$$

□

Korollar 5.38. *Für jede Primzahl p und jede natürliche Zahl m gibt es einen Körper mit p^m Elementen.*

Beweis. Korollar 5.37 gibt uns ein irreduzibles Polynom $f \in \mathbb{F}_p[T]$ vom Grad m. Wegen Proposition 5.35 ist

$$K := \mathbb{F}_p[T]/(f)$$

ein Körper. Außerdem trägt K nach Lemma 5.33 die Struktur eines m-dimensionalen $\mathbb{F}_p$-Vektorraums. Daraus können wir die Kardinalität berechnen:

$$|K| = |\mathbb{F}_p^m| = p^m.$$

□

5.6. **Eindeutigkeit von endlichen Körpern.** Wir haben in Korollar 5.38 einen Körper mit p^m Elementen konstruiert. Wir wissen allerdings noch nichts darüber wie viele Körper mit p^m Elementen es bis auf Isomorphie gibt. Es ist durchaus denkbar, dass für verschiedene irreduzible Polynome f und f' in $\mathbb{F}_p[T]$ die Körper

$$\mathbb{F}_p[T]/(f) \qquad \text{und} \qquad \mathbb{F}_p[T]/(f')$$

nicht isomorph sind.

Beispiel 5.39. Über $\mathbb{Q}$ gibt es viele verschiedene Körpererweiterungen vom Grad 2, also Körper K, die $\mathbb{Q}$ enthalten mit $\dim_{\mathbb{Q}}(K) = 2$. Um das zu sehen betrachten wir $\mathbb{Q}$ als Teilkörper von $\mathbb{R}$. Sei K_1 der Teilkörper von $\mathbb{R}$, der von $\mathbb{Q}$ und $\sqrt{2}$ erzeugt wird und K_2 der Teilkörper, der von $\mathbb{Q}$ und $\sqrt{3}$ erzeugt wir. Dann haben wir Isomorphismen

$$\begin{aligned} \mathbb{Q}[T]/(T^2-2) &\xrightarrow{\sim} K_1 \\ T &\longmapsto \sqrt{2} \end{aligned}$$

und

$$\begin{aligned} \mathbb{Q}[T]/(T^2-3) &\xrightarrow{\sim} K_1 \\ T &\longmapsto \sqrt{3}. \end{aligned}$$

Die Körper K_1 und K_2 kann man also auch durch die Konstruktion aus Abschnitt 5.5 erhalten. Insbesondere sehen wir dadurch mithilfe von Lemma 5.33, dass

$$\dim_{\mathbb{Q}}(K_1) = \dim_{\mathbb{Q}}(K_2) = 2.$$

Genauer gesagt können wir durch Lemma 5.33 die Körper K_1 und K_2 explizit hinschreiben:

$$K_1 = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\} \qquad \text{und} \qquad K_2 = \{a + b\sqrt{3} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$$

Aber K_1 und K_2 sind nicht isomorph, denn wäre

$$\sigma : K_1 \to K_2$$

ein Isomorphismus, so bekommen wir einen Widerspruch, wenn wir das Bild von $\sqrt{2}$ untersuchen:

$$2 = \sigma(2) = \sigma((\sqrt{2})^2) = \sigma(\sqrt{2})^2$$

Die einzigen beiden Elemente in $\mathbb{R}$, die diese Gleichung erfüllen, sind $\sqrt{2}$ und $-\sqrt{2}$, also

$$\sigma(\sqrt{2}) \in \{\pm\sqrt{2}\}.$$

Aber $\pm\sqrt{2} \notin K_2$.

Für endliche Körper sieht die Sache aber anders aus. Wir wollen in diesem Abschnitt zeigen, dass es für jede mögliche Kardinalität p^r *nur einen* Körper mit p^r Elementen gibt.

Proposition 5.40. *Sei p eine Primzahl. Wir betrachten im Polynomring $\mathbb{F}_p[T]$ das Polynom $T^{p^n} - T$ für eine natürliche Zahl n.*

(i) Für $d \in \mathbb{N}$ mit $d|n$ kommt jedes irreduzible Polynom vom Grad d in der Primfaktorzerlegung von $T^{p^n} - T \in \mathbb{F}_p[T]$ genau einmal vor.
(ii) Der Grad d jedes irreduziblen Faktors von $T^{p^n} - T$ teilt n.

Beweis. Übungsaufgabe □

Korollar 5.41. *Seien p eine Primzahl und m eine natürliche Zahl. Dann sind alle Körper mit p^m Elementen isomorph.*

Beweis. Nach Korollar 5.37 gibt es ein irreduzibles Polynom $f \in \mathbb{F}_p[T]$ vom Grad m. Nach Multiplikation mit einer Konstante können wir annehmen, dass f normiert ist. Wir wollen zeigen, dass alle endlichen Körper K der Kardinalität p^m isomorph zu

$$\mathbb{F}_p[T]/(f)$$

sind.

Wir betrachten die Primfaktorzerlegung des Polynoms

$$T^{p^m} - T \in \mathbb{F}_p[T].$$

Nach Proposition 5.40 ist sie von der Form

$$T^{p^m} - T = f_1 \cdot \ldots \cdot f_r,$$

wobei die f_i alle normierten, irreduziblen Polynome über $\mathbb{F}_p$ durchlaufen, deren Grad m teilt. Insbesondere stimmt f mit einem der Polynome f_i überein. Nun schauen wir uns das Polynom $T^{p^m} - T$ als Polynom über K an, also als Element von $K[T]$. Die multiplikative Gruppe $K^\times$ hat die Ordnung $p^m - 1$. Deshalb gilt für alle Elemente $a \in K^\times$ nach Korollar 5.6

$$a^{p^m-1} = 1 \qquad \Rightarrow \qquad a^{p^m} = a.$$

Alle Elemente von $K^\times$ sind daher Nullstellen des Polynoms

$$T^{p^m} - T.$$

Offensichtlich ist auch die Null eine Nullstelle, also sind alle Elemente von K Nullstellen.

Der Körper K hat p^m Elemente und das Polynom $T^{p^m} - T$ hat höchstens p^m Nullstellen (Satz 5.22). Also gibt es *genau* p^m Nullstellen und wir können $T^{p^m} - T$ durch sukzessive Anwendung von Lemma 5.21 in Linearfaktoren zerlegen. Zerlegen wir alle Polynome f_i über K in irreduzible Polynome in $K[T]$ und bilden deren Produkt, so sollte wegen der Eindeutigkeit der Primfaktorzerlegung (Satz 5.20) das gleich rauskommen. Insbesondere zerfällt f daher in $K[T]$ in Linearfaktoren und wir finden in K eine Nullstelle a von f. Mit dieser Nullstelle a definieren wir den Homomorphismus

$$\begin{aligned} \varphi_a : \mathbb{F}_p[T] &\longrightarrow K \\ g &\longmapsto g(a). \end{aligned}$$

Da a eine Nullstelle von f ist, liegt f im Kern von φ_a und wir erhalten einen induzierten Homomorphismus

$$\begin{aligned} \overline{\varphi}_a : \mathbb{F}_p[T]/(f) &\longrightarrow K \\ [g]_f &\longmapsto g(a). \end{aligned}$$

Da f über $\mathbb{F}_p$ irreduzibel ist, ist $\mathbb{F}_p[T]/(f)$ ein Körper und somit $\overline{\varphi}_a$ automatisch injektiv. (A posteriori ist dann (f) schon der ganze Kern von φ_a, aber das nur als Nebenbemerkung.) Außerdem haben beide Seiten die gleiche Kardinalität p^m. Folglich muss $\overline{\varphi}_a$ ein Isomorphismus sein. □

Wir haben damit insbesondere gezeigt, dass für fest gewähltes $m \in \mathbb{N}$ alle Körper der Form

$$\mathbb{F}_p[T]/(f)$$

für ein irreduzibles Polynom f vom Grad m isomorph sind. Wir fassen die Ergebnisse dieses Kapitels in folgendem Satz zusammen:

Satz 5.42. *Die Kardinalität eines endlichen Körpers ist gleich p^m für eine Primzahl p und eine natürliche Zahl m. Umgekehrt gibt es für jede Primzahl p und jede natürliche Zahl m bis auf Isomorphie genau einen endlichen Körper der Kardinalität p^m.*

Beweis. Dass die Kardinalität eines endlichen Körpers von der Form p^m ist, ist die Aussage von Proposition 5.27. Die Existenz eines endlichen Körpers mit p^m Elementen ist der Inhalt von Korollar 5.38 und die Eindeutigkeit ist Korollar 5.41. □

Satz 5.42 rechtfertigt es von *dem* endlichen Körper mit p^m Elementen zu sprechen. Wir benutzen für ihn die Notation $\mathbb{F}_{p^m}$. Man sollte unbedingt aufpassen und $\mathbb{F}_{p^m}$ nicht mit $\mathbb{Z}/p^m\mathbb{Z}$ verwechseln. Diese beiden Ringe sind nur für $m = 1$ isomorph. Für $m > 0$ is $\mathbb{Z}/p^m\mathbb{Z}$ kein Körper, weil es nichttriviale Nullteiler gibt (z.B. $[p]_{p^m}$).

6. Die Riemannsche zeta-Funktion

Die Riemannsche Zeta-Funktion ist für eine komplexe Variable s mit Realteil $\Re(s) > 1$ definiert als

$$\zeta(s) := \sum_{s=1}^{\infty} \frac{1}{n^s}.$$

Sie wurde schon von Euler im 18. Jahrhundert studiert, allerdings nur für reelle Werte von s. Insbesondere interessierte sich Euler für das *Basler Problem*, das nach der Summe über alle reziproken Quadratzahlen $1/n^2$ fragt, also dem Wert $\zeta(2)$. Riemann beschäftigte sich eingehend mit der Zeta-Funktion und zeigte, dass man sie zu einer analytischen Funktion auf $\mathbb{C} \setminus \{1\}$ fortsetzen kann mit einem einfachen Pol bei $s = 1$. Er bewies außerdem die *Funktionalgleichung*, die einen Zusammenhang herstellt zwischen $\zeta(s)$ und $\zeta(1 - s)$.

Die Werte der Riemannschen Zeta-Funktion bei ganzen Zahlen haben große zahlentheoretische Bedeutung. Für positive gerade ganze Zahlen $2n$ kann man sie folgendermaßen berechnen:

$$\zeta(2n) = \frac{(1-)^{n+1} B_{2n} (2\pi)^{2n}}{2(2n)!},$$

wobei B_{2n} die $2n$-te Bernoullizahl ist. Für ungerade positive ganze Zahlen ist keine geschlossene Formel bekannt und diese Werte sind wesentlich mysteriöser. Man weiß immerhin, dass unendlich viele der $\zeta(2n+1)$ irrational sind. Für negative ganze Zahlen und Null gibt es wieder einen Ausdruck mit Bernoullizahlen:

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

Da die Bernoullizahlen rational sind, sind diese Werte rational und gleich Null, wenn n positv und gerade ist.

Wir haben im letzten Abschnitt erwähnt, dass die Riemannschen Zeta-Funktion an allen geraden negativen ganzen Zahlen eine Nullstelle hat. Es ist eine der größten Vermutungen der reinen Mathematik, dass alle weiteren Nullstellen auf der Geraden $\Re(s) = 1/2$ liegen:

Riemannsche Vermutung. *Bis auf die negativen ganzen Zahlen liegen alle Nullstellen der Riemannschen Zeta-Funktion auf der Geraden $\Re(s) = 1/2$.*

Die Nullstellen der Riemannschen Zeta-Funktion stehen im Zusammenhang mit der Verteilung der Primzahlen.

6.1. **Holomorphe Funktionen.** Um die Riemannsche Zeta-Funktion zu untersuchen brauchen wir einige Techniken aus der Funktionentheorie. Die grundlegenden Begriffe stellen wir in diesem Abschnitt zusammen.

Definition 6.1. Ein *Gebiet* in $\mathbb{C}$ ist eine nichtleere, zusammenhängende, offene Teilmenge von $\mathbb{C}$

Für eine Funktion

$$f : D \to \mathbb{C}$$

auf einem Gebiet $D \subseteq \mathbb{C}$ und einen Punkt $z_0 \in D$ betrachten wir den Grenzwert

$$\lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}.$$

Falls er existiert (also für alle Folgen, die zu z_0 konvergieren der entsprechende Grenzwert existiert und jeweils den gleichen Wert ergibt), ist f in z *komplex differenzierbar* und wir bezeichnen den Grenzwert mit f'.

Definition 6.2. Eine *holomorphe* Funktion auf einem Gebiet $D \subseteq \mathbb{C}$ ist eine Funktion

$$f : D \longrightarrow \mathbb{C},$$

die in allen Punkten komplex differenzierbar ist.

Als Vektorraum ist $\mathbb{C}$ isomorph zu $\mathbb{R}^2$. Fassen wir eine komplex differenzierbare Funktion f als eine Funktion nach $\mathbb{R}^2$ auf, so ist sie als solche differenzierbar. Andersherum definiert bei weitem nicht jede differenzierbare Funktion $\mathbb{R}^2 \to \mathbb{R}^2$ eine holomorphe Funktion. Beispielsweise ist

$$z = x + iy \mapsto x$$

nicht holomorph.

Proposition 6.3. *Sei $D \subseteq \mathbb{C}$ ein Gebiet. Eine Funktion*

$$f : D \to \mathbb{C}$$

ist genau dann holomorph, wenn sie analytisch *ist, das heißt wenn es für jeden Punkt $z_0 \in D$ eine offene Umgebung U gibt, in der f eine Reihendarstellung*

$$f(z) = \sum_{i=0}^{\infty} a_i (z - z_0)^i$$

hat mit $a_i \in \mathbb{C}$.

An dieser Proposition sieht man auch, dass eine holomorphe Funktion nicht so viele Freiheitsgrade hat. Sie ist schon (auf U) bestimmt durch die abzählbar vielen Koeffizienten a_i. Das legt nahe, dass sie schon durch abzählbar viele Funktionswerte bestimmt ist. Genauer gilt das folgende Resultat:

Satz 6.4 (Identitätssatz)**.** *Sei $D \subseteq \mathbb{C}$ ein Gebiet und $S \subseteq D$ eine Teilmenge mit einem Häufungspunkt in D. Seien*

$$f_1, f_2 : D \to \mathbb{C}$$

holomorphe Funktionen, so dass

$$f_1(s) = f_2(s)$$

für alle $s \in S$. Dann folgt $f_1 = f_2$.

Definition 6.5. Eine meromorphe Funktion auf einem Gebiet $D \subseteq \mathbb{C}$ ist eine holomorphe Funktion

$$f : D \setminus S \longrightarrow \mathbb{C}$$

für eine diskrete Teilmenge $S \subseteq D$, so dass alle $s \in S$ Polstellen sind, das heißt für jedes $s \in S$ existiert eine Umgebung U von s in D, so dass $1/f$ auf U holomorph ist.

Für eine meromorphe Funktion und jedes s aus der Teilmenge S aus der Definition findet man eine Umgebung U mit $U \cap S = \{s\}$, so dass f auf $U \setminus \{s\}$ eine Reihendarstellung der Form

$$f(z) = \sum_{i=-n}^{\infty} a_i (z - z_0)^i$$

hat, wobei $n \in \mathbb{Z}$ und $a_i \in \mathbb{C}$. Ist $a_{-n} \neq 0$, so heißt n die *Ordnung* der Polstelle. Der Koeffizient a_{-1} von $(z - z_0)^{-1}$ spielt eine besondere Rolle. Wir nennen ihn das *Residuum* von f bei s und schreiben dafür

$$\mathrm{Res}(f, s) = a_{-1}.$$

Satz 6.6 (Residuensatz)**.** *Sei D ein einfach zusammenhängendes Gebiet (also ohne Löcher) und $S \subseteq D$ eine diskrete Teilmenge. Wir betrachten eine holomorphe Funktion*

$$f : D \setminus S \longrightarrow \mathbb{C}$$

und eine stückweise differenzierbare Kurve

$$\gamma : [0, 1] \to D$$

mit $\gamma(0) = \gamma(1)$. Dann gilt

$$\oint_\gamma f(z)dz = 2\pi i \sum_{s \in S} I(\gamma, s)\mathrm{Res}(f, s).$$

Hierbei benutzen wir folgende Notation für das Wegintegral

$$\oint_\gamma f(z)dz := \int_0^1 f(\gamma(t))\gamma'(t)dt$$

und $I(\gamma, s)$ bezeichnet die Windungszahl der Kurve γ um 2, das heißt die Anzahl der Umrundungen, gegen den Uhrzeigersinn gezählt.

6.2. **Das Eulerprodukt.** Wir kehren zurück zur Riemannschen Zeta-Funktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

(für $\Re(s) > 1$). Für die komplexe Variable s benutzen wir die Notation

$$s = \sigma + it.$$

Um die Konvergenz der Zeta-Funktion zu zeigen, werden wir ihre Einschränkung auf die Halbebenen

$$H_{1+\delta} := \{z \in \mathbb{C} \mid \Re(z) > 1 + \delta$$

für $\delta > 0$ untersuchen.

Proposition 6.7. *Auf $H_{1+\delta}$ konvergiert die Reihe $\sum_n n^{-s}$ absolut und gleichmäßig.*

Beweis. Mit der obigen Notation $s = \sigma + it$ erhalten wir

$$n^s = e^{s \log n} = e^{(\sigma+it)\log n} = e^{\sigma \log n} e^{it \log n} = n^s e^{it \log n}.$$

Somit gilt für den Absolutbetrag

$$|n^s| = n^\sigma \geq n^{1+\delta}.$$

Damit ist die konstante Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}}$$

eine Majorante von $\sum_n n^{-s}$, woraus die absolute und gleichmäßige Konvergenz folgt. □

Korollar 6.8. *Für $\Re(s) > 1$ ist die oben definierte Riemannsche Zeta-Funktion $\zeta(s)$ holomorph.*

Beweis. Wir finden δ, so dass

$$\Re(s) > \delta > 1.$$

Dann ist s in $H_{1+\delta}$ enthalten und ζ ist auf $H_{1+\delta}$ holomorph, da ζ nach Proposition 6.7 der Limes einer absolut und gleichmäßig konvergenten Folge holomorpher Funktionen ist. □

Ziel dieses Abschnittes ist es die Produktdarstellung der Riemannschen Zeta-Funktion herzuleiten. Darunter versteht man die Identität

$$\zeta(s) = \prod_{p \text{ prim}} \frac{1}{1 - p^{-s}}.$$

Die rechte Seite bezeichnet man auch als Eulerprodukt und die einzelnen Faktoren

$$\frac{1}{1 - p^{-s}}$$

heißen Eulerfaktoren. Es ist kein Zufall, dass der Eulerfaktor bei p gerade die Potenzreihe ausgewertet bei p^{-s} zur konstanten Funktion $n \mapsto 1$ ist.

Um die Produktformel zu beweisen, müssen wir uns zunächst mit der Konvergenz des Eulerprodukts beschäftigen. Wir erinnern uns daran, dass ein Produkt der Form

$$\prod_{n=1}^{\infty} (1 + f_n)$$

mit holomorphen Funktionen f_n auf einem Gebiet D *normal* konvergiert, falls für jedes Kompaktum $K \subseteq D$ gilt

$$\sum_{n=1}^{\infty} \sup_{z \in K} |f_n(z)| < \infty.$$

In diesem Fall konvergiert das Produkt gleichmäßig auf Kompakta. Daher kommt es nicht auf die Reihenfolge der Faktoren an und der Grenzwert ist eine holomorphe Funktion.

Lemma 6.9. *Das Eulerprodukt*

$$\prod_{p \text{ prim}} \frac{1}{1 - p^{-s}}$$

konvergiert normal auf

$$H := \{z \in \mathbb{C} \mid \Re(z) > 1\}.$$

Beweis. Wir werden für

$$f_p := \frac{1}{1-p^{-s}} - 1 = \frac{p^{-s}}{1-p^{-s}}$$

und $\delta > 0$ zeigen, dass

$$\sum_{p \text{ prim}} \sup_{z \in H_{1+\delta}} |f_p(z)| < \infty.$$

Daraus folgt die normale Konvergenz, da jedes Kompaktum in H in einer der offenen Teilmengen $H_{1+\delta}$ enthalten ist.

Es gilt

$$|\frac{1}{p^s}| = \frac{1}{p^\sigma} < \frac{1}{p^{1+\delta}} < \frac{1}{2}.$$

Daraus folgt

$$|1 - p^{-s}| > \frac{1}{2}$$

und somit ist

$$|f_p| = |\frac{p^{-s}}{1-p^{-s}}| = \frac{|p^{-s}|}{|1-p^{-s}|} < \frac{|p^{-s}|}{1/2} = 2|p^{-s}| < \frac{2}{p^{1+\delta}}.$$

Da

$$\sum_{p \text{ prim}} \frac{1}{p^{1+\delta}} \leq \sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}} < \infty,$$

folgt daraus die normale Konvergenz. □

Satz 6.10 (Produktformel)**.** *Für alle $s \in \mathbb{C}$ mit $\Re(s) > 1$ gilt*

$$\zeta(s) = \prod_{p \text{ prim}} \frac{1}{1-p^{-s}}.$$

Beweis. Sei $(p_i)_{i \in \mathbb{N}}$ die Folge aller Primzahlen (der Größe nach geordnet). Wir betrachten das Eulerprodukt der ersten n davon, also

$$\prod_{i=1}^{n} \frac{1}{1-p_i^{-s}}.$$

Die einzelnen Faktoren bilden den Grenzwert der geometrischen Reihe bezüglich p_i^{-s}. Durch Ausmultiplizieren erhalten wir

$$\prod_{i=1}^{n} \frac{1}{1-p_i^{-s}} = \prod_{i=1}^{n} \sum_{m_i=0}^{\infty} \left(\frac{1}{p_i^s}\right)^{m_i} = \sum_{m_1,\ldots,m_n=0}^{\infty} \frac{1}{p_1^{sm_1} \cdots p_n^{m_n}}.$$

Die Summanden auf der rechten Seite durchlaufen gerade alle Werte $1/n^s$ für natürliche Zahlen, in deren Primfaktorzerlegung nur die ersten n Primzahlen $p_1, \ldots, p_n$ vorkommen. Wegen der Eindeutigkeit der Primfaktorzerlegung kommt jede solche natürliche Zahl nur einmal vor. Im Grenzwert für $n \to \infty$ erhalten wir auf der rechten Seite das Eulerprodukt über alle Primzahlen und auf der linken Seite die Summe über alle $1/n^s$ für alle natürlichen Zahlen, die eine Primfaktorzerlegung besitzen. Wegen der Existenz der Primfaktorzerlegung sind dies alle natürlichen Zahlen.

Über Konvergenz müssen wir uns an dieser Stelle keine Gedanken mehr machen, da wir aus Proposition 6.7 und Lemma 6.9 wissen, dass es auf beiden Seiten nicht auf die Reihenfolge der Summation beziehungswese Multiplikation ankommt. □

Aus dem Beweis der Produktformel kann man die Interpretation ziehen, dass die Produktformel die Existenz und Eindeutigkeit der Primfaktorzerlegung in analytischer Form kodiert. Dies ist die erste einer ganzen Reihe von zahlentheoretischen Erkenntnissen, die in Identitäten über die Riemannsche Zetafunktion versteckt sind.

6.3. **Analytische Fortsetzung und Funktionalgleichung.** Wir beweisen in diesem Abschnitt, dass sich die Riemannsche Zeta-Funktion auf das Gebiet $\{z \in \mathbb{C} \mid \Re(z) > 0\}$ fortsetzen lässt mit einer Polstelle bei $s = 1$. Tatsächlich gibt es eine analytische Fortsetzung auf ganz $\mathbb{C}$. Das werden wir allerdings nicht beweisen um uns nicht zu tief in die Analysis zu stürzen.

Die Fortsetzung beruht auf dem Prinzip der abelschen partiellen Summation:

Proposition 6.11 (abelsche partielle Summation)**.** *Seien $(a_n)_{n\geq n_0}$ eine Folge komplexer Zahlen und*

$$f : [n_0, \infty] \to \mathbb{C}$$

eine stetig differenzierbare Funktion. Für eine reelle Zahl $x \geq n_0$ definieren wir

$$A(x) := \sum_{n_0 \leq n \leq x} a_n.$$

Dann gilt

$$\sum_{n_0 \leq n \leq x} a_n f(n) = A(x)f(x) - \int_{n_0}^{x} A(u)f'(u)du$$

Beweis. Übungsaufgabe. Das Integral zu berechnen ist nicht schwierig, da $A(x)$ eine Treppenfunktion ist und man $f'(u)$ über den Hauptsatz der Integral- und Differenzialrechnung integrieren kann. □

Proposition 6.12. *Die Riemannsche Zeta-Funktion hat eine meromorphe Fortsetzung auf das Gebiet*

$$H_0 = \{z \in \mathbb{C} \mid \Re(z) > 0\}.$$

Genauer gesagt ist ζ auf H_0 holomorph außer bei $s = 1$, wo ζ einen einfachen Pol mit Residuum 1 hat.

Beweis. Wir erinnern uns an die Notation $\lfloor x \rfloor$ für eine reelle Zahl x. Diese bezeichnet die größte ganze Zahl, die kleiner oder gleich x ist. Wir wenden abelsche partielle Summation (Proposition 6.11) auf die konstante Folge $a_n = 1$, $n_0 = 1$ und die Funktion $f(x) = x^{-s}$ an. Dafür brauchen wir die Ableitung von f:

$$f'(x) = -\frac{s}{x^{s+1}}.$$

und die Funktion

$$A(x) := \sum_{n \leq x} a_n = \sum_{n \leq x} 1 = \lfloor x \rfloor.$$

Die Formel für die abelsche partielle Summation nimmt dann die folgende Form an

$$\sum_{n \leq x} \frac{1}{n^s} = \frac{\lfloor x \rfloor}{x^s} + s \int_1^x \frac{\lfloor u \rfloor}{u^{s+1}} du. \tag{11}$$

Für $\sigma = \Re(s) > 1$ konvergiert

$$\frac{\lfloor x \rfloor}{x^s}$$

für $x \to \infty$ gegen 0, denn

$$\left|\frac{\lfloor x \rfloor}{x^s}\right| \leq \left|\frac{1}{x^{s-1}}\right| = \frac{1}{x^{\sigma-1}} \overset{x\to\infty}{\longrightarrow} 0.$$

Aus (11) wird daher im Limes $x \to \infty$ (unter der Annahme $\Re(s) > 1$)

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = s \int_1^{\infty} \frac{\lfloor u \rfloor}{u^{s+1}} du.$$

Man beachte, dass das Integral für $\sigma > 1$ tatsächlich existiert, da

$$\left|\frac{\lfloor u \rfloor}{u^{s+1}}\right| \leq \frac{1}{u^{\sigma}}.$$

Wir spalten das Integral nun folgendermaßen auf

$$\zeta(s) = s \int_1^{\infty} \frac{du}{u^s} - s \int_1^{\infty} \frac{u - \lfloor u \rfloor}{u^{s+1}} du = \frac{s}{s-1} - s \int_1^{\infty} \frac{u - \lfloor u \rfloor}{u^{s+1}} du. \tag{12}$$

Der entscheidende Punkt ist, dass das verbliebene Integral sogar für $\Re(s) > 0$ konvergiert, denn

$$\left|\frac{u - \lfloor u \rfloor}{u^{s+1}}\right| \leq \left|\frac{1}{u^{\sigma+1}}\right|.$$

In der Tat stellt dieses Integral eine holomorphe Funktion auf H_0 dar, denn wir können es als absolut und gleichmäßig konvergente Reihe schreiben:

$$\int_1^{\infty} \frac{u - \lfloor u \rfloor}{u^{s+1}} du = \sum_{n=1}^{\infty} \int_n^{n+1} \frac{u - n}{u^{s+1}} du.$$

Die absolute, gleichmäßige Konvergenz folgt aus der Abschätzung

$$\left|\int_n^{n+1} \frac{u-n}{u^{s+1}} du\right| \leq \sup_{n \leq u \leq n+1} \left|\frac{u-n}{u^{s+1}}\right| \leq \frac{1}{n^{\sigma+1}},$$

denn $\sum_n 1/n^{\sigma+1}$ konvergiert für $\sigma > 0$.

Zusammenfassend gilt für $\Re(s) > 1$ die Gleichung (12). Die rechte Seite definiert aber auch für $\Re(s) > 0$ eine meromorphe Funktion, liefert also eine Fortsetzung. Das Integral in (12) ist holomorph und der Term

$$\frac{s}{s-1} = \frac{1}{s-1} + 1$$

hat einen einfachen Pol bei $s = 1$ mit Residuum 1. Das zeigt die Behauptung. □

Für komplexe Zahlen s mit Realteil $\Re(s) > 0$ kann man an der Produktdarstellung

$$\zeta(s) = \prod_{p \text{ prim}} \frac{1}{1 - p^{-s}}$$

ablesen, dass $\zeta(s) \neq 0$. Genauer gesagt liegt das daran, dass ein normal konvergentes Produkt nur dann Null ist, wenn mindestens einer der Faktoren Null ist. Daher wissen wir schon, dass alle Nullstellen von $\zeta(s)$ Realteil ≤ 1 haben müssen.

Satz 6.13. *Die Riemannsche Zeta-Funktion hat keine Nullstellen auf der Geraden* $\Re(s) = 1$.

Beweis. Angenommen es gibt eine Nullstelle $1+i\tau$ auf der Geraden $\Re(s)=1$. Dann ist $\tau \neq 0$, denn wir wissen schon, dass $\zeta(s)$ bei $s=1$ eine Polstelle hat. Wir betrachten die Funktion

$$F(s) = \zeta(s)^3\zeta(s+i\tau)^4\zeta(s+2i\tau).$$

Der erste Faktor ζ^3 hat bei $s=1$ eine Polstelle der Ordnung 3. Nach Annahme hat $\zeta(s+i\tau)^4$ eine Nullstelle der Ordnung mindestens 4 und $\zeta(s+2i\tau)$ ist holomorph bei $s=1$, weil $\tau \neq 0$. Insgesamt ist somit $F(s)$ für $\Re(s)>0$ definiert und überall holomorph mit einer Nullstelle bei $s=1$.

Das wollen wir zu einem Widerspruch führen, indem wir zeigen, dass für $\Re(s)>1$ der Logarithmus von $|F(s)|$ immer größer als 0 ist. Hierfür brauchen wir den komplexen Logarithmus, der für positive reelle Zahlen mit dem reellen Logarithmus übereinstimmt. Sein Definitionsgebiet ist

$$\mathbb{C} \setminus \mathbb{R}_{\leq 0}.$$

Um $\zeta(s)$ in den Logarithmus einzusetzen, müssen wir uns davon überzeugen, dass die Zeta-Funktion für $\Re(s)>1$ keine nichtpositiven reellen Werte annimmt. Wir erinnern uns daran, dass das Eulerprodukt normal konvergiert (Lemma 6.9), dass also

$$\frac{1}{1-p^{-s}} = 1 + f_p$$

gilt für holomorphe Funktionen f_p mit

$$\sum_{p \text{ prim}} \sup_{s\in K} |f_p(s)| < \infty$$

für alle Kompakta K im Definitionsbereich. Wir haben im Beweis von Lemma 6.9 sogar gezeigt, dass $|f_p(s)|<1$ und daraus kann man folgern, dass der Realteil jedes Eulerfaktors und auch des ganzen Eulerprodukts nicht negativ ist.

Wir erhalten

$$\log\zeta(s) = \sum_{p \text{ prim}} \log\frac{1}{1-p^{-s}} = -\sum_{p \text{ prim}} \log(1-p^{-s}).$$

Wir benutzen nun die Reihenentwicklung des Logarithmus um 1:

$$\log(1+z) = \sum_{m=1}^{\infty} (-1)^{m+1}\frac{z^m}{m},$$

die für $|z|<1$ konvergiert. Für $z=-p^{-s}$ erhalten wir

$$\log\zeta(s) = \sum_{p \text{ prim}} \sum_{m=1}^{\infty} \frac{1}{mp^{-sm}}.$$

Definieren wir

$$\Lambda_1(n) := \begin{cases} \frac{1}{m} & n = p^m, \\ 0 & \text{sonst}, \end{cases}$$

so können wir die Reihe schreiben als

$$\log\zeta(s) = \sum_{n=1}^{\infty} \frac{\Lambda_1(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\Lambda_1(n)}{n^\sigma} e^{-it\log n}$$

und müssen uns nur merken, dass $\Lambda_1(n)$ nichtnegative reelle Zahlen sind.

Letztendlich interessieren wir uns für $\log|\zeta(s)|$. Um das zu berechnen, machen wir uns klar wie man $\log|y|$ für eine komplexe Zahl $y \in \mathbb{C} \setminus \mathbb{R}_{\leq 0}$ aus $\log y$ bestimmen kann. Dazu schreiben wir

$$y = re^{i\varphi}$$

mit $r \in \mathbb{R}_{>0}$ und $\varphi \in (-\pi, \pi)$. Dann gilt

$$\log y = \log r + i\varphi$$

und

$$\log|y| = \log r = \Re(\log y).$$

Angewandt auf $\zeta(s)$ ergibt das

$$\log|\zeta(s)| = \Re(\log\zeta(s)) = \sum_{n=1}^{\infty} \frac{\Lambda_1(n)}{n^\sigma} \cos(t\log n).$$

Damit können wir den Logarithmus von $|F(\sigma)|$ berechnen:

$$\begin{aligned}\log|F(\sigma)| &= 3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma+i\tau)| + \log|\zeta(\sigma+2i\tau)| \\ &= \sum_{n=1}^{\infty} \frac{\Lambda_1(n)}{n^\sigma}(3 + 4\cos(\tau\log n) + \cos(2\tau\log n)).\end{aligned}$$

Für den Ausdruck in Klammern können wir folgende trigonometrische Identität benutzen:

$$2(1+\cos(\alpha))^2 = 3 + 4\cos(\alpha) + \cos(2\alpha).$$

Wir erhalten

$$\log|F(\sigma)| = 2\sum_{n=1}^{\infty} \frac{\Lambda_1(n)}{n^\sigma}(1+\cos(\tau\log n))^2 \geq 0.$$

Daraus folgt

$$|F(\sigma)| \geq 1 \qquad \forall\sigma > 1,$$

aber das steht im Widerspruch zu $F(1) = 0$. □

Wir haben für den Beweis die Produktformel benutzt. Diese gilt nur für den Bereich $\Re(s) > 1$. Durch Grenzwertbetrachtungen haben wir es geschafft Aussagen über den „Rand" $\Re(s) = 1$ zu treffen. Darüber hinaus wird es allerdings wesentlich komplizierter und wir sind der Frage, ob die (nichtoffensichtlichen) Nullstellen alle auf der Geraden $\Re(s) = 1/2$ liegen nur ein winziges bisschen näher gekommen.

6.4. **Dirichlet-Reihen.** Für eine zahlentheoretische Funktion

$$a : \mathbb{N} \longrightarrow \mathbb{C}$$

betrachten wir die Reihe

$$f(s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s},$$

die *Dirichlet-Reihe* zu a. Wir benutzen auch die Notation

$$a_n := a(n),$$

wodurch die Dirichlet-Reihe die Form

$$f(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

annimmt. Beispielsweise ist die Riemannsche Zeta-Funktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

die Dirichlet-Reihe zur zahlentheoretischen Funktion

$$1 : n \mapsto 1.$$

Wir haben die Dirichlet-Reihe zu einer zahlentheoretischen Funktion einfach hingeschrieben ohne uns Gedanken darüber zu machen ob beziehungsweise für welche Werte von s sie konvergiert. Diese Frage wollen wir nun beleuchten.

Definition 6.14. Für eine Dirichlet-Reihe

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

definieren wir die *absolute Konvergenz-Abszisse*

$$\sigma_a(f) := \inf \left\{ \sigma \in \mathbb{R} \mid \sum_{n=1}^{\infty} \frac{|a_n|}{n^\sigma} < \infty \right\}.$$

Sie nimmt Werte in $\mathbb{R} \cup \{\pm\infty\}$. Hierbei bedeutet $\sigma_a(f) = -\infty$, dass die Dirichlet-Reihe f überall konvergiert und $\sigma_a(f) = \infty$, dass f nirgends konvergiert. Da

$$\left|\frac{a_n}{n^s}\right| = \frac{|a_n|}{n^\sigma}$$

nur vom Realteil σ von s abhängt und für $\sigma' > \sigma$ gilt

$$\frac{|a_n|}{n^{\sigma'}} \leq \frac{|a_n|}{n^\sigma},$$

konvergiert f absolut auf der Halbebene

$$H_{\sigma_a(f)} = \{s \in \mathbb{C} \mid \Re(s) > \sigma_a(f)\}.$$

Wir wissen allerdings noch nicht, ob die Konvergenz gleichmäßig auf Kompakta ist, was wir bräuchten um zu folgern, dass f dann eine holomorphe Funktion ist.

Definition 6.15. Die *bedingte Konvergenz-Abszisse* einer Dirichlet-Reihe

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

ist definiert als

$$\sigma_c(f) := \inf \left\{ \sigma \in \mathbb{R} \mid \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ konvergiert} \right\}.$$

Das c in $\sigma_c(f)$ steht für „conditional". Tatsächlich konvergiert die Dirichlet-Reihe f in der Halbebene

$$H_{\sigma_c(f)} = \{s \in \mathbb{C} \mid \Re(s) > \sigma_c(f)\},$$

aber das ist nicht sofort offensichtlich. Es folgt aber aus folgender Proposition.

Proposition 6.16. *Sei*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

eine Dirichlet-Reihe und $s_0 \in \mathbb{C}$, so dass f bei s_0 konvergiert. Wir wählen außerdem einen Winkel $\alpha \in [0, \pi/2)$. Dann konvergiert f gleichmäßig im Winkelbereich

$$W(s_0, \alpha) := \{s_0 + re^{i\varphi} \mid r \geq 0,\ |\varphi| \leq \alpha\}$$

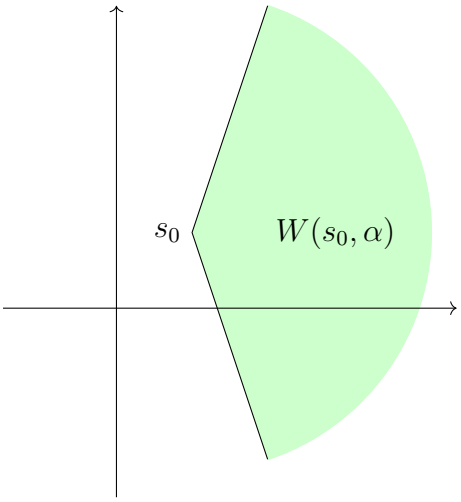

ABBILDUNG 1. Der Winkelbereich $W(s_0, \alpha)$

Beweis. Den Beweis lassen wir weg. Man benutzt abelsche partielle Summation (Proposition 6.11) und schätzt das darin vorkommende Integral ab. □

Korollar 6.17. *Die Dirichlet-Reihe*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

konvergiert in der Halbebene

$$H_{\sigma_c(f)} = \{s \in \mathbb{C} \mid \Re(s) > \sigma_c(f)\}$$

gleichmäßig auf Kompakta gegen eine holomorphe Funktion.

Beweis. Hier muss man sich nur klarmachen, dass jedes Kompaktum K in einem der Winkelbereiche $W(s_0, \alpha)$ für geeignete s_0 und α liegt. Den Punkt s_0 kann man so wählen, dass er links von K liegt:

$$\sigma_c(f) < s_0 < \inf\{\Re(s) \mid s \in K\}.$$

Das Infimum auf der rechten Seite wird angenommen, weil K kompakt ist und ist daher größer als $\sigma_c(f)$. Dann gilt

$$K \subseteq H_{s_0} = \{s \in \mathbb{C} \mid \Re(s) > s_0\}.$$

Die Winkelbereiche $W(s_0, \alpha)$ für wachsendes $\alpha \to \pi/2$ überdecken H_{s_0} und

$$W(s_0, \alpha) \subseteq W(s_0, \alpha')$$

für $\alpha \leq \alpha'$. Da K kompakt ist, ist es folglich in einem der $W(s_0, \alpha)$ enthalten. □

Die absolute und die bedingte Konvergenzabszisse können übereinstimmen. Für die Riemannsche Zeta-Funktion sind sie beide gleich 1. Das muss aber nicht sein. Für die alternierende Reihe

$$f(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}$$

ist

$$\sigma_c(f) = 0 \qquad \text{und} \qquad \sigma_a(f) = 1.$$

Das ist aber schon der Extremfall, wie folgende Proposition zeigt:

Proposition 6.18. *Für eine Dirichlet-Reihe*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

gilt

$$\sigma_a(f) - \sigma_c(f) \leq 1.$$

Beweis. Die Reihe konvergiere bei s_0. Dann müssen wir zeigen, dass sie für alle $\varepsilon > 0$ bei

$$s = s_0 + 1 + \varepsilon$$

absolut konvergiert. Weil f bei $s_0 = \sigma_0 + it_0$ konvergiert, sind die Summanden beschränkt und wir finden eine Konstante $M > 0$, so dass

$$\left|\frac{a_n}{n^{s_0}}\right| = \frac{|a_n|}{n^{\sigma_0}} \leq M \qquad \forall n \in \mathbb{N}.$$

Dann gilt

$$\sum_{n=1}^{\infty} \left|\frac{a_n}{n^s}\right| = \sum_{n=1}^{\infty} \frac{|a_n|}{n^{\sigma_0+1+\varepsilon}} \leq M \sum_{n=1}^{\infty} \frac{1}{n^{1+\varepsilon}} < \infty.$$

□

Für holomorphe Funktionen auf einem Gebiet gilt der Identitätssatz (Satz 6.19). Man könnte ihn so ausdrücken, dass eine holomorphe Funktion identisch Null ist, falls sie auf einer Menge mit Häufungspunkt verschwindet. Das gilt für Dirichlet-Reihen Selbstverständlich auch. Wir haben aber sogar ein stärkeres Resultat:

Satz 6.19 (Identitätssatz für Dirichlet-Reihen)**.** *Sei*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

eine Dirichlet-Reihe mit

$$\sigma_a(f) < \infty.$$

Es gebe eine Folge

$$s_1, s_2, s_3, \ldots \in H_{\sigma_a(f)}$$

von von Nullstellen von f mit

$$\lim_{i \to \infty} s_i = \infty,$$

Dann ist die zahlentheoretische Funktion a gleich Null:

$$0 = a_1 = a_2 = a_3 = \ldots$$

Beweis. Wir nehmen an, dass nicht alle a_n gleich Null sind. Sei k minimal, so dass $a_k \neq 0$. Dann nimmt f die Form

$$f(s) = \frac{a_k}{k^s} + \sum_{n>k} \frac{a_n}{n^s} = \frac{1}{k^s}\left(a_k + \sum_{n>k} \frac{a_n}{(n/k)^s}\right)$$

an. Wir wählen einen beliebigen Punkt $s_0 = \sigma + it_0 \in H_{\sigma_a(f)}$. Dort konvergiert f absolut, weshalb

$$M := \sum_{n>k} \left|\frac{a_n}{(n/k)^{s_0}}\right| = \sum_{n>k} \frac{|a_n|}{(n/k)^{\sigma_0}} < \infty.$$

Wir betrachten nun das Verhalten der Reihe bei $s_0 + r$ für eine komplexe Zahl r mit $\Re(r) > 0$.

$$\left|\sum_{n>k} \frac{a_n}{(n/k)^{s_0+r}}\right| \leq \sum_{n>k} \frac{|a_n|}{(n/k)^{\sigma_0}} \left(\frac{k}{n}\right)^{\Re(r)} \leq \sum_{n>k} \frac{|a_n|}{(n/k)^{\sigma_0}} \left(\frac{k}{k+1}\right)^{\Re(r)} \leq M\left(\frac{k}{k+1}\right)^{\Re(r)}.$$

Da $k/(k+1) < 1$ konvergiert dieser Ausdruck für $\Re(r) \to \infty$ gegen Null. Insbesondere gilt für $\Re(r)$ groß genug

$$\left|\sum_{n>k} \frac{a_n}{(n/k)^{s_0+r}}\right| < |a_k|.$$

Da die Folge $\Re(s_i)$ gegen unendlich geht, gilt dies auch für $r = s_i - s_0$, für genügend großes i, also

$$\left|\sum_{n>k} \frac{a_n}{(n/k)^{s_i}}\right| < |a_k|.$$

Dann kann aber s_i keine Nullstelle von

$$f(s) = \frac{1}{k^s}\left(a_k + \sum_{n>k} \frac{a_n}{(n/k)^s}\right)$$

sein, was im Widerspruch zur Annahme steht. □

Wir können den Identitätssatz für Dirichlet-Reihen auch so formulieren, dass eine Dirichlet-Reihe keine Nullstellen mit beliebig großem Realteil hat. Für allgemeine holomorphe Funktionen ist dies im Allgemeinen nicht richtig. Beispielsweise hat $\sin(z)$ eine Nullstelle bei $n\pi$ für alle $n \in \mathbb{Z}$.

Korollar 6.20. *Seien*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad \textit{und} \qquad g(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

die Dirichlet-Reihen zu den zahlentheoretischen Funktionen $a, b : \mathbb{N} \to \infty$. Falls

$$\sigma_a(f), \sigma_a(g) < \infty$$

und

$$f(s) = g(s)$$

für alle s mit

$$\Re(s) > \max\{\sigma_a(f), \sigma_a(g)\},$$

dann ist $a = b$.

Beweis. Wir wenden den Identitätssatz für Dirichlet-Reihen auf $f - g$ und eine beliebige Folge $(s_i)_{i\in\mathbb{N}}$ mit

$$\Re(s_i) > \max\{\sigma_a(f), \sigma_a(g)\} \qquad \forall i \in \mathbb{N}$$

und

$$\lim_{i\to\infty} \Re(s_i) = \infty$$

an. □

Proposition 6.21. *Seien*

$$a, b : \mathbb{N} \to \mathbb{C}$$

zwei zahlentheoretische Funktionen, deren zugehörigen Dirichlet-Reihen

$$f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}, \qquad g(s) = \sum_{n=1}^{\infty} \frac{b(n)}{n^s}$$

absolute Konvergenz-Abszissen $< \infty$ haben. Dann gilt für $\Re(s) > \max\{\sigma_a(f), \sigma_a(g)\}$

$$f(s)g(s) = \sum_{n=1}^{\infty} \frac{(a * b)(n)}{n^s}.$$

Das Produkt der Dirichlet-Reihen entspricht also der Faltung der entsprechenden zahlentheoretischen Funktionen. Bevor wir die Proposition beweisen erinnern wir uns kurz an die Definition der Faltung zweier zahlentheoretischer Funktionen a und b:

$$(a * b)(n) := \sum_{d|n} a(d) b\left(\frac{n}{d}\right) = \sum_{\substack{d,m \\ dm=n}} a(d)b(m).$$

Beweis. Das können wir einfach nachrechnen:

$$\left(\sum_{d=1}^{\infty} \frac{a(d)}{d^s}\right)\left(\sum_{m=1}^{\infty} \frac{b(m)}{m^s}\right) = \sum_{d,m=1}^{\infty} \frac{a(d)b(m)}{(dm)^s} = \sum_{n=1}^{\infty} \sum_{\substack{d,m \\ dm=n}} \frac{a(d)b(m)}{n^s} = \sum_{n=1}^{\infty} \frac{(a*b)(n)}{n^s}.$$

□

Mithilfe dieser Erkenntnis können wir nun einige Ausdrücke in der Zeta-Funktion berechnen. Dafür brauchen wir noch folgende Definition.

Definition 6.22. Die *Von-Mangoldt-Funktionen* sind folgendermaßen definiert:

$$\Lambda(n) := \begin{cases} \log p & \text{falls } n = p^m \text{ für } p \text{ prim und } m \geq 1 \\ 0 & \text{sonst,} \end{cases}$$

$$\Lambda_1(n) := \begin{cases} \frac{1}{m} & \text{falls } n = p^m \text{ für } p \text{ prim und } m \geq 1 \\ 0 & \text{sonst,} \end{cases}.$$

Die Funktion Λ_1 kam schon im Beweis von Satz 6.13 vor. Es folgt direkt aus den Definitionen, dass

$$\Lambda(n) = \Lambda_1(n) \log n.$$

Außerdem erinnern wir uns an die Teilerfunktion σ_0, die Teilersummenfunktion σ_1 und allgemeiner die höheren Teilersummenfunktionen σ_k:

$$\sigma_k(n) := \sum_{d|n} d^k.$$

Für $k = 0$ ist $\sigma_0(n)$ die Anzahl der Teiler von n und $\sigma_1(n)$ ist die Summe über alle Teiler.

Satz 6.23. *Für eine komplexe Zahl s mit $\Re(s) > 1$ gilt*

(i) $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$,

(ii) $\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}$,

(iii) $\log \zeta(s) = \sum_{n=1}^{\infty} \frac{\Lambda_1(n)}{n^s}$,

(iv) $\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$,

(v) $\zeta^2(s) = \sum_{n=1}^{\infty} \frac{\sigma_0(n)}{n^s}$.

Beweis. (i). Wegen Proposition 6.21 müssen wir eine zahlentheoretische Funktion a finden, so dass

$$a * 1 = \delta,$$

wobei

$$\delta(n) = \begin{cases} 1 & n = 1, \\ 0 & \text{sonst} \end{cases}$$

das neutrale Element der Faltung ist (siehe Proposition 4.12). Das haben wir aber schon in Lemma 4.15 gemacht, wo wir bewiesen haben, dass

$$\mu * 1 = \delta,$$

wobei μ die Möbiussche μ-Funktion ist. Daher ist μ das Inverse von 1 und somit

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Genau genommen müssen wir uns noch über die absolute Konvergenzabszisse von

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

Gedanken machen. Da aber $\mu(n) \leq 1$, ist

$$\sigma_a\Big(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\Big) \leq \sigma_a(\zeta(s)) = 1.$$

(ii). Da die Reihe $\sum_n 1/n^s$ für $\Re(s) > 0$ absolut und gleichmäßig auf Kompakta konvergiert, dürfen wir termweise ableiten:

$$\zeta'(s) = \sum_{n=1}^{\infty} (e^{-s \log n})' = \sum_{n=1}^{\infty} (-\log n) e^{-s \log n} = -\sum_{n=1}^{\infty} \frac{\log n}{n^s}.$$

(iii). Das haben wir schon im Beweis von Satz 6.13 ausgerechnet.

(iv). Hier benutzen wir, dass $\zeta'(s)/\zeta(s)$ die Ableitung von $\log \zeta(s)$ ist, die wir wieder termweise bestimmen dürfen:

$$\frac{\zeta'(s)}{\zeta(s)} = (\log \zeta(s))' = \sum_{n=1}^{\infty} \Lambda_1(n)(e^{-s \log n})' = \sum_{n=1}^{\infty} \Lambda_1(n)(-\log n) e^{-s \log n} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

(v). Hierfür benutzen wir, dass nach Beispiele 4.13 (ii) gilt

$$1 * 1 = \sigma_0.$$

Auf dem Level von Dirichlet-Reihen gibt das mithilfe von Proposition 6.21 genau das geforderte Resultat. □

7. Der Primzahlsatz

Wir haben schon in Abschnitt 2.3 die vage Vorstellung geäußert, dass die Primzahlen für größer werdende natürliche Zahlen immer dünner gesät sind. Diesen Umstand wollen wir in diesem Kapitel quantifizieren. Genauer gesagt werden wir eine asymptotische Formel für die Anzahl der Primzahlen beweisen.

7.1. **Äquivalente Formulierungen.** Wir interessieren uns für die *Primzahlzählfunktion*, auch *Primzahlfunktion* genannt:

$$\begin{aligned} \pi : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \#\{p \leq x \mid p \text{ prim}\} = \sum_{p \leq x \text{ prim}} 1. \end{aligned}$$

Sie ist eine Treppenfunktion, die die Zahl der Primzahlen kleiner oder gleich x angibt.

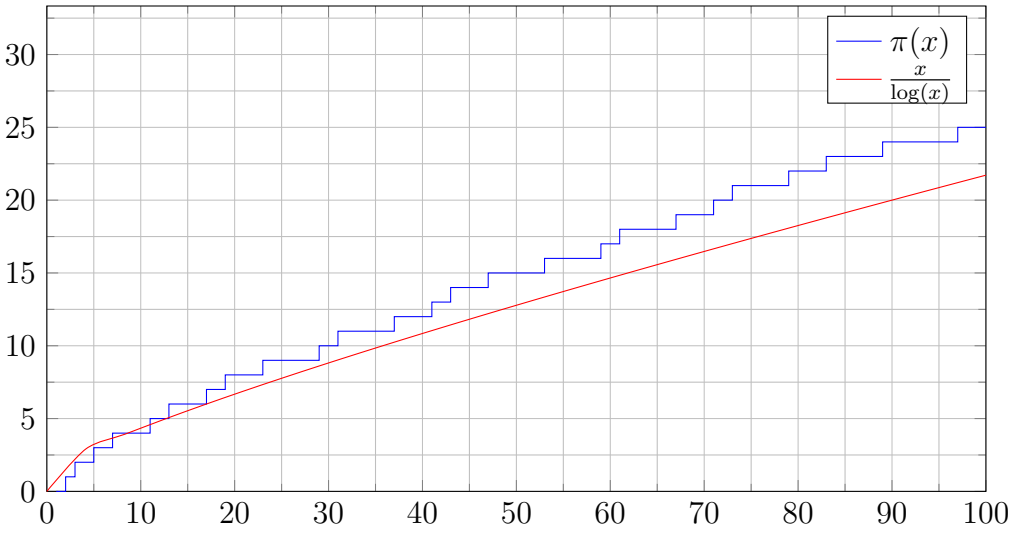

Abbildung 2. Die Primzahlfunktion für $x \leq 100$

Schon Ende des 18. Jahrhunderts haben sich Mathematiker wie Gauß und Legendre damit auseinandergesetzt das asymptotische Verhalten von $\pi(x)$ für große Werte von x zu beschreiben. Sie stellten Formeln auf und vermuteten, dass diese eine Approximation für $\pi(x)$ für $x \to \infty$ darstellen. Heute ist diese Vermutung ein Satz:

Satz 7.1 (Primzahlsatz)**.**

$$\pi(x) \sim \frac{x}{\log x}.$$

Hierbei bedeutet $f(x) \sim g(x)$ für zwei Funktionen $\mathbb{R} \to \mathbb{R}$, dass

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Einen ersten Beweis dafür lieferten unabhängig voneinander Hadamard und de la Vallée Poussin. Ihre Methoden basierten essentiell auf Riemanns Vorarbeit zur Riemannschen Zeta-Funktion. Wir werden in Abschnitt 7.3 einen kürzeren Beweis von Newton vorstellen, der aber ebenso auf der Riemannschen Zeta-Funktion beruht.

Tschebyschev erkannte, dass man statt $\pi(x)$ äquivalent auch folgende Funktion untersuchen kann um den Primzahlsatz zu beweisen:

$$\vartheta(x) := \sum_{p\leq x} \log p$$

Um das asymptotische Verhalten von ϑ und π zu vergleichen, brauchen wir zuerst eine Abschätzung für $\vartheta(x)$. Genauer gesagt wollen wir zeigen dass

$$\vartheta(x) = \mathcal{O}(x).$$

Wir erinnern uns, dass diese Notation bedeutet, dass es eine Konstante $C > 0$ gibt, so dass

$$|\vartheta(x)| \leq Cx$$

für genügend große x.

Lemma 7.2. *Für alle natürlichen Zahlen N gilt*

$$\prod_{p\leq N} p \leq 4^N.$$

Beweis. Wir beweisen die Aussage per Induktion über N. Für $N = 1$ lautet die zu zeigende Ungleichung

$$1 \leq 4,$$

was offensichtlich richtig ist. Auch für $N = 2$ stimmt die Aussage:

$$2 \leq 4^2 = 16.$$

Für den Induktionsschritt werden wir folgende Ungleichung zeigen: Für alle $n \in \mathbb{N}$ gilt

$$\prod_{n<p<2n} p \leq 4^{n-1}. \tag{13}$$

Um das einzusehen betrachten wir den Binomialkoeffizienten

$$\binom{2n-1}{n-1} = \binom{2n-1}{n} = \frac{(2n-1)(2n-2)\cdot\ldots\cdot(n+1)}{(n-1)!}.$$

Jede Primzahl p mit $n < p < 2n$ teilt diesen Binomialkoeffizienten, da p den Zähler, aber nicht den Nenner teilt. Daraus folgt

$$\prod_{n<p<2n} p \leq \binom{2n-1}{n-1}.$$

Den Binomialkoeffizienten können wir über die Binomialformel abschätzen:

$$2\binom{2n-1}{n-1} = \binom{2n-1}{n-1} + \binom{2n-1}{n} \leq \sum_{k=0}^{2n-1} \binom{2n-1}{k} = (1+1)^{2n-1} = 2^{2n-1}.$$

Teilen wir durch 2, erhalten wir

$$\binom{2n-1}{n-1} \leq 4^{n-1},$$

also insgesamt

$$\prod_{n<p<2n} p \leq 4^{n-1}.$$

Hiermit können wir folgendermaßen den Induktionsschritt durchführen. Sei $N > 2$. Wir nehmen an, dass die Ungleichung

$$\prod_{p<N'} p \leq 4^{N'}$$

für alle $N' < N$ gilt und wollen sie für N beweisen. Falls N gerade ist, ist

$$\{p \text{ prim} \mid p \leq N\} = \{p \text{ prim} \mid p \leq N-1\},$$

da $N > 2$ gerade ist und keine Primzahl sein kann. Also gilt

$$\prod_{p\leq N} p = \prod_{p\leq N-1} p \leq 4^{N-1} \leq 4^N$$

Für ungerades N schreiben wir

$$N = 2n - 1$$

und spalten das Produkt folgendermaßen auf:

$$\prod_{p\leq N} p = \left(\prod_{p\leq n} p\right)\left(\prod_{n<p<2n} p\right)$$

Auf den ersten Faktor wenden wir die Induktionsvoraussetzung an und auf den zweiten Faktor die Abschätzung (13):

$$\prod_{p\leq N} p \leq 4^n \cdot 4^{n-1} = 4^{2n-1} = 4^N.$$

□

Korollar 7.3. *Für alle $x \geq 1$ gilt*

$$\vartheta(x) = \sum_{p\leq x} \log p \leq x \log 4.$$

Insbesondere gilt

$$\vartheta(x) = \mathcal{O}(x).$$

Beweis. Wenden wir den Logarithmus auf die Abschätzung aus Lemma 7.2 an, erhalten wir

$$\sum_{p\leq N} \log p = \log\left(\prod_{p\leq N} p\right) \leq \log(4^N) = N \log 4.$$

Für eine reelle Zahl x sei $N = [x]$. Dann gilt

$$\vartheta(x) = \sum_{p\leq x} \log p = \sum_{p\leq N} \log p \leq N \log 4 \leq x \log 4.$$

□

Die gleiche Abschätzung gilt auch für die Primzahlfunktion $\pi(x)$, was jedoch viel einfacher zu zeigen ist:

Lemma 7.4.

$$\pi(x) = \mathcal{O}(x).$$

Beweis. Es gilt

$$\pi(x) = \sum_{p \le x} 1 \le \sum_{x=1}^{\infty} 1 = x.$$

□

Proposition 7.5. *Die folgenden Aussagen sind äquivalent:*

(i) $\pi(x) \sim \dfrac{x}{\log x}$,

(ii) $\vartheta(x) \sim x$.

Beweis. Um $\vartheta(x)$ mit $\pi(x)$ zu vergleichen, wenden wir abelsche partielle Summation an auf

$$a_n = \begin{cases} \log p & n = p \text{ prim} \\ 0 & \text{sonst,} \end{cases}$$
$$f(x) = \frac{1}{\log x},$$
$$n_0 = 2.$$

Mit der Ableitung

$$f'(x) = -\frac{1}{x(\log x)^2}$$

und

$$A(x) = \sum_{n_0 \le n \le x} a_n = \sum_{p \le x} \log p = \vartheta(x)$$

erhalten wir

$$\pi(x) = \sum_{2 \le p \le x} \log p \frac{1}{\log p} = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt$$

Wir wollen zeigen, dass

$$\int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt = O\left(\frac{x}{(\log x)^2}\right).$$

Da

$$\vartheta(x) = \mathcal{O}(x)$$

nach Korollar 7.3, gibt es eine Konstante $C > 0$, so dass

$$\frac{\vartheta(t)}{t} \le C.$$

Daher gilt

$$\int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt \le C \int_2^x \frac{1}{(\log t)^2} dt.$$

Wir teilen nun den Integrationsweg auf in $[2, \sqrt{x}]$ und $[\sqrt{x}, x]$. Auf dem ersten Abschnitt schätzen wir den Integranden durch 1 ab und auf dem zweiten Abschnitt durch $1/(\log\sqrt{x})^2$.

$$\begin{aligned}\int_2^x \frac{\vartheta(t)}{t(\log t)^2}dt &\leq C\left((\sqrt{x}-2)+\frac{x-\sqrt{x}}{(\log\sqrt{x})^2}\right)\\ &\leq C\left(\sqrt{x}+\frac{4x}{(\log x)^2}\right).\end{aligned}$$

Den ersten Term $\sqrt{x}$ kann man für große x vernachlässigen. Also folgt

$$\int_2^x \frac{t(\log t)^2}{\vartheta(t)}dt = O\left(\frac{x}{(\log x)^2}\right)$$

Nun können wir $\pi(x)$ und $\vartheta(x)$ für große x vergleichen:

$$\pi(x) = \frac{\vartheta(x)}{\log x} + O\left(\frac{x}{(\log x)^2}\right).$$

Daraus folgt

$$\frac{\pi(x)}{x/\log x} = \frac{\vartheta(x)}{x} + O\left(\frac{1}{\log x}\right).$$

Im Limes $x \to \infty$ geht $1/\log x$ gegen 0. Daher sind (i) und (ii) äquivalent. □

7.2. **Das analytische Theorem.** Im letzten Abschnitt haben wir gesehen, dass der Primzahlsatz äquivalent ist zu

$$\vartheta(x) := \sum_{p\leq x} \log p \sim x.$$

Um die Asymptotik von $\vartheta(x)$ zu untersuchen, werden wir folgendes Integral studieren:

$$\int_1^\infty \frac{\frac{\vartheta(u)}{u}-1}{u}du = \int_0^\infty \frac{\vartheta(e^t)-e^t}{e^t}dt.$$

Schauen wir uns das Integral an, scheint es sehr plausibel, dass $\vartheta(x) \sim x$ notwendig dafür ist, dass das Integral konvergiert, weil das Integral über $1/u$ nicht konvergiert, also muss der Zähler gegen Null gehen. A priori ist nicht klar, ob das Integral konvergiert und die harte Arbeit besteht darin gerade das zu zeigen. Dafür werden wir folgenden funktionentheoretischen Satz benutzen, dessen Beweis uns in diesem Abschnitt beschäftigt.

Satz 7.6. *Sei*

$$f : \mathbb{R}_{\geq 0} \to \mathbb{C}$$

eine beschränkte, lokal integrierbare Funktion. Angenommen die holomorphe Funktion für $\Re(z) > 0$

$$g(z) := \int_0^\infty f(t)e^{-zt}dt$$

besitzt eine holomorphe Fortsetzung auf $\Re(z) \geq 0$*. Dann existiert das Integral*

$$\int_0^\infty f(t)dt$$

und ist gleich $g(0)$*.*

Man beachte, dass für $\Re(z) > 0$ das Integral

$$\int_0^\infty f(t)e^{-zt}dt$$

konvergiert und eine holomorphe Funktion definiert. Das liegt daran, dass f lokal integrierbar und beschränkt ist, also

$$|f(t)| \leq C$$

für eine Konstante $C > 0$. Daher gilt

$$\int_0^\infty |f(t)e^{-zt}|dt \leq C \int_0^\infty e^{-\Re(z)t}dt = \frac{1}{\Re(z)}.$$

Beweis. Für $T > 0$ betrachten wir die holomorphe Funktion

$$g_T(z) := \int_0^T f(t)e^{-zt}dt.$$

Die Aussage des Satzes lässt sich dann äquivalent ausdrücken durch

$$\lim_{T\to\infty} g_T(0) = g(0).$$

Sei $R > 0$. Für jeden Punkt $z \in \mathbb{C}$ mit $\Re(z) = 0$ und Imaginärteil

$$\Im(z) \in [-2R, 2R]$$

gibt es eine holomorphe Fortsetzung von g auf eine Umgebung von z. Da $[-2R, 2R]$ kompakt ist, finden wir $\delta > 0$, so dass g sich fortsetzen lässt auf das Gebiet

$$D = \{z \in \mathbb{C} \mid \Re(z) > -2\delta,\ |\Im(z)| < 2R\} \cup \{z \in \mathbb{C} \mid \Re(z) > 0\}.$$

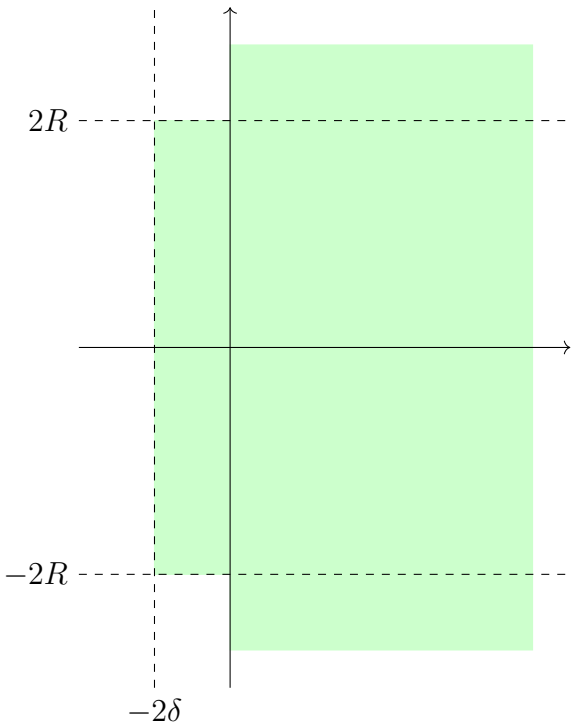

Abbildung 3. Das Gebiet D

Die Funktion

$$h(z) = (g(z) - g_T(z)) \frac{e^{zT}}{z} \left(1 + \frac{z^2}{R^2}\right)$$

ist auf D holomorph bis auf einen einfachen Pol bei $z = 0$. Wir integrieren sie entlang des Weges γ, der definiert ist als der Rand der Fläche

$$\{z \in \mathbb{C} \mid |z| \leq R,\ \Re(z) \geq -\delta\},$$

(im Uhrzeigersinn laufend), abgebildet in Fig. 4.

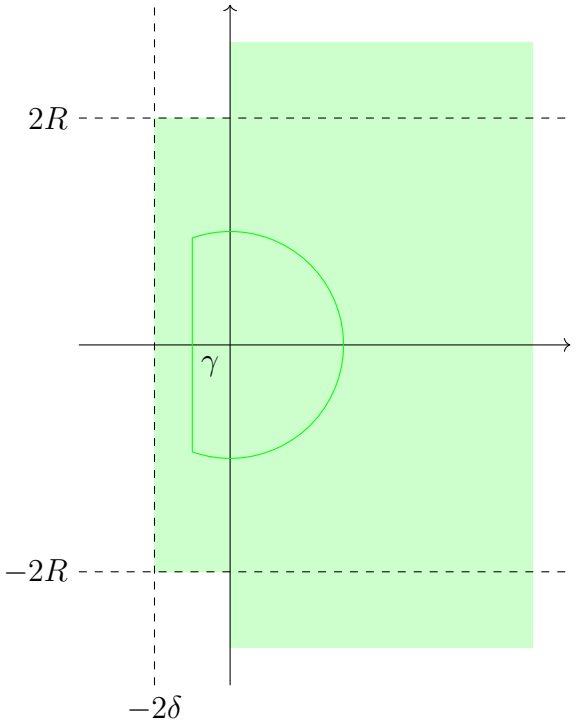

ABBILDUNG 4. Der Weg γ auf D

Nach dem Residuensatz können wir das Integral berechnen als die Summe der Residuen. In unserem Fall gibt es nur einen Pol bei Null und das Residuum ist

$$\mathrm{Res}(h, 0) = \lim_{z \to 0}(zh(z)) = g(0) - g_T(0).$$

Daher erhalten wir

$$g(0) - g_T(0) = \frac{1}{2\pi i} \int_\gamma (g(z) - g_T(z)) \frac{e^{zT}}{z} \left(1 + \frac{z^2}{R^2}\right) dz.$$

Wir wollen nun andererseits zeigen, dass das Integral für große Werte von R beliebig klein wird. Dafür teilen wir den Integrationsweg in zwei Teile γ_+ und γ_-. Hierbei ist γ_+ der Teil von γ, der in der rechten Halbebene $\{\Re(z) > 0\}$ liegt und γ_- der Teil in der linken Halbebene. Um das Integral abzuschätzen wählen wir zuerst eine Konstante $C > 0$, so dass

$$|f(t)| \leq C \qquad \forall z \text{ mit } \Re(z) > 0$$

Auf γ_+ können wir dann folgende Abschätzung machen:

$$|g(z) - g_T(z)| = \left| \int_T^\infty f(t) e^{-zt} dt \right| \leq C \int_T^\infty |e^{-zt}| dt = C \int_T^\infty e^{-\Re(z)t} dt = \frac{C e^{-\Re(z)T}}{\Re(z)}.$$

Um die restlichen Faktoren abzuschätzen denken wir daran, dass auf γ_+ der Betrag von z gleich R ist. Das benutzen wir in folgender Rechnung:

$$\left|1+\frac{z^2}{R^2}\right|^2 = \left|1+\frac{z^2}{z\bar{z}}\right|^2 = \left|1+\frac{z}{\bar{z}}\right|^2 = \left|\frac{\bar{z}+z}{\bar{z}}\right|^2 = \frac{|2\Re(z)|^2}{R^2} = 4\frac{\Re(z)}{R^2}.$$

Insgesamt bekommen wir auf γ_+:

$$|h(z)| \leq \frac{Ce^{-\Re(z)T}}{\Re(z)} \cdot \frac{e^{\Re(z)T}}{R} \cdot 2\frac{\Re(z)}{R} = \frac{2C}{R^2}.$$

Damit ist

$$\int_{\gamma_+} h(z) \leq (\pi R) \cdot \frac{2C}{R^2} = \frac{2\pi C}{R}.$$

Nun widmen wir uns dem Integral über γ_-. Wir spalten es in zwei Teile auf:

$$\int_{\gamma_-} h(z) = \int_{\gamma_-} g(z)\frac{e^{zT}}{z}\left(1+\frac{z^2}{R^2}\right) - \int_{\gamma_-} g_T(z)\frac{e^{zT}}{z}\left(1+\frac{z^2}{R^2}\right) \tag{14}$$

Wir schauen uns zuerst den zweiten Teil an. Da $g_T(z)$ auf ganz $\mathbb{C}$ definiert ist und der Integrand nur bei $z=0$ einen Pol hat, können wir den Integrationsweg γ_- deformieren zu einem Halbkreis

$$\{z \in \mathbb{C} \mid |z| = R, \Re(z) < 0\}.$$

Wir können auf diesem Halbkreis eine ähnliche Abschätzung machen wie für γ_+ oben:

$$|g_T(z)| = \left|\int_0^T f(t)e^{-zt}dt\right| \leq C\int_0^T |e^{-zt}|dt = C\int_0^T e^{-\Re(z)t}dt = C\frac{1-e^{-\Re(z)T}}{\Re(z)}.$$

Für den gesamten Integranden bekommen wir die Abschätzung (beachte $\Re(z) < 0$)

$$\left|g_T(z)\frac{e^{zT}}{z}\left(1+\frac{z^2}{R^2}\right)\right| \leq C\frac{1-e^{-\Re(z)T}}{\Re(z)} \cdot \frac{e^{\Re(z)T}}{R} \cdot 2\frac{-\Re(z)}{R} = 2C\frac{1-e^{\Re(z)T}}{R^2} \leq \frac{2C}{R^2}.$$

Somit ist der zweite Summand im Integral (14) kleiner gleich $2\pi C/R$.

Als letztes untersuchen wir noch das erste Integral in (14). Der Faktor

$$\frac{g(z)}{z}\left(1+\frac{z^2}{R^2}\right)$$

Ist unabhängig von T. Die einzige Abhängigkeit von T im Integranden kommt von e^{zT} und

$$|e^{zT}| = e^{\Re(z)T} \to 0$$

für $T \to \infty$, da auf γ_- der Realteil $\Re(z)$ negativ ist. Wegen des Satzen von der dominierten Konvergenz ($|e^{zT}| \leq 1$), dürfen wir den Limes ins Integral ziehen und erhalten

$$\lim_{T\to\infty} \int_{\gamma_-} g(z)\frac{e^{zT}}{z}\left(1+\frac{z^2}{R^2}\right) = 0.$$

Setzen wir nun alle Teile zusammen erhalten wir im Limes $T \to 0$:

$$\lim_{T\to\infty} |g(0) - g_T(0)| = \lim_{T\to\infty} \frac{1}{2\pi}\left|\int_\gamma (g(z) - g_T(z))\,\frac{e^{zT}}{z}\left(1+\frac{z^2}{R^2}\right)dz\right| \leq \frac{C}{R} + \frac{C}{R} + 0 = \frac{2C}{R}.$$

Da R beliebig groß gewählt werden darf, folgt daraus

$$g(0) = \lim_{T\to\infty} g_T(0),$$

und wir sind fertig. □

7.3. **Beweis des Primzahlsatzes.** Wir haben nun alle Puzzleteile zusammen um den Primzahlsatz

$$\pi(x) \sim \frac{x}{\log x}$$

zu beweisen. Wie schon in Abschnitt 7.2 erwähnt, beruht der Beweis darauf, das Integral

$$\int_1^\infty \frac{\vartheta(u)/u - 1}{u} du = \int_0^\infty \frac{\vartheta(e^t) - e^t}{e^t} dt.$$

zu studieren. Genauer gesagt, müssen wir nur wissen, dass das Integral konvergiert. Um das zu zeigen wollen wir Satz 7.6 anwenden auf

$$f(t) = \frac{\vartheta(e^t) - e^t}{e^t}$$

Lemma 7.7. *Die obige Funktion f ist lokal integrierbar und beschränkt.*

Beweis. Dass die Funktion f lokal integrierbar ist, ist klar, da f stückweise stetig ist. Sie ist beschränkt, da

$$\vartheta(e^t) = O(e^t)$$

nach Korollar 7.3. □

Damit wir Satz 7.6 anwenden können, müssen wir die Bedingungen an

$$g(z) := \int_0^\infty f(t)e^{-zt} dt = \int_0^\infty \left(\vartheta(e^t)e^{-(z+1)t} - e^{-zt}\right) dt$$

prüfen. Wir werden dieses Integral in Termen der Funktion

$$\Phi(s) := \sum_p \frac{\log p}{p^s}.$$

ausdrücken. Dafür wollen wir zunächst wissen, ob $\Phi(s)$ gegen eine holomorphe Funktion konvergiert.

Lemma 7.8. *Die Reihe $\Phi(s)$ konvergiert gleichmäßig auf Kompakta für $\Re(s) > 1$ und definiert daher eine holomorphe Funktion.*

Beweis. Wir erinnern uns daran (Satz 6.23), dass für $\Re(s) > 1$

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^\infty \frac{\Lambda(n)}{n^s}$$

für die Von Mangoldt-Funktion

$$\Lambda(n) = \begin{cases} \log p & n = p^m \text{ für } p \text{ prim und } m \geq 1 \\ 0 & \text{sonst.} \end{cases}$$

Insbesondere konvergiert diese Reihe absolut und gleichmäßig auf Kompakta. Diese ist außerdem eine Majorante für $\Phi(s)$, da

$$\sum_p \frac{\log p}{p^s} \leq \sum_p \sum_{m=1}^\infty \frac{\log p}{p^{ms}} = \sum_{n=1}^\infty \frac{\Lambda(n)}{n^s}.$$

Daher konvergiert auch $\Phi(s)$ absolut und gleichmäßig auf Kompakta gegen eine holomorphe Funktion. □

Lemma 7.9.

$$g(z) = \frac{\Phi(z+1)}{\Phi(z+1)} - \frac{1}{z}.$$

für $\Re(z) > 0$.

Beweis. Wir wenden abelsche partielle Summation an auf

$$a_n = \begin{cases} \log p & n = p \text{ prim}, \\ 0 & \text{sonst}, \end{cases}$$
$$f(x) = \frac{1}{x^s}.$$

Dann ist

$$A(x) = \sum_{p \le x} a_n = \sum_{p \le x} \log p = \vartheta(x)$$

und

$$f'(x) = -\frac{s}{x^{s+1}}.$$

Wir erhalten

$$\sum_{p \le x} \frac{\log p}{p^s} = \frac{\vartheta(x)}{x^s} + s \int_1^x \frac{\vartheta(x)}{x^{s+1}} dx = s \int_0^x e^{-st} \vartheta(e^t) dt.$$

Für $\sigma = \Re(s) > 1$ gilt

$$\lim_{x\to\infty} |\frac{\vartheta(x)}{x^s}| = \lim_{x\to\infty} \frac{\vartheta(x)}{x^\sigma} \le \left(\lim_{x\to\infty} \frac{\vartheta(x)}{x} \right) \left(\lim_{x\to\infty} \frac{1}{x^{\sigma-1}} \right).$$

Der erste Faktor ist beschränkt, da nach Korollar 7.3 gilt $\vartheta(x) = \mathcal{O}(x)$. Der zweite Faktor ist Null, da $\sigma > 1$. Folglich gilt für $\sigma > 1$:

$$\Phi(s) = s \int_0^\infty e^{-st} \vartheta(e^t) dt.$$

Damit können wir g berechnen:

$$g(z) = \int_0^\infty \left(e^{-(z+1)t} \vartheta(e^t) - e^{-zt} \right) dt = \frac{\Phi(z+1}{z+1} - \frac{1}{z}.$$

□

Da $\Pi(z+1)$ nach Lemma 7.8 für $\Re(z) > 0$ holomorph ist, ist auch g holomorph für $\Re(z) > 0$. Die einzige Voraussetzung, die wir noch prüfen müssen um Satz 7.6 anwenden zu können ist, dass sich g für $\Re(z) = 0$ holomorph fortsetzen lässt.

Proposition 7.10. *Die Funktion*

$$g(z) = \frac{\Phi(z+1)}{z+1} - \frac{1}{z}$$

lässt sich holomorph fortsetzen für $\Re(z) \ge 0$.

Beweis. Wir nutzen aus, dass wir schon wissen, dass die Riemannsche Zeta-Funktion $\zeta(s)$ eine meromorphe Fortsetzung für $\Re(s) > 0$ besitzt mit einem einfachen Pol bei $s = 1$

mit Residuum 1 (siehe Proposition 6.12). Jetzt müssen wir nur noch $\Phi(s)$ mit $\zeta(s)$ in Zusammenhang setzen. Nach Satz 6.23 gilt

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = \sum_p \sum_{m=1}^{\infty} \frac{\log p}{p^{ms}}.$$

Das können wir mithilfe der Formel für die geometrische Reihe berechnen, wobei wir jedoch beachten müssen, dass der erste Term $p^0 = 1$ fehlt, den wir dann abziehen müssen.

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \left(\frac{\log p}{1 - p^{-s}} - \log p \right) = \sum_p \frac{p^{-s} \log p}{1 - p^{-s}} = \sum_p \frac{\log p}{p^s - 1}.$$

Wir behaupten, dass das gleich

$$\Phi(s) + \sum_p \frac{\log p}{p^s(p^s - 1)}$$

ist. Das lässt sich leicht nachzuprüfen:

$$\Phi(s) + \sum_p \frac{\log p}{p^s(p^s - 1)} = \sum_p \frac{(p^s - 1)\log p + \log p}{p^s(p^s - 1)} = \sum_p \frac{\log p}{p^s - 1}.$$

Insgesamt erhalten wir

$$-\frac{\zeta'(s)}{\zeta(s)} = \Phi(s) + \sum_p \frac{\log p}{p^s(p^s - 1)} \tag{15}$$

Da $\zeta(s)$ nach Proposition 6.12 eine meromorphe Fortsetzung auf $\Re(s) > 0$ besitzt, gilt dies auch für

$$h(s) := -\frac{\zeta'(s)}{\zeta(s)}.$$

Die Riemannsche Zeta-Funktion hat keine Nullstellen für $\Re(s) \geq 1$ und einen einfachen Pol bei $s = 1$ mit Residuum 1. Daher ist $h(s)$ holomorph für $\Re(s) \geq 1$ außer eventuell bei $s = 1$. Wir behaupten, dass $h(s)$ bei $s = 1$ einen einfachen Pol mit Residuum 1 hat. Dafür schreiben wir

$$\zeta(s) = \frac{1}{s - 1} + q(s)$$

für eine holomorphe Funktion $q(s)$. Dann ist

$$\zeta'(s) = -\frac{1}{(s-1)^2} + q'(s)$$

und

$$h(s) = \frac{\frac{1}{(s-1)^2} + q'(s)}{\frac{1}{s-1} + q(s)} = \frac{1}{s-1} \cdot \frac{1 + (s-1)^2 q'(s)}{1 + (s-1)q(s)}.$$

Der zweite Faktor ist holomorph bei $s = 1$ mit Funktionswert 1. Daraus folgt die Behauptung.

Wir schauen uns jetzt die Reihe

$$\sum_p \frac{\log p}{p^s(p^s - 1)}$$

aus der Gleichung (15) an. Wir wollen zeigen, dass sie für $\Re(s) > 1/2$ absolut und gleichmäßig auf Kompakta konvergiert. Dafür schätzen wir die Summanden

$$\left|\frac{\log p}{p^s(p^s-1)}\right|$$

ab. Für jedes $\varepsilon > 0$ gibt es eine Konstante $C > 0$, so dass

$$\log(x) \leq Cx^\varepsilon$$

für alle $x \geq 1$. Außerdem ist

$$|p^s - 1| \geq |p^s| - 1 \geq \frac{1}{2}p^\sigma$$

für p groß genug (da $\sigma = \Re(s) > 0$). Insgesamt erhalten wir

$$\left|\frac{\log p}{p^s(p^s-1)}\right| \leq \frac{C}{2}\frac{p^\varepsilon}{p^{2\sigma}} = \frac{C}{2}\frac{1}{p^{2\sigma-\varepsilon}}$$

Für $2\sigma - \varepsilon > 1$, also

$$\Re(s) = \sigma > \frac{1}{2} + \frac{\varepsilon}{2}$$

folgt daraus, dass die Reihe absolut konvergiert. Da ε beliebig war, konvergiert die Reihe absolut für $\Re(s) > 1/2$. Dass sie gleichmäßig auf Kompakta konvergiert, folgt da die Majorante

$$\frac{C}{2}\sum_p \frac{1}{p^{2s-\varepsilon}}$$

gleichmäßig auf Kompakta konvergiert. Damit definiert

$$\sum_p \frac{\log p}{p^s(p^s-1)}$$

eine holomorphe Funktion für $\Re(s) > 1$.

Wir haben nun alle Terme in der Gleichung (15) untersucht und schließen daraus, dass $\Phi(s)$ holomorph ist für $\Re(s) \geq 1$ bis auf einen einfachen Pol bei $s = 1$ mit Residuum 1. Damit ist

$$g(z) = \frac{\Phi(z+1)}{z+1} - \frac{1}{z} = -\frac{1}{z+1}\frac{\zeta'(z+1)}{\zeta(z+1)}$$

holomorph für $\Re(z) \geq 0$. Man beachte, dass sich die Polstelle von $\Phi(z+1)/(z+1)$ gerade mit $1/z$ wegkürzt, weil die Residuen beide 1 sind. □

Nun können wir den Beweis des Primzahlsatzes abschließen:

Satz 7.11 (Primzahlsatz)**.** *Es gilt*

$$\pi(x) \sim \frac{x}{\log x}.$$

Korollar 7.12. *Das Integral*

$$\int_1^\infty \frac{\theta(u)/u - 1}{u} du$$

konvergiert.

Beweis. Es gilt

$$\int_1^\infty \frac{\vartheta(u)/u - 1}{u} du = \int_0^\infty \frac{\vartheta(e^t) - e^t}{e^t} dt.$$

Der Integrand

$$f(t) = \frac{\vartheta(e^t) - e^t}{e^t}$$

und die Funktion

$$g(z) = \int_0^\infty f(t) e^{-zt} dt = \int_0^\infty \left(\vartheta(e^t) e^{-(z+1)t} - e^{-zt}\right) dt$$

erfüllen die Voraussetzungen von Satz 7.6: Nach Lemma 7.7 ist f lokal integrierbar und beschränkt. Wir haben in Lemma 7.9 gezeigt, dass

$$g(z) = \frac{\Phi(z+1)}{\Phi(z+1)} - \frac{1}{z}.$$

für $\Re(z) > 0$ und diese Funktion lässt sich nach Proposition 7.10 auf $\Re(z) \geq 0$ fortsetzen. Damit sind alle Voraussetzungen erfüllt und das Korollar folgt aus Satz 7.6. □

Beweis. Nach Proposition 7.5 ist der Primzahlsatz äquivalent zu

$$\vartheta(x) \sim x.$$

Angenommen es gibt eine Konstante C, so dass

$$\limsup_{x>0} \frac{\vartheta(x)}{x} \geq C > 1.$$

Dann gibt es beliebig große $x \in \mathbb{R}$ mit

$$\vartheta(x) \geq Cx.$$

Da $\vartheta(x)$ monoton steigend ist, gilt dann

$$\vartheta(u) \geq Cx$$

für alle $u \geq x$. Daraus folgt die Abschätzung

$$\int_x^{Cx} \frac{\frac{\vartheta(u)}{u} - 1}{u} du \geq \int_x^{Cx} \frac{\frac{Cx}{u} - 1}{u} du = \int_x^{Cx} \frac{Cx - u}{u^2} du = \int_1^C \frac{C - t}{t^2} dt > 0.$$

Im letzten Schritt haben wir die Substitution $u = xt$ vorgenommen. Das Integral auf der rechten Seite ist unabhängig von x. Da aber nach Korollar 7.12 das Integral

$$\int_1^\infty \frac{\theta(u)/u - 1}{u} du$$

konvergiert, müsste

$$\int_x^{Cx} \frac{\frac{\vartheta(u)}{u} - 1}{u} du$$

für große x beliebig klein werden, ein Widerspruch.

Ebenso führt die Annahme

$$\liminf_{x>0} \frac{\vartheta(x)}{x} \leq C < 1$$

auf eine änliche Weise zum Widerspruch: Dann gibt es beliebig große x mit

$$\vartheta(x) \leq Cx$$

und wegen der Monotonie von ϑ ist

$$\vartheta(u) \leq Cx$$

für $u \leq x$. Daraus folgt

$$\int_{Cx}^{x} \frac{\frac{\vartheta(u)}{u} - 1}{u} du \geq \int_{Cx}^{x} \frac{\frac{Cx}{u} - 1}{u} du = \int_{Cx}^{x} \frac{Cx - u}{u^2} du = \int_{C}^{1} \frac{C - t}{t^2} dt < 0.$$

Und wieder führt dies zum Widerspuch, weil das rechte Integral unabhängig von x ist, aber das Integral auf der linken Seite wegen Korollar 7.12 gegen Null konvergieren muss für $x \to \infty$. Zusammenfassend haben wir gezeigt:

$$1 \leq \liminf_{x>0} \frac{\vartheta(x)}{x} \leq \limsup_{x>0} \frac{\vartheta(x)}{x} \leq 1.$$

Folglich gilt

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1$$

oder in anderen Worten

$$\vartheta(x) \sim x.$$

□

7.4. **Größenordnung der Primzahlen.** Eng verbunden mit der Frage nach der Verteilung der Primzahlen ist die Frage nach der Größenordnung der n-ten Primzahl. Tatsächlich lässt sich deren Asymptotik aus dem Primzahlsatz herleiten. Dafür ordnen wir die Primzahlen der Größe nach:

$$p_1 < p_2 < p_3 \ldots.$$

Satz 7.13. *Es gilt die asymptotische Beziehung*

$$p_n \sim n \log n.$$

Beweis. Es gilt

$$\liminf_{n\to\infty} \frac{p_n}{n \log n} \leq \limsup_{n\to\infty} \frac{p_n}{n \log n}$$

und wir wollen zeigen, dass sowohl der Limes superior als auch der Limes inferior gleich 1 sind. Dafür reicht es zu zeigen:

(i) $\limsup_{n\to\infty} \frac{p_n}{n \log n} \leq 1$.
(ii) $\liminf_{n\to\infty} \frac{p_n}{n \log n} \geq 1$,

Für Punkt (i) nehmen wir an, dass

$$\limsup_{n\to\infty} \frac{p_n}{n \log n} > 1.$$

Dann gibt es $\varepsilon > 0$ und beliebig große $n \in \mathbb{N}$ mit

$$p_n \geq (1 + \varepsilon) n \log n.$$

Dass die n-te Primzahl mindestens gleich $(1 + \varepsilon) n \log n$ ist, bedeutet gerade, dass

$$\pi((1 + \varepsilon) n \log n) \leq n.$$

Da es für dieses feste ε beliebig große n gibt, die diese Ungleichung erfüllen, folgt

$$\liminf_{n\to\infty} \frac{\pi((1 + \varepsilon) n \log n)}{n} \leq 1.$$

Aber nach **??** gilt

$$\lim_{n\to\infty} \frac{\pi((1+\varepsilon)n\log n}{n} = 1+\varepsilon > 1.$$

Das ist ein Widerspruch, weshalb

$$\limsup_{n\to\infty} \frac{p_n}{n\log n} \leq 1.$$

Um Punkt (ii) zu zeigen, gehen wir analog vor und nehmen an, dass

$$\liminf_{n\to\infty} \frac{p_n}{n\log n} < 1$$

Dann gibt es $\varepsilon > 0$ und beliebig große n, so dass

$$\liminf_{n\to\infty} \frac{p_n}{n\log n} \leq (1-\varepsilon)n\log n.$$

Für diese n gilt dann

$$\pi((1-\varepsilon)n\log n) \geq n,$$

also

$$\limsup_{n\to\infty} \frac{\pi((1-\varepsilon)n\log n)}{n} \geq 1.$$

Aber nach **??** gilt

$$\lim_{n\to\infty} \frac{\pi((1-\varepsilon)n\log n}{n} = (1-\varepsilon) < 1.$$

□

Abschließend müssen wir noch folgendes Lemma zeigen, das wir im Beweis von Satz 7.13 benutzt haben.

Lemma 7.14. *Für $\lambda > 0$ gilt*

$$\lim_{n\to\infty} \frac{\pi(\lambda n\log n}{n} = \lambda.$$

Beweis. Nach dem Primzahlsatz gilt

$$\begin{aligned}
\liminf_{n\to\infty} \frac{\pi(\lambda n\log n)}{n} &= \liminf_{n\to\infty} \frac{\pi(\lambda n\log n)}{(\lambda n\log n)\,/\log(\lambda n\log n)} \frac{\lambda\log n}{\log(\lambda n\log n)} \\
&= \frac{\lambda\log n}{\log(\lambda n\log n)} \\
&= \lambda\frac{\log n}{\log\lambda + \log n + \log(\log n)} \\
&= \lambda.
\end{aligned}$$

□

7.5. **Die Funktionalgleichung.** In diesem Abschnitt beweisen wir (bis auf ein paar Blackboxen aus der Funktionentheorie, die allerdings nicht zu kompliziert sind) die Funktionalgleichung für die Riemannsche Zeta-Funktion. Sie stellt einen Zusammenhang her zwischen dem Werten $\zeta(s)$ und $\zeta(1-s)$ und ist eines der wichtigsten Resultate im Zusammenhang mit der Riemannschen Zeta-Funktion. Außerdem werden wir die Riemannsche Zeta-Funktion auf die ganze komplexe Ebene analytisch fortsetzen (bis auf den schon bekannten Pol bei $s = 1$).

Es stellt sich heraus, dass die Funktionalgleichung eine eher komplizierte Form hat, die auch direkt nicht so offensichtlich zu beweisen ist. Stattdessen ist es günstiger die Funktion

$$\xi(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

wobei die Γ-Funktion durch das *Euler-Integral*

$$\Gamma(z) := \int_0^\infty t^{z-1}e^{-t}dt$$

definiert ist. Dieses Integral konvergiert für $\Re(z) > 0$, denn

$$\left|\int_0^\infty t^{z-1}e^{-t}dt\right| \leq \int_0^\infty |t^{z-1}e^{-t}|dt = \int_0^\infty t^{\Re(z)-1}e^{-t}dt < \infty.$$

Für $\Re(z) > 0$ ist die Funktion $t^{\Re(z)-1}e^{-t}$ beschränkt und geht wegen der Exponentialfunktion für $t \to \infty$ schnell genug gegen Null damit das Integral endlich ist. Sie erfüllt folgende Funktionalgleichung:

Lemma 7.15. *Für $\Re(z) > 0$ gilt*

$$\Gamma(z+1) = z\Gamma(z).$$

Beweis.

$$z\Gamma(z) = \int_0^\infty zt^{z-1}e^{-t}dt.$$

Mithilfe partieller Integration kann man dieses Integral folgendermaßen umschreiben:

$$z\Gamma(z) = t^z e^{-t}\big|_0^\infty + \int_0^\infty t^z e^{-t}dt = \int_0^\infty t^{(z+1)-1}e^{-t}dt = \Gamma(z+1).$$

□

Korollar 7.16. *Für $n \in \mathbb{N}$ gilt*

$$\Gamma(n) = (n-1)!.$$

Beweis. Es gilt

$$\Gamma(1) = \int_0^\infty e^{-t}dt = -e^{-t}\big|_0^\infty = 1 = 0!$$

Induktiv nehmen wir an, dass wir die Aussage für n bewiesen haben. Dann gilt nach Lemma 7.15

$$\Gamma(n+1) = n\Gamma(n) = n \cdot (n-1)! = n!.$$

□

Die Funktionalgleichung erlaubt es uns außerdem, die Γ-Funktion auf die gesamte komplexe Ebene meromorph fortzusetzen:

Korollar 7.17. *Die Gamma-Funktion hat eine meromorphe Fortsetzung auf die ganze komplexe Ebene mit einfachen Polen bei ganzen Zahlen $z \leq 0$.*

Beweis. Sei $n \in \mathbb{N}$. Mithilfe der Funktionalgleichung (Lemma 7.15) erhalten wir folgende Identität:

$$\Gamma(z) = \frac{\Gamma(z+1)}{z} = \frac{\Gamma(z+2)}{z(z+1)} = \ldots = \frac{\Gamma(z+n+1)}{z(z+1)\cdots(z+n)}.$$

Da $\Gamma(z+n+1)$ für $\Re(z) > -n-1$ eine holomorphe Funktion ist, definiert die rechte Seite eine meromorphe Funktion mit einfachen Polen bei

$$z = 0, -1, \ldots, -n.$$

Wir können n beliebig groß wählen, daher folgt die Aussage des Korollars. □

Kehren wir zurück zur Funktion

$$\xi(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

Im Beweis für die Funktionalgleichung von ξ wird die Thetafunktion

$$\Theta(x) := \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x} \qquad (x > 0)$$

auftauchen. Um auch für sie eine Funktionalgleichung zu zeigen, werden wir Fourrier-Transformierte und die Poissonsche Summenformel brauchen, die wir hier ohne Beweis erklären. Wir betrachten eine stetig differenzierbare Funktion

$$f : \mathbb{R} \to \mathbb{C}$$

mit der Asymptotik $f(x) = \mathcal{O}(|x|^{-2})$ für $x \to \infty$. Dann ist ihre *Fourrier-Transformierte* definiert als

$$\hat{f} := \int_{-\infty}^{\infty} f(x)e^{-2\pi i x t}dx.$$

Lemma 7.18. *Für $\lambda \geq 0$ und*

$$f_\lambda(x) := f(\lambda(x))$$

gilt

$$\hat{f}_\lambda(t) = \frac{1}{\lambda}\hat{f}\left(\frac{t}{\lambda}\right).$$

Beweis. Dies erhält man durch die Substitution $y = \lambda x$ im Integral:

$$\hat{f}_\lambda(t) = \int_{-\infty}^{\infty} f(\lambda x)e^{-2\pi i x t}dx = \frac{1}{\lambda}\int_{-\infty}^{\infty} f(y)e^{-2\pi i y\frac{t}{\lambda}}dy = \frac{1}{\lambda}\hat{f}\left(\frac{t}{\lambda}\right).$$

□

Satz 7.19 (Poissonsche Summenformel)**.** *Sei $f : \mathbb{R} \to \mathbb{C}$ eine stetig differenzierbare Funktion mit $f(x) = \mathcal{O}(|x|^{-2})$ für $x \to \infty$ und $\hat{f}$ ihre Fourrier-Transformierte. Dann gilt*

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

Beweis. [Neu92, Satz 3.2.] □

Lemma 7.20. *Sei $f : \mathbb{R} \to \mathbb{C}$ eine stetig differenzierbare Funktion mit $f(x) = \mathcal{O}(|x|^{-2})$ für $|x| \to \infty$. Sei*

$$f_\lambda(x) := f(\lambda x), \quad \lambda > 0.$$

Dann gilt

$$\hat{f}_\lambda(t) = \frac{1}{\lambda}\hat{f}\left(\frac{t}{\lambda}\right).$$

Beweis.

$$\hat{f}_\lambda(t) = \int_{-\infty}^{\infty} f(\lambda x) e^{-2\pi i x t} dx = \frac{1}{\lambda} \int_{-\infty}^{\infty} f(\lambda x) e^{-2\pi i (\lambda x) \frac{t}{\lambda}} d(\lambda x) = \frac{1}{\lambda} \hat{f}\left(\frac{t}{\lambda}\right)$$

□

Satz 7.21. *Sei*

$$\Theta(x) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 x}, \quad x > 0.$$

Dann erfüllt Θ die Funktionalgleichung

$$\Theta(x) = \frac{1}{\sqrt{x}} \Theta\left(\frac{1}{x}\right).$$

Beweis. Wir wenden die Poissonsche Summenformel (Satz 7.19) auf die Funktion

$$\begin{aligned} f_\lambda : \mathbb{R} &\to \mathbb{C} \\ x &\mapsto f_\lambda(x) = e^{-\pi x^2 \lambda} \end{aligned}$$

an. Deren Fourrier-Transformierte ist

$$\hat{f}_\lambda = \frac{1}{\sqrt{\lambda}} e^{-\pi x^2 / \lambda}.$$

Einsetzen in die Gleichung

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n)$$

liefert

$$\sum_{n \in \mathbb{Z}} e^{-\pi n^2 \lambda} = \frac{1}{\sqrt{\lambda}} \sum_{n \in \mathbb{Z}} e^{-\pi n^2 / \lambda}.$$

□

Korollar 7.22. *Für $x \to 0^+$ gilt $\Theta(x) = \mathcal{O}\left(\frac{1}{\sqrt{x}}\right)$.*

Satz 7.23. *Für $s \in \mathbb{C}$ mit $\Re(s) > 1$ gilt*

$$\Gamma\left(\frac{s}{2}\right) \zeta(s) = \pi^{s/2} \int_0^\infty t^{s/2} \left(\sum_{n=1}^{\infty} e^{-\pi n^2 t} \right) \frac{dt}{t}.$$

Bemerkung. Die Summe unter dem Integral ist gleich $\frac{1}{2}(\Theta(t) - 1)$. Für $t \to 0^+$ ist das gleich $\mathcal{O}\left(\frac{1}{\sqrt{t}}\right)$. Daraus folgt, dass das Integral existiert.

Beweis. Nach Definition ist

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty t^{s/2} e^{-t} \frac{dt}{t}.$$

Wir substituieren $t = \pi n^2 \tilde{t}$ für $n \geq 1$, es gilt $\frac{dt}{t} = \frac{d\tilde{t}}{\tilde{t}}$. Also haben wir nun

$$\Gamma\left(\frac{s}{2}\right) = \pi^{s/2} n^s \int_0^\infty t^{s/2} e^{-\pi n^2 t} \frac{dt}{t}.$$

Nun teilen wir durch n^s und wollen die Summe über n der Gleichungen

$$\Gamma\left(\frac{s}{2}\right) \frac{1}{n^s} = \pi^{s/2} \int_0^\infty t^{s/2} e^{-\pi n^2 t} \frac{dt}{t}$$

betrachten. Die linke Seite ist dann $\Gamma\left(\frac{s}{2}\right)\zeta(s)$, und rechts steht

$$\sum_{n=1}^{\infty}\left(\pi^{s/2}\int_0^{\infty}t^{s/2}e^{-\pi n^2 t}\frac{dt}{t}\right).$$

Nach dem Satz von Fubini können wir die Summe und das Integral vertauschen, und die Aussage ist bewiesen. □

Satz 7.24 (Funktionalgleichung)**.**

(i) Betrachte $\xi(s)=\pi^{s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$. Diese Funktion ξ ist auf der Halbebene $\{\Re(s)>1\}$ holomorph, und lässt sich zu einer meromorphen Funktion auf $\mathbb{C}$ mit Polen bei $s=1$ und $s=0$ fortsetzen. Sie erfüllt die Funktionalgleichung

$$\xi(s)=\xi(1-s).$$

(ii) Die Zetafunktion $\zeta(s)$ lässt sich meromorph auf ganz $\mathbb{C}$ fortsetzen. Sie hat einen einzigen Pol bei $s=1$. Für ζ gilt die Funktionalgleichung

$$\zeta(1-s)=2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

Beweis. Zunächst zeigen wir (i)⇒(ii). Nach (i) gilt

$$\pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)=\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

Also gilt

$$\zeta(1-s)=\pi^{-s+\frac{1}{2}}\Gamma\left(\frac{1-s}{2}\right)^{-1}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

Die Gammafunktion erfüllt außerdem die Identitäten

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)=2^{1-s}\sqrt{\pi}\Gamma(s)$$

und

$$\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(\frac{1+s}{2}\right)=\frac{\pi}{\sin(\pi\frac{1+s}{2})}=\frac{\pi}{\cos\left(\frac{\pi s}{2}\right)}.$$

Erst zweite dann erste einsetzen dann ausrechnen. Einsetzen der ersten und dann der zweiten Identität in die obige Gleichung gibt uns das gewünschte Resultat.

Es gilt noch (i) zu beweisen. Nach Satz 7.23 ist

$$\xi(s)=\int_0^{\infty}t^{s/2}\psi(t)\frac{dt}{t},\quad \Re(s)>1,$$

wobei $\psi(t)=\sum_{n=1}^{\infty}e^{-\pi n^2 t}=\frac{1}{2}(\Theta(t)-1)$. Zunächst betrachten wir nur das Integral von 0 bis 1. Dazu bemerken wir zunächst, dass

$$\psi\left(\frac{1}{t}\right)=\frac{1}{2}\left(\Theta\left(\frac{1}{t}\right)-1\right)=\frac{1}{2}\left(\sqrt{t}\Theta(t)-1\right)=\sqrt{t}\psi(t)-\frac{1}{2}+\frac{1}{2}\sqrt{t}.$$

Daraus folgt

$$\psi(t)=t^{-1/2}\left(\psi\left(\frac{1}{t}\right)+\frac{1}{2}-\frac{1}{2}t^{1/2}\right),$$

und einsetzen in das Integral liefert

$$\begin{aligned}\xi(s) = \int_0^1 t^{s/2}\psi(t)\frac{dt}{t} &= \int_0^1 t^{s/2}t^{-1/2}\left(\psi\left(\frac{1}{t}\right) + \frac{1}{2} - \frac{1}{2}t^{1/2}\right)\frac{dt}{t} \\ &= \int_0^1 t^{(s-1)/2}\psi\left(\frac{1}{t}\right)\frac{dt}{t} + \frac{1}{2}\int_0^1 (t^{(s-1)/2} - t^{s/2})\frac{dt}{t},\end{aligned}$$

wobei der letzte Term zu

$$\frac{1}{2}\int_0^1 (t^{(s-1)/2} - t^{s/2})\frac{dt}{t} = \frac{1}{2}\left(\frac{2t^{(s+1)/2}}{s-1}\Big|_0^1 - \frac{2t^{(s+2)/2}}{s}\Big|_0^1\right) = \frac{1}{s-1} - \frac{1}{s}$$

evaluiert.

Um den ersten Term zu berechnen, führen wir die Substitution $\tilde{t} = \frac{1}{t}$, $\frac{dt}{t} = -\frac{d\tilde{t}}{\tilde{t}}$ durch. Wir erhalten

$$\int_0^1 t^{(s-1)/2}\psi\left(\frac{1}{t}\right)\frac{dt}{t} = \int_1^\infty t^{-(s-1)/2}\psi(t)\frac{dt}{t}.$$

Insgesamt folgt

$$\xi(s) = -\left(\frac{1}{1-s} + \frac{1}{s}\right) + \int_1^\infty (t^{s/2} + t^{(1-s)/2})\psi(t)\frac{dt}{t}.$$

Da $\psi(t)$ für $t \to \infty$ gegen 0 konvergiert, existiert das Integral für alle $s \in \mathbb{C}$. Diese Darstellung gibt uns also eine meromorphe Fortsetzung von ξ nach ganz $\mathbb{C}$. Außerdem ist diese Darstellung invariant gegenüber der Substitution $s \mapsto 1 - s$. □

8. Die Zeta-Funktion für Polynomringe über einem endlichen Körper

Die Riemannsche Zeta-Funktion

$$\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s} = \prod_{p \text{ prim}} \frac{1}{1-p^{-s}}$$

kann man auffassen als die Zeta-Funktion der ganzen Zahlen $\mathbb{Z}$. Für jede Primzahl p hat diese einen Eulerfaktor $(1-p^{-s})^{-1}$. Wir haben in Kapitel 5 an vielen Stellen betont, dass $\mathbb{F}_p[T]$ für den Körper $\mathbb{F}_p$ mit p Elementen viele Gemeinsamkeiten mit $\mathbb{Z}$ hat. Man könnte sich auch die Frage stellen, ob es ein Analogon zur Riemannschen Zeta-Funktion gibt. Da die normierten irreduziblen Polynome die Stelle der Primzahlen einnehmen, sollte die Zeta-Funktion von $\mathbb{F}_p[T]$ einen Eulerfaktor für jedes solche Polynom haben. Nur welche Form sollten die Eulerfaktoren haben? Hier machen wir die Beobachtung, dass p gerade die Kardinalität des Restklassenkörpers

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

ist.

Das können wir auf $\mathbb{F}_p[T]$ übertragen:

Definition 8.1. Für Polynom $f \in \mathbb{F}_p[T]$ definieren wir die Norm

$$|f| := |\mathbb{F}_p[T]/f\mathbb{F}_p[T]|$$

als die Kardinalität des Restklassenkörpers.

Wir haben in Lemma 5.33 gesehen, dass $\mathbb{F}_p[T]/f\mathbb{F}[T]$ ein Vektorraum über $\mathbb{F}_p$ der Dimension $\deg f$. Daher gilt

$$|f| = p^{\deg f}.$$

Den Betrag $|f|$ sollte man als ein Analogon zum Absolutbetrag auf $\mathbb{Z}$ auffassen. Auch dort gilt für ein Element $m \in \mathbb{Z}$:

$$|m| = |\mathbb{Z}/m\mathbb{Z}|.$$

Für irreduzible normierte Polynome P ist nach Proposition 5.35 der Restklassenring $\mathbb{F}_p[T]/P\mathbb{F}_p[T]$ ein Körper mit p^d Elementen, wobei $d = \deg(P)$, also

$$|P| = p^{\deg(P)}.$$

Es stellt sich heraus, dass wir tatsächlich

$$\frac{1}{1-|P|^{-s}}$$

als Eulerfaktor bei P definieren können und dadurch eine sinnvolle Zeta-Funktion bekommen. Diese Funktion wollen wir in diesem Kapitel untersuchen.

8.1. **Die Eulerfunktion für den Polynomring.** Wir erinnern uns an die eulersche φ-Funktion

$$\varphi(n) = \#\{m \in \{0,\dots,n-1\} \mid \mathrm{ggT}(m,n) = 1\} = \begin{cases} 1 & n = 1, \\ \#\,(\mathbb{Z}/n\mathbb{Z})^\times & n \geq 2. \end{cases}$$

Sie ist multiplikativ und eindeutig bestimmt durch ihre Werte bei Primzahlpotenzen:

$$\varphi(p^r) = (p-1)p^{r-1}$$

und tatsächlich kann man für $p > 2$ und $r > 0$ sogar zeigen, dass

$$(\mathbb{Z}/p^r\mathbb{Z})^\times$$

eine zyklische Gruppe der Ordnung $(p-1)p^{r-1}$ ist. Wir wollen in diesem Abschnitt das Analogon für $\mathbb{F}_p[T]$ untersuchen.

Definition 8.2. Für ein Polynom $f \in \mathbb{F}_p[T] \setminus \{0\}$ definieren wir

$$\varphi(f) := \#\{g \in \mathbb{F}_p[T] \mid \mathrm{ggT}(f,g) = 1 \text{ und } \deg(g) < \deg(f)\}$$

Ähnlich wie in Lemma 3.12 haben wir eine alternative Beschreibung von φ mithilfe der Einheiten von $\mathbb{F}_p[T]/f\mathbb{F}_p[T]$. Diese Einheiten haben wir noch nicht bestimmt.

Lemma 8.3. *Für Polynome $f, g \in \mathbb{F}_p[T]$, f nicht konstant gilt*

$$[g]_f \in (\mathbb{F}_p[T]/f\mathbb{F}_p[T])^\times \qquad \Leftrightarrow \qquad \mathrm{ggT}(f,g) = 1.$$

Beweis. Die Restklasse $[g]_f$ ist genau dann eine Einheit, wenn es $h \in \mathbb{F}_p[T]$ gibt mit

$$[h]_f \cdot [g]_f = [1]_f$$

oder mit anderen Worten

$$hg + fa = 1$$

für ein Polynom $a \in \mathbb{F}_p[T]$. Die Existenz von h und a, die diese Gleichung erfüllen, ist wiederum äquivalent dazu, dass $\mathrm{ggT}(f,g) = 1$ (siehe Proposition 5.18). □

Daraus bekommen wir direkt folgende Beschreibung der Eulerfunktion:

Lemma 8.4. *Für ein nichttriviales Polynom $f \in \mathbb{F}_p[T]$ gilt*

$$\varphi(f) = \begin{cases} 1 & f \text{ konstant} \\ \#\left(\mathbb{F}_p[T]/f\mathbb{F}_p[T]\right)^\times & \deg(f) > 0. \end{cases}$$

Beweis. Nach Lemma 5.33 ist

$$[1]_f, \ldots, [T]^{\deg f}$$

eine Basis von $\mathbb{F}_p[T]/f\mathbb{F}_p[T]$ als $\mathbb{F}_p$- Vektorraum. Die Polynome $g \in \mathbb{F}_p[T]$ vom Grad $\deg(g) < \deg(f)$ bilden also ein vollständiges Repräsentantensystem der Restklassen in $\mathbb{F}_p[T]/f\mathbb{F}_p[T]$. Die Klasse $[g]_f$ eines solchen Polynoms ist nach Lemma 8.4 genau dann eine Einheit, wenn $\mathrm{ggT}(f,g) = 1$. Daher ist die Anzahl der Einheiten gerade die Anzahl der zu f teilerfremden Polynome vom Grad kleiner als $\deg(f)$.¨ □

Lemma 8.5. *Für teilerfremde Polynome f und g gilt*

$$\varphi(fg) = \varphi(f) \cdot \varphi(g).$$

Beweis. Wegen des chinesischen Restsatzes (Proposition 5.34) ist

$$\begin{aligned} \varphi : K[T]/(fg) &\longrightarrow K[T]/(f) \times K[T]/(g) \\ [h]_{fg} &\longmapsto ([h]_f, [h]_g) \end{aligned}$$

für teilerfremde Polynome $f, g \in \mathbb{F}_p[T]$ ein Isomorphismus. Wie im Falle von $\mathbb{Z}$ bekommen wir daraus auch eine Zerlegung der Einheiten:

$$\left(\mathbb{F}_p[T]/(fg)\right)^\times \cong \left(\mathbb{F}_p[T]/(f)\right)^\times \times \left(\mathbb{F}_p[T]/(g)\right)^\times.$$

Daraus folgt, dass die Eulerfunktion multiplikativ ist für teilerfremde Faktoren. □

Aus diesem Lemma folgt, dass die Eulerfunktion eindeutig festgelegt ist durch ihre Werte $\varphi(P^r)$ für Potenzen P^r eines irreduziblen Polynoms P. Den Wert $\varphi(P)$ kennen wir schon, da $\mathbb{F}_p[T]/P\mathbb{F}_p[T]$ nach Proposition 5.35 ein Körper ist und somit

$$\varphi(P) = |\left(\mathbb{F}_p[T]/P\mathbb{F}_p[T]\right)^\times| = |P| - 1.$$

Genauer wissen wir sogar wegen Satz 5.24, dass

$$\mathbb{F}_p[T]/P\mathbb{F}_p[T] \cong \mathbb{Z}/(|P|-1)\mathbb{Z}.$$

Wir wollen nun $\varphi(P^r)$ für höhere Potenzen untersuchen.

Lemma 8.6. *Sei $P \in \mathbb{F}_p[T]$ ein irreduzibles Polynom und $r \in \mathbb{N}$. Dann gilt*

$$\varphi(P^r) = |P|^{r-1}(|P| - 1).$$

Beweis. Wir müssen die Anzahl der Polynome vom Grad kleiner als $\deg(P^r) = r\deg(P)$ finden, die teilerfremd zu P^r, also teilerfremd zu P, sind. Da P irreduzibel ist, sind dies gerade die Polynome vom Grad kleiner als $r\deg(P)$, die P nicht teilt. Andersherum können wir auch die Polynome bestimmen, die P als Teiler haben, und danach deren Anzahl von der Zahl aller Polynome (vom Grad $< r\deg(P)$) abziehen. Dafür betrachten wir den Homomorphismus

$$\begin{aligned} \psi : \mathbb{F}_p[T] &\longrightarrow \mathbb{F}_p[T]/P^r\mathbb{F}_p[T] \\ h &\longmapsto [Ph]_{P^r}. \end{aligned}$$

Wir berechnen den Kern:

$$\ker(\psi) = \{h \in \mathbb{F}_p[T] \mid [Ph]_{P^r} = 0\} = \{h \in \mathbb{F}_p[T] \mid P^r | Ph\}$$

$$= \{h \in \mathbb{F}_p[T] \mid P^{r-1} | h\} = P^{r-1}\mathbb{F}_p[T].$$

Daher erhalten wir einen injektiven Homomorphismus

$$\bar{\psi} : \mathbb{F}_p[T]/P^{r-1}\mathbb{F}_p[T] \longrightarrow \mathbb{F}_p[T]/P^r\mathbb{F}_p[T].$$

Dessen Bild besteht gerade aus allen Restklassen von Polynomen, die durch P teilbar sind. Wir erhalten für die Anzahl der Einheiten:

$$\varphi(P^r) = |\left(\mathbb{F}_p[T]/P^r\mathbb{F}_p[T]\right)| - |\left(\mathbb{F}_p[T]/P^{r-1}\mathbb{F}_p[T]\right)| = |P|^r - |P|^{r-1} = |P|^{r-1}(|P|-1).$$

□

Korollar 8.7. *Für $f \in \mathbb{F}_p[T]$ gilt*

$$\varphi(f) = |f| \prod_{P|f} \left(1 - \frac{1}{|P|}\right)$$

Beweis. Sei

$$f = a \prod_{P|f} P^{r_P}$$

die Primfaktorzerlegung von f in irreduzible, normierte Polynome P und eine Konstante a. Dann können wir $\varphi(f)$ mithilfe von Lemma 8.5 und Lemma 8.6 berechnen:

$$\begin{aligned}
\varphi(f) &= \varphi\left(\prod_{P|f} P^{r_P}\right) \\
&= \prod_{P|f} \varphi(P^{r_P}) \\
&= \prod_{P|f} |P|^{r_P-1}(|P|-1) \\
&= \prod_{P|f} |P|^{r_P}(1 - \frac{1}{|P|} \\
&= |f| \prod_{P|f} \left(1 - \frac{1}{|P|}\right)
\end{aligned}$$

□

Bis an diese Stelle hat die Theorie die gleiche Form wie für $\mathbb{Z}$. Wenn man sich die Gruppenstruktur der Einheiten

$$(\mathbb{F}_p[T]/P^r\mathbb{F}_p[T])^\times$$

anschaut, gibt es allerdings erhebliche Unterschiede. Die Gruppe

$$(\mathbb{Z}/q^r\mathbb{Z})^\times,$$

ist für $q > 2$ zyklisch während wir im Falle des Polynomrings über $\mathbb{F}_p$ ein ganz anderes Verhalten haben. Das liegt am Frobeniusautomorphismus, den wir auf den Übungszetteln (Blatt 8, Aufgabe 3c) kennengelernt haben. Dort haben wir das folgende Lemma gezeigt:

Lemma 8.8. *Sei K ein Körper der Charakteristik p. Dann ist*

$$\begin{aligned} \mathrm{Frob}_p : K &\longrightarrow K \\ x &\longmapsto x^p \end{aligned}$$

ein Körperhomomorphismus. Ist K endlich, so ist Frob_p ein Isomorphismus.

Wichtig für uns an dieser Stelle ist, dass Frob_p ein Homomorphismus ist. Der springende Punkt ist die Additivität

$$\mathrm{Frob}_p(x+y) = \mathrm{Frob}_p(x) + \mathrm{Frob}_p(y),$$

also

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

Proposition 8.9. *Sei $P \in \mathbb{F}_p[T]$ ein irreduzibles Polynom und $r \in \mathbb{N}$. Sei*

$$(\mathbb{F}_p[T]/P^r\mathbb{F}_p[T])^{(1)} := \ker\left((\mathbb{F}_p[T]/P^r\mathbb{F}_p[T])^\times \twoheadrightarrow (\mathbb{F}_p[T]/P\mathbb{F}_p[T])^\times\right)$$

der Kern der kanonischen Projektion. Diese ist eine Gruppe der Kardinalität $|P|^{r-1}$ und für r gegen unendlich geht die minimale Anzahl der Erzeuger gegen unendlich.

Beweis. Die Aussage über die Kardinalität folgt durch ein einfaches Zählargument aus Lemma 8.6 zusammen mit dem Homomorphiesatz für Gruppen, weil das Bild der obigen Abbildung genau die Kardinalität $|P|-1$ hat. Nach Definition hat jedes Element in $(\mathbb{F}_p[T]/P^r\mathbb{F}_p[T])^{(1)}$ einen Repräsentanten der Gestalt $a = 1 + bP$.
Um ein Gefühl dafür zu bekommen, was passiert, schauen wir uns den Fall $r = 2$ an (im Fall $r = 1$ ist $(\mathbb{F}_p[T]/P\mathbb{F}_p[T])^{(1)}$ trivial). Mit Hilfe des Frobenius-Homomorphismus sehen wir

$$a^p = 1 + b^p P^p \equiv 1 \mod (P^2)$$

wegen $p \geq 2$. Es ist also $(\mathbb{F}_p[T]/P^2\mathbb{F}_p[T])^{(1)}$ eine Gruppe der Ordnung $|P| = p^{\deg(P)}$ und für alle $[a] \in (\mathbb{F}_p[T]/P^2\mathbb{F}_p[T])^{(1)}$ gilt $[a]^p = 1$. Nach dem Hauptsatz für endliche abelsche Gruppen (den wir auch in der Übungsgruppe auf Blatt 10, Aufgabe 2b) benutzt haben), folgt

$$(\mathbb{F}_p[T]/P^2\mathbb{F}_p[T])^{(1)} \cong (\mathbb{Z}/p\mathbb{Z})^{\deg(P)}.$$

Wir sehen also schon für $r = 2$, dass die Gruppe $(\mathbb{F}_p[T]/P^2\mathbb{F}_p[T])^{(1)}$ i.d.R. nicht zyklisch ist (nur in dem Spezialfall $\deg(P) = 1$).
Den allgemeinen Fall können wir sehr ähnlich zum ersten Fall untersuchen: Sei $s \in \mathbb{N}$ die kleinste Zahl mit $p^s \geq r$. Dann folgt

$$(1+bP)^{p^s} = 1 + (bP)^{p^s} \equiv 1 \mod (P^r).$$

Wählen wir nun ein Erzeugendensystem $a_1, \ldots, a_d$ von $(\mathbb{F}_p[T]/P^r\mathbb{F}_p[T])^{(1)}$ mit minimaler Anzahl d, so erhalten wir einen surjektiven Gruppenhomomorphismus

$$(\mathbb{Z}/p^s\mathbb{Z})^d \twoheadrightarrow (\mathbb{F}_p[T]/P^r\mathbb{F}_p[T])^{(1)},$$

der dadurch festgelegt ist, dass die kanonische Basis von $(\mathbb{Z}/p^s\mathbb{Z})^d$ auf $a_1, \ldots, a_d$ geschickt wird. Dieser ist wohldefiniert, da nach der obigen Rechnung $[a]^{p^s} = 1$ für alle $[a] \in (\mathbb{F}_p[T]/P^r\mathbb{F}_p[T])^{(1)}$ gilt. Vergleichen wir die Ordnungen dieser beiden Gruppen, so sehen

wir $p^{sd} \geq |P|^{r-1} = p^{(\deg P)(r-1)}$ und folglich, da $r > p^{s-1}$ und somit $\log_p(r) + 1 > s$ nach Wahl von s gilt, dass

$$d \geq \frac{(\deg P) \cdot (r-1)}{s} > \frac{(\deg P) \cdot (r-1)}{\log_p(r) + 1} \overset{r \to \infty}{\to} \infty,$$

womit die Behauptung folgt. □

Wir erinnern uns an den Satz von Euler (Satz 3.15), der besagt, dass für $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ teilerfremd gilt

$$a^{\varphi(n)} \equiv 1 \mod n$$

und seinen Spezialfall für $n = p$ prim, den kleinen Fermat (Korollar 3.16):

$$a^p \equiv a$$

für alle $a \in \mathbb{Z}$. Diese Sätze gelten genauso in $\mathbb{F}_p[T]$:

Proposition 8.10. *Für teilerfremde Polynome f und a in $\mathbb{F}_p[T]$ mit $f \neq 0$ gilt*

$$a^{\varphi(f)} \equiv 1 \mod f.$$

Beweis. Man argumentiert genauso wie in $\mathbb{Z}$: Die Gruppe

$$(\mathbb{F}_p[T]/f\mathbb{F}_p[T])^\times$$

hat Ordnung $\varphi(f)$ und daher ist die $\varphi(f)$-te Potenz jedes Elements gleich 1. Jetzt braucht man nur noch zu wissen, dass $[a]_f$ eine Einheit ist, da a und f teilerfremd sind (Lemma 8.3). □

Korollar 8.11. *Für $a \in \mathbb{F}_p[T]$ und ein irreduzibles Polynom $P \in \mathbb{F}_p[T]$ gilt*

$$a^{|P|} \equiv a \mod P.$$

Beweis. Zuerst machen wir uns klar, dass

$$\varphi(P) = |P| - 1$$

nach Lemma 8.6. Falls P nicht a teilt, gilt folglich nach Proposition 8.10

$$a^{|P|-1} \equiv 1 \mod P.$$

Aber dann gilt auch

$$a^{|P|} \equiv a \mod P$$

und diese Gleichung ist offensichtlich auch für $[a]_P = 0$ erfüllt. □

8.2. **Die Zeta-Funktion.** Wie wir schon am Anfang des Kapitels gesehen haben, ist das Analogon in $\mathbb{F}_p[T]$ zum Absolutbetrag der ganzen Zahlen der Betrag

$$|P| = |\,(\mathbb{F}_p[T]/P\mathbb{F}_p[T])\,|.$$

Außerdem spielen unter den ganzen Zahlen ungleich 0 die positiven Zahlen eine besondere Rolle; so lassen sich viele zahlentheoretische Zusammenhänge, wie z.B. die Primfaktorzerlegung, „bis auf Vorzeichen“ formulieren, sodass es oft ausreicht, nur positive ganze Zahlen zu untersuchen. Das Analogon zu den positiven ganzen Zahlen in $\mathbb{F}_p[T]$ sind die normierten Polynome, denn was in $\mathbb{Z}$ „bis auf Vorzeichen“ gilt, gilt in $\mathbb{F}_p[T]$ „bis auf einen Faktor aus $\mathbb{F}_p^\times$“. Jedes Polynom ungleich 0 entspricht in diesem Sinne genau einem normierten Polynom, welches entsteht, indem man es mit dem Inversen seines Leitkoeffizienten multipliziert, ebenso wie jede ganze Zahl ungleich 0 bis auf Vorzeichen genau einer positiven ganzen Zahl entspricht.

Definition 8.12. Die *Riemannsche Zeta-Funktion* $\zeta_p(s)$ *zu* $\mathbb{F}_p[T]$ ist definiert als die Reihe

$$\zeta_p(s) := \sum_{\substack{f \in \mathbb{F}_p[T] \\ f \text{ normiert}}} \frac{1}{|f|^s}.$$

Für jeden Grad $d \geq 0$ gibt es genau p^d viele normierte Polynome vom Grad d in $\mathbb{F}_p[T]$,

Im Gegensatz zur Riemannschen Zetafunktion ist die Zetafunktion von $\mathbb{F}_p[T]$ nicht zu schwierig zu untersuchen. Wir können ganz einfach eine geschlossene Formel angeben:

Satz 8.13. *Die Reihe*

$$\zeta_p(s) = \sum_{\substack{f \in \mathbb{F}_p[T] \\ f \text{ normiert}}} \frac{1}{|f|^s}.$$

konvergiert für $\Re(s) > 1$ *und es gilt*

$$\zeta_p(s) = \frac{1}{1 - p^{1-s}}.$$

Insbesondere besitzt $\zeta_p(s)$ *eine meromorphe Fortsetzung auf die ganze komplexe Ebene mit einem einfachen Pol bei* $s = 1$ *mit Residuum* $1/\log p$.

Beweis. Für ein normiertes Polynom

$$f(T) = T^d + a_{d-1}T^{d-1} + \ldots + a_0$$

in $\mathbb{F}_p[T]$ gilt

$$|f| = p^{\deg(f)} = p^d.$$

Die Anzahl der normierten Polynome vom Grad d ist p^d, denn jeder der d Koeffizienten $a_0, \ldots, a_{d-1}$ ist ein Element von $\mathbb{F}_p$ und kann somit p verschiedene Werte annehmen. Damit kommt der Summand

$$\frac{1}{|f|^s}$$

in der Reihe genau p^d mal vor. Wir erhalten

$$\zeta_p(s) = \sum_{d=0}^{\infty} \frac{p^d}{p^{ds}} = \sum_{d=0}^{\infty} \frac{1}{p^{(d(s-1)}}.$$

Diese Reihe ist die geometrische Reihe für $1/p^{s-1} = p^{1-s}$. Sie konvergiert für

$$|1/p^{s-1}| = \frac{1}{p^{\Re(s)-1}} < 1,$$

also für $\Re(s) > 1$ und der Grenzwert ist

$$\frac{1}{1 - p^{1-s}}.$$

Dieser Ausdruck ist meromorph auf der ganzen komplexen Ebene und hat eine Singularität bei $s = 1$. Um zu zeigen, dass es sich um einen einfachen Pol handelt, reicht es zu zeigen, dass $1 - p^{1-s}$ bei $s = 1$ eine einfache Nullstelle hat. Das sehen wir an der Reihenentwicklung

$$1 - p^{1-s} = 1 - e^{(1-s)\log p} = 1 - \sum_{n=0}^{\infty} \frac{((1-s)\log p)^n}{n!} = (s-1)\log p - \sum_{n=2}^{\infty} \frac{((1-s)\log p)^n}{n!}.$$

Daran kann man auch ablesen, dass das Residuum gleich $1/\log p$ ist. □

Wir können nun mit den gleichen Argumenten wie für die Riemannsche Zeta-Funktion die Produktformel beweisen. Auch hier geht wesentlich die Existenz und Eindeutigkeit der Primfaktorzerlegung ein.

Satz 8.14. *Für* $\mathrm{Res}(s) > 1$ *gibt es eine Darstellung der Zeta-Funktion als Eulerprodukt:*

$$\zeta_p(s) = \prod_{\substack{P \in \mathbb{F}_p[T] \\ \text{normiert, irreduzibel}}} \frac{1}{1 - |P|^{-s}}.$$

Beweis. Das Konvergenzverhalten der Reihe und des Produkts ist ähnlich wie bei der Riemannschen Zeta-Funktion. Auch hier konvergiert die Reihe absolut und gleichmäßig auf Kompakta und das Produkt konvergiert normal. Für $d \in \mathbb{N}$ nummerieren wir die endlich vielen normierten, irreduziblen Polynome vom Grad kleiner gleich d:

$$P_1, \dots, P_m.$$

Um das Produkt

$$\prod_{\deg(P) \le d} \frac{1}{1 - |P|^{-s}} = \prod_{r=1}^{m} \frac{1}{1 - |P_r|^{-s}}$$

zu berechnen, benutzen wir wieder die Formel für die geometrische Reihe und multiplizieren dann aus:

$$\begin{aligned} \prod_{r=1}^{m} \frac{1}{1 - |P_r|^{-s}} &= \prod_{r=1}^{m} \sum_{k_r=0}^{\infty} \frac{1}{|P_r|^{k_r s}} \\ &= \sum_{k_1, \dots, k_m = 0}^{\infty} \frac{1}{(|P|^{k_1} \cdots |P|^{k_m})^s}. \end{aligned}$$

Der Ausdruck $1/(|P|^{k_1} \cdots |P|^{k_m})^s$ durchläuft alle Werte $1/|f|^s$ für normierte Polynome f, in deren Primfaktorzerlegung ausschließlich Polynome vom Grad höchstens d vorkommen. Im Limes $d \to \infty$ erhalten wir die Produktformel. □

8.3. **Das Analogon zum Primzahlsatz.** Wir haben in Kapitel 7 die asymptotische Formel

$$\pi(x) \sim \frac{x}{\log x}$$

für die Anzahl der Primzahlen, die kleiner als x sind, bewiesen. Auch dafür wollen wir ein Analogon für Polynome zeigen. Wir wollen also die Asymptotik der Funktion

$$\pi_p(x) := \#\{P \in \mathbb{F}_p[T] \text{ normiert, irreduzibel} \mid \deg(P) \le x\}$$

untersuchen. Tatsächlich kann man die Anzahl der irreduziblen Polynome viel expliziter bestimmen als die Anzahl der Primzahlen. Wir erinnern uns daran, dass wir mit

$$h_p(m)$$

die Anzahl der normierten, irreduziblen Polynome vom Grad m bezeichnet haben. In der Tat haben wir in den Übungen (Blatt 6, Aufgabe 3(e)) die Formel

$$h_p(m) = \frac{1}{m} \sum_{d \mid m} \mu(d) p^{n/d}$$

bewiesen, mit deren Hilfe wir auch $\pi_p(x)$ bestimmen können. Bevor wir das tun geben wir einen alternativen Beweis für die Formel für $h_p(m)$ an, die die Produktformel der Zeta-Funktion ausnutzt.

Proposition 8.15. *Es gilt*

$$\sum_{d|m} dh_p(d) = p^m.$$

Beweis. In der Produktformel

$$\zeta_p(s) = \prod_{\substack{P\in\mathbb{F}_p[T]\\ \text{normiert, irreduzibel}}} \frac{1}{1-|P|^{-s}}.$$

kommt der Faktor

$$\frac{1}{1-|P|^{-s}} = \frac{1}{1-p^{-s\deg(P)}}$$

genau so oft vor wie es irreduzible, normierte Polynome vom Grad $\deg(P)$ gibt. Die Produktformel nimmt so die Gestalt

$$\zeta_p(s) = \prod_{d=1}^{\infty} \left(\frac{1}{1-p^{-sd}}\right)^{h_p(d)}.$$

an. Jetzt benutzen wir die Darstellung

$$\zeta_p(s) = \frac{1}{1-p^{1-s}}.$$

Setzen wir $u := p^{-s}$, erhalten wir

$$\frac{1}{1-pu} = \prod_{d=1}^{\infty}(1-u^d)^{-h_p(d)}.$$

Wir nehmen nun auf beiden Seiten den Logarithmus

$$-\log(1-pu) = -\sum_{d=1}^{\infty} h_p(d)\log(1-u^d),$$

leiten nach u ab

$$\frac{p}{1-pu} = \sum_{d=1}^{\infty} \frac{dh_p(d)u^{d-1}}{1-u^d}$$

und multiplizieren mit u

$$\frac{pu}{1-pu} = \sum_{d=1}^{\infty} \frac{dh_p(d)u^d}{1-u^d}.$$

Jetzt benutzen wir auf beiden Seiten die geometrische Reihe und erhalten

$$\sum_{m=1}^{\infty}(pu)^m = \sum_{d=1}^{\infty}\sum_{k=1}^{\infty} dh_p(d)u^{kd} = \sum_{m=1}^{\infty}\sum_{d|m} dh_p(d)u^m$$

Vergleichen wir die Koeffizienten von u^m, erhalten wir das Resultat. □

Korollar 8.16.

$$h_p(m) = \frac{1}{m}\sum_{d|m}\mu(d)p^{n/d}$$

Beweis. Das beweist man genau wie auf dem Übungsblatt mithilfe der Möbiusinversion. □

Wir wollen nun also das asymptotische Verhalten von

$$\pi_p(x) = \sum_{\substack{P \text{ irred., normiert} \\ |P| \leq x}} 1 = \sum_{\substack{m \in \mathbb{N} \\ p^m \leq x}} h_p(m)$$

untersuchen. Dafür werden wir zunächst $h_p(m)$ für m gegen unendlich abschätzen.

Lemma 8.17. *Sei n eine natürliche Zahl mit t verschiedenen Primfaktoren. Dann gilt*

$$\sum_{d|n} |\mu(d)| = 2^t$$

Beweis. Sei

$$n = p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$$

die Primfaktorzerlegung von n. Wir erinnern uns an die Definition der μ-Funktion:

$$\mu(m) = \begin{cases} (-1)^r & m = q_1 \cdot \ldots \cdot q_r \text{ quadratfrei} \\ 0 & \text{sonst.} \end{cases}$$

Jeder Teiler d von n, für den $\mu(d)$ nicht Null ist, ist von der Form

$$d = p_1 \varepsilon_1 \cdot \ldots p_t^{\varepsilon_t}$$

für $\varepsilon_i \in \{0, 1\}$. Es gibt dafür 2^t verschiedene Kombinationen, also folgt das gewünschte Resultat. □

Der folgende Satz wird oft als der Primzahlsatz für Polynome bezeichnet

Satz 8.18. *Sei $h_p(n)$ die Anzahl der irreduziblen, normierten Polynome vom Grad n. Dann gilt*

$$h_p(n) = \frac{p^n}{n} + \mathcal{O}\left(\frac{p^{n/2}}{n}\right).$$

Insbesondere haben wir

$$h_p(n) \sim \frac{p^n}{n}.$$

Beweis. Der größte Term in

$$h_p(n) = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}$$

tritt für $d = 1$ auf und lautet p^n/n. Als nächstes kommt $-p^{n/2}/n$, aber nur wenn n durch 2 teilbar ist. Alle weiteren Terme sind kleiner oder gleich $p^{n/3}/n$.

Jetzt benutzen wir, dass die Anzahl der Summanden nach Lemma 8.17 gleich 2^t ist, wobei t die Anzahl der verschiedenen Primfaktoren

$$p_1, \ldots, p_t$$

von n bezeichnet. Damit können wir die Anzahl der Summanden grob abschätzen durch

$$2^t \leq p_1 \cdot \ldots \cdot p_t \leq n.$$

Daher bekommen wir für die verbleibende Summe

$$\left|\sum_{\substack{d|n\\ d\neq 1,2}} \mu(d)p^{n/d}\right| \leq \sum_{\substack{d|n\\ d\neq 1,2}} |\mu(d)|p^{n/3} \leq np^{n/3}.$$

Setzen wir alles zusammen, erhalten wir die Asymptotik für $h_p(n)$:

$$\left|h_p(n) - \frac{p^n}{n}\right| \leq \frac{p^{n/2}}{n} + \frac{np^{n/3}}{n} = \frac{p^{n/2}}{n} + p^{n/3} \leq \frac{p^{n/2}}{n}.$$

□

Setzen wir $x = p^n$, so ist

$$\frac{p^n}{n} = \frac{x}{\log_p x}.$$

Das sieht genauso aus wie im klassischen Primzahlsatz

$$\pi(x) \sim \frac{x}{\log x}.$$

Tatsächlich haben wir in Satz 8.18 die präzisere Form

$$h_p(n) = \frac{x}{\log_p x} + \mathcal{O}\left(\frac{\sqrt{x}}{\log_p x}\right)$$

gezeigt (das ist nur heuristisch, da wir $x = p^n$ gesetzt haben, aber die linke Seite sozusagen nur für $x = p^n$ und nicht für allgemeine x definiert ist). Tatsächlich wird diese präzisere Aussage auch im klassischen Fall vermutet.

Vermutung 1. *Es gilt*

$$\pi(x) = \frac{x}{\log x} + \mathcal{O}\left(\frac{\sqrt{x}}{\log x}\right)$$

Ein Beweis würde die Riemannsche Vermutung brauchen, die jedoch unbewiesen ist.

Wir wollen noch darauf hinweisen, dass die Analogie von Satz 8.18 zum Primzahlsatz nicht vollständig ist, weil wir in Satz 8.18 die Asymptotik von $h_p(n)$ bestimmt haben und nicht die von π_p.

9. Ausblick auf die algebraische und analytische Zahlentheorie

Definition 9.1. Ein *Zahlkörper* ist eine endliche Erweiterung von $\mathbb{Q}$.

Beispiel 9.2. $\mathbb{Q}[\sqrt{2}]$ ist ein Zahlkörper.

Eine natürliche Fragestellung ist dann, was das Analogon zu $\mathbb{Z} \subseteq \mathbb{Q}$ in einem Zahlkörper ist. Im Beispiel wäre es

$$\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}.$$

Allgemein definieren wir für einen Zahlkörper $K/\mathbb{Q}$ den *Ganzabschluss* $\mathcal{O}_K$ von $\mathbb{Z}$ in K als

$$\mathcal{O}_K = \{a \in K \mid \exists f \in \mathbb{Z}[T] \text{ normiert}, f(a) = 0\}.$$

Wir nennen $\mathcal{O}_K$ den *Ganzheitsring* von K.

Beispiel 9.3. Sei $K = \mathbb{Q}[\sqrt{5}]$. Dann ist

$$\mathcal{O}_K = \left\{ a + b\left(\frac{1+\sqrt{5}}{2}\right) \mid a, b \in \mathbb{Z} \right\}$$

der Ganzabschluss von $\mathbb{Z}$ in K, da $\frac{1+\sqrt{5}}{2}$ die Gleichung

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1+\sqrt{5}}{2}\right) - 1 = 0$$

erfüllt, also $\frac{1+\sqrt{5}}{2}$ ist eine Nullstelle des normierten Polynoms $T^2 - T - 1$.

Im Allgemeinen ist $\mathcal{O}_K$ also nicht einfach zu bestimmen. Ein weiteres Problem ist, dass $\mathcal{O}_K$ im allgemeinen nicht euklidisch und auch nicht immer ein Hauptidealring ist. Diese Eigenschaften sind wichtig für die Primfaktorzerlegung, wie wir sie in $\mathbb{Z}$ kennen, ohne diese Eigenschaften gibt es Probleme.

Beispiel 9.4. Sei $K = \mathbb{Q}[\sqrt{-5}]$. Dann ist die Primfaktorzerlegung von der 6 nicht eindeutig:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Diese Elemente sind alle irreduzibel, aber nicht prim. Zum Beispiel gilt

$$2 = ab \Rightarrow a \text{ oder } b \text{ ist Einheit},$$

aber aus $2|(1 + \sqrt{-5})(1 - \sqrt{-5})$ folgt nicht $2 \mid (1 + \sqrt{-5})$ oder $2 \mid (1 - \sqrt{-5})$.

Dieses Problem löst man, indem man Primideale statt Primelemente betrachtet.

Definition 9.5. Sei R ein Ring. Ein Ideal $\mathfrak{p} \subseteq R$ heißt *prim*, falls

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

Bemerkung 9.6. Falls ein Primideal $\mathfrak{p} = (x)$ ein Hauptideal ist, dann gilt

$$a \in \mathfrak{p} = (x) \Leftrightarrow x|a.$$

Diese Definition ist also kompatibel mit der „alten" Definition von *prim*.

Beispiel 9.7 (Fortsetzung von Beispiel 9.4)**.** In $K = \mathbb{Q}[\sqrt{-5}]$ sind $(2, 1 \pm \sqrt{-5})$ und $(3, 1 \pm \sqrt{-5})$ Primideale, und es gilt

$$(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

und

$$(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}).$$

Für Funktionenkörper können wir nach dem selben Prinzip vorgehen.

Definition 9.8. Ein *algebraischer Funktionenkörper* ist eine endliche Erweiterung von einem Körper der Form $\mathbb{F}_p(T)$.

Den Ganzheitsring $\mathcal{O}_K$ eines algebraischen Funktionenkörpers $K/\mathbb{F}_p(T)$ definieren wir als den Ganzabschluss von $\mathbb{F}_p[T]$ in K.

Ist k algebraisch abgeschlossen, so sind alle normierten irreduziblen Polynome $f \in k[T]$ von der Form $f(T) = T - a$. Wir haben also eine Bijektion

$$\begin{aligned} k &\xrightarrow{\sim} \overbrace{\{f \in k[T] \text{ irreduzibel, normiert}\}}^{=:\mathrm{Spec}(k[T]) \text{ das Spektrum von } k[T]} \\ a &\mapsto (T-a). \end{aligned}$$

Betrachtet man diese Abbildung für k nicht algebraisch abgeschlossen, so ist zwar jedes $T - a$ ein irreduzibles, normiertes Polynom, aber es werden nicht alle solche getroffen. Die Situation ist dann etwas komplizierter, aber man sollte es sich so vorstellen, dass das Spektrum $\mathrm{Spec}(k[T])$ auch Informationen über Erweiterungen von k enthält, die zu den Nullstellen anderer irreduzibler Polynome in $k[T]$ gehören.

Das Fazit ist also, dass $\mathrm{Spec}(\mathbb{F}_p[T])$ so etwas wie die affine Gerade $\mathbb{A}^1 = \mathbb{F}_p$ ist. Diese Perspektive motiviert ebenfalls ∞ zu betrachten, indem wir ein Analogon zu $\mathbb{P}^1$ betrachten.

Für eine endliche Erweiterung $K/\mathbb{F}_p(T)$ erhält man kompliziertere Kurven C zusammen mit Abbildungen

$$C \to \mathbb{P}^1,$$

man kann also K verstehen, indem man C mit geometrischen Methoden untersucht.

9.1. **Die Dedekindsche Zetafunktion.** Sei $K/\mathbb{Q}$ endlich. Die Funktion

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \text{Ideal}}} \frac{1}{N(\mathfrak{a})^s}, \quad \Re(s) > 1$$

heißt die *Dedekindsche Zetafunktion* von K, wobei $N(\mathfrak{a}) \in \mathbb{N}$ die Norm eines Ideals ist.

Für $K = \mathbb{Q}$ sind alle Ideale von $\mathbb{Z}$ der Form $\mathfrak{a} = (n)$, und $N((n)) = n$, also ist $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ die Riemannsche Zetafunktion.

Die Zetafunktion $\zeta_K(s)$ konvergiert absolut und gleichmäßig auf Kompakta, und sie hat eine Darstellung als Eulerprodukt

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \text{Primideal}}} \frac{1}{1 - N(\mathfrak{p})^{-s}}, \quad \Re(s) > 1.$$

ζ_K besitzt eine analytische Fortsetzung auf ganz $\mathbb{C}$ mit Pol bei $s = 1$. Das Residuum bei $s = 1$ ist

$$\frac{2^{r_1}(2\pi)^{r_2}\mathrm{Reg}_K h_k}{w_K \sqrt{|D_K|}},$$

wobei

- r_1 die Anzahl der reellen Einbettungen $K \hookrightarrow \mathbb{R}$,
- r_2 die Anzahl der komplexen Einbettungen $K \hookrightarrow \mathbb{C}$,
- Reg_K der Regulator von K (technisch, hat mit Einheiten zu tun),
- h_K die Klassenzahl (gibt gewissermaßen an, wie weit $\mathcal{O}_K$ davon entfernt ist, Hauptidealring zu sein),
- $w_K = \#\mu_K = \#\left\{e^{\frac{2\pi i}{n}} \in K\right\}$ die Anzahl an Einheitswurzeln, die in K enthalten sind,
- und D_K die Diskriminante (Welche Primzahlen verzweigen in K? D.h. $p\mathcal{O}_K = \mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_n^{k_n}$, wobei mind. ein $k_i > 1$, das passiert bei endlich vielen p)

sind.

Diese Definition und die Analogien zur Riemannschen Zetafunktion motivieren die *erweiterte Riemannsche Vermutung*:

Vermutung 2. *Sei K ein Zahlkörper, und ζ_K seine Dedekindsche Zetafunktion. Ist s eine Nullstelle von ζ_K und $0 < \Re(s) < 1$, so gilt schon $\Re(s) = \frac{1}{2}$.*

Für Funktionenkörper $K/\mathbb{F}_p(T)$ kann man eine ähnliche Definition machen. Hier definiert man die Zetafunktion

$$\zeta_K(s) = \sum_{\substack{f \\ \text{Primstelle}}} \frac{1}{N(f)^s}.$$

Man kann zeigen, dass die Zetafunktion eines Funktionenkörpers ζ_K eine Darstellung als gebrochenes Polynom hat:

$$\zeta_K(s) = \frac{L_K(u)}{(1-u)(1-qu)},$$

wo $q = p^n$ die Kardinalität des sogenannten Konstantenkörpers, und $u = q^{-s}$ ist. Die Nullstellen des Polynoms im Zähler $L_K(u)$ sind genau die Nullstellen der Zetafunktion. Für diese Nullstellen u von L_K gilt

$$|u| = q^{-1/2},$$

was äquivalent dazu ist, dass $\Re(s) = \frac{1}{2}$. Diese Aussage heißt auch die *Riemannsche Vermutung für Kurven*, und sie ist bewiesen.

Literatur

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, 1992.

Email address: huebner@math.uni-frankfurt.de

Robert Mayer Strasse 6-8, 60325 Frankfurt