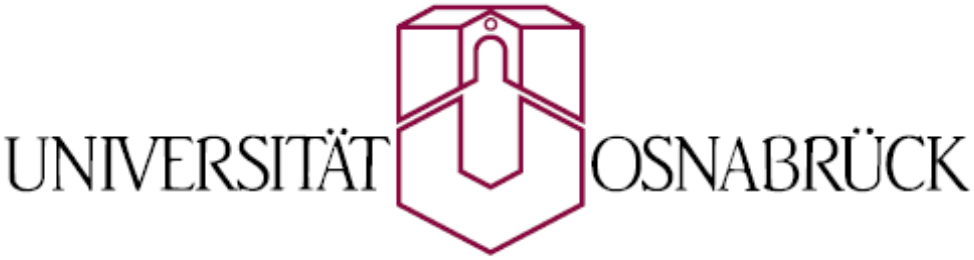

Fachbereich Mathematik / Informatik

Seminar zur Zahlentheorie

Kreisteilungsringe und Kreisteilungskörper

Napoleon Schwan

Betreuer: Prof. Dr. Holger Brenner
Kontakt: nschwan@uos.de

Osnabrück, den 20. April 2009

Inhaltsverzeichnis

Kapitel 1

Kreisteilungspolynome

1.1 Einleitung

Die Theorie der Kreisteilungsringe und -körper gründet sich auf die Teilung des Einheitskreises in n gleiche Abschnitte – oder was gleichbedeutend damit ist – die Konstruktion eines regulären n-Ecks auf dem Einheitskreis.
Eine Grundlage für diese algebraischen Strukturen (Kreisteilungsringe und -körper) ebnet das sogenannte Kreisteilungspolynom. Um dieses verstehen zu können, müssen wir mit der algebraischen Beschreibung des geometrischen Problems beginnen. Erst dann können wir zu den genannten Strukturen gelangen, welche wir hernach untersuchen wollen.

Die Punkte eines regelmäßigen n-Ecks, welche vom Ursprung den Abstand 1 haben, werden algebraisch durch die Gleichung

$$X^n - 1 = 0 \tag{1.1}$$

mit n $\in \mathbb{N}$[1] beschrieben. Diese Gleichung wollen wir die ***n-te Kreisteilungsgleichung*** nennen und deren Lösungen $\zeta_1, \ldots, \zeta_n$ die ***n-ten Einheitswurzeln*** .
Um den Einheitskreis S^1 als Bild einer Funktion f

$$\mathrm{f} : (0, 1] \to S^1 \tag{1.2}$$

darzustellen[2], wählen wir die Abbildungsvorschrift

$$t \longmapsto e^{2\pi i \cdot t} \quad t \in (0, 1]. \tag{1.3}$$

[1] Wir definieren $\mathbb{N}$ als: $\mathbb{N} := \{1, 2, \ldots\}$.

[2] Die Wahl des Definitionsbereichs von f ist reine Geschmackssache. Man könnte genauso gut das Intervall [0, 1) nehmen. Dabei sollte man jedoch berücksichtigen, dass der Index bei den n-ten Einheitswurzeln anders lauten muss, wie wir gleich sehen werden.

Wir betrachten nun nur noch solche Punkte auf dem Kreis, deren n-faches Produkt mit sich selbst 1 ergibt. Es gilt damit

$$(e^{2\pi i \cdot t})^n = 1 \tag{1.4}$$

mit $n \in \mathbb{N}$.
Für welches t ist die angegebene Gleichung erfüllt? – Dazu vereinfachen wir den Ausdruck zu

$$1 = (e^{2\pi i \cdot t})^n = e^{2n \cdot \pi i \cdot t}. \tag{1.5}$$

Wendet man die *Euler'sche Formel*

$$e^{it} = \cos\big(t\big) + i \cdot \sin(t) \tag{1.6}$$

an, so erhält man eine Darstellung der komplexen Exponentialfunktion in Sinus- und Cosinus-Funktion. Diese wiederum haben bekanntlich die Periode 2π. Folglich hat die komplexe Exponentialfunktion die Periode $2\pi i$.
Deshalb erhält man nur für ganzahlige Vielfache von $2\pi i$ die Zahl 1. Dadurch erhält man für t und den freien Parameter n die folgende Bedingung:

$$t \cdot n = k \Longleftrightarrow t = \frac{k}{n} \tag{1.7}$$

wobei $k \in \mathbb{Z}$. Da $t \in (0, 1]$ ist, beschränken wir k noch auf $k \geq 1$ und erhalten

$$t = \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}. \tag{1.8}$$

Schließlich ergibt sich

$$e^{\frac{2\pi i}{n} \cdot k}, \qquad 1 \leq k \leq n. \tag{1.9}$$

Und dies sind gerade die n-ten Einheitswurzeln $\zeta_1, \ldots, \zeta_n$ in der exponentiellen Darstellung. Es gilt[3]:

$$\zeta_k = e^{\frac{2\pi i}{n} \cdot k}, \qquad 1 \leq k \leq n. \tag{1.10}$$

Mit der *Euler'schen Formel* ergibt sich weiter

$$e^{\frac{2\pi i}{n} \cdot k} = \cos\left(\frac{2\pi}{n} \cdot k\right) + i \cdot \sin\left(\frac{2\pi}{n} \cdot k\right) \qquad für \qquad k = 1, \ldots, n. \tag{1.11}$$

Zur Darstellung dieser Lösungen wird – wie auch bei der Darstellung des Einheitskreises – die Gauß'sche Zahlenebene verwendet:

[3]Wie oben bemerkt, läuft bei anderer Wahl des Intervalles des Definitionsbereiches von f (nämlich [0, 1))der Index kann hier von 0 bis n - 1.

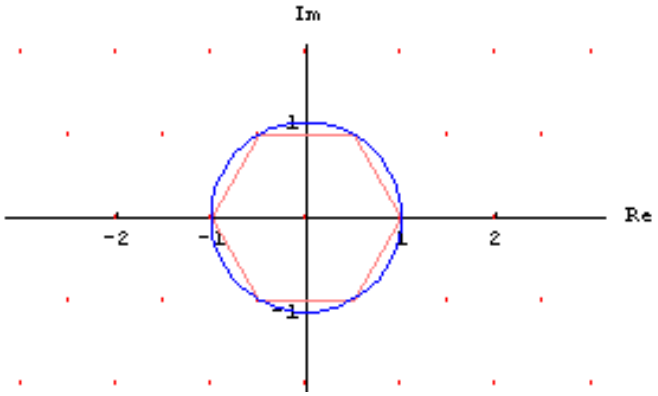

Abbildung 1.1: Das reguläre Sechseck

Der Realteil (Cosinusteil) spiegelt die x-Koordinate, der Imaginärteil (Sinusteil) die y-Koordinate des Punktes wider. Geometrisch entspricht dem Argument $\frac{2\pi}{n} \cdot k$ den im Bogenmaß gerechneten Winkel, welcher vom Punkte (1,0) entgegen dem Uhrzeigersinn verk-facht wird und zum jeweiligen nächsten Eckpunkt führt. Diese Punkte ergeben die Ecken des gesuchten regelmäßigen n-Eckes. Der Abstand dieser Punkte zum Ursprung errechnet sich durch

$$\sqrt{\cos^2\left(\frac{2\pi}{n} \cdot k\right) + \sin^2\left(\frac{2\pi}{n} \cdot k\right)} = \sqrt{1} = 1.$$

Damit liegen sämtliche Punkte auf dem Einheitskreis. Die Muster, denen diese regulären n-Ecke unterworfen sind, lassen sich mithilfe algebraischer Methoden beschreiben. Schließlich lehnen sich diese Darstellungen an denen uns bekannten Begriffen wie *Körpererweiterung*, *Minimalpolynom*, *Zahlbereiche* - und damit eng verbunden - den Begriff der *Diskriminante* an.

1.2 Das n-te Kreisteilungspolynom

Im Folgenden untersuchen wir die Nullstellen des Polynoms $X^n - 1$ genauer: Nach dem *Fundamentalsatz der Algebra* zerfällt $X^n - 1$ über dem Körper der komplexen Zahlen in Linearfaktoren:

$$X^n - 1 = (X - \zeta_1) \cdot (X - \zeta_2) \cdot \ldots \cdot (X - \zeta_n), \tag{1.12}$$

Diese Nullstellen sind paarweise voneinander verschieden, da

$$f' = n \cdot X^{n-1} = n \cdot \frac{X^n}{X} = n \cdot \frac{X^n - 1 + 1}{X} = \underbrace{n \cdot \frac{X^n - 1}{X}}_{0} + \underbrace{n \cdot \frac{1}{X}}_{\neq 0} \neq 0 \tag{1.13}$$

wobei diese Rechnung gewiss nur in char K $\neq$ n richtig ist.
Dieses Kriterium greift aus folgendem Grunde:

- Sei f ein von Null verschiedenes Polynom, welches eine n-fache komplexe Nullstelle, die wir a nennen, besitze. Wir wählen $f \in \mathbb{C}[X]$. f habe ohne Beschränkung der Allgemeinheit die Form:

  $$f = (X - a)^n \cdot g, \text{ wobei } \operatorname{grad}(g) < n < \operatorname{grad}(f).$$

  Dann ist

  $$\begin{aligned} f' &= n \cdot (X - a)^{n-1} \cdot g + (X - a)^n \cdot g' \\ &= \underbrace{(X - a)^{n-1}}_{0} \cdot (n \cdot g + (X - a) \cdot g') = 0 \end{aligned} \tag{1.14}$$

  weil a nach Voraussetzung Nullstelle von f ist.

Fasst man die Nullstellen $\zeta_1, \ldots, \zeta_n$ – also gerade diejenigen Punkte in der Gauß'schen Zahlenebene, welche den Kreis in n gleiche Abschnitte teilen – zu einer Menge zusammen, die wir mit $\mathcal{G}_n$ bezeichnen, so ist $\mathcal{G}_n$ eine abelsche Untergruppe von $\mathbb{C}^*$ bezüglich der Multiplikation, die sogar zyklisch ist.

Beweis:

- $(\mathcal{G}_n, \cdot, 1)$ ist eine *Gruppe*:
  - $\mathcal{G}_n$ **ist *assoziativ***:

    Seien

    $$\zeta_{k_j} = e^{\frac{2\pi i}{n} \cdot k_j} \tag{1.15}$$

wobei $1 \leq k_j \leq n$, $j = 1, 2, 3$ Nullstellen von $X^n - 1$[4].
Dann ist

$$\begin{aligned}(\zeta_{k_1} \cdot \zeta_{k_2}) \cdot \zeta_{k_3} &= e^{\frac{2\pi i}{n} \cdot k_1} \cdot e^{\frac{2\pi i}{n} \cdot k_2} \cdot e^{\frac{2\pi i}{n} \cdot k_3} \\ &= e^{\frac{2\pi i}{n} \cdot ((k_1+k_2)+k_3)} = e^{\frac{2\pi i}{n} \cdot (k_1+(k_2+k_3))} \\ &= \zeta_{k_1} \cdot (\zeta_{k_2} \cdot \zeta_{k_3}) \end{aligned} \tag{1.16}$$

– **$\mathcal{G}_n$ besitzt ein *neutrales Element***:

Offensichtlich ist

$$\zeta_n = e^{\frac{2\pi i}{n} \cdot n} = e^{2\pi i} = 1 \tag{1.17}$$

das neutrale Element von $\mathcal{G}_n$ bzgl. der Multiplikation.

– **Zu jedem beliebigem vorgebenen Element ζ_k existiert ein *inverses Element* in $\mathcal{G}_n$**:

Es ist

$$\begin{aligned}(\zeta_k)^{-1} &= (e^{\frac{2\pi i}{n} \cdot k})^{-1} = e^{\frac{2\pi i}{n} \cdot (-k)} \\ &= \cos\left(-\frac{2\pi}{n} \cdot k\right) + i \cdot \sin\left(-\frac{2\pi}{n} \cdot k\right) \end{aligned} \tag{1.18}$$

Da sowohl der *Cosinus* als auch der *Sinus* die Periode 2π besitzen, schreibt sich weiter

$$\cos\left(-\frac{2\pi k}{n} + \frac{2\pi n}{n}\right) + i \cdot \sin\left(-\frac{2\pi k}{n} + \frac{2\pi n}{n}\right) \tag{1.19}$$

bzw.

$$\cos\left(\frac{2\pi \cdot (n-k)}{n}\right) + i \cdot \sin\left(\frac{2\pi \cdot (n-k)}{n}\right) \tag{1.20}$$

und schließlich

$$e^{\frac{2\pi \cdot (n-k)}{n}} \cdot i = e^{\frac{2\pi i}{n} \cdot (n-k)} \tag{1.21}$$

Der Exponent der letzten Gleichung ist dabei stets positiv oder null, weil $1 \leq k \leq n$ ist. k ist höchstens so groß wie n: Dann ist der Exponent null. Weil n mindestens 1 ist, ist der Exponent mindestens null und damit nie negativ. Darum gilt $1 < n - k < n$

[4] Die Indizierung soll hierbei helfen mehrere Nullstellen von $X^n - 1$ bezeichnen zu können anstelle von nur ζ_k allein.

bzw. $0 \leq n-k \leq n-1$. Wegen der periodischen Eigenschaft der komplexen Exponentialfunktion - die Periodenlänge ist $2\pi i$ - besitzt $(\zeta_k)^{-1}$ dieselbe Form wie ζ_k. Deshalb gilt

$$(\zeta_k)^{-1} \in \mathcal{G}_n. \tag{1.22}$$

– $\mathcal{G}_n$ **ist unter der Multiplikation *abgeschlossen***:

Der Beweis der Abgeschlossenheit erfolgt in ähnlicher Weise. Es gilt

$$\zeta_{k_1} \cdot \zeta_{k_2} = e^{\frac{2\pi i}{n} \cdot k_1} \cdot e^{\frac{2\pi i}{n} \cdot k_2} = e^{\frac{2\pi i}{n} \cdot (k_1+k_2)}. \tag{1.23}$$

Da die komplexe Exponentialfunktion die Periode $2\pi i$ bzw. *Cosinus* und *Sinus* jeweils die Periode 2π besitzen gilt auch

$$e^{\frac{2\pi i}{n} \cdot (k_1+k_2)} = \cos\left(\frac{2\pi}{n} \cdot (k_1+k_2)\right) + i \cdot \sin\left(\frac{2\pi}{n} \cdot (k_1+k_2)\right). \tag{1.24}$$

Weiter schreibt sich dieser Ausdruck zu

$$\cos\left(\frac{2\pi k_1 + 2\pi k_2}{n}\right) + i \cdot \sin\left(\frac{2\pi k_1 + 2\pi k_2}{n}\right) \tag{1.25}$$

oder auch aufgrund der Periode 2π von *Cosinus* und *Sinus* zu

$$\cos\left(\frac{2\pi k_1 + 2\pi k_2 - 2\pi n}{n}\right) + i \cdot \sin\left(\frac{2\pi k_1 + 2\pi k_2 - 2\pi n}{n}\right). \tag{1.26}$$

Ausklammern von 2π in den Argumenten von *Cosinus* und *Sinus* ergibt

$$\cos\left(\frac{2\pi \cdot (k_1 + k_2 - n)}{n}\right) + i \cdot \sin\left(\frac{2\pi \cdot (k_1 + k_2 - n)}{n}\right). \tag{1.27}$$

Schließlich ergibt wiederum die *Euler'sche Formel* die e-Darstellung

$$e^{\frac{2\pi i}{n} \cdot (k_1+k_2-n)}. \tag{1.28}$$

Da bei den n-ten Einheitswurzeln ζ_{k_1} und ζ_{k_2} die Indizes den Beschränkungen $1 \leq k_1 \leq n$ bzw. $1 \leq k_2 \leq n$ unterliegen, also höchstens als Summe $2n$ ergeben können, ergibt dieser Ausdruck insgesamt

$$e^{\frac{2\pi i}{n} \cdot (2n-n)}. \tag{1.29}$$

Jetzt erhält man: $e^{2\pi i} = 1$. Sind k_1 und k_2 am kleinsten, dann sind beide jeweils gleich 1. Daraus ergibt sich

$$e^{\frac{2\pi i}{n}\cdot(2-n)}. \tag{1.30}$$

Jetzt wird das Argument der exponentiellen Darstellung – wie vorhin auch – unter dem *Cosinus* dem *Sinus* eingehend untersucht. Und der genannte Ausdruck schreibt sich zu

$$e^{\frac{2\pi i}{n}\cdot(2-n)} = \cos\left(\frac{2\pi\cdot(2-n)}{n}\right) + i\cdot\sin\left(\frac{2\pi\cdot(2-n)}{n}\right) \tag{1.31}$$

Dies wiederum ist gleichwertig zu

$$\cos\left(\frac{4\pi-2\pi n}{n}\right) + i\cdot\sin\left(\frac{4\pi-2\pi n}{n}\right) \tag{1.32}$$

bzw.

$$\cos\left(\frac{4\pi}{n}\right) + i\cdot\sin\left(\frac{4\pi}{n}\right) = e^{\frac{4\pi i}{n}} = e^{\frac{2\pi i}{n}\cdot 2} = \zeta_2 \in \mathcal{G}_n. \tag{1.33}$$

Kurz: Ist also $k_1 + k_2 \leq n$ hat $\zeta_{k_1}\cdot\zeta_{k_2}$ minimale Potenz. Ist aber $k_1 + k_2 > n$ lässt sich die Potenz aufgrund der Periodizität der komplexen Exponentialfunktion auf eine kleinere Potenz transformieren, derart, dass $k_1+k_2 \leq n$ ist und das Produkt $\zeta_{k_1}\cdot\zeta_{k_2}$ wieder eine n-te Einheitswurzel ist.

- $\mathcal{G}_n$ **ist *abelsch***:
  Mulipliziert man zwei Elemente aus $\mathcal{G}_n$, so ergibt sich nachstehende Gleichung

  $$\zeta_{k_1}\cdot\zeta_{k_2} = e^{\frac{2\pi i}{n}\cdot k_1}\cdot e^{\frac{2\pi i}{n}\cdot k_2} = e^{\frac{2\pi i}{n}\cdot(k_1+k_2)} = e^{\frac{2\pi i}{n}\cdot(k_2+k_1)} = \zeta_{k_2}\cdot\zeta_{k_1} \tag{1.34}$$

  Damit ist $\mathcal{G}_n$ bezüglich der Multiplikation abelsch.

- $\mathcal{G}_n$ **ist sogar *zyklisch***:
  Denn es lässt sich (ohne Beschränkung der Allgemeinheit) stets $\zeta_1 = e^{\frac{2\pi i}{n}}$ als Erzeuger der Gruppe wählen, weil der Exponent jede n-te Einheitswurzel durchläuft. □

Elemente, welche die Eigenschaft besitzen, jedes Element der Gruppe $\mathcal{G}_n$ (multiplikativ ausgedrückt) mit jeder Potenz kleiner gleich n alle Elemente

von $\mathcal{G}_n$ zu durchlaufen (also sog. Erzeuger der Gruppe $\mathcal{G}_n$ sind), erhalten einen gesonderten Namen:

Definition (*primitive n-te Einheitswurzeln*):
Erzeuger der Gruppe $\mathcal{G}_n$ heißen ***primitive n-te Einheitswurzeln***.

Die Variante des vorangehenden Beweises geht von der e-Darstellung der Lösungen der n-ten Kreisteilungsgleichung aus und untersucht dort charakteristische Eigenschaften der komplexen Exponentialfunktion. Unabhängig von der speziellen Darstellung der Lösungen der n-ten Kreisteilungsgleichung, führt der folgende Beweis zum gleichen Ergebnis:

Variante des Beweises:

- $\mathcal{G}_n$ **ist *abgeschlossen* unter der Multiplikation**:

  Seien ζ_{k_1} und ζ_{k_2} n-te Einheitswurzeln, also Elemente mit der Eigenschaft:
  $\zeta_{k_1}^n - 1 = 0$ bzw. $\zeta_{k_1}^n = 1$ und genauso $\zeta_{k_2}^n = 1$. Dann folgt

  $$\zeta_{k_1}^n \cdot \zeta_{k_2}^n = (\zeta_{k_1} \cdot \zeta_{k_2})^n = 1 \cdot 1 = 1. \tag{1.35}$$

  Hier jedoch wird die Kommutativität vorausgesetzt, da bei diesem Potenzgsetz eine Umordnung der Faktoren vorgenommen wird. Die Kommutativität von $\mathcal{G}_n$ folgt aber daraus, dass jede endliche Untergruppe einer kommutativen Gruppe stets wieder kommutativ ist. Um dies zu zeigen, brauchen wir nur noch ein neutrales Element in der Gruppe zu finden und wir müssen außerdem noch zeigen , dass es in der Gruppe zu jedem Element ein multiplikatives Inverses gibt:

- $\mathcal{G}_n$ **hat ein *neutrales Element* der Multiplikation**:
  und dies ist offensichtlich die 1.

- **Zu jedem beliebigem vorgebenen Element ζ_k existiert ein *inverses Element* in $\mathcal{G}_n$**:

  Sei wieder ζ_k eine n-te Einheitswurzel, also $\zeta_k^n = 1$. Dann ist

  $$(\zeta_k^{-1})^n = (\zeta_k^n)^{-1} = 1^{-1} = 1 \tag{1.36}$$

  aufgrund der kommutativen Eigenschaft von $\mathcal{G}_n$.
  Damit ist $\mathcal{G}_n$ eine Untergruppe von $\mathbb{C}^*$. Die zyklische Eigenschaft von $\mathcal{G}_n$ lässt sich wie folgt ableiten: Sei $\zeta_{k_1} \in \mathcal{G}_n$ und $(\zeta_{k_1})^n = 1$. Wenn für ein

$d \in \mathbb{N}$ mit $d|n$, aber $d \neq n$ ebenfalls $(\zeta_{k_1})^d = 1$ gilt, dann ist das Element nicht Erzeuger der Gruppe. Zu Zeigen ist also, dass es mindestens ein Element gibt, für welches n-fach potenziert 1 ergibt, aber keinen echten Teiler d gibt, für welches es d-fach potenziert 1 ergibt. Dieses Element muss es aber aufgrund der Ordnung der Gruppe, die ja n beträgt, geben. Damit gibt es mindestens einen Erzeuger der Gruppe $\mathcal{G}_n$ und damit ist die Gruppe sogar zyklisch. □

Im Folgenden werden die Lösungen der n-ten Kreisteilungsgleichung $X^n - 1 = 0$ für $n = 4$ berechnet.

Beispiel (*Lösungen der vierten Kreisteilungsgleichung*):

- Sei
$$X^4 - 1 = 0 \tag{1.37}$$
die vierte Kreisteilungsgleichung.
Ihre Nullstellen sind 1, -1, i, -i, denn
$$\zeta_1 = e^{\frac{2\pi i}{4}} = \underbrace{\cos\left(\frac{\pi}{2}\right)}_{0} + i \cdot \underbrace{\sin\left(\frac{\pi}{2}\right)}_{1} = i. \tag{1.38}$$
Gleichermaßen ergibt sich
$$\zeta_2 = e^{\frac{2\pi i}{4} \cdot 2} = \underbrace{\cos(\pi)}_{-1} + i \cdot \underbrace{\sin(\pi)}_{0} = -1 \tag{1.39}$$
und auch
$$\zeta_3 = e^{\frac{2\pi i}{4} \cdot 3} = \underbrace{\cos\left(\frac{3\pi}{2}\right)}_{0} + i \cdot \underbrace{\sin\left(\frac{3\pi}{2}\right)}_{-1} = -i. \tag{1.40}$$
Schließlich ist
$$\zeta_4 = e^{\frac{2\pi i}{4} \cdot 4} = e^{2\pi i} = 1. \tag{1.41}$$
Also ist
$$\mathcal{G}_4 = \{1, -1, i, \text{-}i\} \tag{1.42}$$
Ein Erzeuger von $\mathcal{G}_4$ ist beispielweise $e^{\frac{2\pi i}{4}} = i$. Dies lässt sich zum einen aus der der e-Darstellung ableiten, zum anderen auch durch
$$i^1 = i;\ i^2 = -1;\ i^3 = -i;\ i^4 = 1$$

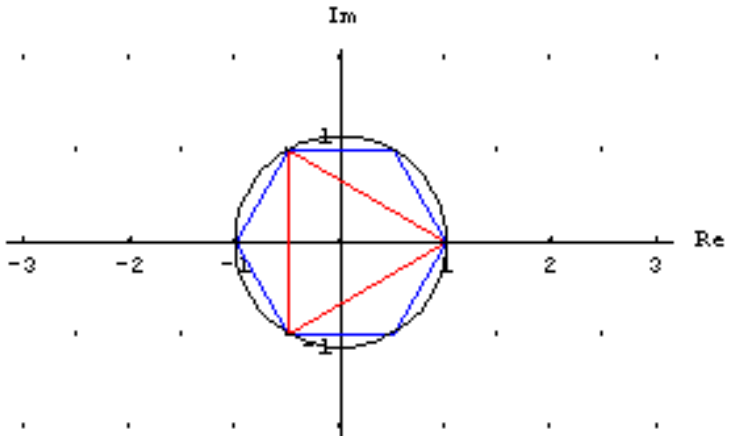

Abbildung 1.2: Das reguläre Drei- und Sechseck

und $|\mathcal{G}_4| = 4$. Das Inverse von $e^{\frac{2\pi i}{4}} = i$ lässt sich auch wie folgt berechnen:

$$(e^{\frac{2\pi i}{4}})^{-1} = e^{\frac{2\pi\cdot(4-1)}{4}\cdot i} = e^{\frac{2\pi i}{4}\cdot 3} \overset{(1.21)}{=} -i \tag{1.43}$$

$-i$ ist auch primitiv, denn

$$(-i)^1 = -i;\ (-i)^2 = -1;\ (-i)^3 = i;\ (-i)^4 = 1.$$

Die primitiven n-ten Einheitswurzeln der Gruppe $\mathcal{G}_n$ spielen eine bedeutende Rolle für die weiteren Überlegungen:
Die primitiven n-ten Einheitswurzeln haben bekanntlich die höchste Ordnung in $\mathcal{G}_n$: Geometrisch lassen sich die primitiven n-ten Einheitswurzeln auch so beschreiben: Haben die primitiven n-ten Einheitswurzeln die Ordnung n und ist d ein Teiler von n, dann beschreiben sie diejenigen Punkte, welche bei Konstruktion des regelmäßigen n-Eckes neuzuerrechnenden Punkte, welche das reguläre d-Eck jedoch nicht besitzt. Sei $m > n$ und gelte auch $n|m$, dann ist vollkommen klar, dass die n-ten Einheitswurzeln unter m nicht mehr primitiv sein können, da sie schon die Ordnung n besitzen. So etwa bei dem regulären Drei- und Sechseck (vgl Abbildung 1.2). Die primitiven sechsten Einheitswurzeln sind die an der y-Achse gespiegelten Punkte des regulären Dreiecks, aber nur von der linken Seite. (-1, 0) bzw. -1 ist in $\mathcal{G}_6$ nicht primitiv, da $(-1)^2 = 1$ und $2|6$. (-1, 0) ist schon Punkt des regelmäßigen Zweiecks.
Die Anzahl der primitiven Elemente der Gruppe $\mathcal{G}_6$ ist – wie man der Skizze entnehmen kann – 2. Diese Anzahl lässt sich mit einfachen Mitteln berechnen, die in diesem Abschnitt behandelt werden. Man könnte auch sagen, dass die primitiven Elemente in gewisser Weise auch die kennzeichnenden Punkte

des regulären n-Ecks beschreiben. Aber man muss auch beachten, dass beispielsweise auch das reguläre $2n$-Eck dieselben Punkte wie das reguläre n-Eck hat und diese Aussage daher für Primzahl-Ecke immer richtig ist, allgemein aber nicht und daher immer relativ zum Teiler betrachtet werden muss.
Um also geometrische Eigenschaften algebraisch beschreiben zu können, werden wir uns im Folgenden eingehend mit den primitiven Elementen beschäftigen. Bisher wissen wir nur, dass die Lösungen der n-ten Kreisteilungsgleichung $X^n - 1 = 0$ eine zyklische (und damit abelsche) Gruppe bilden.
Diese Gruppe $\mathcal{G}_n$ lässt sich sogar auf eine erstaunlich leichte Art und Weise noch genauer darstellen:
Sie besitzt gerade die Form des Restklassenringes eingeschränkt auf die Addition (weil sonst keine Gruppe vorliegt). Das Zählen der primitiven Elemente, welche durch die e-Darstellung zunächst erschwert vorkommt, wird somit deutlich vereinfacht. Und diesen geschilderten Sachverhalt gibt der nachstehende Satz wieder:

Satz 1.1 ($\mathcal{G}_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$):
Jede endliche zyklische Gruppe ist isomorph zu ($\mathbb{Z}/n\mathbb{Z}$, +), wenn n die Ordnung der Gruppe bezeichnet.

Beweis:

- Sei $\mathcal{G}_n$ eine endliche zyklische Gruppe.
  Zu Zeigen: Die Gruppe ist isomorph zu $(\mathbb{Z}/n\mathbb{Z}, +)$. Mit anderen Worten: Es existiert eine bijektive homomorphe Abbildung – die wir kurz ϕ nennen – zwischen den Gruppen. In Zeichen:

$$(\mathbb{Z}/n\mathbb{Z}, +) \cong (\mathcal{G}_n, \cdot) \Longleftrightarrow \exists\, \phi : (\mathbb{Z}/n\mathbb{Z}, +) \longrightarrow (\mathcal{G}_n, \cdot) \tag{1.44}$$

  Um diese Aussage nachvollziehen zu können, betrachten wir die Gestalt der Elemente aus den Gruppen genauer:
  Da $\mathcal{G}_n$ nach Voraussetzung zyklisch ist, lässt sich die Gruppe auch schreiben als

$$\mathcal{G}_n = \langle \zeta_1 \rangle = \{\zeta_1, \ldots, \zeta_n\}\,, \tag{1.45}$$

  wobei ζ_1 den Erzeuger der Gruppe darstellt. Das bedeutet, dass sowohl die Ordnung der Gruppe als auch die Ordnung der Erzeugers übereinstimmen müssen, weil ein Erzeuger einer Gruppe stets die Ordnung der Gruppe besitzen muss.
  Die Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ bestehe aus den Elementen

$$(\mathbb{Z}/n\mathbb{Z}, +) = \{z_1, \ldots, z_n\} \tag{1.46}$$

Wir definieren die Abbildung $\phi : (\mathbb{Z}/n\mathbb{Z}, +) \longrightarrow (\mathcal{G}_n, \cdot)$ durch

$$z_i \longmapsto \zeta_i \quad \text{für } i = 1, \ldots, n$$

Jetzt untersuchen wir die Abbildung ϕ, die Gestalt der Elemente ist bekannt:
Es gilt

$$\phi(z_1 + z_2) = \zeta_1^{z_1+z_2} = \zeta_1^{z_1} \cdot \zeta_1^{z_2} = \phi(z_1) \cdot \phi(z_2). \tag{1.47}$$

Zusätzlich ist auch

$$\phi(0) = \zeta_1^0 = 1. \tag{1.48}$$

Das neutrale Element von $(\mathbb{Z}/n\mathbb{Z}, +)$ wird folglich auf das neutrale Element von $\mathcal{G}_n$ abgebildet. Deshalb liegt eine homomorphe Abbildung zwischen den Gruppen vor. Es muss also nur noch gezeigt werden, dass die Abbildung sowohl *injektiv* als auch *surjektiv* ist:

- **Injektivität der Abbildung**:
  Die Injektivität von ϕ ist gleichbedeutend damit, dass

  $$\ker(\phi) = \{z_i \in (\mathbb{Z}/n\mathbb{Z}, +), \;\; i = 1, \ldots, n \mid \phi(z_i) = 1\} = \{0\}$$

  gilt. Weil ζ_1 Erzeuger von $\mathcal{G}_n$ ist, muss die Ordnung von ζ_1 gerade n sein. Für kleinere n, also $d < n$ und $d|n$, gilt $\zeta_1^d \neq 1$. Damit gibt es genau ein Element aus $(\mathbb{Z}/n\mathbb{Z}, +)$, nämlich das neutrale Element dieser Gruppe, welches diese Gleichung erfüllt. Damit ist die Abbildung ϕ injektiv.

- **Surjektivität der Abbildung**:
  Hier muss gezeigt werden, dass jedes Element der Gruppe $\mathcal{G}_n$ als Bild auftaucht. Da sowohl $\mathcal{G}_n$ als auch $(\mathbb{Z}/n\mathbb{Z}, +)$ n Elemente hat, kann die Abbildung surjektiv konstruiert werden [5] und zwar so:

  $$\begin{aligned} z_1 &\longmapsto \zeta_1 \\ z_2 &\longmapsto \zeta_2 \\ &\vdots \\ z_n &\longmapsto \zeta_n \end{aligned}$$

  wobei hier $z_1 = \overline{1} \in \mathbb{Z}/n\mathbb{Z}$ auf den Erzeuger der Gruppe $\mathcal{G}_n$ abgebildet wird.
  Auf diese Weise taucht jedes Element aus $\mathcal{G}_n$ als Bild der Abbildung ϕ auf. Es folgt: ϕ ist surjektiv.

[5] Dieses Argument könnte man auch bei der Injektivität einbringen!

ϕ ist also injektiv und surjektiv, damit bijektiv. Es liegt folglich eine bijektive homomorphe Abbildung zwischen den Gruppen vor, was die Aussage des Satzes ist. □

Mit dem nachfolgenden Lehrsatz lässt sich die Anzahl der primitiven Elemente von $\mathcal{G}_n \cong \mathbb{Z}/n\mathbb{Z}$ ganz leicht berechnen:

Satz 1.2 (*Anzahl der primitiven Elemente*):
Sei n eine natürliche Zahl mit der Primfaktorzerlegung

$$n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k} \tag{1.49}$$

Dann besitzt $\mathbb{Z}/n\mathbb{Z}$

$$\varphi(n) = \varphi(p_1^{r_1}) \cdot \ldots \cdot \varphi(p_k^{r_k}) \tag{1.50}$$

primitive Elemente.
Dabei drückt $\varphi(n)$ *aus, wie viele Zahlen zwischen 1 und n - 1 teilerfremd zu n sind. Es ist*:

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*| \tag{1.51}$$

Diese Funktion φ *heißt die* ***Euler'sche*** φ ***- Funktion****.*

Beweis:

- Zunächst zeigen wir, dass die zu n teilerfremden Zahlen die Einheiten in $\mathbb{Z}/\mathrm{n}\mathbb{Z}$ sind.
  Sei dazu $a \in \mathbb{Z}/\mathrm{n}\mathbb{Z}$, dann ist

$$(a \cdot b + \underbrace{n \cdot d}_{0}) \bmod n = 1 \bmod n \tag{1.52}$$

  mit $b, d \in \mathbb{Z}/\mathrm{n}\mathbb{Z}$. Also gilt

$$(a \cdot b) \bmod n = 1 \bmod n. \tag{1.53}$$

  Damit Gleichheit gilt, darf weder a noch b ein Nullteiler in $\mathbb{Z}/\mathrm{n}\mathbb{Z}$ sein. Deshalb müssen sowohl a als auch b teilerfremd zu n sein, um die Gleichung zu erfüllen.
  Wie man aus der Gleichung sieht, handelt es sich bei beiden elementen um Einheiten, da sie multipliziert das neutrale Element der Multiplikation in $\mathbb{Z}/\mathrm{n}\mathbb{Z}$ ergeben.
  Als Nächstes wollen wir die Anzahl der Elemente von $\mathbb{Z}/\mathrm{n}\mathbb{Z}$ bestimmen:

Dazu ist es notwendig folgende Eigenschaft der Euler'schen φ - Funktion zu Zeigen:

$$\varphi(n) = \varphi(p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}) = \varphi(p_1^{r_1}) \cdot \ldots \cdot \varphi(p_k^{r_k}) \tag{1.54}$$

Weil die Euler'sche φ - Funktion – auch anders formuliert – die Anzahl der Einheiten des Restklassenringes $\mathbb{Z}/\mathrm{n}\mathbb{Z}$ angibt, ist die im Satz formulierte Aussage dasselbe wie

$$(\mathbb{Z}/(n))^* \cong (\mathbb{Z}/(p_1^{r_1}))^* \times \ldots \times (\mathbb{Z}/(p_k^{r_k}))^*. \tag{1.55}$$

Diese Behauptung ist damit eine Folge aus dem *Chinesischen Restsatz*, da eine Einheit in $\mathbb{Z}/\mathrm{n}\mathbb{Z}$ genau dann vorliegt, wenn auch eine Einheit in dem Produktring auf der rechten Seite vorliegt. Damit ist die Euler'sche φ - Funktion mutliplikativ.
Den Wert von $\varphi(n)$ lässt sich konkret ausrechnen. Dazu bestimmen wir die primitiven Elemente von $\mathbb{Z}/(p_1^{r_1})$ und übertragen das Ergebnis auf die übrigen Restklassenringe.
Da die primitiven Elemente zu p_1 teilerfremd sind, gibt es in $\mathbb{Z}/(p_1^{r_1})$ $p_1^{r_1} - p_1^{r_1-1}$ pimitive Elemente. Insgesamt ergibt sich

$$\varphi(n) = (p_1^{r_1} - p_1^{r_1-1}) \cdot \ldots \cdot (p_k^{r_k} - p_k^{r_k-1}) \tag{1.56}$$

Es lassen sich also mithilfe der Euler'schen φ - Funktion die primitiven Elemente mit der Primfaktorzerlegung einer gegebenen natürlichen Zahl genau bestimmen. □

Diese beiden Sätze ergeben jetzt zusammen:

1. $\mathcal{G}_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$
2. Die Anzahl der primitiven Elemente von $\mathcal{G}_n$ beträgt $\varphi(n)$.

Wie man durch die Lösungen der Kreisteilungsgleichung an alle Punkte des regelmäßigen n-Ecks kommt, so sollen die Nullstellen des folgenden Polynoms alle primitiven Elemente von $\mathcal{G}_n$ enthalten.

Definition (*n-tes Kreisteilungspolynom*):
Seien $\zeta_{k_1}, \ldots, \zeta_{k_{\varphi(n)}}$ die primitiven Elemente von $\mathcal{G}_n$.
Das Polynom

$$\Phi_n(X) := (X - \zeta_{k_1}) \cdot \ldots \cdot (X - \zeta_{k_{\varphi(n)}}) \overset{\substack{Satz \\ 1.2}}{=} \prod_{\substack{1 \le k \le n \\ ggT(k,n)=1}} (X - \zeta_k) \tag{1.57}$$

heißt ***n-tes Kreisteilungspolynom***.

Die Lösungen der Gleichung

$$\Phi_n(X) = 0 \tag{1.58}$$

ergeben dann die primitiven Elemente. Weil das Polynom Produkt von $\varphi(n)$ Linearfaktoren ist, ist der Grad des n-ten Kreisteilungspolynomes ebenfalls $\varphi(n)$.

Beispiel (*Berechnung eines Kreisteilungspolynomes*):

- Sei wieder $X^4 - 1 = 0$ die vierte Kreisteilungsgleichung. Zu bestimmen sind die primitiven Elemente von $\mathcal{G}_4$:
  In $\mathcal{G}_4$ gibt es
  $$\varphi(4) = \varphi(2^2) = 2^2 - 2^1 = 2 \tag{1.59}$$
  primitive Elemente, nämlich i und $-i$. 1 und -1 sind keine primitiven Elemente, da
  $$1^1 = 1;\ 1^2 = 1 \text{ und } (-1)^1 = -1;\ (-1)^2 = 1$$
  und $|\mathcal{G}_4| = 4 \neq 2$.
  Dann berechnet sich $\Phi_4(X)$ aus:
  $$\Phi_4(X) = (X - i) \cdot (X + i) = X^2 - i^2 = X^2 + 1. \tag{1.60}$$

Wie die Rechnungen zeigen, ist es sehr ungemütlich, die n-ten Kreisteilungspolynome auf diese Weise auszurechnen, weil zunächst alle primitiven Elemente von $\mathcal{G}_n$ bestimmt werden müssen.
Der folgende Satz gibt zwei verschiedene Ansätze zur Berechnung n-ter Kreisteilungspolynome an:

Satz 1.3 (*Berechnung n-ter Kreisteilungspolynome*):

- ***Rekursives Bestimmen des n-ten Kreisteilungspolynomes:***

  Es gilt
  $$X^n - 1 = \prod_{\substack{d \in \mathbb{N} \\ d|n}} \Phi_d(X) \tag{1.61}$$

  In Worten: *Die n-te Kreisteilungsgleichung entspricht dem Produkt d-ter Kreisteilungspolynome ($d \leq n$), deren Grad den Grad der n-ten Kreisteilungsgleichung echt und unecht teilt. Unter unechtem Teilen wollen wir die Teile d = 1 und d = n verstehen.*

- ***Direktes Bestimmen des n-ten Kreisteilungspolynomes:***

  Umgekehrt errechnet sich das n-te Kreisteilungspolynom direkt aus der Gleichung:

$$\Phi_n(X) = \prod_{\substack{d \in \mathbb{N} \\ d|n}} (X^d - 1)^{\mu(\frac{n}{d})} \tag{1.62}$$

  wobei μ eine Funktion darstellt, welche angewandt auf eine natürliche Zahl

$$n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}, \text{ mit } k \text{ paarweisen verschiedenen Primzahlen,}$$

  die folgenden Eigenschaften hat:

$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1 \\ (-1)^k & \text{falls } r_i = 1, \text{ für } i = 1, \ldots, k \\ 0 & \text{sonst} \end{cases}$$

  *Diese Funktion μ ist die sogenannte **Möbiusfunktion**.*

Beweis:

- Das Polynom $X^n - 1$ besitzt n verschiedene Nullstellen, welche die Form

$$\zeta_k = e^{\frac{2\pi i}{n} \cdot k}, \text{ mit } 1 \leq k \leq n$$

  haben und in der Menge $\mathcal{G}_n$ zusammengefasst werden, die bzgl. der Multiplikation eine zyklische Gruppe bilden.
  Jedes Element besitzt in dieser Gruppe eine gewisse Ordnung. Ist die Ordnung gleich n, dann handelt es sich um primitive n-te Einheitswurzeln.
  Diese sind die Nullstellen des n-ten Kreisteilungspolynoms $\Phi_n(X)$, welche als Faktor im Produkt auf der rechten Seite der Gleichung stehen.
  Der Rest der Elemente von $\mathcal{G}_n$ muss nach dem *Satz von Lagrange* als Ordnung ein Teiler von n sein.
  Diese Teiler wollen wir vereinfachend mit d bezeichnen. Wie die primitiven n-ten Einheitswurzeln Nullstellen des n-ten Kreisteilungspolynoms sind, so liefern die d-ten Kreisteilungspolynome gleich Null gesetzt die primitiven d-ten Einheitswurzeln.
  Insgesamt ergibt sich also das Produkt der d-ten Kreisteilungspolynome, wobei d ein Teiler von n ist, was gerade die erste Aussage des Satzes war.

- Diese Aussage beweist man mit der Umkehrfunktion der Möbiusfunktion, worauf wir aber verzichten wollen. □

Beispiele (*Bestimmung einiger Kreisteilungspolynome mit* ***Satz 1.3***):

- Gesucht ist wieder das 4-te Kreisteilungspolynom.
  Nach der ersten Aussage des vorangehenden Satzes gilt die Beziehung:

$$X^4 - 1 = \prod_{\substack{d \in \mathbb{N} \\ d|4}} \Phi_d(X) = \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_4(X) \tag{1.63}$$

  Folglich ist:

$$\Phi_4(X) = \frac{X^4 - 1}{\Phi_1(X) \cdot \Phi_2(X)} \tag{1.64}$$

  Dann ist

$$\Phi_1(X) = X - 1, \tag{1.65}$$

  weil

$$X - 1 = \prod_{\substack{d \in \mathbb{N} \\ d|1}} \Phi_d(X) = \Phi_1(X) \tag{1.66}$$

  und schließlich

$$\Phi_2(X) = X + 1, \tag{1.67}$$

  weil

$$X^2 - 1 = \prod_{\substack{d \in \mathbb{N} \\ d|2}} \Phi_d(X) = \Phi_1(X) \cdot \Phi_2(X) \tag{1.68}$$

  Also

$$\Phi_2(X) = \frac{X^2 - 1}{\Phi_1(X)} = \frac{X^2 - 1}{X - 1} = X + 1. \tag{1.69}$$

  Zusammen ergibt sich dann

$$\Phi_4(X) = \frac{X^4 - 1}{\Phi_1(X) \cdot \Phi_2(X)} = \frac{X^4 - 1}{(X - 1) \cdot (X + 1)} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1. \tag{1.70}$$

  Mit der zweiten Aussage des Satzes berechnet sich das 4-te Kreisteilungspolynom wie folgt:

$$\begin{aligned} \Phi_4(X) &= \prod_{\substack{d \in \mathbb{N} \\ d|4}} (X^d - 1)^{\mu(4/d)} \\ &= (X - 1)^{\mu(4/1)} \cdot (X^2 - 1)^{\mu(4/2)} \cdot (X^4 - 1)^{\mu(4/4)} \\ &= (X - 1)^{\mu(4)} \cdot (X^2 - 1)^{\mu(2)} \cdot (X^4 - 1)^{\mu(1)}. \end{aligned} \tag{1.71}$$

Da

$$\mu(4) = \mu(2^2) = 0 \tag{1.72}$$

und

$$\mu(2) = \mu(2^1) = (-1)^1 = -1, \tag{1.73}$$

weil nur eine Primzahl vorkommt (k = 1), sowie

$$\mu(1) = \mu(2^2) = 1 \tag{1.74}$$

gilt, erhält man als 4-tes Kreisteilungspolynom

$$\Phi_4(X) = (X-1)^0 \cdot (X^2-1)^{-1} \cdot (X^4-1)^1 = \frac{X^4-1}{X^2-1} = X^2+1. \tag{1.75}$$

Der Vorteil dieser Formel ist, dass zur Berechnung nicht die d-ten Kreisteilungspolynome mit $d|n$ berechnet werden müssen, sondern die Struktur der Polynome bereits durch X^d-1 vorgegeben ist und in Abhängigkeit von der natürlichen Zahl die Potenzen dieser Polynome noch zu bestimmen sind.

- Als zweites wollen wir Φ_{10} bestimmen. Man rechnet:

$$X^{10}-1 = \prod_{\substack{d\in\mathbb{N}\\ d|10}} \Phi_d(X) = \Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_5(X)\cdot\Phi_{10}(X) \tag{1.76}$$

bzw.

$$\Phi_{10}(X) = \frac{X^{10}-1}{\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_5(X)} \tag{1.77}$$

Φ_1 und Φ_2 sind aus obiger Rechnung schon bekannt. Es fehlt nur noch $\Phi_5(X)$, also:

$$X^5-1 = \prod_{\substack{d\in\mathbb{N}\\ d|5}} \Phi_d(X) = \Phi_1(X)\cdot\Phi_5(X) \tag{1.78}$$

Darum ist

$$\Phi_5(X) = \frac{X^5-1}{\Phi_1(X)} = \frac{X^5-1}{X-1} = X^4+X^3+X^2+X+1. \tag{1.79}$$

Insgesamt erhält man durch Polynomdivision

$$\Phi_{10}(X) = X^4-X^3+X^2-X+1. \tag{1.80}$$

Mit der direkten Methode erhält man

$$\begin{aligned}\Phi_{10}(X) &= \prod_{\substack{d\in\mathbb{N}\\ d|10}} (X^d-1)^{\mu(10/d)} \qquad (1.81)\\ &= (X-1)^{\mu(10)}\cdot(X^2-1)^{\mu(5)}\cdot(X^5-1)^{\mu(2)}\cdot(X^{10}-1)^{\mu(1)}.\end{aligned}$$

Nach Definition der Möbiusfunktion ist

$$\mu(1)=1. \qquad (1.82)$$

Weiter ist

$$\mu(2^1)=(-1)^1=-1 \qquad (1.83)$$

und genauso

$$\mu(5^1)=(-1)^1=-1. \qquad (1.84)$$

Schließlich ergibt

$$\mu(10)=\mu(2\cdot 5)=(-1)^2=1, \qquad (1.85)$$

weil nun zwei Primfaktoren der Potenz 1 vorkommen. Oben eingesetzt ergibt dann

$$\begin{aligned}\Phi_{10}(X) &= (X-1)^1\cdot(X^2-1)^{-1}\cdot(X^5-1)^{-1}\cdot(X^{10}-1)^1\\ &= \frac{(X-1)\cdot(X^{10}-1)}{(X^2-1)\cdot(X^5-1)} \qquad (1.86)\end{aligned}$$

Dieser Ausdruck lässt sich mit Division von $X-1$ durch X^2-1 vereinfachen, sodass insgesamt Folgendes herauskommt:

$$\begin{aligned}\Phi_{10}(X) &= \frac{X^{10}-1}{(X+1)\cdot(X^5-1)}=\frac{X^{10}-1}{X^6+X^5-X-1}\\ &= X^4-X^3+X^2-X+1. \qquad (1.87)\end{aligned}$$

Die Nullstellen von $\Phi_{10}(X)$ sind sehr mühsam zu berechnen und die Nullstellen von $\Phi_{11}(X)$ nach dem *Satz von Abel* mithilfe von Wurzelausdrücken nicht mehr darstellbar. Deshalb ist bei hohem Grad von $\Phi_n(X)$ die e-Darstellung äußerst hilfreich. Dadurch lassen sich zumindest die Punktkoordinaten auf dem Einheitskreis mithilfe der *Euler'schen Formel* näherungsweise bestimmen.

- Sei nun allgemein p eine Primzahl. Dann gilt

$$\Phi_p(X)=X^{p-1}+X^{p-2}+\ldots+X^2+X+1. \qquad (1.88)$$

Denn es ist:

$$X^p - 1 = \prod_{\substack{d \in \mathbb{N} \\ d|p}} \Phi_d(X) = \Phi_1(X) \cdot \Phi_p(X) \tag{1.89}$$

oder auch

$$\Phi_p(X) = \frac{X^p - 1}{\Phi_1(X)} = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + X^2 + X + 1. \tag{1.90}$$

Wiederum ergibt sich mit der zweiten Methode

$$\begin{aligned} \Phi_p(X) &= \prod_{\substack{d \in \mathbb{N} \\ d|p}} (X^d - 1)^{\mu(p/d)} = (X-1)^{\mu(p)} \cdot (X^{10} - 1)^{\mu(1)} = \frac{X^p - 1}{X - 1} \\ &= X^{p-1} + X^{p-2} + \ldots + X^2 + X + 1. \end{aligned} \tag{1.91}$$

Aus dem obigen Satz lässt sich aber noch mehr entnehmen:
Die p-ten Kreisteilungspolymome, wobei p eine Primzahl ist, besitzen gegenüber den n-ten Kreisteilungspolynomen, wobei $p|n$ und $n \in \mathbb{N}$, verhältnismäßig die meisten Nullstellen, wenn man die Anzahl der Nullstellen der Kreisteilungspolynome mit den Lösungen der Kreisteilungsgleichung vergleicht. Um diese Beobachtung geometrisch zu deuten, betrachten wir ein festes n und nehmen der Einfachheit halber an, dass n nur einen Primteiler p besitzt. Dann gilt mit dem obigen Lehrsatz die Gleichung

$$X^n - 1 = \Phi_1(X) \cdot \Phi_p(X) \cdot \Phi_n(X) \tag{1.92}$$

Da die regulären n-Ecke nur x-Achsen symmetrisch sind, wenn n ungerade ist und x-Achsen und y-Achsen symmetrisch sind, wenn n gerade ist, werden die Punkte des regulären n-Ecks maßgeblich von den Punkten des regulären p-Ecks bestimmt. Die primitiven Elemente von $\mathcal{G}_n$ sind als Punkte in der Gauß'schen Zahlenebenen entweder Spiegelungen an der x-Achse oder Spiegelungen an der y-Achse von den Punkten des regulären p-Ecks. Wir werden im letzten Abschnitt des Zweiten Kapitels schließlich zeigen, dass die regulären p-Ecke die Gitterstruktur im Koordinatensystem bestimmen und werden anhand von geometrischen Anschauungen diese Tatsachen untermauern.

Allen n-ten Kreisteilungspolynomen ist aber grundweg gemein, dass ihre Koeffizienten ganzzahlig sind[6]. Und dies besagt auch der nachstehende

[6]Diese Tatsache hat u.a. eine sehr große Bedeutung für die Beschreibung der Gitterstrukturen.

Satz 1.4:
Es ist

$$\Phi_n(X) \in \mathbb{Z}[X] \quad \forall n \in \mathbb{N}. \tag{1.93}$$

Beweis:
Vollständige Induktion nach n.

- **Induktionsverankerung**:
  Es sei $n = 1$. Dann ist $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.

- **Induktionsschritt**:
  $n - 1 \rightarrow n$: Sei also die Behauptung richtig für alle $n - 1$. Zeige, dass die Behauptung auch für n gültig ist.
  Nach Definition des n-ten Kreisteilungspolynoms $\Phi_n(X)$ ist das Polynom stets normiert, da der Koeffizient der höchsten Potenz immer 1 ist. Aufgrund der Induktionsvoraussetzung ist das Polynom

$$P := \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X) \tag{1.94}$$

  normiert mit Koeffizienten aus $\mathbb{Z}$.
  Nach dem vorangehenden Satz **(Satz 1.3)** zerfällt die n-te Kreisteilungsgleichung $X^n - 1$ in d-te Kreisteilungspolynome, wobei d die Zahl n echt und unecht teilt. Diese Aussage ist gleichbedeutend mit der Formulierung, dass die Division von $X^n - 1$ und dem gerade definierten Polynom P ohne Rest mit $\Phi_n(X)$ aufgeht. Da sowohl $X^n - 1$ als auch P ganzzahlige Koeffizienten besitzen und P auch noch normiert ist, muss $\Phi_n(X)$ ebenfalls ganzzahlige Koeffizienten besitzen. Also gilt die Aussage auch für n. □

Die n-ten Kreisteilungspolynome sind also ganzzahlig. Aber die Annahme, dass die von Null verschiedenen Koeffizienten der n-ten Kreisteilungspolynome nur 1 oder -1 sind, wie man aus den ersten Kreisteilungspolynomen vermuten könnte, lässt sich im Allgemeinen nicht bestätigen; im Gegenteil: Durch ein Gegenbeispiel zeigt sich, dass die Annahme falsch ist.
So errechnet sich für das 105-te Kreisteilungspolynom mit eine der beiden Aussagen von **Satz 1.3** (*Rekursives oder direktes Bestimmen des n-ten Kreis-*

teilungspolynomes):

$$\begin{aligned}\Phi_{105}(X) &= X^{48}+X^{47}+X^{46}-X^{43}-X^{42}-2\cdot X^{41}-X^{40}-X^{39}\\ &\quad +X^{36}+X^{35}+X^{34}+X^{33}+X^{32}+X^{31}-X^{28}-X^{26}-X^{24}\\ &\quad -X^{22}-X^{20}+X^{17}+X^{16}+X^{15}+X^{14}+X^{13}+X^{12}-X^{9}\\ &\quad -X^{8}-2\cdot X^{7}-X^{6}-X^{5}+X^{2}+X+1. \qquad (1.95)\end{aligned}$$

Polynome mit großem n kaann man leichter mit dem Computer berechnen. Ich habe hier zur Berechnung dieses Polynomes das Programm *Mathematica* benutzt. Mit dem Befehl `Cyclotomic[105, X]` wird das Polynom in der Unbestimmten X ausgegeben. Auf der Seite

`http://mathworld.wolfram.com/CyclotomicPolynomial.html`

kann man alles Grundlegende zu den Kreisteilungspolynom nachlesen und mithilfe von Animationen und Bilder nachvollziehen.

Damit wissen wir, dass die n-te Kreisteilungsgleichung gleich dem Produkt d-ter Kreisteilungspolynome – mit $1 \leq d \leq n$ und $d|n$ – ist, welche außerdem ganzzahlig sind. Der folgende Satz besagt, dass diese Faktoren sogar irreduzibel über $\mathbb{Q}$ sind. Es ergibt sich also insgesamt, dass die n-te Kreisteilungsgleichung eine Darstellung in irreduzible Faktoren über $\mathbb{Q}$ besitzt.

Satz 1.5:

- *Das n-te Kreisteilungspolynom $\Phi_n(X)$ ist für jedes $n \in \mathbb{N}$ irreduzibel über $\mathbb{Q}$.*
- *Speziell gilt:*
  1. *$\Phi_n(X)$ ist Minimalpolynom der primitiven Elemente.*
  2. *Der Grad von Φ_n ist immer eine gerade natürliche Zahl für $n \geq 3$.*

Beweis:

- Um die Irreduzibilität von $\Phi_n(X)$ zu zeigen, genügt es – nach dem Lemma von Gauß – zu Zeigen, dass das normierte Polynom $\Phi_n(X)$ irreduzibel über $\mathbb{Z}[X]$ ist.
  Sei also $h \in \mathbb{Z}[X]$ ein irreduzibler Faktor von $\Phi_n(X)$. Dann gibt es ein $f \in \mathbb{Z}[X]$ derart, dass
  $$\Phi_n(X) = h \cdot f, \qquad (1.96)$$
  wobei sowohl f als auch h aufgrund des n-ten Kreisteilungspolynomes normiert sind.

Sei ζ_k eine primitive n-te Einheitswurzel, die ohne Beschränkung der Allgemeinheit Nullstelle des Polynomes h ist. Sei weiter p eine zu n teilerfremde Primzahl.
Aufgrund der Teilerfremdheit zwischen p und n gilt, dass ζ_k^p wiederum eine primitive n-te Einheitswurzel ist und damit auch Nullstelle von Φ_n ist. Damit ist ζ_k^p entweder Nullstelle von h oder Nullstelle von f. Ist ζ_k^p Nullstelle von f, so folgt daraus, dass umgekehrt für ζ_k gelten muss, dass ζ_k Nullstelle von $f(X^p)$ sein muss.
Folglich wäre h ein Teiler von $f(X^p)$ in $\mathbb{Q}[X]$. Dann gäbe es ein Polynom $k \in \mathbb{Q}[X]$, sodass

$$f(X^p) = h \cdot k \tag{1.97}$$

Da $\Phi_n(X) \in \mathbb{Z}[X]$ ist auch $f \in \mathbb{Z}[X]$ und auch $f(X^p)$. Da die Division durch $h \in \mathbb{Z}[X]$ aufgeht, ist auch $k \in \mathbb{Z}[X]$. Um Näheres über den Teiler k zu erfahren, betrachten wir die Restklassenabbildung

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \tag{1.98}$$

und wenden sie auf $f(X^p)$ hin an, so erhält man mithilfe des Frobenius-Automorphismus die Beziehung:

$$\pi(f(X^p)) = (\pi(f))(X^p) = \pi(f^p) = \pi(f)^p. \tag{1.99}$$

Weiterhin gilt dann

$$\pi(f(X^p)) = \pi(h \cdot k) = \pi(h) \cdot \pi(k), \tag{1.100}$$

weil $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist.
Sei d echter Teiler von $\pi(f)$ in $\mathbb{Z}/p\mathbb{Z}$, dann ist d ebenso echter Teiler von $\pi(g)$.
Das würde aber heißen, dass

$$\Phi_n(X) = \pi(k) \cdot \pi(g) \cdot \pi(h) \tag{1.101}$$

durch d^2 teilbar ist, also das Polynom $X^n - 1$ eine doppelte Nullstelle besäße, was wir aber am Anfang dieses Abschnittes widerlegt haben. Widerspruch!
Deshalb gilt

$$f = k = h = \Phi_n(X). \tag{1.102}$$

- *Zu den Spezialfällen*:

  1. Diese Aussage wurde schon beim Beweis der Irreduzibilität mitgezeigt.

2. Wenn n gerade ist besitzt die n-te Kreisteilungsgleichung $X^n - 1 = 0$ die beiden rationalen Lösungen 1 und -1. Wenn n ungerade ist besitzt die n-te Kreisteilungsgleichung $X^n - 1 = 0$ nur die rationale Lösungen 1. Die übrigen Nullstellen sind komplex. Weil zu jeder komplexen Nullstelle auch ihre konjugiert komplexe eine Lösung von $\Phi_n(X) = 0$ ist, ist, falls n gerade ist, $\varphi(n)$ wiederum gerade und wird gerade, falls n ungerade ist. □

Kapitel 2

Kreisteilungsringe und Kreisteilungskörper

2.1 Der n-te Kreisteilungskörper

Da nach **Satz 1.5** die n-te Kreisteilungsgleichung einerseits über $\mathbb{Q}$ nicht vollständig in Linearfaktoren zerfällt, andererseits es jedoch über dem Körper der komplexen Zahlen geschieht, suchen wir den kleinsten Zerfällungskörper der n-ten Kreisteilungsgleichung. Diesen Körper benennen wir wie folgt:

Definition (*n-ter Kreisteilungskörper*):
Sei $X^n - 1 \in \mathbb{Q}[X]$ mit $n \in \mathbb{N}$. Dann heißt der kleinste Körper, über dem das
gegebene Polynom vollständig in Linearfaktoren zerfällt, der ***n-te Kreisteilungskörper*** und wird mit $\mathcal{K}_n$ bezeichnet.

Weil die Nullstellen der n-ten Kreisteilungsgleichung eine zyklische Gruppe, die wir mit $\mathcal{G}_n$ bezeichnet haben, bilden, nimmt man einen Erzeuger davon, etwa ζ_1, und fügt dieses Element und all seine Linearkombination zu $\mathbb{Q}$ hinzu. Also hat $\mathcal{K}_n$ stets die Gestalt $\mathbb{Q}(\zeta_1)$, weil das primitive Element ζ_1 beim Potenzieren jedes Element der Gruppe $\mathcal{G}_n$ durchläuft.
Da das Minimalpolynom $\Phi_n(X)$, also das n-te Kreisteilungspolynom, den Grad $\varphi(n)$ besitzt, ist der Grad der Körpererweiterung:

$$[\mathbb{Q}(\zeta_1) : \mathbb{Q}] = \varphi(n).$$

Beispiele (*Berechnung einiger n-ter Kreisteilungskörper*):

- Der erste und zweite Kreisteilungskörper ist $\mathbb{Q}$ selbst, da sowohl die erste Kreisteilungsgleichung

  $$X - 1$$

  als auch die zweite Kreisteilungsgleichung

  $$X^2 - 1 = (X - 1) \cdot (X + 1)$$

  über $\mathbb{Q}$ vollständig in Linearfaktoren zerfällt.

- Der dritte Kreisteilungskörper ist $\mathcal{K}_3 = \mathbb{Q}(\frac{-1+\sqrt{-3}}{2}) = \mathbb{Q}(\sqrt{-3})$, weil für die dritte Kreisteilungsgleichung gilt

  $$X^3 - 1 \overset{\substack{Satz \\ 1.3}}{=} \Phi_1(X) \cdot \Phi_3(X) = (X - 1) \cdot (X^2 + X + 1).$$

  Nach **Satz 1.5** sind die n-ten Kreisteilungspolynome für alle $n \in \mathbb{N}$ irreduzibel über $\mathbb{Q}$. Damit liegt eine Darstellung der 3-ten Kreisteilungsgleichung in irreduzible Faktoren vor. Berechnung der Nullstellen von $\Phi_3(X)$ ergibt

  $$\Phi_3(X) = X^2 + X + 1 = 0 \tag{2.1}$$

  bzw.

  $$X^2 + X + \frac{1}{4} + \frac{3}{4} = \left(X + \frac{1}{2}\right)^2 + \frac{3}{4} = 0 \tag{2.2}$$

  und letztlich

  $$\left(X + \frac{1}{2}\right)^2 = -\frac{3}{4} \Leftrightarrow X + \frac{1}{2} = \pm\frac{\sqrt{-3}}{2} \Leftrightarrow X = \frac{-1 \pm \sqrt{-3}}{2} \tag{2.3}$$

  Da $\sqrt{-3} \notin \mathbb{Q}$ adjungieren wir dieses Element zu $\mathbb{Q}$ und erhalten dadurch $\mathbb{Q}(\sqrt{-3})$.

- Der vierte Kreisteilungskörper $\mathcal{K}_4$ ist $\mathbb{Q}(i)$, da

  $$X^4 - 1 \overset{\substack{Satz \\ 1.3}}{=} \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_4(X) = (X - 1) \cdot (X + 1) \cdot (X^2 + 1)$$

  und bekanntlich besitzt $X^2 + 1$ die Nullstellen i und -i. Beide besitzen die Ordnung 4 in $\mathcal{G}_4$, sind folglich primitive Elemente.

- Der sechste Kreisteilungskörper $\mathcal{K}_6$ ist derselbe wie $\mathcal{K}_3$, er lautet nämlich: $\mathbb{Q}(\frac{1+\sqrt{-3}}{2}) = \mathbb{Q}(\sqrt{-3})$, weil

$$\begin{aligned} X^6 - 1 &\overset{\substack{Satz \\ 1.3}}{=} \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_3(X) \cdot \Phi_6(X) \\ &= (X-1) \cdot (X+1) \cdot (X^2 + X + 1) \\ &\quad \cdot (X^2 - X + 1) \end{aligned} \tag{2.4}$$

  Man berechnet:

$$X^2 - X + \frac{1}{4} + \frac{3}{4} = \left(X - \frac{1}{2}\right)^2 + \frac{3}{4} = 0 \tag{2.5}$$

  bzw.

$$\left(X - \frac{1}{2}\right)^2 = -\frac{3}{4} \Leftrightarrow X - \frac{1}{2} = \pm\frac{\sqrt{-3}}{2} \Leftrightarrow X = \frac{1 \pm \sqrt{-3}}{2} \tag{2.6}$$

  Diese beiden Nullstellen sind die primitiven Elemente. Dagegen sind die Nullstellen von $\Phi_3(X)$ keine primitiven Elmente, da sie die Ordnung 3 besitzen. Aber gerade weil sich diese Nullstellen von den primitiven Elementen nur um eine Einheit (nämlich -1) unterscheiden, sind die beiden Kreisteilungskörper $\mathcal{K}_3$ und $\mathcal{K}_6$ identisch:
  Somit ist

$$\left(1, \sqrt{-3}\right) \tag{2.7}$$

  $\mathbb{Q} - Basis$ von $\mathcal{K}_6$ und durch die Linearkombination

$$\frac{1}{2} \cdot 1 + \left(-\frac{1}{2}\right) \cdot \sqrt{-3} \tag{2.8}$$

  erhält man die Nullstelle $\frac{1-\sqrt{-3}}{2}$ von $\Phi_6(X)$. Die andere Nullstelle ist die komplex konjugierte, welche man wiederum durch

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \sqrt{-3} \tag{2.9}$$

  errechnet.

- Ähnlich verhält es sich bei dem achten Kreisteilungskörper $\mathcal{K}_8$. Es gilt:

$$\begin{aligned} X^8 - 1 &\overset{\substack{Satz \\ 1.3}}{=} \Phi_1(X) \cdot \Phi_2(X) \cdot \Phi_4(X) \cdot \Phi_8(X) \\ &= (X-1) \cdot (X+1) \cdot (X^2+1) \cdot (X^4+1) \end{aligned} \tag{2.10}$$

Die Nullstellen von $X^4 + 1$ sind

$$X^4 + 1 = (X^2 + i) \cdot (X^2 - i) \Longrightarrow X^2 + i = 0 \quad \vee \quad X^2 - i = 0 \tag{2.11}$$

also

$$X = \pm i\sqrt{i} \quad \text{oder} \quad X = \pm\sqrt{i} \tag{2.12}$$

Folglich ist $\mathcal{K}_8 = \mathbb{Q}(i, \sqrt{i})$. Dann bilden die Elemente $(1, i, \sqrt{i}, i \cdot \sqrt{i})$ eine $\mathbb{Q}$-Basis und der Grad der Körpererweiterung beträgt 4, das Minimalpolynom hat also den Grad 4, was mit dem Grad des errechneten 8-ten Kreisteilungspolynom

$$\Phi_8(X) = X^4 + 1 \tag{2.13}$$

übereinstimmt.

Auffallend ist, dass beim n-ten Kreisteilungskörper im Vergleich zu seinem Primzahlteiler p stets neue Wurzelausdrücke hinzutreten, die zum Ursprungskörper hinzutreten, d.h. die Primzahlen bestimmen maßgeblich die Struktur des Körpers, mit anderen Worten: die p-ten Kreisteilungskörper sind ein Unterkörper der n-ten Kreisteilungskörper
Dieses Ergebnis ist eine unmittelbare Folge aus dem ersten Aussage von **Satz 1.3**, weil ja schließlich die n-ten Kreisteilungspolynome aufgrund ihrer Nullstellen die Gestalt des n-ten Kreisteilungskörpers bestimmen. Wiederum lassen sich n-te Kreisteilungspolynome durch gewisse Formeln auch aus anderen gewinnen. So gilt beispielsweise auch die Gleichheit

$$\Phi_{2m}(X) = \Phi_m(-X) \tag{2.14}$$

mit ungeradem m und $m \neq 1$, welche wir aber hier nicht zeigen wollen.

2.2 Der n-te Kreisteilungsring

Bevor wir zum Begriff des Kreisteilungsringes kommen, wollen wir noch einige wichtige Begriffe einführen. Einer von ihnen ist der Begriff des ***Zahlbereichs***. Mit diesem wird folgende Situation kurz beschrieben:
Sei R ein Integritätsbereich und K der Quotientenkörper von R. Sei weiter $K \subseteq L$ eine endliche Körpererweiterung. All diejenigen Elemente aus dem Erweiterungskörper L, die Nullstelle eines normierten Polynomes mit Koeffizienten aus R sind (also $f \in R[X]$ und Lösung der Gleichung f = 0 sind) bilden einen kommutativen Ring, der sogar ein Integritätsbereich ist den wir kurz mit S bezeichnen. Wir wollen im denjenigen Falle S einen ***Zahlbereich*** (oder auch einen ***Ganzheitsring***) von R nennen, wenn K = Q gilt[1]. Als Diagramm erhalten wir:

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ K & \longrightarrow & L \end{array}$$

Wie sich jedes Element des Erweiterungskörpers L als K - Basis formulieren lässt, so lässt sich auch auf Ringebene jedes Element dieser Ringerweiterung S als R - Basis darstellen.
Hier beschränken wir uns mit Ringerweiterungen von $R = \mathbb{Z}$ und mit Körperweiterungen von $K = \mathbb{Q}$. Das Aussehen der Körpererweiterungen von $\mathbb{Q}$ bzgl. des n-ten Kreisteilungskörpers haben wir im letzten Abschnitt erörtert. Jetzt untersuchen wir die Gestalt der Ringerweiterung von $\mathbb{Z}$, also die Gestalt des Ringes S. Es ergibt sich also folgendes Diagramm

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & S = ? \\ \downarrow & & \downarrow \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}(\zeta_{k_n}) \end{array}$$

wobei ζ_{k_n} eine primitive n-te Einheitswurzel darstellt mit $n \in \mathbb{N}$ und $1 \leq k_n \leq n$.
Lässt sich außerdem jedes Element bei einer Ringerweiterung $R \subseteq S$, wie wir sie oben beschrieben haben, als Linearkombination von Elementen aus S und Koeffizienten aus R eindeutig darstellen, so nennen wir dies eine ***Ganzheitsbasis von*** S ***über*** R.
Im Falle, dass $R = \mathbb{Z}$ und $S = \mathbb{Z}[i]$ gilt, erhält man als $\mathbb{Z}$-Basis $(1, i)$.
Der bisher im Diagramm mit S bezeichnete Ring erhält einen gesonderten

[1] Diese Einschränkung müssen wir vornehmen, weil wir sonst falsche Aussagen erhalten würden.

Namen:

Definition (*n-ter Kreisteilungsring*):
Der Ganzheitsring im n-ten Kreisteilungskörper heißt der ***n-te Kreisteilungsring*** und wird mit $\mathcal{R}_n$ bezeichnet.

Eine unveränderliche Größe eines kommutativen Ringes ist die sogenannte ***Diskriminante*** . Die Diskriminante des quadratischen Polynoms X^2+pX+q mit $p, q \in \mathbb{R}$ ist bekanntlich ein Maß dafür, ob die Gleichung $X^2+pX+q=0$ über dem Körper der reellen Zahlen $\mathbb{R}$ eine, keine oder zwei Lösungen besitzt. Es ist

$$\begin{aligned} X^2 + p \cdot X + q &= 0 \\ \iff X^2 + p \cdot X &= -q \\ \iff X^2 + p \cdot X + \frac{p^2}{4} &= q - \frac{p^2}{4} \\ \iff \left(X + \frac{p}{2}\right)^2 &= q - \frac{p^2}{4} \\ \iff \left(X + \frac{p}{2}\right)^2 &= \frac{4q - p^2}{4} \\ \iff X + \frac{p}{2} &= \pm\sqrt{\frac{4q - p^2}{4}} \end{aligned} \tag{2.15}$$

Dann ist die Diskriminante des Polynomes bekanntlich $4q - p^2$, denn nach diesem Ausdruck richtet sich, ob das Polynom eine, keine oder zwei Lösungen über dem Körper der reellen Zahlen besitzt: Ist $4q - p^2 < 0$, so besitzt die Gleichung keine reelle Lösung, ist $4q - p^2 = 0$, so besitzt die Gleichung genau eine Lösung und gilt $4q - p^2 > 0$, so besitzt sie genau zwei Lösungen.
Um den Begriff der Diskriminante auf ein Polynom und später auf einen Zahlbereich zu übertragen, betrachten wir die Nullstellen des gegebenen Polynoms. Es wird sich herausstellen, dass aus den Nullstellen des Polynoms die Diskriminante errechnet werden kann.
Die Nullstellen lauten

$$X_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{4q - p^2}{4}}. \tag{2.16}$$

Jetzt subtrahieren wir die Nullstellen voneinander und erhalten

$$\begin{aligned} -\frac{p}{2}+\sqrt{\frac{4q-p^2}{4}}-\left(-\frac{p}{2}-\sqrt{\frac{4q-p^2}{4}}\right) &= -\frac{p}{2}+\sqrt{\frac{4q-p^2}{4}}+\frac{p}{2}+\sqrt{\frac{4q-p^2}{4}} \\ &= \sqrt{\frac{4q-p^2}{4}}+\sqrt{\frac{4q-p^2}{4}} \\ &= \sqrt{4q-p^2} \end{aligned} \tag{2.17}$$

Um die Diskriminante zu erhalten, muss nur noch quadriert werden. Im Allgemeinen lautet die Formel für Polynome n-ten Grades wie folgt:

Definition (*Diskriminante eines Polynomes*) :
Sei

$$f=\prod_{i=1}^{n}(X-\alpha_i) \tag{2.18}$$

ein Polynom vom Grad n.
Dann wird die ***Diskriminante des Polynoms*** f definiert durch

$$\Delta(f):=\prod_{i<k}(\alpha_k-\alpha_i)^2. \tag{2.19}$$

Dies ist offensichtlich dasselbe wie

$$(-1)^{\frac{1}{2}\cdot n\cdot(n-1)}\prod_{i=1}^{n}f'(\alpha_i) \tag{2.20}$$

wobei

$$f'=\sum_{i=1}^{n}\prod_{k\neq i}(X-\alpha_k). \tag{2.21}$$

die formale Ableitung (durch Anwendung der Kettenregel) bezeichnet. Diese Gleichheit werden wir später noch benötigen!
Durch diese Größe können auch Zahlbereiche beschrieben: Ist $f\in\mathbb{Z}[X]$ und zusätzlich irreduzibel über $\mathbb{Z}[X]$ und damit auch über $\mathbb{Z}[X]$, so wird durch die Gleichung $f=0$ eine Ringerweiterung von $\mathbb{Z}$ beschrieben. Im allgemeineren Fall sieht dies so aus:
Seien R und S kommutative Ringe mit $R\subseteq S$. Ist $f\in R[X]$ und irreduzibel über $R[X]$, so heißt

$$\Delta(S):=\Delta(f) \tag{2.22}$$

die ***Diskriminante des Zahlbereichs S***.
Um also die Diskriminante eines Zahlbereichs S zu erhalten, fordern wir zusätzlich, dass die Nullstellen des Polynomes f nur Elemente aus S ergeben und außerdem $f \in R[X]$ gilt.
Beispielsweise wird durch die Gleichung

$$\mathbb{Z}[X] \ni X^2 + 1 = 0 \tag{2.23}$$

die Ringerweiterung

$$\mathbb{Z}[X]/(X^2 + 1) \cong \mathbb{Z}[i] \tag{2.24}$$

ausgedrückt, denn die Lösung der Gleichung $X^2 + 1 = 0$ ergibt $X = \pm i \notin \mathbb{Z}$. Durch Substitution von $X + 1$ in X erhält man

$$X^2 + 2X + 2 = 0, \tag{2.25}$$

worauf man das Eisenstein'sche Kriterium mit $p = 2$ anwenden kann und das Polynom $X^2 + 1$ irreduzibel über $\mathbb{Z}[X]$ und damit auch irreduzibel über dem Quotientenring $\mathbb{Q}[X]$ ist. Also ist $\mathbb{Z}[i]$ ein Zahlbereich.
Schließlich verallgemeinern wir noch einen wichtigen Begriff, nämlich den der Norm. Bekanntlich ist

$$N(i) = i \cdot (-i) = -1 \in \mathbb{Z} \tag{2.26}$$

oder

$$N(a + bi) = (a + bi) \cdot (a - bi) = a^2 + b^2 \in \mathbb{Z}, \tag{2.27}$$

wenn $a, b \in \mathbb{Z}$. Aber was machen wir mit $i\sqrt{i} \notin \mathbb{Z}[i]$?

$$i\sqrt{i} \cdot (-i\sqrt{i}) = i \neq N(i\sqrt{i}) \in \mathbb{Z} \tag{2.28}$$

Die bisherige Beschreibung der Norm als Multiplikation von den Zahlen $a+bi$ und $a - bi$ mit $a, b \in \mathbb{Z}$ reicht also nur für Körper- bzw. Ringerweiterungen vom Grad 2 aus. Für unsere Verwendung der Norm ist es aber schwierig eine einheitliche Definition der Norm anzugeben, da wir uns sonst in eine Kette von Beweisen von Äquivalenzen verstricken würden, nur um die Eigenschaften der Norm vollständig darzulegen. Das wollen wir dem Leser auf keinen Fall zumuten. Deswegen listen wir im Folgenden die Eigenschaften der Norm auf, um auf diese Weise eine Art Übersicht für die Beschreibung des Begriffes ***Norm*** angeben zu können, die wir in dem nachstehenden Beweis es **Satzes 2.1** zur Beschreibung der sogenannten Kreisteilungsringe alle benötigen werden.

Eigenschaften der Norm :

Sei $R \subseteq S$ eine Ringerweiterung vom Grad n, wobei R und S kommutative Ringe bezeichnen.
Dann versteht man unter der ***Norm N eines Elementes*** $a \in S$ eine Abbildung

$$N : S \longrightarrow R \tag{2.29}$$

welche folgende Eigenschaften besitzt:

- Sei $n \in \mathbb{N}$. Dann ist der konstante Term des Minimalpolynomes f des Elementes a vom Grad n gerade die Norm von a.

  - **Beispiel**:
    Das Minimalpolynom zu $i \in \mathbb{Z}[i]$ über $\mathbb{Q}$ lautet bekanntlich X^2+1. Der konstante Term ist hier 1. Dann ist $N(i) = 1$.
    Mit derselben Methode kann man $N(1 - i\sqrt{i})$ bestimmen. Man rechnet:

$$\begin{aligned} X &= 1 - i\sqrt{i} \\ (X-1)^2 &= (-i\sqrt{i})^2 = -1 \cdot i = -i \\ (X-1)^4 &= -1 \\ X^4 - 4X^3 + 6X^2 - 4X + 2 &= 0 \end{aligned}$$

    Durch Anwendung des Eisenstein'sche Kriterium mit $p = 2$ erhalten wir, dass es sich hierbei tatsächlich um das Minimalpolynom von $1 - i$ handelt.
    Es folgt, dass $N(1 - i\sqrt{i}) = 2$ gilt.

- Die Norm eines Elementes $a \in S$ ist das Produkt ihrer Konjugierten.

  - **Beispiel**:
    Die zu i konjugierte Zahl ist $-i$. Damit ist $N(i) = i \cdot (-i) = 1$.
    Jetzt können wir auch die Norm von $i\sqrt{i}$ berechnen! Es ist

$$N(i\sqrt{i}) = i\sqrt{i} \cdot (-i\sqrt{i}) \cdot \sqrt{i} \cdot (-\sqrt{i}) = 1.$$

    Die Konjugierten von $i\sqrt{i}$ haben dann ebenfalls die Norm 1.

- Sei $b \in R$ und $[S : R] = n$, wobei $n \in \mathbb{N}$. Dann ist $N(b) = b^n$.

  - **Beispiel**:
    Sei $R = \mathbb{Z}$ und $S = \mathbb{Z}[i]$. Dann ist $[\mathbb{Z}[i] : \mathbb{Z}] = 2$, also ist $N(9) = 9^2 = 81$.

Die verallgemeinerten Eigenschaften der Norm sind veträglich mit den bisherigen Auffassungen!

Mit diesen Mitteln können wir den folgenden Satz, welche die einfache Struktur der Kreisteilungsringe beschreibt, leichter beweisen:

Satz 2.1 (*Gestalt und Diskriminante des n-ten Kreisteilungsringes*):

- *Sei ζ_{k_n} eine primitive n-te Einheitswurzel, wobei $n \in \mathbb{N}$ und $1 \leq k_n \leq n$. Dann ist $\mathbb{Z}[\zeta_{k_n}]$ der Ring der ganzen Zahlen im n-ten Kreisteilungskörper.*

- *Ihre Diskriminante bestimmt sich durch*

$$\Delta(\mathbb{Z}[\zeta_{k_n}]) = \prod_{i=1}^{k} \Delta(\mathbb{Z}[\zeta_{k_{q_i}}])^{\varphi(\frac{n}{q_i})} \tag{2.30}$$

  mit der kanonischen Primfaktorzerlegung $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ und $q := p^r$ sowie

$$\Delta(\mathbb{Z}[\zeta_{k_q}]) = (-1)^{\frac{1}{2}\cdot\varphi(q)} \cdot q^{\varphi(q)} \cdot p^{-\frac{q}{p}}. \tag{2.31}$$

Beweis[2]:

- Der Beweis lässt sich in zwei Hauptkomponenten unterteilen:
  In der ersten beweisen wir die obige Aussage für Primzahlpotenzen und in der zweiten für eine beliebige natürliche Zahl, welche Produkt von Primzahlpotenzen ist.

  1. **Primzahlpotenzen**:
     Zur leichteren Notation schreiben wir

$$q := p^r \text{ mit } r > 1.$$

     Sei also ζ_{k_q} eine primitive q -te Einheitswurzel. Das Minimalpolynom zu einer primitiven q-ten Einheitswurzel ist – nach **Satz 1.5** – das q-te Kreisteilungspolynom. Dieses errechnet sich durch die Gleichung:

$$\Phi_q(X) \overset{\substack{Satz \\ 1.3}}{=} \prod_{\substack{d|q \\ d\in\mathbb{N}}} (X^d - 1)^{\mu\left(\frac{q}{d}\right)} = \frac{X^q - 1}{X^{p^{r-1}} - 1}, \tag{2.32}$$

[2]Dieser Beweis orientiert sich an der Darstellung Jürgen Neukirch *Algebraische Zahlentheorie* [3]

weil beim Teiler $d = p^{r-1}$ der Exponent

$$\mu\left(\frac{p^r}{p^{r-1}}\right) = \mu(p^1) = (-1)^1 = -1 \tag{2.33}$$

steht.
Bei den kleineren Teilern, deren Exponenten jeweils um 1 kleiner sind als die vorherigen ist der Quotient zwischen q und d weder 1 noch ist eines der Exponenten von p gleich 1.
Folglich sind deren Exponenten Null und müssen nicht berücksichtigt werden. Damit ist

$$\Phi_q(X) = X^{p^{r-1}\cdot(r-1)} + \ldots + X^{p^{r-1}} + 1. \tag{2.34}$$

Seien $\zeta_{k_1}, \ldots, \zeta_{k_{\varphi(q)}}$ die zueinander komplex - konjugierten Zahlen. Dann schreibt sich das q-te Kreisteilungspolynom – durch Anwendung der Definition des n-ten Kreisteilungspolynomes auf q – auch zu

$$\Phi_q(X) = \prod_{i=1}^{\varphi(q)} (X - \zeta_{k_i}). \tag{2.35}$$

Weil das n-te Kreisteilungspolynom - wie in **Satz 1.4** bewiesen – ganzzahlige Koeeffizienten besitzt, hat das q-te Kreisteilungspolynom erst recht ganzzahlige Koeffizienten. Dadurch wird eine Ganzheitsgleichung für den Ring $\mathcal{R}_q$ beschrieben.
Die Diskriminante des q-ten Kreisteilungsringes ist dann:

$$\begin{aligned}
\pm\,\Delta(1, \zeta_{k_q}, \ldots, \zeta_{k_q}^{\varphi(q)-1}) &= \prod_{i\neq j}(\zeta_{k_i} - \zeta_{k_j}) \\
&= (-1)^{\frac{1}{2}\cdot\varphi(q)\cdot(\varphi(q)-1)} \prod_{i=1}^{\varphi(q)} \Phi_q'(\zeta_{k_i}) \\
&= (-1)^{\frac{1}{2}\cdot\varphi(q)^2-\varphi(q)} \prod_{i=1}^{\varphi(q)} \Phi_q'(\zeta_{k_i}) \\
&= (-1)^{\frac{1}{2}\cdot\varphi(q)} \prod_{i=1}^{\varphi(q)} \Phi_q'(\zeta_{k_i}) \\
&= (-1)^{\frac{1}{2}\cdot\varphi(q)} N(\Phi_q'(\zeta_{k_q})).
\end{aligned} \tag{2.36}$$

Differenzieren wir die Gleichung

$$(X^{p^{r-1}} - 1) \cdot \Phi_q(X) = X^q - 1 \tag{2.37}$$

und setzen für ζ_{k_q} in X ein, so erhalten wir

$$\underbrace{p^{r-1} \cdot \zeta_{k_q}^{p^{r-2}} \cdot \Phi_q(\zeta_{k_q})}_{0} + (\zeta_{k_q}^{p^{r-1}} - 1) \cdot \Phi_q'(\zeta_{k_q}) = q \cdot \zeta_{k_q}^{q-1} \qquad (2.38)$$

bzw.

$$\Phi_q'(\zeta_{k_q}) = \frac{q \cdot \zeta_{k_q}^{q-1}}{\zeta_{k_q}^{p^{r-1}} - 1} = \frac{q \cdot \zeta_{k_q}^{-1}}{\zeta_{k_q}^{p^{r-1}} - 1} \qquad (2.39)$$

Weiter ist

$$N(\Phi_q'(\zeta_{k_q})) = N\left(\frac{q \cdot \zeta_{k_q}^{-1}}{\zeta_{k_q}^{p^{r-1}} - 1}\right). \qquad (2.40)$$

Da die Norm multplikativ ist, also aus $N(a \cdot b) = N(a) \cdot N(b)$ für beliebige Elemente eines kommutativen Ringes R gilt, dürfen wir die Norm des Zähler und die Norm des Nenners getrennt bestimmen. Es ergibt sich für

$$N(q \cdot \zeta_{k_q}^{-1}) = \underbrace{N(q)}_{q^{\varphi(q)}} \cdot \underbrace{N(\zeta_{k_q}^{-1})}_{(\pm 1)^{\varphi(q)}} = q^{\varphi(q)}, \qquad (2.41)$$

da $\varphi(q)$ – wie wir in **Satz 1.5** gezeigt haben – stets eine gerade natürliche Zahl für $n \geq 3$ ist.
Schließlich brauchen wir nur noch die Norm des Nenners auszurechnen, um die Diskriminante des q-ten Kreisteilungsringes zu berechnen. Dazu bestimmen wir zunächst $N(\zeta_{k_q} - 1)$. Offensichtlich ist $\zeta_{k_q} - 1$ Nullstelle vom Polynom $\Phi_q(X + 1)$. Folglich ist deren Norm

$$\Phi_q(0 + 1) = \Phi_q(1) = p. \qquad (2.42)$$

Die letzte Gleichheit zeigt man durch vollständige Induktion nach r, also den Potenzen von p, da wir ja $q := p^r$ gesetzt haben. (Hier haben wir verwendet, dass die Norm eines Elementes dem konstanten Term des Minimalpolynoms entspricht.)
Genauso ergibt sich für $N(\zeta_{k_q}^{p^{r-1}} - 1)$ der Ausdruck:

$$N(\zeta_{k_q}^{p^{r-1}} - 1) = p^{\frac{q}{p}} \qquad (2.43)$$

Dann resultiert für die Diskriminante des Kreisteilungsringes die Gleichheit:

$$\Delta(1, \zeta_{k_q}, \ldots, \zeta_{k_q}^{\varphi(q-1)}) = (-1)^{\frac{1}{2} \cdot \varphi(q)} \cdot q^{\varphi(q)} \cdot p^{-\frac{q}{p}}. \qquad (2.44)$$

Damit hätten wir die Diskriminante des q-ten Kreisteilungsringes beschrieben.
Im Folgenden wollen wir beweisen, dass die zum q-ten Kreisteilungskörper zugehörige Kreisteilungsring $\mathcal{R}_q$ die Gestalt $\mathbb{Z}[\zeta_{k_q}]$ hat.
Weil $\mathcal{R}_q$ sämtliche q-ten Einheitswurzeln enthält und deren Minimalpolynome – nach **Satz 1.4** – ganzzahlige Koeffizienten besitzt, gilt

$$\mathbb{Z}[\zeta_{k_q}] \subseteq \mathcal{R}_q. \tag{2.45}$$

Zugleich ist auch

$$\Delta(1, \zeta_{k_q}, \ldots, \zeta_{k_q}^{\varphi(q-1)}) \cdot \mathcal{R}_n \subseteq \mathbb{Z}[\zeta_{k_q}], \tag{2.46}$$

da . Wie wir schon bei der Berechnung der Diskriminante errechnet haben, ist

$$N(\zeta_{k_q} - 1) = \Phi_q(0 + 1) = p. \tag{2.47}$$

Folglich ist $\zeta_{k_q} - 1$ eine Primzahl in $\mathcal{R}_q$, weil deren Norm eine Primzahl in den ganzen Zahlen ist. Also erzeugt diese Zahl auch in $\mathcal{R}_q$ ein Primideal, sodass die Isomorpie

$$\mathcal{R}_q/(1 - \zeta_{k_q})\mathcal{R}_q \cong \mathbb{Z}/p\mathbb{Z} \tag{2.48}$$

gilt. Wir betrachten im Folgenden die kanonischen Ringhomomorphismen

$$\mathbb{Z} \to \mathcal{R}_q \to \mathcal{R}_q/(1 - \zeta_{k_q})\mathcal{R}_q \cong \mathbb{Z}/p\mathbb{Z}. \tag{2.49}$$

Besitzen zwei Elemente x und y, wobei $x \in \mathcal{R}_q$ und $y \in \mathbb{Z}$ dieselbe Restklasse in $\mathcal{R}_q/(1-\zeta_{k_q})\mathcal{R}_q$ bzw. $\mathbb{Z}/p\mathbb{Z}$, so ist deren Differenz ein Element des Primideals $(1 - \zeta_{k_q})\mathcal{R}_q$. Deshalb erhalten wir

$$\mathcal{R}_q = \mathbb{Z} + (1 - \zeta_{k_q}) \cdot \mathcal{R}_q. \tag{2.50}$$

Gleichheit gilt sogar auch dann noch, wenn

$$\mathcal{R}_q = \mathbb{Z}[\zeta_{k_q}] + (1 - \zeta_{k_q}) \cdot \mathcal{R}_q \tag{2.51}$$

gilt, denn die q-ten Einheitswurzeln sind ja Elemente aus $\mathcal{R}_q$. Jetzt werden wir die Beschreibung von $\mathcal{R}_q$ präzisieren, indem wir den schwächsten Punkt der Gleichung ändern. Das ist hier der Term $(1 - \zeta_{k_q})$:
Multiplikation mit $(1 - \zeta_{k_q})$ ergibt:

$$(1 - \zeta_{k_q}) \cdot \mathcal{R}_q = (1 - \zeta_{k_q}) \cdot \mathbb{Z}[\zeta_{k_q}] + (1 - \zeta_{k_q})^2 \cdot \mathcal{R}_q. \tag{2.52}$$

bzw.

$$(1-\zeta_{k_q})^2 \cdot \mathcal{R}_q + \mathbb{Z}[\zeta_{k_q}] = \mathcal{R}_q, \tag{2.53}$$

da zu dem Ring $\mathcal{R}_q$ und zum Ring $\mathbb{Z}[\zeta_{k_q}]$ nichts Neues hinzukommt. Dies ergibt eine andere Sichtweise auf die Gleichung!
Wenn man dieses Verfahren immer wieder anwendet erhält man schließlich

$$(1-\zeta_{k_q})^t \cdot \mathcal{R}_q + \mathbb{Z}[\zeta_{k_q}] = \mathcal{R}_q \quad \forall t \geq 1 \tag{2.54}$$

Ist $t = \varphi(q) \cdot \left(r \cdot \varphi(q) - \frac{q}{p} \right)$ so folgt aufgrund von

$$p \cdot \mathcal{R}_q = (1-\zeta_{k_q})^{\varphi(q)} \cdot \mathcal{R}_q \tag{2.55}$$

letzlich die Gleichheit

$$\mathcal{R}_q = (1-\zeta_{k_q})^t \cdot \mathcal{R}_q + \mathbb{Z}[\zeta_{k_q}] = q^{\varphi(q)} \cdot p^{\frac{-q}{p}} \cdot \mathcal{R}_q + \mathbb{Z}[\zeta_{k_q}] = \mathbb{Z}[\zeta_{k_q}]. \tag{2.56}$$

2. **Für eine natürliche Zahl n**:
Sei $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$ die Primfaktorzerlegung der gegebenen natürlichen Zahl. Sei weiter $\zeta_{k_{q_i}}$ mit $i = 1, \ldots, k$ eine primitive q_i-te Einheitswurzel und wir erhalten

$$\mathbb{Q}(\zeta_{k_n}) = \mathbb{Q}(\zeta_{q_1}) \cdot \ldots \cdot \mathbb{Q}(\zeta_{q_k}). \tag{2.57}$$

Für jedes der i bilden die Elemente

$$1, \zeta_{k_{q_i}}, \ldots, \zeta_{k_{q_i}}^{\varphi(q_i)-1} \tag{2.58}$$

also eine Ganzheitsbasis über $\mathbb{Z}$.
Damit lässt sich jedes aus $\mathcal{R}_n$ in der Form

$$a_0 + a_1 \cdot \zeta_{k_n} + \ldots + a_{\varphi(n)-1} \cdot \zeta_{k_n}^{\varphi(n)-1} \tag{2.59}$$

darstellen wegen $[\mathbb{Q}(\zeta_{k_n}) : \mathbb{Q}] = \varphi(n)$, womit wir eine Ganzheitsbasis für den n-ten Kreisteilungsing gefunden haben.
Die allgemeine Diskriminantenformel erhält man, indem man in Gleichung (2.35) anstelle von q n setzt und die multiplikative Eigenschaft der Euler'schen φ-Funktion ausnutzt. □

Beispiele (*Bestimmung von Diskriminanten*):

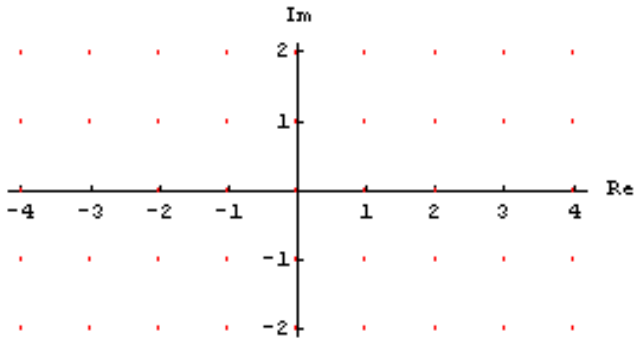

Abbildung 2.1: Das Gauß'sche Gitter

1. Wir rechnen die Diskriminante vom vierten Kreisteilunngsring $\mathcal{R}_4 = \mathbb{Z}[i]$ aus:
   Es ist
   $$\Delta(1,i) = (\pm 2)^{2^{2-1}\cdot(2\cdot 2-2-1)} = (\pm 2)^{2\cdot(4-2-1)} = (\pm 2)^2 = 4 \tag{2.60}$$
2. Nun dasgleiche für den achten Kreisteilungsring $\mathcal{R}_8 = \mathbb{Z}[i,\sqrt{i}]$:
   $$\Delta(1,i,\sqrt{i},i\sqrt{i}) = 4^4 = 256 \tag{2.61}$$

Geometrisch stellen die n-ten Kreisteilungsringe $\mathcal{R}_n$ die Gitterpunkte dar, denen das reguläre n-Eck unterliegt. Das Gauß'sche Gitter wird durch den vierten Kreisteilungsring $\mathbb{Z}[i]$ beschrieben (siehe Abbildung 2.1).
Das Eisenstein'sche Gitter beschreiben die Kreisteilungsringe $\mathcal{R}_3 = \mathcal{R}_6 = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ (siehe dazu Abbildung 2.2). Nach dem obigen Lehrsatz wissen wir, dass der zum n-ten Kreisteilungskörper $\mathcal{K}_n = \mathbb{Q}(\zeta_{k_n})$ zugehörige n-te Kreisteilungsring die Gestalt $\mathcal{R}_n = \mathbb{Z}[\zeta_{k_n}]$ hat. Damit überträgt sich auch die Struktur des Kreisteilungskörpers auf den Kreisteilungsring, welcher geometrisch die unterliegende Gitterstruktur des regulären n-Ecks ausdrückt. Daraus folgt dann, dass die p-ten Kreisteilungsringe – wie es ja auch analog bei den Kreisteilungskörpern der Fall ist – die unterliegende Gitterstruktur des regulären n-Ecks maßgeblich bestimmen.
Aber schon bei $n = 5$ lässt sich kein Gitter mehr angeben, weil das Gitter im $\mathbb{R}^{\varphi(n)} = \mathbb{R}^4$ nicht mehr sichtbar für uns ist. Darum existiert nur für kleine und wenige n eine geometrische Anschauung für den n-ten Kreisteilungsring.
Die Kreisteilungsringe haben meist einen Beweiszweck: Beispielsweise lässt sich über den dritten Kreisteilungsring die Fermat'sche Vermutung für $n = 3$ beweisen, welche besagt, dass die Gleichung
$$x^3 + y^3 = z^3 \Longleftrightarrow x^3 + y^3 + z^3 = 0 \tag{2.62}$$

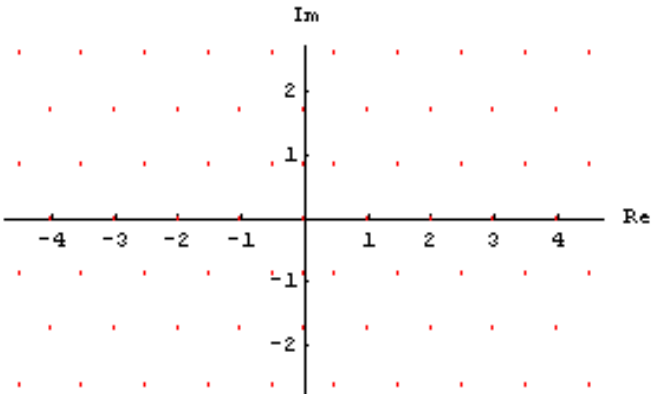

Abbildung 2.2: Das Eisenstein'sche Gitter

keine nichttrivialen Lösungen besitzt, wobei $x, y, z \in \mathbb{Z}$. Dieses Problem wollen wir aber hier nicht erörtern!
Die Kreisteilungskörper schließlich findet Anwendung bei der Beantwortung der Frage, unter welchen Bedingungen ein reguläres n-Eck mit Zirkel und Lineal konstruierbar ist.

Literaturverzeichnis

[1] Bernhard Hornfeck *Algebra*. Walter de Gruyter, Berlin, 1976.

[2] Armin Leutbecher *Zahlentheorie – Eine Einführung in die Algebra*. Springer, Berlin, 1996.

[3] Jürgen Neukirch *Algebraische Zahlentheorie*. Springer, Berlin, 1992.

[4] Günther Scheja, Uwe Storch *Lehrbuch der Algebra – Teil 2*. B. G. Teubner, Stuttgart, 1988.

[5] Heinrich Weber *Lehrbuch der Algebra I*. Chelsea Publishing Company, New York, 1898.

[6] Heinrich Weber *Lehrbuch der Algebra II*. Chelsea Publishing Company, New York, 1898.

Index