Schyren-Gymnasium
Pfaffenhofen

Abiturjahrgang
2013/2015

S E M I N A R A R B E I T

Rahmenthema des Wissenschaftspropädeutischen Seminars:

Komplexe Zahlen

Leitfach: Mathematik

Thema der Arbeit:

Gaußsche Zahlen mit Elementen der Zahlentheorie

Verfasser/in:
Elke Kalupar

Kursleiter/in:
Herr Dr. Kern

Abgabetermin: *spätestens 4. November 2014*

Bewertung	Note	Notenstufe in Worten	Punkte		Punkte
schriftliche Arbeit				x 3	
Abschlusspräsentation				x 1	
				Summe:	
				Gesamtleistung nach § 61 (7) GSO = Summe:2 (gerundet)	

Datum und Unterschrift der Kursleiterin bzw. des Kursleiters

Inhaltsverzeichnis

1. Einleitung – Was ist Zahlentheorie?

„Die Mathematik ist eine Art Spielzeug, welches die Natur uns zuwarf zum Troste und zur Unterhaltung in der Finsternis.“ *Jean-Jacques Rousseau*

Die Zahlentheorie betrachtet die Zahlen und jene Fragen, die sich aus ihnen ergeben und versucht diese Fragen mit Verwendung der Zahlen zu beantworten. In den natürlichen Zahlen hat man das Phänomen der Primzahlen, also einer Zahl, die nur durch sich selbst und eins teilbar ist, beobachtet. Nun fragt man sich, wie viele es gibt oder wie man diese Zahlen finden kann. Diese Beobachtungen versucht man auf andere Zahlen zu übertragen. So findet man immer neue Probleme, die gelöst werden können. Ob man sich damit, wie Rousseau sagt, nur in der Finsternis beschäftigt oder auch in glücklicheren Zeiten, hängt von der Liebe zu den Zahlen ab.

2. Definition eines Rings

Zunächst möchte ich erklären, was man unter einem mathematischen Ring versteht. Ein Ring ist eine Menge R mit zwei Operationen $+$ und $\cdot$, man schreibt $(R, +, \cdot)$. Dieser muss die folgenden Axiome erfüllen.

2.1 Axiome vgl. [1 S. 69f], [2 S. 3]

(A1) $(R, +)$ ist eine abelsche Gruppe:

Zuerst muss für die Menge $(R, +)$ gelten, dass sie eine abelsche Gruppe ist, das heißt für die Gruppe gilt das Assoziativgesetz: $a, b, c \in R$: $(a + b) + c = a + (b + c)$. Dazu existiert ein neutrales Element e: $a, e \in R$: $a + e = a$. Nimmt man hier die ganzen Zahlen als Beispiel ist $e = 0$. Außerdem muss ein inverses Element h existieren: $a, e, h \in R$: $a + h = e$. In $\mathbb{Z}$ könnte beispielsweise $a = 3$ sein und daraus ergibt sich für $h = -3$. Gelten nur diese drei Eigenschaften ist die Menge $(R, +)$ eine Gruppe, damit sie aber eine abelsche Gruppe ist, muss sie kommutativ bzgl. der Addition sein: $a, b \in R$: $a + b = b + a$.

(A2) $(R, \cdot)$ ist eine Halbgruppe:

Damit die Menge $(R, \cdot)$ eine Halbgruppe ist, muss für diese lediglich das Assoziativgesetz gelten, das heißt: $a, b, c \in R$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(A3) Für $(R, +, \cdot)$ gilt das Distributivgesetz

Nun betrachten wir die Menge $(R, +, \cdot)$ mit beiden Operationen. Diese muss in einem Ring die Distributivität erfüllen, sowohl rechtsseitig: $a, b, c \in R: (a + b) \cdot c = a \cdot b + b \cdot c$, als auch linksseitig: $a, b, c \in R: a \cdot (b + c) = a \cdot b + a \cdot c$

Sind die Axiome **(A1)** bis **(A3)** erfüllt, so hat man bereits einen Ring. Jedoch haben solche Ringe, mit dem Ring $\mathbb{Z}$, den wir schon kennen, wenig zu tun. Es gibt also noch speziellere Formen des Rings, von welchen wir die Wichtigsten im Folgenden betrachten.

(A4) Der unitäre Ring:

In diesem Ring muss für die Halbgruppe $(R, \cdot)$ zusätzlich zu den oben genannten Axiomen ein neutrales Element f existieren: $a, f \in R: f \cdot a = a = a \cdot f$. In den meisten Ringen nennt man $f = 1$, oder Einselement. Nimmt man zur Veranschaulichung wieder die ganzen Zahlen, so ist es selbstverständlich, dass $z \cdot 1 = 1 \cdot z = z \quad f\text{ür } alle\ z \in \mathbb{Z}$.

(A5) Der kommutative Ring:

Ein kommutativer Ring muss zunächst alle Eigenschaften eines unitären Rings erfüllen und zusätzlich kommutativ bzgl. der Multiplikation sein, d.h. $a, b \in R: a \cdot b = b \cdot a$.

Beispiele für einen kommutativen Ring sind die ganzen Zahlen $\mathbb{Z}$ und die ganzen gaußschen Zahlen $\mathbb{G}$.

2.2 Rechenregeln vgl. [1 S. 69]

Nachdem wir jetzt wissen, was ein Ring ist, möchte man in diesem auch rechnen können. Das ist ziemlich einfach, denn in Ringen operiert man mit den bekannten Rechenregeln. Im Folgenden erläutere ich diese noch einmal kurz.

- **(R1)** Jedes Element multipliziert mit Null, ergibt Null: $a \in R: a \cdot 0 = 0 \cdot a = 0$
- **(R2)** Multipliziert man einen negativen Faktor mit einem positiven, so ist das Produkt negativ: $a, b \in R: (-a) \cdot b = -(a \cdot b)$
- **(R3)** Multipliziert man zwei negative Faktoren miteinander, so ist das Produkt positiv: $a, b \in R: (-a) \cdot (-b) = a \cdot b$
- **(R4)** Es gilt „Punkt-vor-Strich“, was das Setzen vieler Klammern erübrigt: $a, b, c \in R: (a \cdot b) + c = a \cdot b + c$

2.3 Einheit vgl. [1 S. 70], [3 S. 51]

Man nennt ein Element des Rings R eine Einheit $a \in R$, wenn: $a, b \in R: a \cdot b = b \cdot a = 1$. Für eine bessere Vorstellung, kann man sich $b = a^{-1} = \frac{1}{a}$ denken, obwohl die Division im Ring nicht vorhanden ist. Es gibt in einem Ring ja lediglich die zwei Operationen $+$ und $\cdot$. In den ganzen Zahlen $\mathbb{Z}$ existiert für fast jedes Element$a$ das Inverse Element $\frac{1}{a}$ nicht. Die einzigen Elemente, für die ein solches existiert, sind 1 und -1.

Als weiteres Beispiel nehmen wir die reellen Zahlen $\mathbb{R}$. Betrachten wir eine reelle Zahl r, dann gibt es immer eine andere reelle Zahl $\frac{1}{r}$ für die gilt, $r \cdot \frac{1}{r} = 1$ für $r \neq 0$. Es sind also alle reelle Zahlen außer 0 Einheiten.

2.4 Teiler vgl. [1 S. 85]

In einem Ring$(R, +, \cdot)$ nennt man eine Zahl a Teiler von b, man sagt $a\ teilt\ b$ und schreibt $a \mid b$, falls es eine Zahl $r \in R$ gibt mit $b = r \cdot a$

Um das genauer zu erklären, sollten wir bedenken, dass es in einem Ring die Operation Geteilt nicht gibt. Anders ausgedrückt werden in diesem Fall also nur diejenigen Zahlen Teiler genannt, bei denen die Division aufgehen würde. $a \mid b$ also, wenn b ein Vielfaches von a ist.

2.5 Norm vgl. [1 S. 76,87]

Eine Funktion $n: R \setminus \{0\} \longrightarrow \mathbb{N}_0$, nennt man Norm auf einem nullteilerfreien Ring R, falls es für alle $a, b \in R\ mit\ a \neq 0$ Elemente $q, r \in R$ gibt mit $b = qa + r$ und $n(r) < n(a)$ oder $r = 0$. Die Norm dient meist als eine Art Größenbestimmung, sodass auch in nicht geordneten Mengen, das sind Mengen, in denen es kein $\leq$ gibt. Beispielsweise bei den komplexen Zahlen ist es nicht möglich zu sagen, dass $1 + i \leq 2 + i$ ist. Der Betrag einer ganzen Zahl ist eine Norm, die viele kennen, jedoch nicht unbedingt wissen, dass es eine Norm ist.

3. Der Gaußsche Zahlring vgl. [4]

Carl Friedrich Gauß war in vielen Bereichen seiner Zeit voraus, auch für die Zahlentheorie war er von großer Bedeutung. Er hat viele mathematische Probleme beweisen können unter anderem hat er auch, die nach ihm benannten gaußschen Zahlen eingeführt.

Abbildung 1: Carl Friedrich Gauß vgl. [5]

3.1 Menge der ganzen gaußschen Zahlen vgl. [3 S. 49]

Die Menge der ganzen gaußschen Zahlen ist: $\mathbb{G} = \{a + bi | a, b \in \mathbb{Z}\}$. Sie ist also eine Teilmenge der komplexen Zahlen $\mathbb{C}$. Man kann sie in gewisser Weise mit der Teilmenge $\mathbb{Z}$ von $\mathbb{R}$ vergleichen. Denn sowohl in $\mathbb{G}$, als auch in $\mathbb{Z}$ wird nur ein abzählbar unendlicher Teil betrachtet, das heißt es gibt nur so viele ganze Zahlen und gaußsche Zahlen, wie es natürliche Zahlen gibt. Für eine ganze gaußsche Zahl $z = a + bi$ müssen der Realteil $Re(z)$ und ihr Imaginärteil $Im(z)$ ganzzahlig sein. Graphisch veranschaulicht bildet die Menge $\mathbb{G}$ alle Zahlen, die im Koordinatensystem auf den ganzzahligen Gitternetzpunkten in der komplexen Ebene liegen. Das werden wir später beweisen.

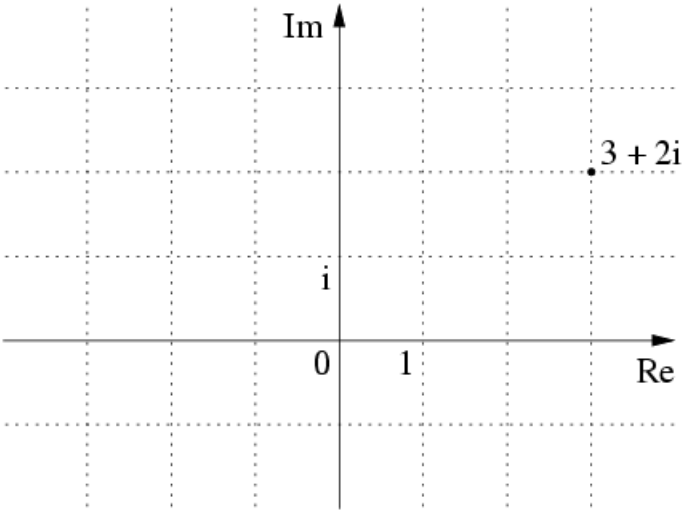

Abbildung 2: vgl. [9]

3.2 Einheit, Teiler, Norm vgl. [3 S. 49-51]

In diesem Punkt möchte ich noch einmal speziell auf den Ring der ganzen gaußschen Zahlen bezogen zeigen, was Einheit, Teiler und Norm sind.

Um ganze gaußsche Zahlen von den ganzen Zahlen $(a, b, c, \ldots)$ abzugrenzen werden oft griechische Buchstaben $(\alpha, \beta, \gamma, \ldots)$ verwendet.

Für die ganzen gaußschen Zahlen $\mathbb{G}$ sind die Einheiten $1, i, -1, -i$.

Beweis:

$$1 \cdot 1 = 1 \Rightarrow b = 1$$
$$i \cdot (-i) = 1 \Rightarrow b = -i$$
$$-1 \cdot (-1) = 1 \Rightarrow b = -1$$
$$-i \cdot i = 1 \Rightarrow b = i$$

Als nächstes wollen wir uns anschauen, was ein Teiler in $\mathbb{G}$ ist. Für $\alpha, \beta \in \mathbb{G}$ nennt man α einen Teiler von β, geschrieben $\alpha|\beta$, wenn ein $\gamma \in \mathbb{G}$ existiert, für das $\alpha \cdot \gamma = \beta$ gilt. Im Grunde ist diese Definition nichts anderes als bei 2.4 bereits erklärt. Lediglich $\alpha, \beta \; und \; \gamma$ sind jetzt ganze gaußsche Zahlen. Natürlich muss auch hier berücksichtigt werden, dass man beim Teilen nicht aus der Menge der ganzen gaußschen Zahlen fällt. Damit das klarer wird, möchte ich noch ein paar Beispiele zu Teilern vorstellen.

$$-2i \mid 8, denn \; (-2i) \cdot (4i) = 8$$
$$3 + 3i \mid 18, denn \; (3 + 3i) \cdot (3 - 3i) = 9 + 9i - 9i + 9 = 18$$
$$3 + i \mid 16 + 2i, denn \; (3 + i) \cdot (5 - i) = 15 + 5i - 3i + 1 = 16 + 2i$$

Wie schon erwähnt, ist das Teilen auch im gaußschen Zahlring nicht ganz perfekt. Dazu müsste er ein Körper sein. Es gibt nämlich viele Zahlen, die nicht Teiler aller anderen Zahlen sind.

$1 + i \nmid 4 + 3i$, denn es müsste eine ganze gaußsche Zahl geben, für die $(1 + i) \cdot (a + bi) = a - b + i(a + b) = 4 + 3i$. Es müsste für das Gleichungssystem $a - b = 4$ und $a + b = 3$ eine ganzzahlige Lösung geben. Jedoch ist $a = 3{,}5$ und $b = -0.5$

Schließlich möchte ich die Norm definieren. Die Norm einer ganzen gaußschen Zahl $\alpha = a + bi \in \mathbb{G}$ ist die natürliche Zahl oder Null $N(\alpha) = (a + bi) \cdot (a - bi) = a^2 + b^2$. Im Koordinatensystem ist die Norm also das Quadrat des Betrags einer ganzen gaußschen Zahl. Außerdem gilt für alle $\alpha, \beta \in \mathbb{G}$:

$$N(\alpha \cdot \beta) = N\big((a + bi) \cdot (c + di)\big) = N(ac - bd + (ad + bc)i) =$$
$$= (ac - bd)^2 + (ad + bc)^2 = a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 =$$
$$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = a^2(c^2 + d^2) + b^2(c^2 + d^2) =$$
$$= (a^2 + b^2)(c^2 + d^2) = N(\alpha) \cdot N(\beta)$$

Zudem gilt die Teilbarkeitsbeziehung $N(\alpha)|N(\beta)$, denn $\alpha \cdot \gamma = \beta$, also muss $N(\beta) = N(\alpha \cdot \gamma) = N(\alpha) \cdot N(\gamma)$

3.3 Isomorphie zu $\mathbb{Z} \times \mathbb{Z}$ vgl. [1 S. 71]

Oben bei 3.1 haben wir uns die ganzen gaußschen Zahlen bereits in einem Gitternetz vorgestellt. Das ist allerdings nur möglich, wenn $\mathbb{G}$ zu $\mathbb{Z} \times \mathbb{Z}$ isomorph ist. Zwei Ringe heißen isomorph, wenn es zwischen ihnen einen Isomorphismus gibt. Der Begriff Isomorphie setzt sich aus den griechischen Wörtern ìsos, was „gleich“ bedeutet und morphé, was die „Gestalt“ heißt, zusammen vgl. [5 S. 678,683]. Ein Isomorphismus ist ein bijektiver Homomorphismus. Ein Homomorphismus ist eine Funktion φ, die Elemente eines Rings $(R, +, \cdot)$ auf Elemente eines zweiten Rings $(S, \oplus, \odot)$ abbildet und dabei die Struktur des Rechnens erhält. In Formeln ausgedrückt schreibt man:

$$\varphi: R \to S$$
$$r \mapsto \varphi(r)$$
$$\varphi(a + b) = \varphi(a) \oplus \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$$
$$\varphi(1_R) = 1_S$$

Das Einselement des einen Rings wird auf das Einselement des anderen Rings abgebildet. Zudem wird das Bild der Summe der Elemente a und b auf die Summe der Bilder von a und b abgebildet, genauso beim Produkt. Eine solche Funktion φ ist bijektiv, wenn sie injektiv und surjektiv ist. Ein Homomorphismus ist injektiv, wenn keine zwei (oder mehr) Elemente aus R auf das gleiche Element in S abgebildet werden (siehe Abbildung 3).

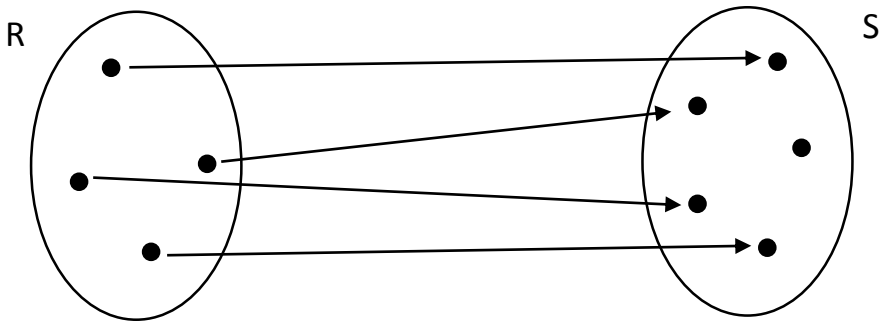

Abbildung 3 [selbst erstellt]

Eine Funktion ist surjektiv, wenn jedes Element aus S einen Partner in R hat (siehe Abbildung 4).

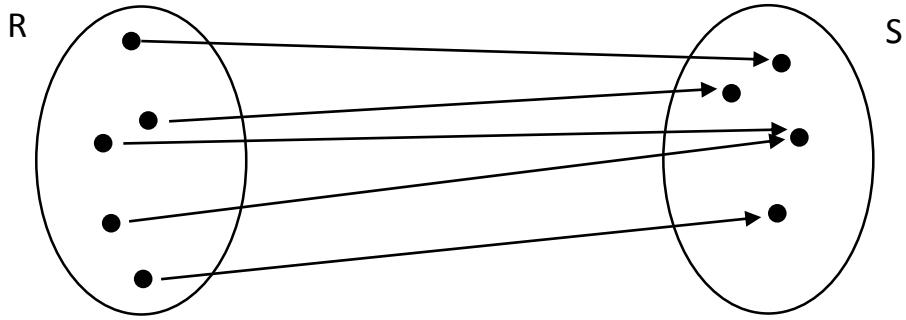

Abbildung 4 [selbst erstellt]

Die Tatsache, dass jedes Element aus R abgebildet wird, in Abbildungen 3 und 4 also ein Pfeil von ihm wegführt, folgt schon daraus, dass wir es mit einer Funktion zu tun haben.

Existiert ein solcher bijektiver Homomorphismus, also ein Isomorphismus, zwischen zwei Ringen, enthalten sie gleich viele Elemente.

Damit wir uns $\mathbb{G}$ als Gitternetz $\mathbb{Z} \times \mathbb{Z}$ vorstellen können, suchen wir also eine Abbildung, die den Raum von $\mathbb{G}$ in das Gitternetz $\mathbb{Z} \times \mathbb{Z}$ unter strenger Erhaltung der Rechenarten umformt.

Wir haben also die Ringe $(\mathbb{G}, +, \cdot)$ und $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$. Für die Operationen in $\mathbb{Z} \times \mathbb{Z}$ gilt:

$$(a|b) + (c|d) = (a + c|b + d)$$
$$(a|b) \cdot (c|d) = (ac - bd|ad + bc)$$

Was vielleicht etwas verwirrend sein kann, ist dass es jetzt drei verschiedene Plus-Rechenarten und drei verschiedene Mal-Rechenarten gibt, nämlich die zu $\mathbb{G}$, $\mathbb{Z} \times \mathbb{Z}$ und $\mathbb{Z}$ gehörigen. Wenn rechts und links vom Rechenzeichen zwei Elemente aus $\mathbb{G}$ bzw. $\mathbb{Z} \times \mathbb{Z}$ bzw. $\mathbb{Z}$ stehen, wird selbstverständlich die zu der jeweiligen Menge gehörigen Rechenart verwendet. Wir schreiben der Lesbarkeit halber immer das gleiche Zeichen verwenden, was so üblich ist.

Sei φ: $\mathbb{G} \rightarrow \mathbb{Z} \times \mathbb{Z}$ eine Funktion mit $\varphi(a + bi) = (a|b)$.

Homomorphie-Eigenschaft:

$$\varphi\big((a + bi) + (c + di)\big) = \varphi\big((a + c) + (b + d)i\big) = (a + c|b + d) =$$
$$= (a|b) + (c|d) = \varphi(a + bi) + \varphi(c + di)$$
$$\varphi\big((a + bi) \cdot (c + di)\big) = \varphi(ac - bd + (ad + bc)i) =$$
$$= (ac - bc|ad + bc) = (a|b) \cdot (c|d) = \varphi(a + bi) \cdot \varphi(c + di)$$

Das Einselement in $\mathbb{G}$ ist $1 + 0i$, das Einselement in $\mathbb{Z} \times \mathbb{Z}$ ist $(1|0)$.

$$\varphi(1 + 0i) = (1|0)$$

$\Rightarrow \varphi$ ist ein Homomorphismus

Bijektivität:

Als erstes betrachten wir die Injektivität von φ. Sei $\mathbb{G} \ni \alpha = a + bi$, $\mathbb{G} \ni \beta = c + di$ mit $\alpha \neq \beta$. Das bedeutet also, dass nicht gleichzeitig $a = c$ und $b = d$ sein kann. Jetzt müssen wir zeigen, dass α und β von φ nicht auf das gleiche Element in $\mathbb{Z} \times \mathbb{Z}$ abgebildet werden. Betrachte $\varphi(\alpha) = (a|b)$, $\varphi(\beta) = (c|d)$ und die Gleichung $(a|b) = (c|d)$. Die Gleichung ist nur dann wahr, wenn $a = c$ und $b = d$. Das kann nach der Annahme aber nicht eintreten. $\Rightarrow \varphi(\alpha) \neq \varphi(\beta)$. α und β werden also von φ auf verschiedene Elemente in $\mathbb{Z} \times \mathbb{Z}$ gesendet, also ist φ injektiv.

Zusätzlich muss φ noch surjektiv sein. Wähle $(a|b) \in \mathbb{Z} \times \mathbb{Z}$. Jetzt müssen wir ein Element aus $\mathbb{G}$ finden, welches auf $(a|b)$ abgebildet wird. Dieses Element ist $a + bi$. Es wird also jedes Element aus $\mathbb{Z} \times \mathbb{Z}$ von φ getroffen.

$\Rightarrow \varphi$ surjektiv $\Rightarrow \varphi$ bijektiv $\Rightarrow \varphi$ ist Isomorphismus

$\mathbb{G}$ ist damit isomorph zu $\mathbb{Z} \times \mathbb{Z}$. Damit haben wir gezeigt, dass sich die ganzen gaußschen Zahlen als Gitternetz darstellen lassen, die Addition sich als eine Art „Vektoraddition“ darstellen lässt und die Multiplikation sich als Drehstreckung darstellen lässt.

3.4 Primelemente vgl. [1 S. 94f], [3 S. 51-54]

Wir nennen eine ganze gaußsche Zahl prim, wenn sie außer den Einheiten und ihren Assoziierten keine weiteren Teiler hat. Die Assoziierten einer Zahl α sind α mit jeweils einer Ein-

heit multipliziert, also $\alpha, i\alpha, -\alpha, -i\alpha$. Es ist nichts Besonderes, dass eine Zahl durch ihre Assoziierten teilbar ist, denn das gilt für jede Zahl:

Sei $\alpha \in \mathbb{G}$, so müssen wir ein $\gamma \in \mathbb{G}$ finden, sodass

$$\alpha \cdot \gamma = \alpha \Rightarrow \gamma = 1 \Rightarrow \alpha|\alpha$$
$$i\alpha \cdot \gamma = \alpha \Rightarrow \gamma = -i \Rightarrow i\alpha|\alpha$$
$$-\alpha \cdot \gamma = \alpha \Rightarrow \gamma = -1 \Rightarrow -\alpha|\alpha$$
$$-i\alpha \cdot \gamma = \alpha \Rightarrow \gamma = i \Rightarrow -i\alpha|\alpha$$
$$\text{für alle } \alpha \in \mathbb{G}$$

Die Menge aller Teiler einer Primzahl π ist also $T(\pi) = \{1, i, -1, -i, \pi, i\pi, -\pi, -i\pi\}$. Die Menge aller Gaußschen Primzahlen nennen wir $\mathbb{GP}$.

4. Finden des größten gemeinsamen Teilers

4.1 Euklidischer Algorithmus vgl. [6 S. 34-37]

Der euklidische Algorithmus ist ein Verfahren zum Finden des größten gemeinsamen Teilers (ggT) von zwei Zahlen, man schreibt $ggT(x, y)$. Dieser wurde von Euklid ungefähr 300 v.Chr. in seinem Werk „Die Elemente“ beschrieben. Allgemein ist ein Algorithmus eine systematische Rechenmethode mit bestimmten Anweisungen, also wie ein Kochrezept. Es ist jetzt nicht mehr notwendig durch Überlegen auf den ggT zu kommen, was gerade bei sehr großen Zahlen schwierig ist. Auch für den Computer ist es so möglich den ggT zu finden.

Zunächst müssen wir ein paar Voraussetzungen kennen. Jede Zahl hat nur Teiler, die im Betrag kleiner oder gleich groß wie sie selbst sind und folgernd daraus hat jede Zahl nur endlich viele Teiler. Da wir uns noch in der Menge $\mathbb{Z}$ befinden, ist es einfach aus dieser endlichen Menge der Teiler, den größten Teiler $d = ggT(a, b)$ zu finden. Beispiel:

$$a = 74 \quad Teiler: \{1,2,37,74\}$$
$$b = 21 \; Teiler: \{1,3,7,21\}$$
$$\Rightarrow ggT(74,21) = 1$$

Würde man jetzt größere Zahlen nehmen, wird es schwieriger und aufwendiger alle Teiler zu finden. Daher wäre es sinnvoll den euklidischen Algorithmus zu verwenden. Ich möchte zunächst mit einer einfachen Tatsache beginnen.

Wir können im Bereich der ganzen Zahlen $\mathbb{Z}$ eine beliebige Zahl mit einer anderen teilen, allerdings bleibt hier oft ein Rest übrig. Zum Beispiel:

$$381 \div 5 = 76\ Rest\ 1$$

Man kann also auch schreiben: $76 \cdot 5 + 1 = 381$

Dass dies möglich ist, haben wir bereits in der Grundschule gelernt. Folgender Satz beschreibt das.

$$a = bq + r \qquad für\ alle\ a, b \in \mathbb{Z}\ mit\ b > 0\ und\ q, r \in \mathbb{Z}, wobei\ 0 \leq r < b$$

Um diesen Satz zu beweisen, muss man bedenken, dass es zwei Möglichkeiten für a gibt. Entweder ist a ein Vielfaches von b, also die Division geht auf,

$$a = b \cdot q \ \Rightarrow r = 0$$

oder a ist kein Vielfaches von b. In letzterem Fall können wir aber darauf schließen, dass a zwischen $b \cdot q$ und ihrem nächsten Vielfachen $b \cdot (q + 1)$ liegt. In Formeln ausgedrückt:

$$b \cdot q < a < b \cdot (q + 1)$$

Jetzt wollen wir natürlich den Unterschied zwischen $b \cdot q$ und a, also den Rest, berechnen. Hierfür formen wir obigen Satz um:

$$r = a - (b \cdot q)$$

Damit r die Voraussetzungen erfüllt, muss es positiv und kleiner als b sein. Andernfalls gibt es mehrere Möglichkeiten für den Rest. Wir wissen bereits $b \cdot q < a$ also ist $r > 0$. Außerdem kann man die Ungleichung so umformen, dass man sieht $r < b$:

$$a = bq + (a - bq)$$
$$a < bq + b$$
$$bq + \underbrace{(a - bq)}_{r} < bq + b$$

Wir haben nun den obigen Satz $a = bq + r$ bewiesen. Wenn wir daraus folgern können $ggT(a, b) = ggT(b, r)$ so funktioniert der euklidische Algorithmus. Zunächst nehmen wir diese Aussage an und probieren ein Beispiel aus, um die Funktionsweise des Algorithmus zu veranschaulichen.

$$a = 74 \quad b = 21$$
$$74 = 21 \cdot 3 + 11$$
$$ggT(74{,}21) = ggT(21{,}11)$$

$$21 = 11 \cdot 1 + 10$$
$$ggT(21,11) = ggT(11,10)$$
$$11 = 10 \cdot 1 + 1$$
$$ggT(11,10) = ggT(10,1)$$
$$10 = 1 \cdot 10 + 0$$
$$\Rightarrow ggT(74,21) = ggT(1,0)$$

Man wiederholt dieses Verfahren also solange, bis $r = 0$ ist.

Kommen wir nun zurück zu der Gleichung $ggT(a,b) = ggT(b,r)$ und versuchen diese zu beweisen. Wir wissen bereits $a = bq + r$, also suchen wir uns eine Zahl u_1 die sowohl in a, als auch in b enthalten ist. Diese Zahl $u_1 \in gT(a,b)$ ist also ein gemeinsamer Teiler. Wir haben also: $a = s_1u_1 \quad b = t_1u_1$

Wir können einfach überprüfen, dass u_1 auch in dem Rest r enthalten sein muss, denn

$$r = a - bq = s_1u_1 - t_1u_1 \cdot q = u_1(s_1 - t_1q)$$

Somit ist u_1 ebenfalls ein Teiler von r. Damit ist ein Teiler von a, b auch ein Teiler von r. Allerdings müssen wir auch wissen, ob die Umkehrung stimmt, also ob ein Teiler von b, r auch ein Teiler von a ist. Wir haben also: $b = s_2u_2 \quad r = t_2u_2$

$$a = bq + r = s_2u_2 \cdot q + t_2u_2 = u_2(s_2q + t_2)$$

Jetzt können wir sagen, dass jeder gemeinsame Teiler von a, b ein gemeinsamer Teiler von b, r ist.

$$gT(a,b) = gT(b,r)$$

Wir können also alle gemeinsamen Teiler finden und da diese Menge endlich ist auch den größten Teiler. Der euklidische Algorithmus funktioniert folglich. Bei den ganzen gaußschen Zahlen $\mathbb{G}$ werden wir es schwieriger haben, da diese keine geordnete Menge sind.

4.2 Division mit Rest in $\mathbb{G}$ vgl. [3 S. 54-56]

Wie oben bereits erwähnt, haben wir in der Menge der ganzen gaußschen Zahlen das Problem, dass diese keine geordnete Menge sind. Das heißt, wir wissen nicht, ob eine Zahl größer ist als die andere. Aus diesem Grund nehmen wir uns die Norm als Hilfe, denn diese ordnet jeder gaußschen Zahl eine Natürliche zu (siehe 2.5) und somit können wir das Wissen von 4.1 anwenden.

Wir beginnen also mit einem ähnlichen Satz:

$$\alpha, \beta \in \mathbb{G}\, mit\, \beta \neq 0$$

$$\kappa, \varrho \in \mathbb{G}$$

$$\alpha = \beta \cdot \kappa + \varrho \quad mit\, N(\varrho) < N(\beta)$$

Diese Gleichung hat im vorherigen Punkt das Teilen mit Rest dargestellt. Jetzt stellt sich die Frage was beim „Teilen“ von zwei ganzen gaußschen Zahlen passiert, da es im Ring der ganzen gaußschen Zahlen nicht existiert. Wir versuchen also:

$$\frac{\alpha}{\beta} = A + Bi \qquad A, B \in \mathbb{Q}$$

Wir nehmen uns die Elemente also aus $\mathbb{Q}$, weil wir wissen, dass teilen hier funktioniert. Die Zahl $A + Bi$, die wir nun haben, liegt auf keinem Gitternetzpunkt. Daher suchen wir uns jetzt diejenige ganze gaußsche Zahl $\kappa = x + yi$, die am nächsten Gitternetzpunkt liegt. Der Abstand zwischen diesen beiden Punkten ist dann der Rest geteilt durch β, der bei der Division entsteht. Um sich ein besseres Bild davon zu machen verwenden wir diese graphische Darstellung:

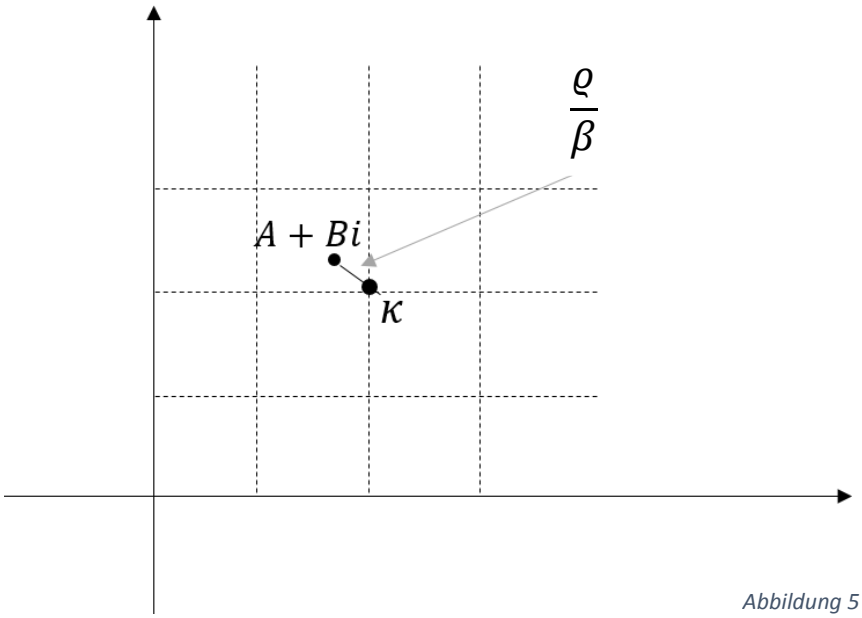

Abbildung 5 [selbst erstellt]

Es wird also immer der Gitternetzpunkt ausgewählt, der von der Zahl $A + Bi$ am wenigsten weit entfernt ist. Diese Regel müssen wir jetzt noch mathematisch aufschreiben:

$$|A - x| \leq \frac{1}{2} \quad und \quad |B - y| \leq \frac{1}{2}$$

Das bedeutet, dass der am weitesten entfernte Punkt, der noch zu einem Gitternetzpunkt gehört die Mitte des Quadrats ist. Rechnerisch findet man κ also durch Runden von A und B. Liegt der Punkt in der Mitter eines Quadrats, so nehmen wie denjenigen Gitterpunkt mit kleinstem Real- und Imaginärteil, wir runden also ab. Als nächsten Schritt wollen wir den Rest ϱ finden. Wir formen obigen Satz um:

$$\varrho = \alpha - \kappa \cdot \beta$$

Jetzt klammern wir β aus und setzen ein.

$$\varrho = \beta\left(\frac{\alpha}{\beta} - \kappa\right) = \beta(A + Bi - \kappa) = \beta\big(A + Bi - (x + yi)\big) = \beta((A - x) + (B + y)i)$$

Damit die Gleichung einer Division mit Rest eindeutig ist, haben wir gefordert, dass $N(\varrho) < N(\beta)$ ist. Die Norm ist notwendig, weil $\mathbb{G}$ keine geordnete Menge ist. Wir berechnen die Norm von ϱ:

Multiplikativität d. Norm

$$N(\varrho) = N(\beta\big((A - x) + (B - y)i\big) \overset{\downarrow}{=} N(\beta) \cdot N\big((A - x) + (B - y)i\big)$$

$$= N(\beta) \cdot ((A - x)^2 + (B - y)^2) \leq N(\beta) \cdot [\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2] = N(\beta) \cdot \frac{1}{2} < N(\beta)$$

Jetzt haben wir gezeigt, dass $N(\varrho)$, wie gefordert kleiner als $N(\beta)$ ist. Zu jedem Zahlenpaar α, β können wir jetzt die Gleichung $\alpha = \beta\kappa + \varrho$ finden. In Analogie an das Teilen mit Rest bei den ganzen Zahlen $\mathbb{Z}$ können wir auch schreiben: $\alpha \div \beta = \kappa\ Rest\ \varrho$

Die Existenz des Teilens mit Rest in $\mathbb{G}$ legt nahe, dass es eine ähnliche Möglichkeit den ggT zu finden, geben müsste. Wir suchen also ein Analogon zum euklidischen Algorithmus. Wir nennen ihn Divisionsalgorithmus für die ganzen gaußschen Zahlen. Zuerst müssen wir definieren was der $ggT(\alpha, \beta)$ zweier Zahlen im Ring $\mathbb{G}$ ist. Wir nennen δ den größten gemeinsamen Teiler von α, β, wenn δ ein gemeinsamer Teiler ist und jeder andere Teiler von α, β ein Teiler von δ ist. Wir schreiben $ggT(\alpha, \beta) = \delta$.

Es gibt immer vier größte gemeinsame Teiler, weil jedes Assoziierte also $\delta, -\delta, i\delta, -i\delta$ auch die Definition des ggT erfüllt. Betrachten wir nun zwei gaußsche Zahlen $\alpha_0, \beta_0 \in \mathbb{G}$.

$$\alpha_0 = \kappa_0\beta_0 + \varrho_0 \quad mit\ N(\varrho_0) < N(\beta_0)$$

Daraus folgt (analog zu bei 4.1):

$$ggT(\alpha_0, \beta_0) = ggT(\beta_0, \varrho_0)$$

Zur Bestimmung des $ggT(\alpha_0, \beta_0)$ geht man also wie folgt vor. Wir stellen die Gleichung $\alpha_0 = \kappa_0\beta_0 + \varrho_0$ auf. Ist $\varrho = 0$, so ist $ggT(\alpha_0, \beta_0) = ggT(\beta_0, 0) = \beta_0$. Anderenfalls dividiert man $\beta_0 \div \varrho_0$ und erhält dadurch die Gleichung $\beta_0 = \kappa_1\varrho_0 + \varrho_1 \ mit\ N(\varrho_1) < N(\varrho_0)$. Ist $\varrho_1 \neq 0$ führt man eine weitere Iteration durch. Weil die Folge $N(\beta_0) > N(\varrho_0) > N(\varrho_1) > \cdots > N(\varrho_{n-1}) > N(\varrho_n) = 0$ eine absteigende endliche Folge ist, bricht unser Algorithmus nach dem n-ten Schritt sicher ab.

Das sieht man leicht anhand der Zeichnung:

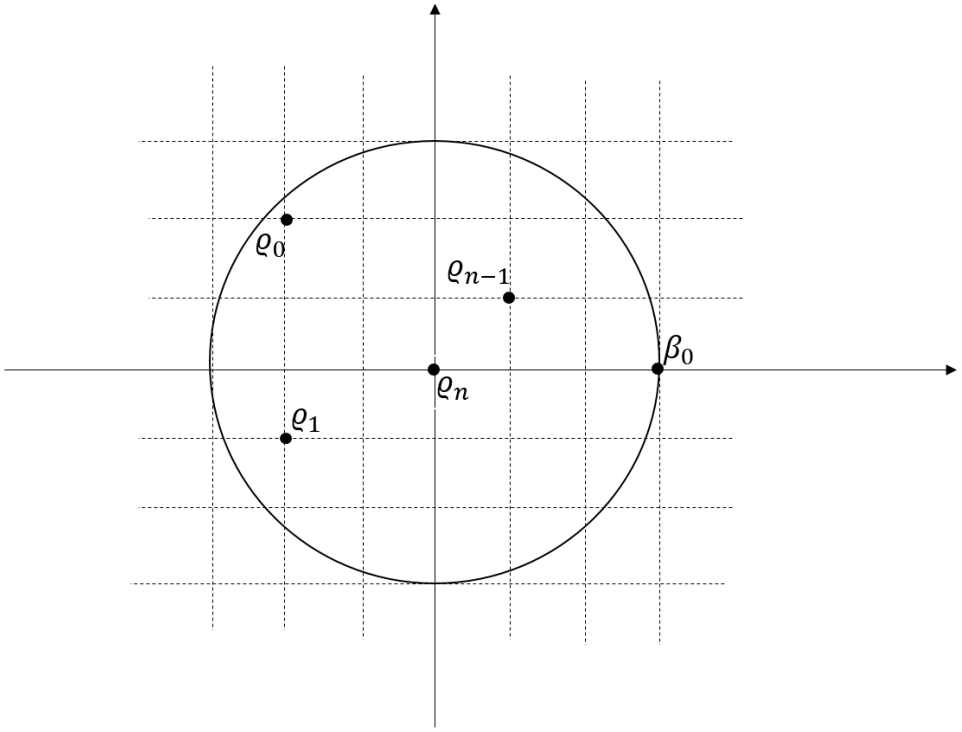

Abbildung 6 [selbst erstellt]

Man erkennt leicht, dass es innerhalb eines Kreises mit Radius $\sqrt{N(\beta_0)}$ nur endlich viele Gitterpunkte gibt. Deswegen gibt es immer eine Zahl $n \in \mathbb{N}$, sodass $N(\varrho_n) = \varrho_n = 0$.

Wir erhalten dadurch die Gleichungskette $ggT(\alpha_0, \beta_0) = ggT(\beta_0, \varrho_0) = ggT(\varrho_0, \varrho_1) = \cdots = ggT(\varrho_{n-1}, \varrho_n) = ggT(\varrho_{n-1}, 0) = \varrho_{n-1}$.

Wir haben also den Divisionsalgorithmus um den ggT zweier ganzer gaußscher Zahlen zu finden, gefunden. Diesen wollen wir anhand eines Beispiels veranschaulichen.

$\alpha = -21 + 18i \qquad b = -13 - i$

Zuerst müssen wir κ_0 finden.

$$\frac{-21+18i}{-13-i} = \frac{(-21+18i)(-13+i)}{169+1} = \frac{255-255i}{170} = \frac{3}{2} - \frac{3}{2}i$$

$$\Rightarrow Abrunden \Rightarrow 1 - i = \kappa_0$$

Als nächstes berechnen wir ϱ_0.

$$\varrho_0 = \alpha - \beta\kappa = (-21+18i) - \big((-13-i)\cdot(1-i)\big) = (-21+18i) - (-14+12i)$$
$$= -7+6i$$

Jetzt setzen wir in die Gleichung $\alpha = \beta\kappa_0 + \varrho_0$ ein.

$$-21+18i = (-13-i)\cdot(1-i) + (-7+6i)$$
$$ggT(-21+18i, (-13-i) = ggT(-13-i, -7+6i)$$

Für die Iteration müssen wir wie zuvor κ_1 und ϱ_1 finden.

$$\frac{-13-i}{-7+6i} = \frac{(-13-i)(-7-6i)}{49+36} = \frac{85+85i}{85} = 1+i$$

$$\Rightarrow man\ muss\ nicht\ runden \Rightarrow \varrho_1 = 0$$

$$ggT(-21+18i, -13-i) = ggT(-13-i, -7+6i) = ggT(-7+6i, 0) = -7+6i$$

5. Ausblick

In der ganzen Arbeit haben wir gesehen, dass es viele Parallelen zwischen den ganzen Zahlen $\mathbb{Z}$ und den ganzen gaußschen Zahlen $\mathbb{G}$ gibt. Würde man also alles, was man über die ganzen Zahlen weiß für die ganzen gaußschen Zahlen weiterspinnen, so erschließen sich einem annähernd unbegrenzte Möglichkeiten in der Welt der ganzen gaußschen Zahlen. Man könnte zum Beispiel untersuchen, ob es gaußsche Primzahlen bestimmter Archetypen gibt oder welche Zahlen n-te Wurzeln besitzen. Doch das wäre eine weitere Seminararbeit.

Literaturverzeichnis

1. **Wüstholz, Gisbert.** *Algebra.* Wiesbaden : Vieweg, 2004.

2. **Thomas, Ihringer.** *Allgemeine Algebra.* Lemgo : Heldermann, 2003.

3. **Joachim, Engel.** *Komplexe Zahlen und ebene Geometrie.* München : Oldenbourg, 2011.

4. **Wikipedia.** [Online] [Zitat vom: 24. 04 2014.] http://de.wikipedia.org/wiki/Gau%C3%9F#Beitr.C3.A4ge_zur_Zahlentheorie.

5. *Brockhaus Enzyklopädie, Zehnter Band.* Mannheim : F.A. Brockhaus, 1989.

6. Courant Richard, Robbins Herbert. *Was ist Mathematik?* Heidelberg : Springer, 2001.

7. Rousseau, Jean-Jacques. [Online]

8. Wikipedia. [Online] [Zitat vom: 24. 04 2014.] http://commons.wikimedia.org/wiki/File:Carl_Friedrich_Gauss.jpg .

9. Wikipedia. [Online] [Zitat vom: 24. 04 2014.] http://commons.wikimedia.org/wiki/File:Gaussian_integer_lattice.png .

Erklärung:

„Ich habe die Seminararbeit ohne fremde Hilfe angefertigt und nur die im Literaturverzeichnis angeführten Quellen und Hilfsmittel benützt.“

Ort	Datum	Unterschrift