**7. Die ganzen Gauß'schen Zahlen.**

Wir betrachten den Körper $\mathbb{C}$ der komplexen Zahlen. Es ist $\mathbb{C} = \mathbb{R}^2$ mit komponentenweiser Addition und mit Multiplikation $[a_1, a_2][b_1, b_2] = [a_1b_1 - a_2b_2, a_1b_2 + a_2b_1]$. Dies ist bekanntlich ein Körper und man setzt $i = [0, 1]$ und schreibt dann $a_1 + a_2i$ statt $[a_1, a_2]$. (Es ist $i^2 = -1$, also schreibt man manchmal auch $i = \sqrt{-1}$.) Sind $a_1, a_2 \in \mathbb{R}$ und $a = a_1 + a_2i$, so nennt man $\overline{a} = a_1 - a_2i$ die zu $a$ *konjugierte komplexe* Zahl. Die Zuordnung $a \mapsto \overline{a}$ ist ein Körper-Automorphismus von $\mathbb{C}$. Wir betrachten die folgenden Teilmengen:

$$\mathbb{Q}[i] = \{z \in \mathbb{C} \mid a = a_1 + a_2i, \text{ mit } a_1, a_2 \in \mathbb{Q}\}$$
$$\mathbb{Z}[i] = \{z \in \mathbb{C} \mid z = z_1 + z_2i\} \text{ mit } z_1, z_2 \in \mathbb{Z}\}$$

Man sieht sehr leicht: $\mathbb{Q}[i]$ ist ein Unterkörper von $\mathbb{C}$ und $\mathbb{Z}[i]$ ist ein Unterring von $\mathbb{Q}[i]$. Man nennt $\mathbb{Z}[i]$ den Ring der *ganzen Gauß'schen Zahlen.*

Betrachte die folgende Abbildung

$$N\colon \mathbb{Z}[i] \to \mathbb{N}_0 \quad \text{mit } N(z) = z\overline{z} \text{ für } z \in \mathbb{Z}[i],$$

man nennt $N(z)$ die *Norm* von $z$. Schreibt man $z = z_1 + z_2i$ mit $z_1, z_2 \in \mathbb{Z}$, so ist $N(z) = z_1^2 + z_2^2$. Natürlich gilt: *Genau dann ist* $N(z) = 0$, *wenn* $z = 0$. Und es ist

$$N(zz') = N(z)N(z') \quad \text{für alle } z, z' \in \mathbb{Z}[i].$$

Wir betrachten im folgenden den Ring $\mathbb{Z}[i]$. Wenn also ring-theoretische Begriffe verwendet werden (wie "invertierbares" Element, "Prim-Element" usw, so ist gemeint: *invertierbar in* $\mathbb{Z}[i]$ bzw. *Prim-Element in* $\mathbb{Z}[i]$, usw. Da $Z[i]$ ein nullteilerfreier kommutativer Ring ist, hat man in $\mathbb{Z}[i]$ den Teilbarkeits-Begriff zur Verfügung ($z|z'$ genau dann, wenn es $z''$ mit $zz'' = z'$ gibt).

Wichtig: *Sind* $a, b \in \mathbb{Z}$ *und gilt* $a|b$ *in* $\mathbb{Z}[i]$, *so gilt* $a|b$ *in* $\mathbb{Z}$ (die Umkehrung gilt auch, ist aber trivial). Beweis: Sei $a|b$ in $\mathbb{Z}[i]$. Es gibt also $z \in \mathbb{Z}[i]$ mit $az = b$. Sei $z = z_1 + z_2i$ mit $z_1, z_2 \in \mathbb{Z}$. Dann ist $b = az = a(z_1 + z_2i) = az_1 + bz_2$, und demnach stimmen die Realteile $b$ und $az_1$ überein: es gibt also $z_1 \in \mathbb{Z}$ mit $b = az_1$.

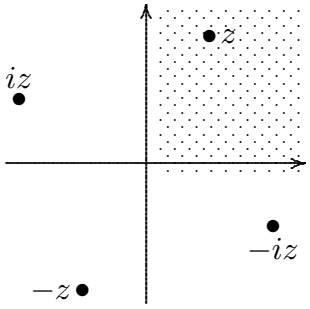
Ganz wichtig ist auch folgende Regel: *Aus* $z|z'$ *in* $\mathbb{Z}[i]$ *folgt die Teilbarkeitsbeziehung* $N(z)|N(z')$. Denn wenn $z|z'$ gilt, so gilt auch $\overline{z}|\overline{z'}$, also $N(z) = z\overline{z}|z'\overline{z'} = N(z')$.

**7.1. Die invertierbaren Elemente in $\mathbb{Z}[i]$.**

**Lemma.** *Es ist* $z$ *in* $\mathbb{Z}[i]$ *genau dann invertierbar, wenn* $N(z) = 1$. *Es gibt genau vier invertierbare Elemente, nämlich* $1, -1, i, -i$.

Beweis: Sei $z \in \mathbb{Z}[i]$ invertierbar, also etwa $zz' = 1$ mit $z' \in \mathbb{Z}[i]$. Aus $zz' = 1$ folgt $1 = N(zz') = N(z)N(z')$. Da $N(z), N(z') \in \mathbb{N}_0$, folgt $N(z) = 1$. Ist $z = z_1 + z_2i$ mit $z_1, z_2 \in \mathbb{Z}$ und gilt $1 = N(z) = z_1^2 + z_2^2$, so ist offensichtlich $z$ eines der vier Elemente $1, -1, i, -i$. Und natürlich sind diese Elemente in $\mathbb{Z}[i]$ invertierbar.

Man nennt $z, z'$ *assoziiert,* wenn gilt: $z|z'$ und $z'|z$. Genau dann sind $z, z'$ assoziiert, wenn es ein invertierbares Element $\epsilon$ mit $z' = \epsilon z$ gibt. Ist $z \neq 0$, so gibt es genau vier zu $z$ assoziierte Elemente, nämlich $z, iz, -z, -iz$ (hier haben wir die Elemente in der Reihenfolge notiert, wie sie in der reellen Ebene durch Drehung um $90^o$ um den Ursprung (= Multiplikation mit $i$) auseinander hervorgehen:




(Übungsaufgabe: Sei $z = z_1 + z_2 i$ mit $z_1, z_2 \in \mathbb{Z}$. Genau dann sind $z, z'$ assoziiert, wenn $z$ auf einer der beiden Koordinatenachsen oder auf einer der beiden Diagonalen (definiert durch $z_2 = z_1$ bzw. $z_2 = -z_1$) liegt.) Assozierte Elemente haben natürlich die gleiche Norm, die Umkehrung gibt aber nicht!

**7.2. Euklid'scher Algorithmus.**

**Satz.** *Sind $a, b \in \mathbb{Z}[i]$ mit $b \neq 0$, so gibt es $q, r \in \mathbb{Z}[i]$ mit*

$$a = qb + r \quad \text{und } N(r) < N(b).$$

(der Beweis zeigt, dass man sogar $N(r) \leq \frac{1}{2}N(b)$ verlangen darf).

Beweis: Da $\mathbb{Q}[i]$ ein Körper ist, gibt es $c = \frac{a}{b} \in \mathbb{Q}[i]$ sei $c = c_1 + c_2 i$ mit $c_1, c_2 \in \mathbb{Q}$. Wir schreiben $c_i$ in der Form $c_i = q_i + s_i$, dabei sei $q_i$ eine ganze Zahl und es gelte $|s_i| \leq \frac{1}{2}$ (ist $c_i - \lfloor c_i \rfloor \leq \frac{1}{2}$, so nimm $c_i = \lfloor c_i \rfloor$, andernfalls nimm $c_i = \lfloor c_i \rfloor + 1$). Sei $q = q_1 + q_2 i$, $s = s_1 + s_2 i$ und $r = sb$. Es ist:

$$a = bc = (q + s)b = qb + sb = qb + r,$$

und

$$N(sb) = N(s)N(b) = (s_1^2 + s_2^2)N(b) \leq (\tfrac{1}{4} + \tfrac{1}{4})N(b) = \tfrac{1}{2}N(b).$$

**Folgerung 1.** Je zwei von Null verschiedene Elemente in $\mathbb{Z}[i]$ haben einen größten gemeinsamen Teiler (genauer: es gibt vier größte gemeinsame Teiler, nämlich eine Klasse assoziierter Elemente) (dabei nennt man $c$ einen *größten gemeinsamen Teiler* von $a, b$, falls gilt: erstens, $c|a$ und $c|b$; zweitens: aus $d|a$ und $d|b$ folgt $d|c$).

**Folgerung 2:** Ist $c$ größter gemeinsamer Teiler von $a$ und $b$, so gibt es $x, y$ mit $c = xa + yb$ (Bezout).

**Folgerung 3.** Irreduzible Elemente sind prime Elemente. ($a$ heißt *irreduzible,* wenn $a$ weder das Nullelement noch invertierbar ist, und wenn aus $a = bc$ folgt, dass $b$ oder $c$ invertierbar ist; $a$ heißt prim, wenn aus $a|bc$ folgt $a|b$ oder $a|c$).

**Folgerung 4.** *Der Ring $\mathbb{Z}[i]$ ist ein Ring mit eindeutiger Primfaktorzerlegung (also ein "faktorieller" Ring):* Jedes Element, das weder Null noch invertierbar ist, lässt sich als Produkt von Primelementen schreiben — und diese Faktorisierung ist im wesentlichen eindeutig, denn für Produkte von Primelementen gilt: sind $p_i, q_j$ Primelemente mit $1 \le i \le r$ und $1 \le j \le s$ und $p_1 \cdots p_r = q_j \cdots q_s$, so ist $r = s$ und es gibt eine Permutation $\sigma$ der Menge $\{1, 2, \ldots, r\}$, sodass $p_i$ und $q_{\sigma(i)}$ assoziert sind, für alle $i$.

Wählen wir für jedes Primelement den Repräsentanten $x = x_1 + ix_2$ mit $x_1 > 0$ und $x_2 \ge 0$ und nennen diese Menge $P$, so gilt: *Die von Null verschiedenen ganzen Gauß'schen Zahlen entsprechen bijektiv den Paaren $(\epsilon, v)$ wobei $\epsilon$ eines der vier invertierbaren Elemente ist und $v\colon P \to \mathbb{N}_0$ eine Abbildung mit endlichem Träger, und zwar wird dem Paar $(\epsilon, v)$ die Zahl $\epsilon \prod_{p\in P} p^{v_p}$ zugeordnet.*

### 7.3. Die Prim-Elemente.

Vorbemerkung: Ist $N(z) = p$ eine Primzahl, so ist $z$ Prim-Element. Denn aus $z = z'z''$ folgt $p = N(z) = N(z')N(z'')$, also muss eine der beiden Zahlen $N(z'), N(z'')$ gleich 1 sein, und demnach muss $z'$ oder $z''$ invertierbar sein.

Beispiel 1: $N(1 + i) = 2$, also ist $1 + i$ Prim-Element. Die zu $1 + i$ assoziierten Elemente sind:

$$1 + i, \quad 1 - i = -i(1 + i), \quad -1 + i = i(1 + i), \quad -1 - i = -(1 + i).$$

Beispiel 2: Sei $p \equiv 1 \mod 4$. Dann gibt es $x, y$ mit $x^2+y^2 = p$, also $N(x+iy) = p$, und auch $N(x - iy) = p$, also sind die Elemente $x + iy, x + iy$ Primelemente. Die zu $x + iy$ assoziierten Elemente sind

$$x + iy, \quad y - ix = -i(x + iy), \quad -y + ix = i(x + iy), \quad -x - iy = -(x + iy).$$

Die zu $x - iy$ assoziierten Elemente sind

$$x - iy, \quad -y - ix = -i(x - iy), \quad y + ix = i(x - iy), \quad -x + iy = -(x - iy).$$

Sei $p \equiv 3 \mod 4$. Es ist $N(p) = p^2$. Sei $p = z'z''$ mit $z', z'' \in \mathbb{Z}[i]$. Es ist $N(p) = N(z')N(z'')$. Ist $N(z') = 1$, so ist $z'$ invertierbar. Ist $N(z') = p^2$, so ist $N(z'') = 1$, also $z''$ invertierbar. Und $N(z') = p$ geht nicht, da sich $p$ nicht als Summe zweier Quadrate schreiben lässt.

Wir haben viele Prim-Elemente gefunden. Wir zeigen nun, dass es keine weiteren gibt:

*Jedes Prim-Element $z$ ist Teiler einer rationalen Primzahl.* Beweis: Es ist $z\overline{z} = N(z) \in \mathbb{N}$. Schreibe $N(z)$ als Produkt $p_1 \cdots p_t$ von rationalen Primzahlen. Da $z$ prim in $\mathbb{Z}[i]$ ist, ist $z$ ein Teiler einer dieser Zahlen $p_i$.

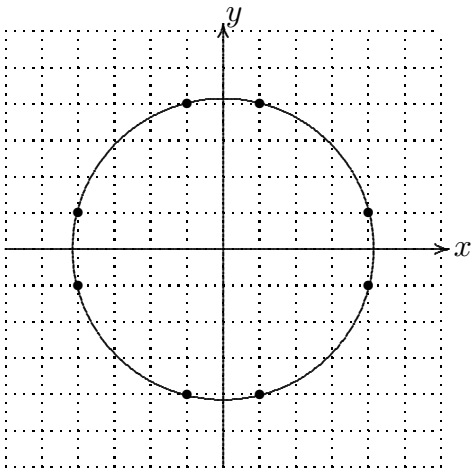
Sei also $z$ Prim-Element in $\mathbb{Z}[i]$, sei $p$ rationale Primzahl mit $z|p$. Es ist dann $N(z)|N(p) = p^2$, also entweder $N(z) = p$ oder $N(z) = p^2$ (denn $N(z) = 1$ würde ja bedeuten, dass $z$ invertierbar ist).

Wir unterscheiden drei Fälle für $z = z_1 + iz_2$.

Fall 1. $N(z) = 2$. Aus $z_1^2 + z_2^2 = 2$ folgt natürlich unmittelbar $z_1, z_2 \in \{1, -1\}$, und diese vier möglichen Elemente $z$ sind alle assoziiert zu unserem Repräsentanten $1 + i$.

Fall 2. $N(z) = p$ ungerade Primzahl. Da $p$ Summe zweier Quadratzahlen ist, ist $p \equiv 1 \mod 4$. Es ist $(z_1 + iz_2)(z_1 - iz_2) = z_1^2 + z_2^2 = p$. Die beiden Faktoren $z_1 + iz_2$, $z_1 - iz_2$ sind Primelemente, also ist dies die (eindeutige!) Primfaktorzerlegung von $p$: jeder Primteiler von $p$ im Ring der ganzen Gauß'schen Zahlen ist assoziiert zu $z_1 + iz_2$ oder $z_1 - iz_2$.

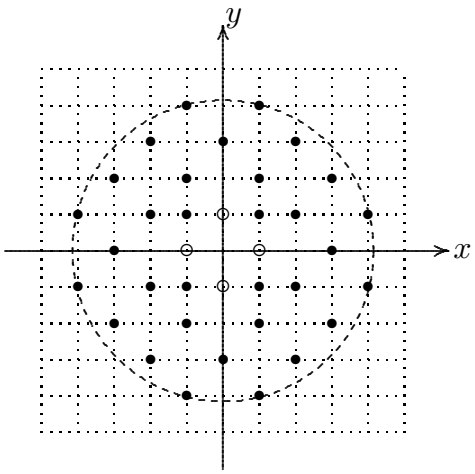
Im folgenden Bild sieht man die Prim-Elemente $z$ mit $N(z) = 17$.




Dass es genau 8 derartige Elemente gibt, folgt aus der eindeutigen Primfaktor-Zerlegung in $\mathbb{Z}[i]$: Zerlegt man $p = 17$ im Ring $\mathbb{Z}[i]$ in Primfaktoren, so gibt es nur zwei Faktoren (und jeder dieser Faktoren hat vier assoziierte Elemente).

Fall 3. $N(z) = p^2$. Aus $z\overline{z} = N(z) = p^2$ folgt, dass $z$ ein Teiler von $p^2$ ist. Da wir voraussetzen, dass $z$ ein Primelement ist, folgt: $z$ ist ein Teiler von $p$. Da $z$ und $p$ die gleiche Norm haben, folgt: $z$ ist assoziiert zu $p$, also ist $z$ eine der Zahlen $p, -p, ip, -ip$. Wäre $p \equiv 1 \mod p$, so könnten wir $p$ als Produkt zweier Faktoren mit Norm $p$ schreiben, dann wäre aber $z$ kein Primelement. Also folgt: $p \equiv 3 \mod 4$.

Im folgenden Koordinatensystem sind die Prim-Elemente $z$ in $\mathbb{Z}[i]$ mit $N(z) \leq 17$ eingetragen (markiert durch $\bullet$); auch die Einheiten sind (durch $\circ$) hervorgehoben.




**7.4. Die Anzahl der ganzen Gauß'schen Zahlen mit fester Norm.**

Für $n \in \mathbb{N}$ sei $\tau(n)$ die Anzahl der ganzen Gauß'schen Zahlen mit Norm $n$, dies ist gerade die Menge der Paare $[x, y] \in \mathbb{Z}^2$ mit $x^2 + y^2 = n$ (wie in 5.1.6 eingeführt).

**Satz.** *Sei* $n = 2^e \cdot p_1^{e_1} \cdots p_s^{e_s} \cdot q_1^{f_1} \cdots q_t^{f_t}$ *mit Primzahlen* $p_i \equiv 1 \mod 4$ *und* $q_j \equiv 3 \mod 4$. *Dann ist*

$$\tau(n) = \begin{cases} 4(e_1+1)\cdots(e_s+1) & \text{falls alle } f_i \text{ gerade sind} \\ 0 & \text{sonst.} \end{cases}$$

Beweis: Dies folgt aus der Eindeutigkeit der Primfaktorzerlegung und unserer Kenntnis der Primelemente. Wir betrachten also Zahlen $z \in \mathbb{Z}[i]$ mit $N(z) = n$. Wir schreiben $z$ als Produkt von Primelementen, genauer: als Produkt einer Einheit (dafür gibt es vier Möglichkeiten) und Repräsentanten unserer Primelemente. Sei also $z = \epsilon z_1 \cdots z_m$ mit einer Einheit $\epsilon$ und Repräsentanten $z_1, \ldots, z_m$.

Es ist $n = N(z) = N(z_1) \cdots N(z_m)$. Für jedes $z_i$ ist $N(z_i) = p$ oder $N(z_i) = p^2$, jedem $z_i$ ist also eine Primzahl zugeordnet.

Ist diese Primzahl $p \equiv 3 \mod 4$, so ist $N(z_i) = p^2$. In der Faktorisierung $n = 2^e \cdot p_1^{e_1} \cdots p_s^{e_s} \cdot q_1^{f_1} \cdots q_t^{f_t}$ handelt es sich also um eine der Primzahlen der Form $q_i$. Der zugehörige Exponent $f_j$ muss gerade sein, und $\frac{1}{2} f_j$ ist die Anzahl dieser Faktoren $z_i$. Hier gibt es keine Wahlmöglichkeit.

Für $p \equiv 1 \mod 4$ gibt es dagegen zwei mögliche Repräsentanten $a, b$ mit Norm $p$. Wir haben demnach für vorgegebenes $e = e_i$ genau $e+1$ Möglichkeiten, um Produkte von $a$ und $b$ mit Norm $p^e$ zu bilden, nämlich $a^e, a^{e-1}b, \ldots, ab^{e-1}, b^e$.

**7.5. Der Satz von Jacobi.**

**Satz (Jacobi).** *Es ist* $\frac{1}{4}\tau(n)$ *gleich der Differenz der Anzahl der Teiler* $d$ *von* $n$ *mit* $d \equiv 1 \mod 4$ *und der Anzahl der Teiler* $d$ *von* $n$ *mit* $d \equiv 3 \mod 4$ (und dies ist eine multiplikative Funktion).

Beweis: Definiere eine Funktion $\gamma\colon \mathbb{N} \to \mathbb{Z}$ durch

$$\gamma(n) = \begin{cases} 0 & n \text{ gerade}, \\ 1 \quad \text{falls} & n \equiv 1 \mod 4, \\ -1 & n \equiv 3 \mod 4. \end{cases}$$

Diese Funktion ist multiplikativ (sogar stark multiplikativ). Also ist auch die summatorische Funktion $\delta = \gamma * U$ multiplikativ. Es ist

$$\delta(n) = \sum\nolimits_{d|n} \gamma(d),$$

dies ist also die Differenz der Anzahl der Teiler $d$ mit $d \equiv 1 \mod 4$ und der Anzahl der Teiler $d$ mit $d \equiv 3 \mod 4$.

Zu zeigen ist demnach:

$$\delta(n) = \begin{cases} (e_1+1)\cdots(e_s+1) & \text{falls alle } f_i \text{ gerade sind} \\ 0 & \text{sonst.} \end{cases}$$

Wegen der Multiplikativität von $\delta$ (und der Funktion, die rechts notiert ist), braucht man die Formel nur für Primzahlpotenzen $n = p^e$ zu beweisen. Sei also $p$ eine Primzahl. Es ist

$$\delta(p^e) = \gamma(1) + \gamma(p) + \cdots + \gamma(p^e).$$

Für $p = 2$ steht hier $1+0+\cdots+0 = 1$. Für $p \equiv 1 \mod 4$ ist jeder Summand $\gamma(p^i) = 1$, also $\delta(p^e) = e+1$. Für $p \equiv 3 \mod 4$ ist $\gamma(1) + \gamma(p) + \cdots + \gamma(p^e) = 1 - 1 + 1 - \cdots$ mit insgesamt $e+1$ Summanden; also $\delta(p^e) = 1$ falls $e$ gerade und $\delta(p^e) = 0$ falls $e$ ungerade. Damit ist der Satz bewiesen.

**Ausblick:** $\mathbb{Z}[i]$ *ist der Ring der ganz-algebraischen Zahlen im Zahlkörper* $\mathbb{Q}[i]$.

In der algebraischen Zahlentheorie betrachtet man endliche Körpererweiterungen $\mathbb{Q} \subseteq K$ (also Körper $K$, die $\mathbb{Q}$ enthalten, sodass $K$ ein endlich dimensionaler $\mathbb{Q}$-Vektorraum ist), man nennt einen solchen Körper einen *Zahlkörper*. Mit $\mathcal{O}_K$ wird die Menge der ganz-algebraischen Elemente in $K$ bezeichnet (also die Menge der Nullstellen von normierten Polynomen mit Koeffizienten in $\mathbb{Z}$). Der Unterring $\mathcal{O}_K$ ist der einzige Unterring $R$ von $K$, der "normal" ist und dessen additive Gruppe $(R, +)$ eine freie abelsche Gruppe vom Rang $\dim_{\mathbb{Q}} K$ ist. Hier betrachten wir den Fall $K = \mathbb{Q}[i]$.

**Lemma.** *Für* $K = \mathbb{Q}[i]$ *gilt:* $\mathcal{O}_K = \mathbb{Z}[i]$.

Beweis: Die Behauptung folgt aus der Faktorialität von $\mathbb{Z}[i]$, denn jeder faktorielle Ring ist "normal" (man kann dies aber auch direkt beweisen).