Gehelen van Gauss

Hector Mommaerts

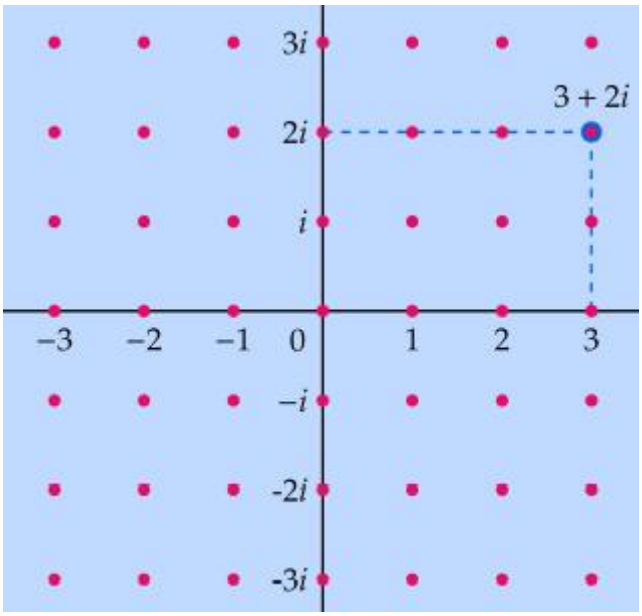
Hoofdstuk 1

Definities

- Gehelen van Gauss zijn complexe getallen van de vorm $a + bi$ waarbij $a, b \in \mathbb{Z}$. De verzameling van alle gehelen van Gauss noteren we met $\mathbb{Z}(i)$. Dus

  $$\mathbb{Z}(i) = \{a + bi : a, b \in \mathbb{Z}\}$$

  De verzameling van alle gehelen van Gauss kan worden voorgesteld door de roosterpunten in het vlak.



- De gewone optelling van complexe getallen is een interne bewerking in $\mathbb{Z}(i)$. Deze optelling is associatief en commutatief. Bovendien is

$0 \in \mathbb{Z}(i)$ het neutraal element en elk element $a + bi$ heeft een symmetrisch element voor de optelling in $\mathbb{Z}(i)$, namelijk $-a - bi$. Dus:

$$\mathbb{Z}(i), + \text{ een commutatieve groep}$$

- Ook de gewone vermenigvuldiging van complexe getallen is een interne bewerking in $\mathbb{Z}(i)$. Ze is commutaief en associatief. $1 \in \mathbb{Z}(i)$ is het neutraal element en de vermenigvuldiging is distributief ten opzichte van de optelling. Bijgevolg is:

$$\mathbb{Z}(i), +, . \text{ een commutatieve ring met eenheidselement}$$

- De norm van een complex getal $z = a + bi$, genoteerd door $N(z)$, is het kwadraat van zijn modulus, dus

$$N(a + bi) = a^2 + b^2$$

De norm is multiplicatief, m.a.w. $N(z_1.z_2) = N(z_1).N(z_2)$.

Hoofdstuk 2

Deelbaarheid

- We weten dat $\mathbb{Z}(i), +, .$ een ring is, net zoals de verzameling van de gehele getallen $\mathbb{Z}$, of de verzameling van de nxn matrices. Het al dan niet bestaan van nuldelers is belangrijk in een ring. a en b zijn nuldelers als $a.b = 0$ zonder dat $a = 0$ of $b = 0$. Een commutatieve ring zonder nuldelers noemt men een integriteitsdomein. De gehele getallen hebben geen nuldelers, dus $\mathbb{Z}, +, .$ is een integriteitsdomein.
  De verzameling vierkante matrices heeft wel nuldelers.
  Neem $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ en $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Dan is $A.B = O$ en $A \neq O$ en $B \neq O$.

- De vraag is nu of er nuldelers zijn bij de gehelen van Gauss. Men kan bewijzen dat er geen zijn, en dus geldt:

  Stelling 2.1. $\mathbb{Z}(i), +, .$ *is een integriteitsdomein*

- In een ring heeft niet elk element een invers element voor de vermenigvuldiging. Een element dat wel een invers heeft noemen we een *eenheid*. De eenheden van $\mathbb{Z}$ zijn ± 1. De eenheden voor de ring van de vierkante matrices van orde n zijn de inverteerbare matrices, de matrices met determinant verschillend van 0. Wat zijn dan de eenheden in $\mathbb{Z}(i)$? Door gebruik te maken van de theorie der stelsels kan men gemakkelijk bewijzen dat:

  Stelling 2.2. *De eenheden van* $\mathbb{Z}(i)$ *zijn* $\pm 1, \pm i$.

- Het idee van delen zonder rest kan men vanuit $\mathbb{Z}$ veralgemenen naar een willekeurige ring. a is een deler van b, we noteren $a|b$, als er een element c in de ring bestaat waarvoor geldt dat $b = a.c$. Een priem

element is dan een element zonder echte delers, op uitzondering van eenheden.

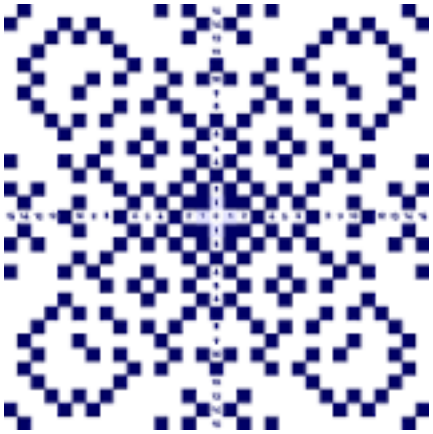
- Een uniek factorisatiedomein (UFD) is een integriteitsdomein R, waarin ieder element van R, dat geen nul is en geen eenheid van R is, kan worden geschreven als een product van priemelementen van R. Zo is $\mathbb{Z}$ een UFD. Men kan ook bewijzen dat:

  Stelling 2.3. $\mathbb{Z}(i), +, .$ *is een uniek factorisatiedomein.*

- De vraag is dan natuurlijk wat de priemelementen zijn in $\mathbb{Z}(i)$. Omdat $2 = (1+i)(1-i)$ is het niet zeker dat priemgetallen in $\mathbb{Z}$ automatisch ook priemelementen zijn in $\mathbb{Z}(i)$. En zijn er nog andere priemelementen, die dus geen priemgetallen in $\mathbb{Z}$ zijn?

  Stelling 2.4. *De priemelementen in $\mathbb{Z}(i)$ zijn getallen $a + bi$ met:*

  - $a = 0$ *of* $b = 0$ *en de andere is een priemgetal van de vorm* $\pm(4n+3)$.
  - $a \neq 0$ *en* $b \neq 0$ *en* $N(a+bi) = a^2 + b^2$ *is een priemgetal.*



- Een voorbeeld van een ontbinding van $z = -7 + 24i$:
  - We bepalen eerst de norm van z: $N(z) = 625 = 5^4$
  - We zoeken 4 gehel van Gauss met norm 5.
  - Een geheel getal van Gauss met norm 5is bijvoorbeeld $2 + i$.
  - Dus $-7 + 24i = (2+i)^4$.

- Ook bij de gehelen van Gauss blijkt er zoiets als deling met rest te bestaan. Natuurlijk ziet die er wat moeilijker uit dan in $\mathbb{Z}$, maar de onderliggende gedachte is in grote lijnen hetzelfde. Hier is een voorbeeld waarbij we het complexe getal 7 gedeeld hebben door het complexe getal $1 + 2i$.
  $7 = (1 + 2i)(1 - 3i) + i$. Het quotiënt blijkt in dit geval $1 - 3i$ te zijn en de rest bedraagt i. Als je het quotiënt $\dfrac{7}{1+2i}$ in de vorm $a + bi$ schrijft, kom je op het complexe getal $\frac{7}{5} - \frac{14}{5}i$ uit en dat behoort niet tot de gehelen van Gauss. Maar $1 - 3i$ is een geheel getal van Gauss dat wel dicht bij $\frac{7}{5} - \frac{14}{5}i$ ligt. Daarom nemen we $1 - 3i$ als quotiënt. De rest, in ons geval i, zou dan ook klein moeten zijn. Een geschikte maat voor klein is de modulus. We eisen namelijk dat de modulus van de rest kleiner is dan de modulus van de deler.

Hoofdstuk 3

Idealen

- Gegeven is een commutatieve ring R,+,.. Een deelgroep I van R,+ is een ideaal van R als $R.I = I$.
- Als I een ideaal is van R, dan construeert men de verzameling $a + I$: $a \in R$: de quotiëntring of factorring R/I. Men definieert volgende bewerkingen: $(a + I) + (b + I) = a + b + I$ en $(a + I).(b + I) = ab + I$. Hiermee krijgt de quotiëntring een ringstructuur.
- Als $I = \langle a \rangle$, dan zegt men dat I voortgebracht wordt door 1 element. Dergelijk ideaal noemt men een hoofdideaal. Als in een integriteitsdomein R elk ideaal een hoofdideaal is , noemen we die ring een hoofdideaal domein. Elk hoofdideaal domein is een UFD.
- Een ideaal I is een priemideaal als het niet de ring zelf is, en als voor elke twee elementen x en y uit de ring, het product $x.y$ slechts in I ligt als x of y zelf in I ligt. Een ideaal I van R is priem als en slechts als de factorring R/I een integratiedomein is.
- Een ideaal I is maximaal als het niet de ring zelf is en als er geen ideaal J bestaat zodat $I \subset J \subset R$. Een ideaal I van R is maximaal dan en slechts dan als de factorring R/I een veld is.
- Elke ring heeft een maximaal ideaal. Een maximaal ideaal is altijd een priemideaal. In hoofdideaal domeinen geldt ook de omgekeerde eigenschap.
- De verzameling van alle gehele n-vouden, $n\mathbb{Z}$, is een hoofdideaal van $\mathbb{Z}$. De quotiëntring is $\mathbb{Z}_n$. Als n priem is dan is $n\mathbb{Z}$ een maximaal ideaal en dus ook een priemideaal. Hier komt trouwens de naam priemideaal van.

- Ook $\mathbb{Z}(i)$ is een hoofdideaal domein, dus de maximale idealen zijn de priemidealen. De priemidealen worden voortgebracht door de priemelementen van $\mathbb{Z}(i)$. Zo is bijvoorbeeld $I = \langle 2+i \rangle$ een priemideaal. Want $N(2+i) = 5$ en dus is $2+i$ een priemelement van $\mathbb{Z}(i)$. De factorring $\mathbb{Z}(i)/I \cong \mathbb{Z}_5$ is inderdaad een veld.