

(6.13) Korollar. *I en kvadratisk talring $R = \mathbb{Z}[\xi]$ eksisterer irreducible opløsninger for alle elementer.*

Bevis. Dette følger af Bemærkning (5.14), idet vi som funktion $\nu: R \rightarrow \mathbb{Z}$ kan bruge funktionen $\nu(\alpha) := |\mathbf{N}(\alpha)|$. Øjensynlig er ν nedad begrænset, og det følger af Sætning (6.12), at hvis δ er en ikke-triviell divisor i α , så er $\nu(\delta) < \nu(\alpha)$. \square

(6.14) Irreducible elementer. En delvis oversigt over primelementer og irreducible elementer $x + y\xi$ i en kvadratisk talring $R = \mathbb{Z}[\xi]$ er indeholdt i følgende to resultater:

(1) *Antag, at $\pi = x + y\xi$, hvor de hele tal x, y er primiske. Da er π et primelement i R , hvis og kun hvis $\mathbf{N}(\pi) = \pm p$, hvor p er et primtal.*

„hvis“: I beviset skal vi bruge, for et naturligt tal n , at kvotientringen $R/(n)$ er en endelig ring med n^2 elementer. Hertil bemærkes, at hovedidealet (n) består af alle tal $ns + nt\xi$, altså af alle tal $u + v\xi \in R$, hvor u og v er delelige med n . Modulo (n) er hvert element $u + v\xi \in R$ altså kongruent med ét af de n^2 elementer af formen $q + r\xi$, hvor $0 \leq q, r \leq n - 1$.

Antag nu for et primtal p , at $\mathbf{N}(\pi) = \pm p$, altså $p = \pm \pi \pi'$. Specielt er π så en ikke-trivell divisor i p , og derfor er $(p) \subset (\pi) \subset R$. Nu var $|R/(p)| = p^2$, og af inklusionerne følger, at ordenen af $R/(\pi)$ er en ikke-trivell divisor i ordenen af $R/(p)$. Altså er $|R/(\pi)| = p$. Som bekendt er en ring med p elementer et legeme. Derfor er $R/(\pi)$ et legeme, og specielt et integritetsområde. Altså er (π) et primideal, og derfor er π et primelement.

„kun hvis“: Antag, at π er et primelement. Det hele tal $\mathbf{N}(\pi)$ er ikke nul og ikke ± 1 , så $\mathbf{N}(\pi)$ kan skrives som et fortegn gange et produkt af primtal. Da $\pi \pi' = \mathbf{N}(\pi)$, går π op i dette produkt, og dermed i en af faktorerne. Der findes altså et primtal p således, at π går op i p , dvs $p = \pi \delta$ med et element $\delta \in R$. Heraf fås $p^2 = \mathbf{N}(\pi) \mathbf{N}(\delta)$. Da π ikke er en enhed, er $\mathbf{N}(\pi) = \pm 1$ udelukket. Hvis $\mathbf{N}(\delta) = \pm 1$, ville δ være en enhed, og ligningen $\pi = \delta^{-1} p$ ville være i modstrid med, at x, y var primiske. Altså er også $\mathbf{N}(\delta) = \pm 1$ udelukket. Af ligningen $p^2 = \mathbf{N}(\pi) \mathbf{N}(\delta)$ følger derfor, at $\mathbf{N}(\pi) = \pm p$, som ønsket.

(2) *Lad p være et primtal. Da er p irreducibelt i R , hvis og kun hvis den diofantiske ligning,*

$$x^2 - bxy + cy^2 = \pm p, \quad (6.14.1)$$

ikke har løsninger $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Yderligere er p et primelement i R , hvis og kun hvis kongruensen,

$$z^2 - bz + c \equiv 0 \pmod{p}, \quad (6.14.2)$$

ikke har løsninger $z \in \mathbb{Z}$.

Antag først, at ligningen (6.14.1) har en løsning (x, y) , svarende til et element $\pi = x + y\xi$ i R således, at $\mathbf{N}(\pi) = \pm p$. Da er $p = \pm \mathbf{N}(\pi) = \pm \pi \pi'$. Specielt er p altså reducibelt (dvs ikke irreducibelt) i R . Antag omvendt, at p er reducibelt i R , altså at der findes en fremstilling $p = \pi \delta$, hvor π og δ ligger i R og ikke er enheder. Det følger, at $p^2 = \mathbf{N}(\pi) \mathbf{N}(\delta)$. Da $\mathbf{N}(\pi)$ og $\mathbf{N}(\delta)$ er forskellige fra ± 1 , følger det, at de begge er lig med $\pm p$. Vi har altså $\mathbf{N}(\pi) = \pm p$, og $\pi = x + y\xi$ svarer til en løsning (x, y) til ligningen (6.14.1).

Antag dernæst, at kongruensen (6.14.2) har en løsning, altså at der findes hele tal z og d og en ligning $z^2 - bz + c = pd$. Vi har $z^2 - bz + c = \mathbf{N}(z + \xi) = (z + \xi)(z + \xi')$, så specielt

er p divisor i produktet $(z + \xi)(z + \xi')$. Hvis p var et primelement i R , ville p være divisor i en af faktorerne, i modstrid med at intet af tallene,

$$\frac{z + \xi}{p} = \frac{z}{p} + \frac{1}{p}\xi, \quad \frac{z + \xi'}{p} = \frac{z - b}{p} - \frac{1}{p}\xi,$$

tilhører R . Altså er p ikke et primelement i R .

Antag i stedet, at kongruensen ikke har løsninger. For at vise, at p er et primelement, betragtes i R en ligning $p\delta = \alpha\beta$, hvor $\delta \neq 0$. Det skal vises, at p er divisor i α eller i β . Af ligningen følger $p^2 N(\delta) = N(\alpha)N(\beta)$, så specielt går p op i produktet $N(\alpha)N(\beta)$. Da p er et primtal, kan vi antage, at p går op i $N(\alpha)$. Er $\alpha = x + y\xi$, har vi altså kongruensen,

$$x^2 - bxy + cy^2 \equiv 0 \pmod{p}. \quad (6.14.3)$$

Vi påstår, at p er divisor i y . Antag nemlig, indirekte, at p ikke går op i y . Da er restklassen af y modulo p en primisk restklasse. Der findes altså et helt tal w således, at $wy \equiv 1 \pmod{p}$. Multiplicer de to sider af kongruensen (6.14.3) med w^2 . Med $z := wx$ får vi da en løsning til kongruensen (6.14.2), i modstrid med antagelsen. Altså går p op i y . Af kongruensen (6.14.3) slutter vi derfor, at p går op i x^2 , og dermed i x . Altså går p op i $\alpha = x + y\xi$.

(6.15) Eksempel. (1) Betragt Gauss' talring $R := \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$. For normen har vi $N(x + iy) = x^2 + y^2$. Vi har $N(1 + i) = 1^2 + 1^2 = 2$. Da 2 er et primtal, er tallet $1 + i$ altså et primelement i R . Tilsvarende er $N(2 + i) = 2^2 + 1^2 = 5$, så tallet $2 + i$ er et primelement. Det følger også, at primtallene 2 og 5 er reducible i $\mathbb{Z}[i]$. Primtallet 3 er irreducibelt i R , fordi ligningen $x^2 + y^2 = 3$ ikke har heltalsløsninger. Primtallet 3 er endda et primelement i $\mathbb{Z}[i]$, fordi kongruensen $z^2 + 1 \equiv 0 \pmod{3}$ ikke har løsninger.

(2) Betragt ringen $R := \mathbb{Z}[\sqrt{-5}]$, med diskriminant $D = -20$. Med $\xi := \sqrt{-5}$ har vi $N(x + y\xi) = x^2 + 5y^2$. Vi har $N(1 + \sqrt{-5}) = 1 + 5 = 2 \cdot 3$. Ingen elementer i R har øjensynlig norm 2 eller norm 3. Altså kan intet element i R være en ikke-triviell divisor i $1 + \sqrt{-5}$. Tallet $1 + \sqrt{-5}$ er altså et irreducibelt element i R . Af samme grund følger det, at $1 - \sqrt{-5}$ er irreducibel. Da $N(2) = 2^2$ og $N(3) = 3^2$, følger det tilsvarende, at 2 og 3 er irreducible. Vi har altså i $\mathbb{Z}[\sqrt{-5}]$ to irreducible opløsninger af tallet 6,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

(3) Betragt ringen $R := \mathbb{Z}[\sqrt{10}]$, med diskriminant 40. Her er tallene 2 og 5 irreducible. Det skal altså vises, at ligningerne $x^2 - 10y^2 = \pm 2$ og $x^2 - 10y^2 = \pm 5$ ikke har løsninger. For den første ligning regnes modulo 5: for en løsning ville vi få $x^2 \equiv \pm 2$, i modstrid med at et kvadrat modulo 5 er kongruent med 0, 1, eller 4. For den anden ligning regnes modulo 8. Det er klart, at x må være ulige, og følgelig er $x^2 \equiv 1$. Videre er $-10y^2 \equiv 6y^2$ og $6y^2$ er kongruent med 0 når y er lige og kongruent med 6 når y er ulige. Altså er $x^2 - 10y^2$ kongruent med 1 eller 7, i modstrid med at $x^2 - 10y^2 = \pm 5$. Nu følger det videre, at tallet $\sqrt{10}$ er irreducibelt, thi $\sqrt{10}$ har norm -10 , og en ikke-triviell divisor i $\sqrt{10}$ måtte derfor have norm ± 2 eller ± 5 . Vi har altså i $\mathbb{Z}[\sqrt{10}]$ to irreducible opløsninger af tallet 10,

$$10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}.$$