Komplekse tal og polynomier

John Olsen

1 Indledning

Dette sæt noter er forelæsningsnoter til foredraget 'Komplekse tal, polynomier og legemsudvidelser'. Noterne er beregnet til at blive brugt sammen med foredraget.

I afsnit 2 bliver de fundamentale definitioner givet og, vi viser, at de komplekse tal er et legeme. I afsnit 3 tolker vi de komplekse tal geometrisk og giver et argument for eksistens. I afsnit 4 udvider vi den velkendte eksponentialfunktion til de komplekse tal. I afsnit 5 defineres polynomiumsringe og forskellige basale egenskaber ved polynomier. I afsnit 6 defineres de såkaldte cyklotomiske polynomier. De n'te enhedsrødder bliver defineret og deres algebraiske struktur vil blive beskrevet. I afsnit 7 defineres hvad der menes med en legemsudvidelse af $\mathbb{Q}$. Vi vil konstruere specielle legemsudvidelser af $\mathbb{Q}$ kaldet de cyklotomiske legemer ud fra de cyklotomiske polynomier og deres rødder. Tilsidst ser vi lidt på Fermats sidste sætning.

Forudsætningerne for at kunne gå igang med noterne er en vis erfaring med at regne med sin og cos. Hvis man ikke kender til vektorregning, kan man ikke forstå argumentet for eksistens af $\mathbb{C}$ i Bemærkning 3.6, men det er ikke centralt i fremstillingen. Det forudsættes også, at læseren har en vis erfaring med at regne med polynomier.

2 De komplekse tals legeme

I dette afsnit vil vi vise, at $\mathbb{C}$, som defineres senere, udgør et legeme. Vi starter med en del indledende definitioner.

Definition 2.1. En *ring*[1], R, er en mængde, der er udstyret med en addition, $+$ og en multiplikation, $\cdot$, så der gælder, at

1. for alle $r, s \in R$ er $r + s \in R$.
2. for alle $r, s \in R$ er $r \cdot s \in R$.
3. addition er kommutativt: $r + s = s + r$ for alle $r, s \in R$.
4. addition er associativt: $(r + s) + t = r + (s + t)$ for alle $r, s, t \in R$.
5. for alle $r \in R$ eksisterer der et $0 \in R$ så $r + 0 = r$.
6. for alle $r \in R$ eksisterer der et $s \in R$ så $r + s = 0$.
7. multiplikation er associativt: $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ for alle $r, s, t \in R$.
8. multiplikation er distributiv: $(r + s) \cdot t = rt + st$ for alle $r, s, t \in R$.

[1] Strengt taget definerer vi en ring med enhed. I disse noter vil vi, når vi skriver ring, mene ring med enhed.

9. for alle $r \in R$ eksisterer der et $1 \in R$, så $r \cdot 1 = 1 \cdot r = r$.

Definition 2.2. Lad R være en ring. R kaldes en *kommutativ ring*[2], hvis der for alle $r, s \in R$ gælder at $r \cdot s = s \cdot r$.

Definition 2.3. Lad R være en ring. Et *legeme* er en kommutativ ring, hvor der gælder, at for alle $r \neq 0 \in R$ eksisterer et $s \in R$, så $rs = 1$. Hvis ringen ikke er kommutativ kaldes det et *skævlegeme*.

Definition 2.4. Lad R være en (kommutativ) ring. $S \subseteq R$ er en (kommutativ) *delring*, hvis $0, 1 \in S$ og S er en (kommutativ) ring under addition og multiplikation fra R.

Definition 2.5. Lad R være et legeme. $S \subseteq R$ er et *dellegeme*, hvis S er en delring fra R og, hvis S er et et legeme under addition og multiplikation fra R.

Eksempel 2.6. Det tilrådes læseren at tjekke, at alle punkterne i Defintion 2.1 og 2.2 er opfyldt for $\mathbb{Z}$. Det vil sige, at $\mathbb{Z}$ er en kommutativ ring. Endvidere bør læseren tjekke at alle punkterne i Defintion 2.1, 2.2 og 2.3 er opfyldt for $\mathbb{Q}$ og $\mathbb{R}$. Det vil sige, at $\mathbb{Q}$ og $\mathbb{R}$ er legemer. Overvej også, at $\mathbb{Z}$ er en delring af $\mathbb{Q}$ og $\mathbb{Q}$ er et dellegeme af $\mathbb{R}$.

Vi vil nu motivere en udvidelse af de reelle tal. Man lærer tidligt i skolesystemet metoder til at løse ligninger af typen $ax + b = c$, hvor $a, b, c \in \mathbb{R}$, $a \neq 0$, hvor løsningen selvfølgeligt er $x = (c - b)/a$. Senere i forløbet lærer man, hvorledes man løser ligninger af formen $ax^2 + bx + c = 0$, hvor $a, b, c \in \mathbb{R}$, $a \neq 0$. Løsningen til denne ligning er $x = (-b \pm \sqrt{D})/2a$, hvor $D = b^2 - 4ac$. Ligningen har to løsninger hvis $D > 0$, en løsning hvis $D = 0$ og ingen løsninger, hvis $D < 0$.

Specielt har ligningen $x^2 + 1 = 0$ ingen løsning i de reelle tal. Hvis man uden at tænke over, om det har mening indsætter $\sqrt{-1}$ i ligningen, får man $(\sqrt{-1})^2 + 1 = -1 + 1 = 0$. Det betyder at $\sqrt{-1}$ faktisk løser ligningen!

Det vil sige, at vi søger en ring, R, som har følgende tre egenskaber

1. R er et legeme
2. $\mathbb{R} \subseteq R$
3. $\sqrt{-1} \in R$.

Vi definerer en delmængde af R kaldet $\mathbb{C}$ ved

$$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R},\ i = \sqrt{-1}\}.$$

Denne delmængde kaldes *de komplekse tal*. Vi vil indtil videre *antage* at en sådan delmængde eksisterer. Et argument for eksistens gives i Bemærkning 3.6.

Definition 2.7. Lad $z = x + iy \in \mathbb{C}$ være et komplekst tal. x kaldes for realdelen af z og y kaldes for imaginærdelen af z. Real- og imaginærdel betegnes henholdsvis $\Re(z)$ og $\Im(z)$.

For at gøre $\mathbb{C}$ til en ring, skal vi definere en addition og en multiplikation på $\mathbb{C}$.

Definition 2.8. Lad $z, w \in \mathbb{C}$ være givet ved $z = x + iy$ og $w = a + ib$. Da er

[2]Strengt taget definerer vi en kommutativ ring med enhed. I disse noter vil vi, når vi skriver kommutativ ring, mene kommutativ ring med enhed.

1. $z + w = (x + a) + i(y + b)$
2. $zw = (x + iy)(a + ib) = xa - yb + ixb + iya = (xa - yb) + i(xb + ya)$.

Før vi kan se, at $\mathbb{C}$ er et legeme, skal vi have nogle flere regneregler på banen.

Definition 2.9. Lad $z, w \in \mathbb{C}$ være givet ved $z = x + iy$ og $w = a + ib$. Da er

1. $z - w = (x - a) + i(y - b)$
2. $z/w = (x + iy)/(a + ib) = (x + iy)(a - ib)/(a + ib)(a - ib)$
   $= ((xa + yb) + i(ya - xb))/(a^2 + b^2)$, $w \neq 0$
3. $1/z = (x - iy)/(x^2 + y^2)$, $z \neq 0$

Bemærkning 2.10. I definitionen af multiplikation og division skal man frem for at memorere slutformlen i højere grad huske på, hvordan den er udledt.

Definition 2.11. Lad $z \in \mathbb{C}$ være et komplekst tal givet ved $z = x + iy$. Da er *længden* eller *normen* af z givet ved $|z| = \sqrt{x^2 + y^2}$.

Nu kan vi formulere den første vigtige sætning.

Sætning 2.12. $\mathbb{C}$ *er et legeme.*

Proof. Vi skal vise at punkterne 1-9 i Definition 2.1, Definition 2.2 og Definition 2.3 er opfyldt. Punkt 1 og 2 er oplagte per konstruktion af $+$ og $\cdot$. Punkterne 3 og 4 følger af de tilsvarende egenskaber for reelle tal.

For at vise at punkt 5 og 9 er opfyldt lader vi $z \in \mathbb{C}$, $z = x + iy$ være vilkårlig. Hvis vi sætter $0 = 0 + i0$ er $z + 0 = z$. Hvis vi sætter $1 = 1 + i0$, ses det, at $z1 = z$.

For at vise at punkt 6 er opfyldt lader vi $z \in \mathbb{C}$, $z = x + iy$ være vilkårlig. Vi ser at $-z = -x - iy$ opfylder at $z + (-z) = 0$. Punkt 7 og 8 vises ved en direkte udregning, der overlades til læseren.

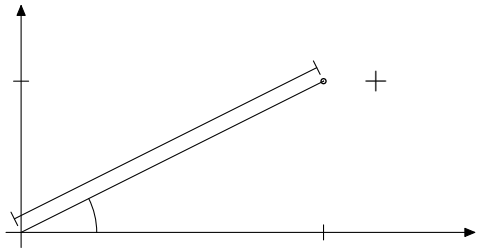
Nu har vi vist, at $\mathbb{C}$ er en ring. Vi skal vise, at $\mathbb{C}$ er en kommutativ ring. Lad $z, w \in \mathbb{C}$ og lad $z = x + iy$ og $w = a + ib$. Da er $zw = (xa - yb) + i(xb + ya)$, men da $x, y, a, b \in \mathbb{R}$ er $xa = ax$, $yb = by$, $xb = bx$ og $ya = ay$. Dermed er $zw = (ax + by) + i(bx + ay) = wz$.

Vi skal tilsidst se, at $\mathbb{C}$ er et legeme. Lad $z \in \mathbb{C}$ være vilkårlig og lad $z = x + iy \neq 0$. Da er $1/z = (x - iy)/(x^2 + y^2)$. Det ses, at $z(1/z) = (x + iy)((x - iy)/(x^2 + y^2)) = (x^2 + y^2)/(x^2 + y^2) = 1$. □

Bemærkning 2.13. Da $i0 = 0$, ses det at $\{x + i0 \mid x \in \mathbb{R}\} = \{x \mid x \in \mathbb{R}\} = \mathbb{R}$. Det betyder, at $\mathbb{R} \subseteq \mathbb{C}$ er et dellegeme. Da i åbenlyst er i $\mathbb{C}$, er $\mathbb{C}$ altså vores ønskede udvidelse af $\mathbb{R}$.

3 Geometrisk fortolkning af $\mathbb{C}$

Casper Wessel, digteren Johan Hermann Wessels bror, var den første til at fortolke den algebraiske struktur geometrisk som punkter i planen, det vil sige at se $x + iy$ som vektoren (x, y).



Figur 1. Den komplekse talplan.

Bemærkning 3.1. Der findes en anden måde at opskrive komplekse tal på. Som det ses på figuren er $z = x + iy$ entydigt givet ved talparret (r, θ), hvor $r = |z|$, og hvor θ er vinklen med den positive 1.-akse. Talparret (r, θ) kaldes opskrivningen af z på polarform. r kaldes modulus for z og θ kaldes argumentet for z og betegnes med henholdsvis $|z|$ og $\arg(z)$. Ud fra figuren kan man også se, at $|z|$ er defineret ud fra Pythagoras sætning.

Lad os se, hvorledes man kan oversætte fra den ene til den anden opskrivning. Det formulerer vi i et lemma.

Lemma 3.2. *Lad $z = x + iy$. Da er $\theta = \cos^{-1}(x/r)$ og $\theta = \sin^{-1}(y/r)$. Hvis $z = 0$, er der uendeligt mange vinkler, der bestemmer z. Længden af z er $r = |z| = \sqrt{x^2 + y^2}$.*

Hvis vi har z opskrevet som (r, θ) er $x = r\cos\theta$ og $y = r\sin\theta$.

Proof. Dette følger direkte fra definitionen af cos og sin. □

Bemærkning 3.3. Læg mærke til at et komplekst tal har én modulus men uendeligt mange argumenter. Det skyldes, at en drejning på 360° eller 2π giver det samme punkt i planen.

Det viser sig at være meget nemmere at multiplicere to komplekse tal, når de er opskrevet på polarform. Det formuleres i følgende proposition.

Proposition 3.4. *Lad $z_1, z_2 \in \mathbb{C}$ og lad $z_1 = (r_1, \theta_1)$ og $z_2 = (r_2, \theta_2)$. Da er $z_1 z_2 = (r_1 r_2, \theta_1 + \theta_2)$*

Proof. Beviset benytter faktisk intet andet end additionsformlerne for sin og cos og definition af multiplikation af to komplekse tal, Definition 2.8. Additionsformlerne for sin og cos ser ud som følger:

$$\begin{aligned} \cos(\theta_1 + \theta_2) &= \cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2), \\ \sin(\theta_1 + \theta_2) &= \cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2). \end{aligned} \tag{1}$$

Beviset for disse to formler udelades.

Vi har set, at hvis $z_1 = (r_1, \theta_1)$ og $z_2 = (r_2, \theta_2)$ er $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ og $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$. Ved at benytte formlen for multiplikation af to komplekse tal, får man

$$\begin{aligned} z_1 z_2 &= (r_1\cos(\theta_1) r_2\cos(\theta_2) - r_1\sin(\theta_1) r_2\sin(\theta_2)) \\ &\quad + i(r_1\cos(\theta_1) r_2\sin(\theta_2) + r_1\sin(\theta_1) r_2\cos(\theta_2)) \\ &= r_1 r_2(\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)) \\ &\quad + i r_1 r_2(\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2)) \\ &= r_1 r_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)), \end{aligned}$$

hvor vi i tredje lighedstegn har brugt additionsformlerne, formel (1) for sin og cos. Vi ser dermed, at $z_1 z_2 = (r_1 r_2, \theta_1 + \theta_2)$, som skulle vises. □

Eksempel 3.5. Lad $z_1 = (8, 11\pi/12)$ og $z_2 = (\frac{1}{2}, 19\pi/12)$. Hvad er $z_1 z_2$? Vi benytter sætningen overfor og får $z_1 z_2 = (4, 5\pi/2) = (4, \pi/2)$. Ved at tegne tallet i den komplekse talplan ses det at $(4, \pi/2)$ svarer til tallet $4i$. Man kunne også oversætte polarformerne til sædvanlig form og så bruge definitionen af multiplikation, men det er meget mere besværligt.

Bemærkning 3.6. Vi vil nu give en skitse af et argument for eksistens af $\mathbb{C}$.

Man identificerer det komplekse tal $x + iy$ med vektoren $(x, y) \in \mathbb{R}^2$ og ser at i svarer til vektoren $(0, 1)$. Addition i $\mathbb{C}$ svarer til sædvanlig vektoraddition i planen. Ved at opskrive $z = x + iy$ og $w = a + ib$ på polarform ses det, at multiplikation også blot er en operation mellem de to tilhørende vektorer.

4 Den komplekse eksponentialfunktion

I dette afsnit udvider vi eksponentialfunktionen til de komplekse tal.

Definition 4.1. Lad $z \in \mathbb{C}$ og lad $z = x + iy$. Da er $e^z = e^x(\cos y + i \sin y)$.

Bemærkning 4.2. Hvis $z = x + i0$ er $e^z = e^x$. Det betyder, at den komplekse eksponentialfunktion er identisk med den velkendte eksponentialfunktion, hvis inputtet er et reelt tal.

Bemærkning 4.3. Hvis man lader $z = i\pi$, får man $e^{i\pi} = e^0(\cos \pi + i \sin \pi)$. Dermed har vi, at $e^{i\pi} = -1$ eller $e^{i\pi} + 1 = 0$. Denne formel kaldes Eulers identitet og den knytter på smukkeste vis tallene e, π, 1 og 0 sammen.

Vi har følgende vigtige sætning om den komplekse eksponentialfunktion.

Sætning 4.4. *Lad $z, w \in \mathbb{C}$. Da er $e^{z+w} = e^z e^w$.*

Proof. Overlades til læseren som en øvelse. □

Sætning 4.5. *Den komplekse eksponentialfunktion er periodisk med periode $2\pi i$, det vil sige for alle $z \in \mathbb{C}$, er $e^z = e^{z+2\pi i}$.*

Proof. Dette er klart, idet sin og cos er 2π periodiske. □

Bemærkning 4.6. Hvis $\theta \in \mathbb{R}$ er $e^{i\theta} = \cos\theta + i \sin\theta$ per definition af eksponentialfunktionen. Hvis $z = (r, \theta)$ har vi set, at vi kan omskrive z, så $z = r(\cos\theta + i \sin\theta)$. Dermed er $z = re^{i\theta}$. Dette giver os endnu en let måde at multiplicere komplekse tal på. Hvis $z_1 = (r_1, \theta_1)$ og $z_2 = (r_2, \theta_2)$ er $z_1 z_2 = r_1 e^{i\theta_1} r_2 e^{i\theta_2} = r_1 r_2 e^{i(\theta_1+\theta_2)}$. Vi har undervejs brugt Sætning 4.4.

Tilsidst viser vi en vigtig formel opkaldt efter den franske matematiker Abraham de Moivre.

Sætning 4.7 (de Moivres formel). *Lad $\theta \in \mathbb{R}$ og lad $n \in \mathbb{N}$. Da er*

$$(\cos(\theta) + i \sin(\theta))^n = \cos(n\theta) + i \sin(n\theta).$$

Proof. Per definition af den komplekse eksponentialfunktion er $e^{i\theta} = \cos(\theta) + i \sin(\theta)$. Ved at benytte Sætning 4.4 n gange får vi, at $(e^{i\theta})^n = e^{in\theta}$. Dermed er $(\cos(\theta) + i \sin(\theta))^n = \cos(n\theta) + i \sin(n\theta)$, som skulle vises. □

5 Polynomier

I dette afsnit vil vi se lidt nærmere på polynomier med koefficienter i en kommutativ ring. Vi vil se at denne mængde faktisk igen er en ring. Vi vil se nærmere på polynomiet $x^n - 1$ og rødderne for dette polynomium, der kaldes de n'te enhedsrødder. Vi vil også se nærmere på deres algebraiske struktur. Tilsidst konstrueres de cyklotomiske polynomier ud fra de n'te enhedsrødder.

Lad i det følgende R være en kommutativ ring.

Definition 5.1. R er et integritetsområde, hvis der for $s, t \in R$ med $st = 0$ gælder, at enten $s = 0$ eller $t = 0$.

Bemærkning 5.2. Det tilrådes læseren at overveje at alle ringene $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$ er integritetsområder. Faktisk gælder det også, at alle legemer er integritetsområder.

I det følgende vil vi antage at R er et integritetsområde.

Definition 5.3. Polynomiumsringen $R[x]$ er

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_0, \ldots, a_n \in R\}.$$

Multiplikationen og additionen i polynomiumsringen er for $f = a_0 + a_1 x + \cdots + a_n x^n$ og $g = b_0 + b_1 x + \cdots + b_m x^m$ givet ved (antag at $m \leq n$ og $b_i = 0$ hvis $i > m$)

$$\begin{aligned} f + g &= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \\ fg &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 a_2 b_0)x^2 + \cdots + a_n b_n x^{n+m}. \end{aligned} \tag{2}$$

Lemma 5.4. *Polynomiumsringen $R[x]$ er et integritetsområde.*

Proof. Overlades til læseren. □

Definition 5.5. Lad $f \neq 0 \in R[x]$. Graden af $f = a_0 + a_1 x + \cdots + a_n x^n$ er

$$\deg(f) = \max\{n \mid a_n \neq 0\}.$$

Hvis $m = \deg(f)$ og $a_m = 1$ kaldes f et monisk polynomium.

Proposition 5.6 (Gradformlen). *Lad $f, g \in R[x] \setminus \{0\}$. Da gælder, at*

$$\deg(fg) = \deg(f) + \deg(g).$$

Proof. Overlades til læseren. □

Begreberne division, 'rest' og 'går op i' giver også mening i en vilkårlig polynomiumsring. Dette formuleres i følgende proposition.

Proposition 5.7. *Lad $g \in R[x]$ være et monisk polynomium. Givet et $f \in R[x]$ eksisterer der et $r \in R[x]$, så*

$$f = qg + r,$$

hvor $q \in R[x]$ og enten $r = 0$ eller $\deg(r) < \deg(g)$, hvis $r \neq 0$.

Bemærkning 5.8. r kaldes resten. Hvis $r = 0$ siges g at 'gå op i' f. Dette betegnes $g \mid f$. Hvis $r \neq 0$ går g ikke op i f. Det betegnes $g \nmid f$

Definition 5.9. Lad $\alpha \in R$ og $f \in R[x]$. α kaldes en rod for f hvis $f(\alpha) = 0$. Multipliciteten af α som rod er det største $n \in \mathbb{N}$, så $(x - \alpha)^n \mid f$.

Nu kan vi formulere en vigtig sætning om polynomier i $\mathbb{C}[x]$. Motivationen for at konstruere $\mathbb{C}$ var, at man i $\mathbb{C}$ havde løsning til ligningen $x^2 + 1 = 0$. Faktisk viser det sig at i $\mathbb{C}$ har et n'te-gradspolynomium præcis n rødder talt med multiplicitet. Dette formuleres i næste sætning.

Sætning 5.10 (Algebraens fundamentalsætning). *Ethvert polynomium $f \in \mathbb{C}[x]$ af grad n, $f = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$, har præcist n komplekse rødder talt med multiplicitet.*

Proof. Udelades. □

Bemærkning 5.11. Hvis vi lader $\{\alpha_1, \ldots, \alpha_n\}$ være de ikke nødvendigvis forskellige rødder for f fremgår det også fra Algebraens fundamentalsætning, at f kan skrives som $f = a_n(x - \alpha_1) \cdots (x - \alpha_n)$.

Bemærkning 5.12. Sætning 5.10 siger intet om, hvordan man finder disse rødder. Faktisk kan man vise, at der kun findes en eksplicit løsningsformel for løsning af ligninger af grad mindre end eller lig 4! Dette blev vist af den norske matematiker Niels Henrik Abel.

Bemærkning 5.13. Hvis man rent praktisk skal finde q og r, vil man oftest benytte polynomiers division. Denne metode er kendt fra skolen, hvis ringen er $\mathbb{Z}, \mathbb{Q}$ eller $\mathbb{R}$, men metoden virker også for f, g i en vilkårlig polynomiumsring.

Definition 5.14. En enhed i en ring R er et element der har en multiplikativ invers. Mængden af enheder betegnes R^*. Mere formelt er

$$R^* = \{u \in R \mid \exists v \in R \colon uv = 1\}$$

Eksempel 5.15. Enhederne i $\mathbb{Z}$ er ± 1. Enhederne i et legeme L er ifølge definitionen af et legeme $L \setminus \{0\}$. Enhederne i $L[x]$ er også $L \setminus \{0\}$, dvs. de konstante ikke 0 polynomier.

Sidste bemærkning følger af næste proposition, da legemer er integritetsområder.

Proposition 5.16. *Lad R være en ring. Da er $R^* = R[x]^*$.*

Proof. Da $R \subseteq R[x]$ er det klart at $R^* \subseteq R[x]^*$.

Lad $f \in R[x]^*$. Da eksisterer $g \in R[x]$, så $fg = 1$. Da $R[x]$ er et integritetesområde får vi fra gradformlen, at $\deg(f) = \deg(g) = 0$. Dette betyder at $f, g \in R$ og dermed, at $f, g \in R^*$. Dermed er $R[x]^* \subseteq R^*$. □

Definition 5.17. Et element, s, i en ring R kaldes irreducibelt hvis $s \neq 0$, $s \notin R^*$ og hvis $u, v \in R$ og $s = uv$, er enten u eller v en enhed.

Definition 5.18. Et $x \neq 0 \in R \setminus R^*$ siges at have en faktorisering i irreducible elementer, hvis der eksisterer $p_1, \ldots, p_r \in R$, så $x = p_1 \cdots p_r$.

x siges at have entydig faktorisering i irreducible elementer, hvis der for enhver anden faktorisering $x = p_1 \cdots p_r = q_1 \cdots q_s$ gælder at ethvert p_i for $i = 1, \ldots r$ går op i et q_j for et $j = 1, \ldots, s$.

En ring R kaldes et entydigt faktoriseringsområde hvis der for alle $x \neq 0 \in R \setminus R^*$ gælder at de har entydig faktorisering i irreducible elementer.

Eksempel 5.19. De irreducible elementer i $\mathbb{Z}$ er $\pm p$, hvor p er et primtal. Faktisk gælder at et element i $\mathbb{Z}$ er irreduciblet hvis og kun hvis det er et primtal.

De irreducible polynomier i $\mathbb{C}[x]$ er polynomier, f, på formen $f = ug$, hvor g er et monisk 1.-gradspolynomium, u en enhed i $C[x]$; idet vi ved (Algebraens fundamentalsætning) at alle polynomier f splitter i et produkt af førstegradspolynomier og disse ikke er enheder i $\mathbb{C}[x]$.

Eksempler på irreducible polynomier i $\mathbb{Q}[x]$ er x^2-2 og x^2+1. x^2+1 er også et eksempel på er irreducibelt polynomium i $\mathbb{R}[x]$.

Vi skal senere se på polynomier i $\mathbb{Z}[x]$. Vi ønsker et kriterium der afgør hvorvidt disse polynomier er irreducible i $\mathbb{Q}[x]$. Et sådant kriterium formulerer vi i næste sætning.

Sætning 5.20 (Eisensteins kriterium). *Lad $f = a_0 + a_1x + \cdots + a_nx^n$ være et polynomium med $\deg(f) > 0$ i $\mathbb{Z}[x]$. Hvis der eksisterer et primtal $p \in \mathbb{Z}$, så $p \nmid a_n$, $p \mid a_i$ for alle $i < n$ og $p \nmid a_0^2$, er f irreducibelt i $\mathbb{Q}[x]$.*

Proof. Udelades. □

6 Cyklotomiske polynomier og n'te enhedsrødder

I dette afsnit vil vi behandle nogle specielle polynomier kaldet de cyklotomiske polynomier. Den danske oversættelse af cyklotomisk er cirkeldeling, så på dansk kaldes disse polynomier for cirkeldelingspolynomier.

Definition 6.1. En n'te enhedsrod er et $\alpha \in \mathbb{C}$, så $\alpha^n = 1$. En primitiv n'te enhedsrod er et $\alpha \in \mathbb{C}$, så $\alpha^n = 1$, men hvor $\alpha^d \neq 1$ for $1 \leq d < n$. En enhedsrod er et element der er en m'te enhedsrod for et $m \in \mathbb{N}$.

Notation 6.2. Vi sætter $\zeta_n = e^{i2\pi/n}$ og $\zeta_n^k = (\zeta_n)^k = e^{i2\pi k/n}$

Bemærkning 6.3. De n'te enhedsrødder er tallene ζ_n^k, $k \in \mathbb{N}$. Fra regneregler for eksponentialfunktionen fås $(\zeta_n^k)^n = (e^{i2\pi k/n})^n = e^{i2\pi kn/n} = e^{i2\pi k} = e^{i2\pi} = 1$, da exp er 2π-periodisk.

Per definition af n'te enhedsrødder er de n'te enhedsrødder nulpunkterne for polynomiet $x^n - 1$. Algebraens fundamentalsætning medfører, at der er præcist n forskellige n'te enhedsrødder. Det betyder, at ζ_n^k, $1 \leq k \leq n$ er de n n'te enhedsrødder. Fra Bemærkning 5.11 får man, at

$$x^n - 1 = \prod_{k=1}^{n}(x - \zeta_n^k),$$

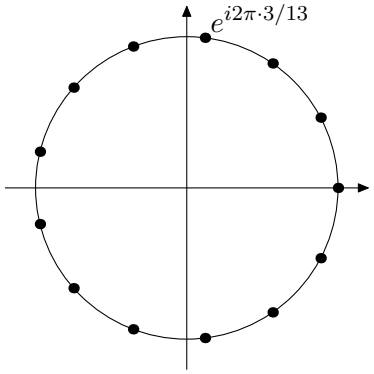
da $x^n - 1$ er monisk.

Bemærkning 6.4. Tallene $C_n = \{\zeta_n^k\}_{k=1}^n$ udgør en gruppe under multiplikation. Det vil sige, at følgende gælder

1. $1 \in C_n$, nemlig $\zeta_n^n = e^{i2\pi n/n} = 1$
2. $\zeta_n^{k_1}\zeta_n^{k_2} \in C_n$, idet $\zeta_n^{k_1}\zeta_n^{k_2} = e^{i2\pi k_1/n}e^{i2\pi k_2/n} = e^{i2\pi(k_1+k_2)/n} = \zeta_n^{(k_1+k_2)} = \zeta_n^j \in C_n$, hvor j er resten af $k_1 + k_2$ ved division med n.
3. For hvert $\zeta_n^{k_1}$ eksisterer der et inverselement, $\zeta_n^{k_2}$, så $\zeta_n^{k_1}\zeta_n^{k_2} = 1$. Tallet k_2, $1 \leq k_2 \leq n$, er bestemt af at $k_1 + k_2 = n$.

Faktisk er C_n frembragt af ζ_n, da de andre elementer er potenser af ζ_n. Da siges C_n at være en cyklisk gruppe frembragt af ζ_n.

Eksempel 6.5. For $n = 13$ ser enhedsrødderne således ud:



Figur 2.

$C_{13} = \{\zeta_{13}^k\}_{k=1}^{13}$ er de 13 13'ende enhedsrødder. Vi ser, at $e^{i2\pi 13/13} = e^{i2\pi} = 1$. Betragt for eksempel $e^{i2\pi 8/13} = \zeta_{13}^8$ og $e^{i2\pi 7/13} = \zeta_{13}^7$. Da er $\zeta_{13}^8\zeta_{13}^7 = \zeta_{13}^{15} = \zeta_{13}^2$, da 2 er resten af 15 ved division med 13. $\zeta_{13}^2 \in C_{13}$. Betragt for eksempel $e^{i2\pi 6/13} = \zeta_{13}^6$. Da er $e^{i2\pi 7/13} = \zeta_{13}^7$ inverselement til ζ_{13}^6, idet $\zeta_{13}^6\zeta_{13}^7 = \zeta_{13}^{13} = 1$.

Definition 6.6. Lad $a, b \in R$. En fælles divisor af a, b er et $c \in R$, så $c \mid a$ og $c \mid b$. En største fælles divisor er en fælles divisor d, så der for alle fælles divisorer c af a, b gælder at $c \mid d$. En største fælles divisor af a, b betegnes $\gcd(a, b)$. Hvis $\gcd(a, b) = 1$ siges a, b at være indbyrdes primiske.

Definition 6.7. Polynomiet

$$\Phi_n = \prod_{\substack{k=1 \\ \gcd(n,k)=1}}^{n} (x - \zeta_n^k)$$

kaldes det n'te cyklotomiske polynomium.

Vi vil nu formulere to resultater vedrørende de cyklotomiske polynomier.

Lemma 6.8. *$\Phi_n \in \mathbb{Z}[x]$ for alle $n \in \mathbb{N}$, $n \geq 1$.*

Proof. Udelades. □

Sætning 6.9. *Φ_n er irreducibelt i $\mathbb{Q}[x]$ for alle $n \in \mathbb{N}$, $n \geq 1$.*

Proof. Udelades. □

Bemærkning 6.10. Man kan vise at

$$x^n - 1 = \prod_{d|n} \Phi_d.$$

Denne formel giver en iterativ procedure til at finde de cyklotomiske polynomier.

Eksempel 6.11. Nu vil vi explicit beregne de første 4 cyklotomiske polynomier.

Den første enhedsrod er klart 1, så $\Phi_1 = x - 1$. Den anden enhedrod er -1, så fra formlen $x^n - 1 = \prod_{d|n} \Phi_d$ fås at $\Phi_2 = (x^2 - 1)/(x - 1) = x + 1$. Da $2 \nmid 3$ er $\Phi_3 = (x^3 - 1)/\Phi_1 = x^2 + x + 1$. Tilsvarende haves at $3 \nmid 4$, så $\Phi_4 = (x^4 - 1)/\Phi_1\Phi_2 = x^2 + 1$.

7 Legemsudvidelser

Hvis vi er interesseret i at finde rødderne for et polynomium $f \in \mathbb{Q}[x]$, skal vi så lede i hele $\mathbb{C}$, hvor vi ved at vi kan finde alle rødderne, eller kan vi nøjes med et dellegeme af $\mathbb{C}$. Det er klart at vi ikke kan være sikre på at rødderne altid er reelle, et modeksempel på dette er polynomiet $x^2 + 1$, der jo har rødder $\pm i$. Vi vil betragte de cyklotomiske polynomier og konstruere udvidelseslegemer af $\mathbb{Q}$ med hensyn til disse polynomier. Dette udvidelseslegeme vil per konstruktion indeholde alle rødderne for polynomiet og vil være et dellegeme af $\mathbb{C}$. Disse legemer kaldes de cyklotomiske legemer.

Definition 7.1. En legemsudvidelse $L \subset \mathbb{Q}$ er et legeme L, så $\mathbb{Q}$ er et dellegeme af L.

Eksempel 7.2. $\mathbb{C} \supset \mathbb{Q}$ og $\mathbb{R} \supset \mathbb{Q}$ er begge legemsudvidelser af $\mathbb{Q}$.

Definition 7.3. Lad $\zeta_n = e^{i2\pi/n}$ som før. Vi definerer

$$\mathbb{Q}(\zeta_n) = \{a_0 + \zeta_n a_1 + \zeta_n^2 a_2 + \cdots + \zeta_n^{n-2} a_{n-2} \mid a_i \in \mathbb{Q}\}$$

Proposition 7.4. *$\mathbb{Q}(\zeta_n)$ er et dellegeme af $\mathbb{C}$.*

Proof. Udelades, se eksemplet nedenfor. □

Bemærkning 7.5. Bemærk at rødderne for både Φ_n og $x^n - 1$ som ønsket er elementer i $\mathbb{Q}(\zeta_n)$.

Bemærkning 7.6. Man kan måske undre sig over hvorfor linearkombinationen stopper ved $n - 2$. For at se dette skal vi bruge polynomiers division. Det overlades til læseren at overveje at følgende er rigtigt.

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

Ved indsættelse af ζ_n i ligningen fås

$$\zeta_n^n - 1 = (\zeta_n - 1)(\zeta_n^{n-1} + \zeta_n^{n-2} + \cdots + \zeta_n + 1)$$

$\zeta_n^n - 1 = 0$ per definition af ζ_n. $\zeta_n - 1 \neq 0$, da ζ_n er en frembringer for den cykliske gruppe C_n. Dermed er $0 = \zeta_n^{n-1} + \zeta_n^{n-2} + \cdots + \zeta_n + 1$ og dermed er $\zeta_n^{n-1} = -\zeta_n^{n-2} - \cdots - \zeta_n - 1$. Dermed er $\zeta_n^{n-1} \in \mathbb{Q}(\zeta_n)$.

Eksempel 7.7. Vi vil gennemregne beviset for Proposition 7.4 i tilfældet $n = 3$. Først ser vi at $\mathbb{Q}(\zeta_3) = \{a + b\zeta_3 \mid a, b \in \mathbb{Q}\}$, ifølge bemærkningen ovenfor, idet vi har faktoriseringen $x^3 - 1 = (x - 1)(x^2 + x + 1)$. Dermed er $\zeta_3^2 = -\zeta_3 - 1$.

Da $\mathbb{Q}(\zeta_3)$ skal være et dellegeme af $\mathbb{C}$ skal vi se at $\mathbb{Q}(\zeta_3)$ er lukket under multiplikation og addition fra $\mathbb{C}$. Det er oplagt at $\mathbb{Q}(\zeta_3)$ er lukket under addition. Vi skal se at $\mathbb{Q}(\zeta_3)$ er lukket under multiplikation fra $\mathbb{C}$. Det følger fra udregningen $(a_1 + a_2\zeta_3)(b_1 + b_2\zeta_2) = a_1b_1 + a_1b_2\zeta_3 + b_1a_2\zeta_3 + a_2b_2\zeta_3^2 = a_1b_1 + a_1b_2\zeta_3 + b_1a_2\zeta_3 + a_2b_2(-\zeta_3 - 1) = (a_1b_1 - a_2b_2) + (a_1b_2 + b_1a_2 - a_2b_2)\zeta_3 \in \mathbb{Q}(\zeta_3)$. Da $0, 1 \in \mathbb{Q}(\zeta_3)$ er $\mathbb{Q}(\zeta_3)$ en delring af $\mathbb{C}$. $\mathbb{Q}(\zeta_3)$ er en kommutativ delring af $\mathbb{C}$ da $\mathbb{Q}$ er en kommutativ ring. Beviset for dette er det samme som beviset for, at $\mathbb{C}$ er en kommutativ ring.

Vi skal se at $\mathbb{Q}(\zeta_3)$ er et dellegeme af $\mathbb{C}$. Det vil sige givet $a + b\zeta_3 \neq 0 \in \mathbb{Q}(\zeta_3)$ skal vi finde $x + y\zeta_3 \in \mathbb{Q}(\zeta_3)$, så $(a + b\zeta_3)(x + y\zeta_3) = 1$. Ved at multiplicere fås $ax + (ay + bx)\zeta_3 + by\zeta_3^2 = 1$. Ved at bruge $\zeta_3^2 = -\zeta_3 - 1$ fås $ax - by + (ay + bx - by)\zeta_3 = 1$. Dermed

skal vi løse ligningerne $ax - by = 1$ og $ay + bx - by = 0$. Dette kan gøres ved hjælp af den velkendte determinantmetode eller ved følgende indsættelsesmetode. Detaljerne i disse udregninger overlades til læseren. Ved isolering af x i den første ligning fås $x = (1+by)/a$. Da $a + b\zeta_3 \neq 0$ kan vi uden tabt af generalitet antage at $a \neq 0$. Ved indsættelse i den anden ligning fås $y = -b/(a^2 + b^2 - ab)$. Ved indsættelse af dette i den anden ligning fås $x = 1/a - b^2a/(a^2 + b^2 - ab)$. Det vil sige at det ønskede inverselement til $a + b\zeta_3$ er $1/a - b^2a/(a^2 + b^2 - ab) - (b/(a^2 + b^2 - ab))\zeta_3$.

En meget berømt sætning i matematikken er Fermats sidste sætning.

Sætning 7.8 (Wiles, 1994). *Lad $x, y, z \in \mathbb{Z}$ og $n \in \mathbb{N}$. Ligningen $x^n + y^n = z^n$ har ingen løsninger x, y, z med $x, y, z \neq 0$ for $n > 2$.*

Der er umiddelbart ingen sammenhæng mellem Fermats sidste sætning og teorien for enhedsrødder og uvidelseslegemer vi hidtil har set lidt på. Men ved at gå 100 år tilbage i matematikhistorien finder vi en interessant og vigtig sammenhæng.

Den franske matematiker Lame viste følgende specialtilfælde af Fermats sidste sætning.

Sætning 7.9 (Euler, Lame). *Lad $x, y, z \in \mathbb{Z}$. Ligningen $x^3+y^3 = z^3$ har ingen løsninger for $x, y, z \in \mathbb{Z}$ med $x, y, z \neq 0$.*

Bemærkning 7.10. Lames bevis benytter et virkeligt smart trick. I stedet for kun at betragte ligningen over $\mathbb{Z}$ betragtede han den over den større ring $\mathbb{Z}[\zeta_3] = \{a+\zeta_3 b \mid a, b \in \mathbb{Z}\}$. Beviset for, at $\mathbb{Z}[\zeta_3]$ faktisk er en kommutativ delring af $\mathbb{C}$, er helt det samme som beviset for, at $\mathbb{Q}(\zeta_3)$ er en kommutativ delring af $\mathbb{C}$. Undervejs i beviset bruges igen at $\zeta_3^2 = \zeta_3 - 1$. Detaljerne overlades til læseren. I denne ring har man nemlig den (entydige) faktorisering

$$x^3 + y^3 = (x + y)(x + \zeta_3 y)(x - \zeta_3^2 y).$$

Med lidt mere teori end vi kan give her, er det let at vise, at der ikke findes tal $x, y, z \in \mathbb{Z}[\zeta_3]$, $x, y, z \neq 0$, så $(x + y)(x + \zeta_3 y)(x - \zeta_3^2 y) = z^3$.

For p et primtal med $p > 3$ betragtede Lame ringen $\mathbb{Z}[\zeta_p] = \{a_0 + \zeta_p a_1 + \cdots \zeta_p^{p-2} a_{p-2} \mid a, b \in \mathbb{Z}\}$. I denne ring har man faktoriseringen

$$x^p + y^p = (x + y)(x + \zeta_p y) \cdots (x - \zeta_p^{p-1} y).$$

Lames troede, at han havde vist Fermats sidste sætning for alle primtal p, men der var en fejl i Lames bevis. Fejlen var at han antog at $\mathbb{Z}[\zeta_p]$ er et entydigt faktoriseringsområde for alle primtal p. Det er generelt forkert, men rigtigt i ringen $\mathbb{Z}[\zeta_3]$.

Den tyske matematiker Kummer opdagede fejlen og gav et bevis for Fermats sidste sætning under forudsætning at eksponenten p er et primtal, der opfylder noget bestemt, som det vil føre for vidt at komme ind på her.

Bemærkning 7.11. I Bemærkning 5.12 bemærkede vi at der ingen eksplicit formel er til at finde rødderne for et 5.-grads polynomium. Der er en stor og udviklet teori for legemsudvidelser og det er denne teori man benytter til at bevise dette faktum. Denne teori kaldes også Galois teori efter den store franske matematiker Evariste Galois. De cyklotomiske legemer er eksempler på det man kalder for Galois udvidelser af $\mathbb{Q}$.

8 Øvelser

Opgaver mærket med ($\star$) er svære.

Øvelse 8.1. Det komplekse tal z har modulus π og argument π. Opskriv z på formen $x + iy$. Tegn z i den komplekse plan.

Øvelse 8.2. Lad $z = 1 + i$.

1. Opskriv z på polarform.
2. Beregn z^6. Skriv resultatet på formen $x + iy$.
3. Tegn z og z^6 i den komplekse plan.

Øvelse 8.3. Lad $z = -\sqrt{3} + i$.

1. Opskriv z på polarform.
2. Beregn z^4. Skriv resultatet på formen $x + iy$.
3. Tegn z og z^4 i den komplekse plan.

Øvelse 8.4. Lad $z = 1 + 2i$, $w = 2 - i$ og $v = -1 + 3i$.

1. Tegn z, w, v i den komplekse plan.
2. Beregn $1/z$, $1/w$ og $1/v$ og tegn $1/z$, $1/w$ og $1/v$ i den komplekse plan.
3. Opskriv z, w og v på polarform.
4. Beregn produktet zwv. Tegn produktet zwv i den komplekse plan.

Øvelse 8.5. Tegn mængden $\{z \in \mathbb{C} \mid z = e^{i\theta},\ \theta \in [0, 2\pi]\}$ i den komplekse talplan.

Øvelse 8.6. ($\star$) Lad $z, w \in \mathbb{C}$. Vis at $zw = 0$ hvis og kun hvis $z = 0$ eller $w = 0$. Vink til $\Rightarrow$: Hvis $s, t \in \mathbb{R}$ og $st = 0$ medfører det, at $s = 0$ eller $t = 0$. Skriv $z = x + iy$ og $w = a + ib$ og brug Definition 2.8 til at slutte det ønskede.

Øvelse 8.7. Lad D være et område i den komplekse plan givet i polære koordinater ved

$$D = \left\{ (r, \theta) \mid 1 \leq r \leq 2,\ \frac{5\pi}{6} \leq \theta \leq \frac{5\pi}{3} \right\}.$$

1. Tegn området D i den komplekse plan.
2. Find de fire hjørner z_1, z_2, z_3 og z_4 i D og skriv dem på formen $re^{i\theta}$ og $x + iy$.
3. Beregn produktet $z_1 z_2 z_3 z_4$ og angiv resultatet på tegningen i (1).
4. ($\star$) Find den reelle og komplekse faktorisering af polynomiet $z^3 + 1$.
5. ($\star$) Find alle komplekse tal z, der løser ligningen $e^{3z} = -1$. Hint: Brug (4).

Øvelse 8.8. ($\star$) I denne øvelse skal vi vise Sætning 4.4. Lad $z, w \in \mathbb{C}$ og $z = x + iy$, $w = a + ib$.

1. Opskriv e^z og e^w.

2. Beregn produktet $\mathrm{e}^z\,\mathrm{e}^w$ og benyt additionsformlerne, formel (1), for sin og cos til at vise Sætning 4.4.

Øvelse 8.9. ($\star$) Vis Lemma 5.4. Overvej også, at $R[x]$ er et integritetsområde.

Øvelse 8.10. ($\star$) Benyt formlen for produkt af to polynomier, formel (2), til at vise gradformlen. Overvej at formlen ikke gælder hvis R ikke er et integritetsområde. (Hint: Benyt igen formlen for et produkt af to polynomier, formel (2).)

Øvelse 8.11.

1. Opskriv elementerne i C_6.

2. Tegn elementerne i C_6 i et koordinatsystem.

3. ($\star$) Vis, at C_6 udgør en gruppe.

Øvelse 8.12. Lad Φ_n være det n'te cyklotomiske polynomium.

1. Vis ved hjælp af Eisensteins kriterium at Φ_3 og Φ_4 er irreducible i $\mathbb{Q}(x)$.

2. Beregn Φ_5 og Φ_6.

Øvelse 8.13. ($\star$) Det gælder generelt at $f \in \mathbb{Z}[x]$ er irreducibelt i $\mathbb{Q}[x]$ hvis og kun hvis der for $a, b \in \mathbb{Z}$, $a \neq 0$ gælder at $f(ax+b)$ er irreducibelt i $\mathbb{Q}[x]$.

1. Vis, ved hjælp af Eisensteins kriterium at polynomiet $x^4 + x^3 - 3x^2 - 5x + 4$ er irreducibelt i $\mathbb{Q}[x]$. Hint: substituer x med $x - 1$

2. Vis, at polynomiet $x^4 - 6x^2 + 8x + 7$ er irreducibelt i $\mathbb{Q}[x]$. Hint: substituer x med $x + 1$.