
KTH Engineering Sciences

KTHs Matematiska Cirkel

# Polynom

Dan Petersen
Kathrin Vorwerk

Institutionen för matematik, 2010
Finansierat av Marianne och Marcus Wallenbergs Stiftelse

# Innehåll

# Några ord på vägen

Detta kompendium är skrivet för att användas som litteratur till KTHs Matematiska Cirkel under läsåret 2010–2011 och består av sju avsnitt samt ett inledande avsnitt om mängdlära. Kompendiet är inte tänkt att läsas enbart på egen hand, utan ska ses som ett skriftligt komplement till undervisningen på de sju träffarna.

Som den mesta matematik på högre nivå är kompendiet kompakt skrivet. Detta innebär att man i allmänhet inte kan läsa det som en vanlig bok. Istället bör man pröva nya satser och definitioner genom att på egen hand exemplifiera. Därmed uppnår man oftast en mycket bättre förståelse av vad dessa satser och deras bevis går ut på.

Övningsuppgifterna är fördelade i två kategorier. De med udda nummer har facit, och syftet med dessa är att eleverna ska kunna räkna dem och på egen hand kontrollera att de förstått materialet. De med jämna nummer saknar facit och kan användas som examination. Det rekommenderas dock att man försöker lösa även dessa uppgifter även om man inte examineras på dem. Om man kör fast kan man alltid fråga en kompis, en lärare på sin skola eller någon av författarna.

Vi bör också nämna att få av uppgifterna är helt enkla. Kika därför inte i facit efter några få minuter, om du inte löst uppgiften, utan prata först med kompisar eller försök litet till. Alla uppgifter ska gå att lösa med hjälp av informationen i detta kompendium.

KTHs Matematiska Cirkel finansieras av Marianne och Marcus Wallenbergs Stiftelse. Vi tackar Dan Laksov, Roy Skjelnes och Tomas Ekholm, alla från Institutionen för Matematik vid KTH, Alan Sola vid Oklahoma State University samt Johan Wild vid Europaskolan i Strängnäs för deras givande kommentarer om denna skrift.

## Några ord om Cirkeln

KTHs Matematiska Cirkel, i dagligt tal benämnd Cirkeln, startade 1999. Dess ambition är att sprida kunskap om matematiken och dess användningsområden utöver vad eleverna får genom gymnasiekurser, och att etablera ett närmare samarbete mellan gymnasieskolan och högskolan. Cirkeln skall särskilt stimulera elevernas matematikintresse och inspirera dem till fortsatta naturvetenskapliga studier. Lärarna på cirkeln kan vid behov ge eleverna förslag på ämnen till projektarbeten vid gymnasiet.

Till varje kurs skrivs ett kompendium som distribueras gratis till eleverna. Detta material, liksom övriga uppgifter om KTHs Matematiska Cirkel, finns tillgängligt på

`http://www.math.kth.se/cirkel`

Cirkeln godkänns ofta som en gymnasiekurs eller som matematisk breddning på gymnasieskolorna. Det är upp till varje skola att godkänna Cirkeln som en kurs och det är lärarna från varje skola som sätter betyg på kursen. Lärarna är självklart också välkomna till Cirkeln och många har kommit överens med sin egen skola om att få Cirkeln godkänd som fortbildning eller som undervisning. Vi vill gärna understryka att föreläsningarna är öppna för alla gymnasieelever och lärare.

Vi har avsiktligt valt materialet för att ge eleverna en inblick i matematisk teori och tankesätt och presenterar därför både några huvudsatser inom varje område och bevisen för dessa resultat. Vi har också som målsättning att bevisa alla satser som används om de inte kan förutsättas bekanta av elever från gymnasiet. Detta, och att flera ämnen är på universitetsnivå, gör att lärarna och eleverna kan uppleva programmet som tungt, och alltför långt över gymnasienivån. Meningen är emellertid inte att lärarna och eleverna skall behärska ämnet fullt ut och att lära in det på samma sätt som gymnasiekurserna. Det viktigaste är att eleverna kommer i kontakt med teoretisk matematik och får en inblick i *matematikens väsen*. Vår förhoppning är att lärarna med denna utgångspunkt skall ha lättare att upplysa intresserade elever om KTHs Matematiska Cirkel och övertyga skolledarna om vikten av att låta både elever och lärare delta i programmet.

## Några ord om betygssättning

Ett speciellt problem tidigare år har varit betygssättningen. Detta borde emellertid bara vara ett problem om lärarna använder sig av samma standard som de gör när de sätter betyg på ordinarie gymnasiekurser. Om utgångspunkten istället är att eleverna skall få insikt i matematiken genom att gå på föreläsningarna och att eleven gör sitt bästa för att förstå materialet och lösa uppgifterna, blir betygsättningen lättare. Självklart betyder det mycket vad eleverna har lärt av materialet i kursen, men lärarna kan bara förvänta sig att ett fåtal elever behärskar ämnet fullt ut. I det perspektivet blir det lätt att använda de officiella kriterierna:

*Godkänd:* Eleven har viss insikt i de moment som ingår i kursen och kan på ett godtagbart sätt redovisa valda delar av kursen såväl muntligt som skriftligt. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

*Väl godkänd:* Eleven har god insikt i flera moment från kursen. Eleven kan redovisa dessa moment både skriftligt och muntligt och dessutom uppvisa lösningar på problem som givits på kursen. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

*Mycket väl godkänd:* Eleven har mycket god insikt i flera moment av kursen och lämnar skriftliga redovisningar av flera delar av kursen eller lämnar lösningar på problem som givits på kursen. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

Det är också möjligt att skolorna samarbetar, så elever från en skola redovisar eller lämnar rapport för en lärare i en annan skola.

Författarna, september 2010

# 0 Mängdlära

## 0.1 Mängder

Låt oss börja med att titta på ett av de mest grundläggande begreppen i matematiken, nämligen mängder. En mängd är en samling objekt, som till exempel tal, och dessa objekt kallar vi för *element* i mängden. Det enklaste sättet att beskriva en mängd är att räkna upp dess element. Ett sådant exempel är

$$A = \{1, 3, a, 7\}.$$

Detta betyder att $A$ är en mängd som innehåller elementen $1, 3, a$ och 7. Ett annat sätt att beskriva en mängd är att skriva $\{x \in D \mid \text{villkor på } x\}$. Med detta menar man mängden av alla element i $D$ som uppfyller de givna villkoren. Som exempel tar vi

$$B = \{n \in \{1, 2, 3, \dots\} \mid n \text{ är udda}\}$$

och

$$C = \{y \in \{1, 2, 3, 4\} \mid y > 2\}.$$

Mängden $B$ innehåller alla udda positiva heltal, medan $C$ innehåller alla element från mängden $\{1, 2, 3, 4\}$ som är större än 2. Alltså har vi

$$B = \{1, 3, 5, 7, 9, 11, \dots\} \quad \text{och} \quad C = \{3, 4\}.$$

Vi bryr oss inte om i vilken ordning eller hur många gånger elementen räknas upp och därmed gäller till exempel

$$\{1, 2, 3, 4\} = \{3, 1, 4, 2\} = \{1, 3, 3, 1, 2, 4, 4, 1, 3, 2, 4\}.$$

Om $A$ är en mängd och $x$ är ett element i mängden $A$ så skriver vi $x \in A$ och säger att $x$ *tillhör* $A$. Exempelvis gäller $17 \in \{n \mid n \text{ är ett udda heltal}\}$ och $b \in \{a, b, 10, 3\}$. Att ett element $x$ inte tillhör mängden $A$ skrivs $x \notin A$. Den *tomma mängden* innehåller ingenting och betecknas $\varnothing$.

**Exempel 0.1.1.** Låt $A = \{4, 5, 8, 4711, 12, 18\}$ och $B = \{x \in A \mid x > 10\}$. Då är $B = \{12, 18, 4711\}$ medan $\{x \in A \mid x < 3\} = \varnothing$. Vidare har vi att $4 \in A$ men $4 \notin B$. ▲

**Definition 0.1.2.** Låt $A$ och $B$ vara mängder. Om alla element i mängden $A$ också är element i mängden $B$ så sägs $A$ vara en *delmängd* till $B$. Detta betecknas $A \subseteq B$.

**Exempel 0.1.3.** Mängden $\{1, a\}$ är en delmängd till $\{1, 3, a\}$, eftersom alla element i $\{1, a\}$ finns i mängden $\{1, 3, a\}$. Vi skriver $\{1, a\} \subseteq \{1, 3, a\}$. ▲

**Definition 0.1.4.** Antag att $A$ och $B$ är mängder. *Unionen* av $A$ och $B$ består av de element som ligger i någon av mängderna och betecknas $A \cup B$. *Snittet* av $A$ och $B$ består av de element som ligger i båda mängderna och betecknas $A \cap B$.

**Exempel 0.1.5.** Låt $A = \{1, 3, 5, 6\}$ och $B = \{5, 8, 3, 4711\}$. Då har vi $A \cup B = \{1, 3, 5, 6, 8, 4711\}$ och $A \cap B = \{3, 5\}$. ▲

Det är dags att titta på några viktiga talmängder. Den mängd vi använder för att räkna föremål är de *naturliga talen* $\{0, 1, 2, 3, \dots\}$. Denna mängd betecknas $\mathbb{N}$. Tar vi med negativa tal får vi heltalen $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. Beteckningen kommer från tyskans *zahl* som betyder tal. Mängden av alla kvoter av två heltal $p/q$ där $q \neq 0$ innehåller t.ex. $2/3, -7/243$ och $25/1$. Vi kallar mängden de *rationella talen* och betecknar den med $\mathbb{Q}$. Slutligen betecknar vi med $\mathbb{R}$ de *reella talen*, det vill säga alla tal på tallinjen, exempelvis $0, -1, 3/2, -527/3, \sqrt{2}$ och $\pi$. Notera att $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

**Exempel 0.1.6.** Vi har att $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geqslant 0\}$. ▲

**Exempel 0.1.7.** Mängden $\{n \in \mathbb{Z} \mid n = 2 \cdot k \text{ för något } k \in \mathbb{Z}\}$ är mängden av alla jämna heltal. Denna mängd kan också skrivas som $\{2 \cdot k \mid k \in \mathbb{Z}\}$, eller som $\{\dots, -4, -2, 0, 2, 4, \dots\}$. ▲

**Exempel 0.1.8.** Låt oss påpeka att en mängd även kan ha andra mängder bland dess element. Exempelvis kan vi låta

$$A = \{2, 3, \{-1, 1\}, 4\},$$

och vi har att $\{-1, 1\} \in A$, det vill säga mängden $\{-1, 1\}$ är ett element i mängden $A$. ▲

Låt $\Omega$ vara en godtycklig mängd. Vi kommer i följande exempel antaga att alla mängder $A, B, C, \dots$ är delmängder till $\Omega$. Vi definierar två vanliga operationer på mängder:

1. $A \setminus B = \{x \in A \mid x \notin B\}$
2. $A^c = \Omega \setminus A = \{x \in \Omega \mid x \notin A\}$

Mängden $A^c$ kallas för *komplementet till* $A$.

Låt oss studera några exempel på hur man visar påståenden om allmänna mängder.

**Exempel 0.1.9.** Två mängder $B$ och $C$ sägs vara *disjunkta* om de inte har några gemensamma element. Visa att $B$ och $C$ är disjunkta om och endast om $B \cap C = \varnothing$.

**Lösning.** Antag att $B$ och $C$ är disjunkta. Antag att $x \in B \cap C$, det vill säga att $x \in B$ och $x \in C$. Men detta betyder att $B$ och $C$ har $x$ som gemensamt element, vilket motsäger att $B$ och $C$ är disjunkta. Alltså måste $B \cap C = \varnothing$.

Omvänt, antag att $B \cap C = \varnothing$. Det betyder att det inte finns något element som tillhör både $B$ och $C$. Alltså har $B$ och $C$ inga gemensamma element, det vill säga att $B$ och $C$ är disjunkta.

Nu har vi alltså visat två saker, dels att om $B$ och $C$ är disjunkta så gäller $B \cap C = \varnothing$, dels att om $B \cap C = \varnothing$ så är $B$ och $C$ disjunkta. Tillsammans betyder detta att $B$ och $C$ är disjunkta om och endast om $B \cap C = \varnothing$. ▲

**Exempel 0.1.10.** Visa att $A$ och $A^c$ är disjunkta.

**Lösning.** Enligt föregående exempel är det vi ska visa att $A \cap A^c = \varnothing$. Antag att $x \in A \cap A^c$. Det betyder att $x \in A$ och att $x \in A^c$. Det senare betyder per definition att $x \notin A$, vilket är en motsägelse. Alltså måste $A \cap A^c = \varnothing$. ▲

## 0.2 Funktioner

Innan vi gör en allmän definition av vad en funktion är kan det vara på sin plats att titta på något välbekant, nämligen en formel som $f(x) = x^2 + 1$. Detta är ett exempel på en funktion. Formeln säger att om vi tar ett tal $x \in \mathbb{R}$ så får vi ett nytt tal $f(x) \in \mathbb{R}$ genom att göra beräkningen $x^2 + 1$; till exempel får vi $f(2) = 2^2 + 1 = 5$. Vi säger att $f$ är en funktion från de reella talen till de reella talen, eftersom både det vi stoppar in, $x$, och det vi får ut, $f(x)$, är reella tal. Vi brukar beteckna detta med $f : \mathbb{R} \to \mathbb{R}$.

**Definition 0.2.1.** Låt $X$ och $Y$ vara mängder. En *funktion* $f\colon X \to Y$ är ett sätt att till varje element $a \in X$ tilldela ett välbestämt element $b \in Y$. Vi skriver $f(a) = b$. Vi säger att $a$ *avbildas* på $b$ och att $b$ är *bilden* av $a$.

**Anmärkning 0.2.2.** Ofta säger man att $f$ är en funktion från $X$ till $Y$ istället för att använda beteckningen $f : X \to Y$. Ett vanligt alternativ till ordet funktion är *avbildning*.

**Exempel 0.2.3.** Betrakta mängderna $A = \{1, 2, 3\}$ och $B = \{1, 2, \ldots, 100\}$. Ett exempel på funktion $f : A \to B$ ges av $f(n) = 2n$ för $n \in A$. Vi har alltså att $f(1) = 2$, $f(2) = 4$ och $f(3) = 6$. Per definition måste vi ha $f(x) \in B$ för alla $x \in A$, och detta gäller ju här eftersom

$$f(1) = 1 \in B, \quad f(2) = 4 \in B, \quad \text{och} \quad f(3) = 6 \in B.$$

I detta exempel definieras funktionen $f$ av formeln $f(n) = 2n$, men det är inte alls nödvändigt att det finns en formel som beskriver hur funktionen verkar. Om vi som här har en funktion från den *ändliga* mängden $A = \{1, 2, 3\}$ kan man till exempel definera funktionen med hjälp av en tabell:

| $n$ | $f(n)$ |
|---|---|
| 1 | 2 |
| 2 | 4 |
| 3 | 6 |

▲

**Exempel 0.2.4.** Låt $h(x) = 3/2 \cdot x^2 - x^3$. Detta definierar en funktion $h$ från $\mathbb{R}$ till $\mathbb{R}$. Vi har exempelvis att

$$h(1) = \frac{1}{2}, \quad \text{och} \quad h(-2) = 14.$$ ▲

## Övningar

**Övning 0.1.** Låt $A = \{1, 2, 3, 4, \ldots\}$, $B = \{1, 3, 5, 7, \ldots\}$, $C = \{2, 4, 6, 8, \ldots\}$ och $D = \{1, 4, 19, 36, 101\}$. Bestäm mängderna

1. $B \cup C$,
2. $B \cap C$,
3. $D \cap C$,
4. $\{x \in D \mid x \in B\}$,
5. $\{x \in A \mid x = y + 1 \text{ för något } y \in D\}$,
6. $\{x + 1 \mid x \in D\}$.

**Övning 0.2.** Låt $\mathbb{N} = \{0, 1, 2, \ldots\}$ och $B_n = \{1, 2, \ldots, n\}$ för $n = 1, 2, 3, \ldots$. Visa att $\mathbb{N} \setminus \{0\} = B_1 \cup B_2 \cup B_3 \cup \cdots$.

**Övning 0.3.** Låt $\Omega$ vara en mängd och $A, B, C \subseteq \Omega$. Visa att

$$((A \cap C) \cup (B \cap C^c))^c = (A^c \cap C) \cup (B^c \cap C^c).$$

**Övning 0.4.** Låt $\Omega$ vara en mängd och $A \subseteq \Omega$. Visa att $\Omega = A \cup A^c$.

# 1 Komplexa tal

I det här kapitlet inför vi de *komplexa talen* och vi motiverar varför de introducerades i matematiken. Vi utarbetar hur räknesätten addition, subtraktion, multiplikation och division fungerar för komplexa tal. Dessutom visar vi hur man kan föreställa sig komplexa tal som punkter i planet. Vi diskuterar olika sätt att representera komplexa tal och ger även en geometrisk tolkning av räknesätten.

## 1.1 Komplexa tal och dess räkneoperationer

Låt oss börja med att betrakta ekvationen $x^2 + 1 = 0$. Ekvationen har inga lösningar bland de reella talen eftersom kvadraten av ett reellt tal aldrig kan vara negativ. Dock har den en lösning i de så kallade komplexa talen, som vi ska införa i detta kapitel, och som är en större mängd av "tal" än de reella. Historiskt sett var detta motivationen till att införa komplexa tal: om man hade en polynomekvation utan lösningar, kunde man få fram korrekta resultat genom att räkna vidare som om ekvationen faktiskt hade en lösning. Vad man gjorde var att införa ett nytt tal $i$, som man räknade med som om det var en lösning till just ekvationen $x^2 + 1 = 0$. Det visade sig att de reella talen tillsammans med detta tal $i$ faktiskt räckte för att lösa alla polynomekvationer.

Vi vill alltså hitta en mängd av tal som ska innehålla alla reella talen (eftersom alla tal som vi redan känner fortfarande ska vara tal) samt det nya talet $i$. Dessutom ska räknesätten addition, subtraktion, multiplikation och division vara definierade och fungera på samma sätt som vi är vana från de reella talen.

Det är inte alls uppenbart att vi överhuvudtaget kan göra som vi vill.

**Definition 1.1.1.** Ett *komplext tal* är ett tal på formen

$$z = a + bi, \quad \text{där} \quad a, b \in \mathbb{R}. \tag{1.1}$$

Notera att i vår definition av ett komplext tal så har vi inte sagt någonting om att $i^2 = -1$: detta kommer i stället att följa av definitioner som kommer senare. Vi tänker bara på $i$ som en symbol som hittills inte har givits någon mening.

Det reella talet $a$ kallas för $z$:s *realdel*, och vi skriver $a = \mathrm{Re}(z)$. Talet $b$ är $z$:s *imaginärdel* och betecknas $b = \mathrm{Im}(z)$.

Mängden av alla komplexa tal, det vill säga,

$$\{z = a + bi : a, b \in \mathbb{R}\}$$

brukar betecknas med $\mathbb{C}$.

**Anmärkning 1.1.2.** För enkelhetens skull kommer vi att skriva $a + i$ istället för $a + 1i$, $a - bi$ istället för $a + (-b)i$ och $a$ istället för $a + 0i$.

Vi använder nu de kända räknesätten för $\mathbb{R}$ och inför motsvarande räknesätt för komplexa tal. Vi delar för enkelhetens skull upp definitionerna.

**Definition 1.1.3.** Låt $z = a + bi$ och $w = c + di$ vara godtyckliga komplexa tal. *Summan* av $z$ och $w$ ges av

$$z + w = (a + c) + (b + d)i \tag{1.2}$$

och *differensen* av $z$ och $w$ är

$$z - w = (a - c) + (b - d)i \tag{1.3}$$

Vi noterar att detta är väldefinierat eftersom $a+c$ och $b+d$ samt $a-c$ och $b-d$ är definierade för reella tal $a$, $b$, $c$, $d$. Resultatet av additionen och subtraktionen är ett nytt komplext tal. Dessutom känns definitionen naturlig eftersom additionen och subtraktionen sker komponentvis: Realdelen av summan är lika med summan av realdelarna och likaså med differensen. Vi ska senare se hur operationerna kan tolkas geometriskt.

Vi fortsätter med att definiera multiplikation.

**Definition 1.1.4.** Låt $z = a + bi$ och $w = c + di$ vara godtyckliga komplexa tal. *Produkten* av $z$ och $w$ definieras som

$$z \cdot w = (ac - bd) + (ad + bc)i. \tag{1.4}$$

Vi ser igen att definitionen är meningsfull eftersom uttrycken $ac$, $bd$, och så vidare, samt summor och differensen av dem, är meningsfulla för reella tal $a$, $b$, $c$ och $d$.

Vi vill att talet $i$ beter sig som att ekvationen $i^2 = -1$ stämmer samt att alla vanliga räknelagar gäller även för komplexa tal. Detta tvingar oss att definiera produkten som vi gjorde ovan som följande räkning visar.

$$(a + bi)(c + di) = ac + bci + adi + bdi^2 = ac - bd + bci + adi.$$

**Exempel 1.1.5.** Sätt $z = \sqrt{2}+i$ och $w = 1/17-i$. Då har vi enligt definitionen av addition och subtraktion att

$$z + w = (\sqrt{2} + i) + (1/17 - i) = \frac{17\sqrt{2} + 1}{17} + 0i = \frac{17\sqrt{2} + 1}{17}$$

samt

$$z - w = (\sqrt{2} + i) - (1/17 - i) = \frac{17\sqrt{2} - 1}{17} + 2i.$$

Vi använder definitionen av produkt för att beräkna

$$\begin{aligned} zw &= (\sqrt{2} + i)(1/17 - i) \\ &= \left(\sqrt{2} \cdot 1/17 - 1 \cdot (-1)\right) + \left(\sqrt{2} \cdot (-1) + 1 \cdot (1/17)\right) i \\ &= \frac{\sqrt{2} + 17}{17} + \frac{1 - 17\sqrt{2}}{17} i. \end{aligned}$$

▲

**Definition 1.1.6.** Om $a = 0$ i $z = a + bi$ säger vi att $z$ är *rent imaginärt* och om $b = 0$ att $z$ är *reellt*.

**Anmärkning 1.1.7.** De reella talen $\mathbb{R}$ kan identifieras med en delmängd av de komplexa talen, nämligen med mängden

$$\{z \in \mathbb{C} : \mathrm{Im}(z) = 0\},$$

Detta är nödvändigt eftersom vi från notationen inte kan skilja på det reella talet $a \in \mathbb{R}$ och det komplexa talet $a = a + 0i \in \mathbb{C}$. Men om båda är samma för oss så blir det inget problem.

Om $x$ och $y$ är reella, måste vi dock kontrollera att vi får samma resultat för

$$x + y \text{ och } x \cdot y,$$

oavsett om vi ser $x$ och $y$ som reella tal eller komplexa tal. Vi beräknar

$$(x + 0i) + (y + 0i) = (x + y) + 0i = x + y$$

vilket är samma resultat som med den vanliga additionen för reella tal. På samma sett får vi $xy$ som produkt oavsett hur vi räknar.

**Anmärkning 1.1.8.** Det gäller att

$$i^2 = i \cdot i = (0 + i)(0 + i) = -1 + 0i = -1.$$

Vår uträkning visar alltså att $i$ verkligen har egenskapen

$$i^2 = -1,$$

det vill säga, $i$ löser ekvationen $x^2 + 1 = 0$ som det skulle.

Nu återstår bara att ange vad vi ska mena med division av komplexa tal. Innan vi gör detta ska vi införa lite notation.

**Definition 1.1.9.** *Konjugatet* av $z = a + bi \in \mathbb{C}$ är

$$\bar{z} = a - bi. \tag{1.5}$$

Vi genomför en liten räkning som visar sig vara användbar:

$$z \cdot \bar{z} = (a + bi) \cdot (a - bi) = (a^2 + b^2) + (-ab + ab)i = a^2 + b^2.$$

Vi noterar att $z \cdot \bar{z}$ alltid är reellt.

**Definition 1.1.10.** Låt $z \in \mathbb{C}$. Det reella talet $\sqrt{z \cdot \bar{z}}$ kallas *absolutbeloppet* av det komplex talet $z$ och betecknas med $|z|$.

Vi är nu redo att definiera division för komplexa tal.

**Definition 1.1.11.** Låt $z = a + bi$ vara ett godtyckligt komplext tal och låt $w = c+di \neq 0$ vara ett komplext tal skild från 0. *Kvoten* av $z$ och $w$ definieras som det komplexa talet

$$\frac{z}{w} = \frac{1}{w\bar{w}} \cdot z \cdot \bar{w} \tag{1.6}$$

Vi ser att detta är en meningsfull definition eftersom vi vet hur man multiplicerar ett komplext tal med ett reellt tal – vi multiplicerar bara imaginärdel och realdel var för sig.

**Exempel 1.1.12.** Låt $z = \sqrt{2} + i$ och $w = 1 - i$. Vi har $w\bar{w} = 2$ samt $z\bar{w} = (\sqrt{2}+1) + (1-\sqrt{2})i$, vilket ger oss $z/w = (\sqrt{2}+1)/2 + ((1-\sqrt{2})/2)i$. ▲

## 1.2 Räknelagar för komplexa tal

Vi har flera gånger i detta kapitel nämnt att alla räkneregler som gäller för vanliga reella tal gäller även för komplexa tal. Detta är ett påstående som inte är uppenbart och som verkligen måste bevisas utifrån definitionerna för komplexa tal. Vi gör inte detta i detalj, eftersom ett detaljerat bevis skulle ges av flera sidor inte särskilt upplysande räkning. Dock formulerar vi exakt vad vi menar med att alla vanliga räknelagar gäller. Låt $x, y$ och $z$ vara godtyckliga komplexa tal. Då gäller att

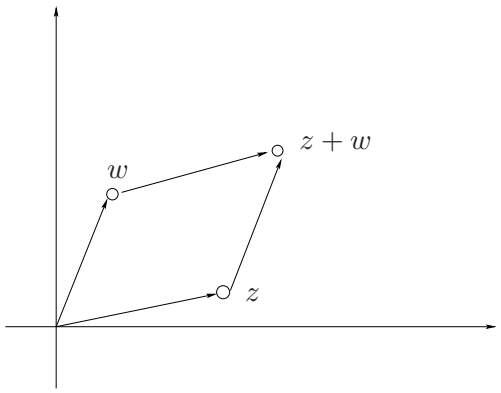
$$\begin{aligned}
0 \cdot z &= 0 \\
1 \cdot z &= z \\
0 + z &= z \\
x + y &= y + x \\
xy &= yx \\
(x+y)z &= xz + yz \\
(x+y) + z &= x + (y+z) \\
(xy)z &= x(yz).
\end{aligned}$$

Dessutom kan vi subtrahera och dividera komplexa tal, vilket innebär följande: för alla komplexa tal $x$ finns ett komplext tal $-x$ sådant att $x + (-x) = 0$, och för varje nollskilt komplext tal $y$ finns ett komplext tal $1/y$ sådant att $y \cdot (1/y) = 1$. Vi har också räknelagar för komplexkonjugatet:

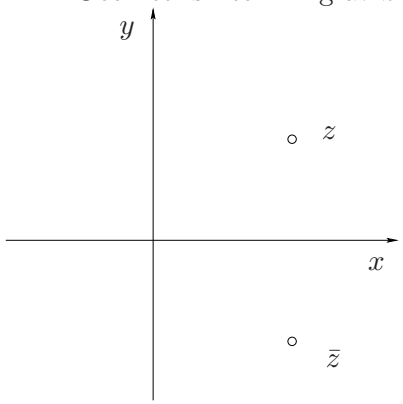
$$\begin{aligned}
\overline{x+y} &= \overline{x} + \overline{y} \\
\overline{x \cdot y} &= \overline{x} \cdot \overline{y}
\end{aligned}$$

## 1.3 Geometrisk tolkning

Vi lovade att ge en geometrisk tolkning av de komplexa talen. Alla punkter i planet kan beskrivas med hjälp av två reella tal, punkternas så kallade koordinater.




Figur 1.1: Geometrisk tolkning av $z + w$.



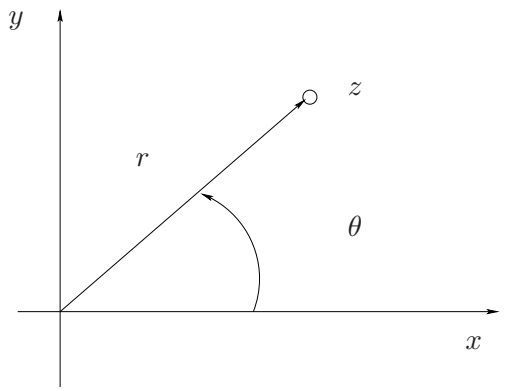

Figur 1.2: Punkten $z$ och dess konjugat $\bar{z}$.

**Definition 1.3.1.** Vi identifierar punkten $(a, b)$ i planet med det komplexa talet $a + bi$ och tvärtom. På det sättet identifierar vi mängden $\mathbb{C}$ av alla komplexa tal med planet. Vi kan se de reella talen - som vi identifierade med alla komplexa tal med imaginärdel 0 - som $x$-axeln i planet.

Eftersom de komplexa talen har identifierats med punkter i planet känns det naturligt att försöka tolka räkneoperationerna på $\mathbb{C}$ geometriskt.

Vi börjar med att betrakta addition och subtraktion. Låt därför $z = a + ib$ och $w = c + id$ vara två komplexa tal. Vi kan rita upp dem som punkter i planet genom att använda $a$ respektive $c$ som $x$-koordinater och $b$ respektive $d$ som $y$-koordinater. Summan $z + w$ är enligt definitionen det komplexa talet $a + c + i(b + d)$, och vi ser att motsvarande punkt har $x$-koordinaten $a + c$ och $y$-koordinaten $b + d$. Detta betyder att punkten som svarar mot summan $z + w$ är hörnpunkten i parallellogrammen som bestäms av $z$ och $w$ (se Figur 1.1). På ett liknande sätt kan man ge subtraktion av komplexa tal en geometrisk tolkning. Vi överlämnar detta som en övning.

Vi kan även tolka den nya räkneoperationen konjugering geometriskt: $a + bi$ motsvarar punkten $(a, b)$ och $a - bi$ motsvarar punkten $(a, -b)$. Därmed innebär konjugering att vi speglar i $x$-axeln.




Figur 1.3: Polära koordinater.

För att kunna ge multiplikation och division en geometrisk tolkning behöver vi införa ett annat sätt att beskriva komplexa tal som punkter i planet. Detta gör vi i nästa avsnitt.

## 1.4 Polär form

Vi betraktar återigen en figur. Vi kan beskriva en punkt i planet genom att ange dess avstånd från origo, $r$, samt den vinkel som den räta linjen från origo till punkten bildar med $x$-axeln, se Figur 1.3. Vi beräknar avståndet med hjälp av Pythagoras sats och får

$$r = \sqrt{a^2 + b^2},$$

vilket är absolutbeloppet av det komplexa talet $z = a + ib$. Vi noterar att $r = 0$ om och endast om $z = 0$.

Vinkeln $\theta$ kallas för *argumentet* av $z$, och vi skriver $\theta = \arg(z)$. Om $z = 0$ är $\arg(z)$ odefinierat. Genom att projicera på $x$-axeln och $y$-axeln ser vi att $x$-koordinaten för punkten $z$ kan skrivas med hjälp av $\theta$ som $r\cos\theta$, medan $y$-koordinaten blir $r\sin\theta$. Detta ger

$$z = r(\cos\theta + i\sin\theta),$$

eller $z = |z|(\cos\theta + i\sin\theta)$ om man föredrar det.

När vi multiplicerar komplexa tal i polär form får vi uttryck som innehåller summor av produkter av sinus och cosinus. Dessa uttryck kan förenklas med hjälp av de så kallade additionsformlerna för sinus och cosinus som vi dock inte ska visa.

**Hjälpsats 1.4.1** (Additionsformlerna för sin och cos)**.** *Det gäller att*

$$\sin(\theta + \phi) = \sin\theta\cos\phi + \cos\theta\sin\phi$$
$$\cos(\theta + \phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$$

*för alla reella tal $\theta$ och $\phi$.*

Låt nu $z = r(\cos\theta + i\sin\theta)$ och $w = s(\cos\phi + i\sin\phi)$ vara två komplexa tal i polär form. Vi multiplicerar $z$ och $w$ och får

$$\begin{aligned} z \cdot w &= r(\cos\theta + i\sin\theta) \cdot s(\cos\phi + i\sin\phi) \\ &= rs\cos\theta\cos\phi - rs\sin\theta\sin\phi + i(rs\cos\theta\sin\phi + rs\sin\theta\cos\phi) \end{aligned}$$

Vi använder additionsformlerna för sinus och cosinus från Hjälpsats 1.4.1 och får

$$z \cdot w = rs[\cos(\theta + \phi) + i\sin(\theta + \phi)]. \tag{1.7}$$

Nu ser vi vad multiplikation av två komplexa tal innebär geometriskt: man multiplicerar talens avstånd från origo med varandra och adderar vinklarna som de räta linjerna till punkterna bildar med $x$-axeln. Vi kan sammanfatta detta med formlerna

$$|z \cdot w| = |z| \cdot |w| \quad \text{och} \quad \arg(zw) = \arg(z) + \arg(w).$$

Liknande räkningar kan genomföras för division. I polära koordinater blir kvoten av talen $z$ och $w$, $w \neq 0$, det komplexa talet som i polära koordinater kan skrivas

$$\frac{z}{w} = \frac{r}{s}[\cos(\theta - \phi) + i\sin(\theta - \phi)],$$

det vill säga, vi dividerar talens absolutbelopp och subtraherar de tillhörande vinklarna:

$$\left|\frac{z}{w}\right| = \frac{|z|}{|w|} \quad \text{och} \quad \arg(z/w) = \arg(z) - \arg(w).$$

Eftersom uttrycket $\cos\theta + i\sin\theta$ används så ofta när man arbetar med komplexa tal är det smidigt att hitta ett förkortat skrivsätt för det. Man kan därför införa den *komplexa exponentialfunktionen*

$$e^{i\theta} = \cos\theta + i\sin\theta,$$

som är en funktion som till varje reellt $\theta$ tillordnar ett komplext tal $e^{i\theta}$. Vi kan vidare notera att

$$\left|e^{i\theta}\right| = \sqrt{\cos^2\theta + \sin^2\theta} = 1.$$

Vi kan nu skriva det komplexa talet $z = a + ib$ på ett kompakt sätt:

$$z = re^{i\theta}$$

där alltså $r = |z|$ och $\theta = \arg(z)$. Genom att använda formeln (1.7), med $r = s = 1$, erhåller vi

$$e^{i\theta}e^{i\phi} = e^{i(\theta+\phi)}.$$

## Övningar

**Övning 1.1.** Beräkna $z+w$, $z-w$, $zw$ och $z/w$ för

1. $z = 3+i$ och $w = -1+4i$
2. $z = -\sqrt{2}i$ och $w = 2-5i$.

**Övning 1.2.** Visa att distributiva lagen gäller även för komplexa tal: För godtyckliga $z, w, v \in \mathbb{C}$ är $(z+w)v = zv + wv$

**Övning 1.3.** Visa att $\mathrm{Re}(z) = (z+\overline{z})/2$ och $\mathrm{Im}(z) = (z-\overline{z})/2i$.

**Övning 1.4.** Visa att $|zw| = |z||w|$ för $z, w \in \mathbb{C}$.

**Övning 1.5.** Visa triangelolikheten $|z+w| \leqslant |z|+|w|$ för $z, w \in \mathbb{C}$. Visa även den så kallade omvända triangelolikheten $|x-y| \geqslant |x|-|y|$. för $z, w \in \mathbb{C}$.

**Övning 1.6.** Lös andragradsekvationen $z^2 + iz + 2 = 0$ genom att använda kvadratkomplettering.

**Övning 1.7.** Antag känt att man kan derivera en funktion $\mathbb{R} \to \mathbb{C}$ genom att derivera real- och imaginärdel var för sig. Visa att $\frac{d}{d\theta}e^{i\theta} = ie^{i\theta}$.

# 2 Induktion och polynom

I detta kapitel introduceras de föremål som kursen kommer att handla om, nämligen polynom. Efter att ha gett den formella definitionen av vad vi menar med ett polynom bevisar vi även vissa egenskaper hos polynom. En del av de här egenskaperna, till exempel den så kallade *faktorsatsen*: ett polynom har $x_0$ som rot om och endast om polynomet är jämnt delbart med $(x - x_0)$, kan för en del tyckas självklara eftersom att de är så välbekanta. Dock krävs det lite arbete för att ge ett formellt bevis.

Den kanske allra viktigaste satsen som visas i detta kapitel är dock divisionsalgoritmen, som visar att den så kallade "liggande stolen"-metoden som används för att dividera heltal med varandra även kan användas för att dividera polynom med varandra. Polynomdivision kommer att användas precis hela tiden i detta häfte.

Innan vi kan göra något av detta, måste vi dock införa en kraftfull bevismetod som kallas *induktionsprincipen*. Induktion är ett effektivt sätt att organisera en typ av bevis där sanningshalten av ett påstående reduceras till sanningshalten av ett "mindre" påstående, i en mening som kommer att preciseras i kapitlet. Just när man arbetar med polynom är induktion speciellt viktigt, eftersom väldigt många bevis använder sig av denna metod på ett naturligt sätt. I dessa fall används oftast metoden i fallet att man ska visa ett påstående om ett godtyckligt polynom, och det "mindre" påståendet är att visa påståendet för ett polynom av lägre grad än det man startade med.

Många av bevisen i kapitlet, och i resten av kompendiet, bygger på induktionsargument.

## 2.1 Induktion

I denna kapitel ska vi införa en grundläggande bevismetod som kommer att spela en central roll i många bevis i resten av kompendiet. Vi börjar med ett exempel.

**Exempel 2.1.1.** Vi vill beräkna summan

$$1 + 2 + 3 + \ldots + (n-1) + n$$

av de första $n$ naturliga talen. För de första exemplen vi provar fås följande resultat:

$$1 = 1, \quad 1 + 2 = 3, \quad 1 + 2 + 3 = 6, \quad 1 + 2 + 3 + 4 = 10$$

Om vi försöker gissa en formel så kommer vi kanske på att

$$1 = \frac{1 \cdot 2}{2}, \quad 3 = \frac{2 \cdot 3}{2}, \quad 6 = \frac{3 \cdot 4}{2}, \quad 10 = \frac{4 \cdot 5}{2}.$$

Vi förmodar nu att följande formel gäller

$$1 + 2 + 3 + \ldots + (n-1) + n = \frac{n(n+1)}{2}. \tag{2.1}$$

Genom uträkning har vi redan visat att formel (2.1) gäller om $n = 1, 2, 3, 4$. Men metoden att bara räkna ut summan kommer inte att hjälpa oss om vi vill bevisa likheten för alla naturliga talen $n$. *Antag* istället att formel (2.1) gäller för något $n$. Vi vill undersöka om den också gäller för nästkommande naturliga tal $n + 1$. Vi betraktar summan för $n + 1$ närmare och får med lite räkning:

$$1 + 2 + \ldots + n + (n + 1) = (1 + 2 + \ldots + n) + (n + 1)$$

Vi använder vårt antagande att formel (2.1) gäller för $n$ och ersätter den första parentesen. Det ger

$$\begin{aligned} 1 + 2 + \ldots + n + (n + 1) &= \frac{n(n+1)}{2} + (n + 1) \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \end{aligned}$$

Vi har visat att påståendet stämmer för $n + 1$.

Låt oss sammanfatta: Vi har genom uträkning för små värden av $n$ gissat Formel (2.1). Speciellt visade vi på det sättet att Formel (2.1) gäller för $n = 1$. Sedan har vi visat att om likheten gäller för något naturligt tal $n$, så gäller den även för nästkommande tal $n + 1$. Då stämmer den för alla naturliga tal! ▲

Detta är idén bakom induktionsprincipen.

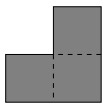
**Induktionsprincipen 2.1.2.** Antag att vi har formulerat ett påstående för varje naturligt talen $n \in \mathbb{N}$ med $n \geqslant n_0$. Antag vidare att följande gäller:

1. Påståendet för $n = n_0$ är sant.
2. Om påståendet för något $n \geqslant n_0$ är sant, så är det för $n + 1$ sant också.

Då är påståendet sant för alla naturliga talen $n \geqslant n_0$.

Här är ett annorlunda exempel där induktionsprincipen används.

**Exempel 2.1.3.** Antag att i ett schackbräde av storlek $2^n \times 2^n$ har en ruta blivit borttagen. Vi vill visa att man kan täcka det resulterande schackbrädet med L-formade bitar (se Figur 2.1) som inte överlappar varandra.

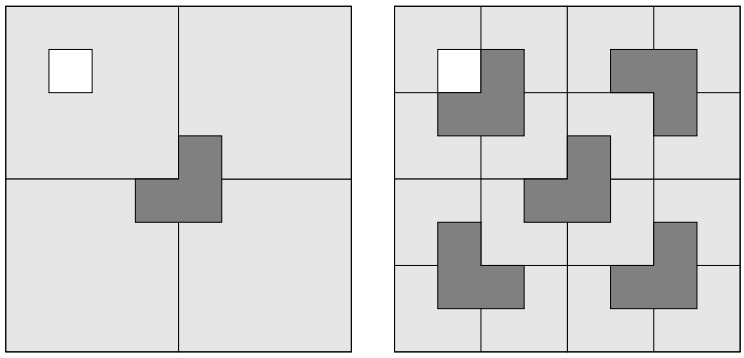


Figur 2.1: En L-bit

Vi ska lösa denna uppgift med hjälp av induktionsprincipen.

Om $n = 1$, så har vi ett $2 \times 2$ schackbräde där en ruta är borttagen. Den borttagna rutan är uppenbarligen ett hörn av brädet, och de resterande rutorna täcks exakt av en L-bit.

Antag att vi har visat påståendet för något $n \in \mathbb{N}$. Vi ska visa det för $n + 1$. Varje schackbräde av storlek $2^{n+1} \times 2^{n+1}$ kan delas i fyra lika stora kvadratiska delar av storlek $2^n \times 2^n$. Den borttagna rutan ligger i en av de fyra delbrädena, och de andra tre delbrädena är hela. Vi täcker var sitt hörn av de tre hela delbrädena genom att lägga en L-bit i mitten av det stora brädet där alla delbräden möts (se figur 2.2). Nu har vi fyra delbräden som alla fyra har en ruta borttagna. Varje sådant kan vi täcka med L-bitar enligt vårt induktionsantagande. På detta sätt kan vi täcka hela det stora brädet.



Figur 2.2: Stegvis övertäckning av schackbrädet med L-bitar

▲

## 2.2 Polynom

**Definition 2.2.1.** En funktion $f : \mathbb{C} \to \mathbb{C}$ på formen

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

där $a_i \in \mathbb{C}$ kallas ett *polynom*. Talen $a_i$ kallas koefficienter till polynomet. Om $a_n = 1$ kallas polynomet *moniskt*. Om alla koefficienter är reella kallas polynomet *reellt*.

Vi kan addera och multiplicera polynom enligt de vanliga räknereglerna:

$$\begin{aligned}(1 + x) + (2 - 3x + x^2) &= 3 - 2x + x^2 \\ (1 + x) \cdot (2 - 3x + x^2) &= 1 \cdot (2 - 3x + x^2) + x \cdot (2 - 3x + x^2) \\ &= 2 - 3x + x^2 + 2x - 3x^2 + x^3 = 2 - x - 2x^2 + x^3.\end{aligned}$$

Polynomet som är konstant lika med 0 för alla $x \in \mathbb{C}$ har en speciell roll. Detta är *nollpolynomet* $p = 0$ vars alla koefficienter lika med 0.

**Definition 2.2.2.** Ett polynom $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$ där $a_n \neq 0$ säges vara *av grad* $n$, vilket betecknas $\deg f = n$. Ett polynom av grad 0 kallas konstant. Graden av nollpolynomet är definierat som $-\infty$.

Med andra ord: Graden av ett polynom är den största exponenten bland alla termer med nollskilda koefficienter. Att nollpolynomet har grad $-\infty$ kan verka onaturligt och konstigt. Vi ber dock läsaren att inte lägga för stor vikt på denna detalj; definitionen är som den är för att alla kommande satser ska gälla även för nollpolynomet.

Vi kan säga följande om graden av en summa och en produkt av två polynom.

**Hjälpsats 2.2.3.** *Låt $f$ och $g$ vara polynom av grad $n$ och $m$, d.v.s.* $\deg f = n$ *och* $\deg g = m$. *Det gäller att* $\deg(f+g) \leqslant \max\{\deg f, \deg g\}$ *och* $\deg(fg) = \deg f + \deg g$.

Vi lämnar beviset av Hjälpsats 2.2.3 som övningsuppgift.

**Hjälpsats 2.2.4.** *Om två polynom $f$ och $g$ uppfyller att $f \neq 0$ och $fg = 0$, så är $g = 0$.*

*Bevis.* Låt $f \neq 0$ och $g \neq 0$ vara nollskilda polynom. Då är $\deg f \geqslant 0$ och $\deg g \geqslant 0$, till skillnad från graden $-\infty$ av nollpolynomet. Enligt Lemma 2.2.3 är $\deg(fg) = \deg f + \deg g \geqslant 0$. Alltså kan inte $fg = 0$ gälla. □

En mängd tillsammans med räkneoperationen multiplikation som uppfyller villkoret att produkten av två nollskilda element inte kan vara noll kallas för *integritetsområde*. Två exempel på integritetsområden är $\mathbb{R}$ och $\mathbb{C}$. Enligt Sats 2.2.4 är även mängden av alla polynom ett integritetsområde.

## 2.3 Polynomdivision

Från de naturliga talen känner vi till egenskapen att man kan utföra division med rest: för två naturliga tal $n$ och $m$ där $m \neq 0$ finns det unika naturliga tal $q$ och $r$ så att $0 \leqslant r < m$ och

$$\frac{n}{m} = q + \frac{r}{m},$$

där $q$ är *kvoten* vid divisionen och $r$ är *resten*. För att slippa räkna med bråk föredrar vi att skriva föregående ekvation som $n = qm + r$. En liknande egenskap gäller för polynom. Vi börjar med att visa att det existerar polynom som motsvarar $q$ och $r$, och i en senare sats visar vi att de är unika.

**Sats 2.3.1** (Division med rest för polynom)**.** *Låt $f$ och $g \neq 0$ vara polynom. Då finns det polynom $q$ och $r$ sådana att* $\deg r < \deg g$ *och* $f = qg + r$.

Vi visar satsen med hjälp av induktion. Men innan vi gör det betraktar vi ett enkelt exempel för att få en känsla för vad som händer.

**Exempel 2.3.2.** Låt

$$f(x) = x^3 + 2x^2 - 3x + 1$$

och

$$g(x) = x^2 + 1,$$

så att $\deg f = 3$ och $\deg g = 2$. Vi ska hitta polynom $q$ och $r$ så att $f = qg + r$ och där $\deg r < 2$. Om vi multiplicerar $g$ med $x$ får vi polynomet $x \cdot g(x) = x^3 + x$. Detta har grad 3 och det har samma $x^3$-koefficient som $f(x)$. Om vi subtraherar $xg(x)$ från $f(x)$, får vi ett polynom av lägre grad eftersom båda termer som innehåller $x^3$ tar ut varandra. Låt oss kalla resultatet för $f_1$:

$$f_1(x) = f(x) - xg(x) = 2x^2 - 4x + 1$$

Vi ser att $\deg f_1 = 2 < \deg f$.

Nu kan vi använda samma idé igen. Vi multiplicerar $g$ med 2 och får vi polynomet $2x^2 + 2$. Om vi subtraherar detta från $f_1$, får vi ett polynom av ännu lägre grad. Låt oss kalla detta polynom för $f_2(x)$:

$$f_2(x) = f_1(x) - 2g(x) = -4x - 1$$

Nu är $\deg f_2 = 1 < \deg g$ och det blir enkelt att dividera $f_2$ med $g$. Det gäller att

$$f_2(x) = -4x - 1 = 0 \cdot g(x) + (-4x - 1)$$

Vi kan nu gå baklänges i räkningen och får följande:

$$\begin{aligned} f_1(x) &= f_2(x) + 2g(x) = 2g(x) + (-4x - 1) \\ f(x) &= f_1 + xg(x) = (2 + x)g(x) + (-4x - 1) \end{aligned}$$

Alltså är polynomen som vi ville hitta $q(x) = 2 + x$ och $r(x) = -4x - 1$. Vi ser att även gradvillkoret är uppfyllt, då $\deg r = 1 < \deg g$.

Det finns en bra och kompakt metod att skriva upp beräkningen av $q(x)$ och $r(x)$ som vi gjorde ovan. Sättet kallas *"liggande stolen"* och finns nedan för vårt exempel. Gå igenom diagrammet och lista ut hur det fungerar; alla polynom där förekommer redan i räkningen ovan.

$$\begin{array}{rrrrrrrrrr} & x & + & 2 & & & & & & \\ \cline{2-10} & (x^3 & + & 2x^2 & - & 3x & + & 1) & \multicolumn{2}{|r}{x^2+1} \\ - & (x^3 & & & + & x) & & & & \\ \cline{2-7} & & & 2x^2 & - & 4x & + & 1 & & \\ & & - & (2x^2 & & & + & 2) & & \\ \cline{3-8} & & & & - & 4x & - & 1 & & \end{array}$$

▲

Vad hände i exemplet? Vi skulle dividera polynomet $f$ med polynomet $g$. Vi reducerade problemet till samma uppgift för ett annat polynom $f_1$ som hade lägre grad, $\deg f_1 < \deg f$. Denna reducering upprepade vi, och fick ett polynom $f_2$ där uppgiften var enkel. Sedan använde vi lösningen för $f_2$ för att beräkna lösningen till vår ursprungliga uppgift. Eftersom gradtalen av alla polynom som förekom på vägen blev mindre och mindre, var vi garanterade att komma till ett polynom med grad mindre än $\deg g$, där vi kunde lösa uppgiften direkt.

*Bevis av Sats 2.3.1 (Division med rest för polynom).* Vi börjar med att betrakta specialfallet när $\deg g = 0$, d.v.s. när $g$ är konstant. Då är $g(x) = c$ för något $c \in \mathbb{C}$ och eftersom $g$ inte är nollpolynomet, är $c \neq 0$. Vi kan då skriva $f = \frac{f}{c}g + 0$ och får $q(x) = f(x)/c$ och $r(x) = 0$ som uppfyller $\deg r = -\infty < 0 = \deg g$.

Betrakta nu det allmänna fallet när $\deg g = m > 0$. Vi skriver

$$g(x) = b_m x^m + \ldots + b_1 x + b_0$$

där $b_m \neq 0$. Vi visar existensen av $q$ och $r$ genom induktion över $\deg f$.

Antag först, som basfall för induktionen, att $\deg f < m$. Vi kan då skriva $f$ på formen $f = 0g + f$ och eftersom $\deg f < m = \deg g$ kan vi sätta $q = 0$ och $r = f$.

Antag nu att påståendet stämmer när $f$ har grad högst $n$ för något $n \geqslant m-1$. Låt $f$ vara ett polynom av grad $n+1 \geqslant m$:

$$f(x) = a_{n+1}x^{n+1} + a_n x^n + \ldots + a_2 x^2 + a_1 x + a_0$$

Som i exemplet subtraherar vi en lämplig multipel av $g$ från $f$ för att få ett polynom av lägre grad.

$$\begin{aligned} f_1(x) &= f(x) - \frac{a_{n+1}}{b_m}x^{n+1-m}g(x) \\ &= \left(a_{n+1}x^{n+1} + \ldots + a_1 x + a_0\right) - \frac{a_{n+1}}{b_m}x^{n+1-m}\left(b_m x^m + \ldots b_1 x + b_0\right) \\ &= \left(a_n - \frac{a_{n+1}}{b_m}b_{m-1}\right)x^n + \ldots + \left(a_{n+1-m} - \frac{a_{n+1}}{b_m}b_0\right)x^{n+1-m} + \\ &\quad + a_{n-m}x^{n-m} + \ldots + a_2 x^2 + a_1 x + a_0. \end{aligned}$$

Vi ser att $\deg f_1 \leqslant n$ eftersom koefficienterna framför $x^{n+1}$ i både $f(x)$ och $\frac{a_{n+1}}{b_m}x^{n+1-m}g(x)$ tar ut varandra, och vi kan använda vårt induktionsantagande. Eftersom $\deg f_1 \leqslant n$, kan vi skriva $f_1$ på formen $f_1 = q_1 g + r$ för polynom $q_1$ och $r$ där $\deg r < \deg g$. Vi får följande uttryck för $f$:

$$\begin{aligned} f(x) &= f_1(x) + \frac{a_{n+1}}{b_m}x^{n+1-m}g(x) \\ &= q_1(x)g(x) + r(x) + \frac{a_{n+1}}{b_m}x^{n+1-m}g(x) \\ &= \left(q_1(x) + \frac{a_{n+1}}{b_m}x^{n+1-m}\right)g(x) + r(x) \end{aligned}$$

Vi har alltså hittat $q(x) = q_1(x) + \frac{a_{n+1}}{b_m} x^{n+1-m}$ och $r(x)$ med $\deg r < \deg g$. □

Som för de naturliga talen, visar det sig att polynomen $q$ och $r$ är entydigt bestämda av $f$ och $g$. Detta ger oss divisionssatsen för polynom, som är motsvarigheten för divisionssatsen för de naturliga talen.

**Sats 2.3.3** (Divisionssatsen för polynom)**.** *Låt $f$ och $g \neq 0$. Då finns det unika polynom $q$ och $r$ så att* $\deg r < \deg g$ *och $f = q \cdot g + r$.*

*Bevis.* Vi har redan visat existensen av $q$ och $r$ i Sats 2.3.1. Det kvarstår att visa att de är unika. Antag att både $q_1$ och $r_1$, och $q_2$ och $r_2$, uppfyller villkoren. I så fall är

$$q_1 g + r_1 = q_2 g + r_2.$$

Vi skriver om och får

$$(q_1 - q_2)g = r_2 - r_1.$$

Vi jämför gradtalen av polynomen på båda sidor av ekvationen: Om $q_1 - q_2 \neq 0$, så har vänstersidan enligt Lemma 2.2.3 grad minst $\deg g$. Både $r_1$ och $r_2$ har grad mindre än $\deg g$ enligt våra antaganden och enligt Lemma 2.2.3 gäller det att $\deg(r_1 - r_2) < \deg g$. Detta är en motsägelse, så $q_1 - q_2 = 0$ och därmed även $r_1 = r_2$. □

**Definition 2.3.4.** Låt $f, g, q$ och $r$ vara polynom som uppfyller att $f = qg + r$ och där $\deg r < \deg g$. Vi kallar $q$ *kvoten* och $r$ *resten* vid division av $f$ med $g$.

Vi kan definiera vad det betyder att två polynom delar varandra på samma sätt som för de naturliga talen.

**Definition 2.3.5.** Vi säger att polynomet $f$ är delbart med polynomet $g$ om det finns ett polynom $q$ så att $f = qg$.

## 2.4 Rötter och faktorsatsen

Vi ska nu betrakta *nollställen* av polynom närmare, och med hjälp av divisionssatsen för polynom visa den så kallade faktorsatsen.

**Hjälpsats 2.4.1.** *Givet ett polynom $f(x)$ och ett tal $\alpha \in \mathbb{C}$, så gäller ekvationen*

$$f(x) = q(x)(x - \alpha) + f(\alpha)$$

*för något polynom $q(x)$. Med andra ord: resten av $f$ vid division med $x - \alpha$ är lika med funktionsvärdet $f(\alpha)$.*

*Bevis.* Enligt restsatsen för polynom, tillämpad på $f(x)$ och $g(x) = x - \alpha$, kan vi skriva $f(x)$ på formen $f(x) = q(x)(x - \alpha) + r(x)$ där $r(x)$ är ett polynom av grad mindre än $\deg g = 1$. Alltså är $r(x) = c$ för något $c \in \mathbb{C}$. Sätter vi $x = \alpha$ i ekvationen $f(x) = q(x)(x - \alpha) + c$, får vi $f(\alpha) = c$. □

**Definition 2.4.2.** Ett tal $\alpha \in \mathbb{C}$ kallas ett *nollställe* eller en *rot* till polynomet $f(x)$ om $f(\alpha) = 0$.

**Sats 2.4.3** (Faktorsatsen)**.** *Låt $f$ vara ett polynom och $\alpha \in \mathbb{C}$. Talet $\alpha$ är en rot till $f$ om och endast om $f$ är delbart med polynomet $x - \alpha$.*

*Bevis.* Antag först att $f$ är delbart med polynomet $x - \alpha$. Vi kan då skriva $f(x) = (x - \alpha)q(x)$ för något polynom $q(x)$. Om vi sätter in $x = \alpha$ får vi

$$f(\alpha) = (\alpha - \alpha)q(\alpha) = 0$$

oavsett värdet $q(\alpha)$. Alltså är $\alpha$ en rot till $f$.

Antag nu att $\alpha$ är en rot till $f$, dvs $f(\alpha) = 0$. Enligt Lemma 2.4.1 kan vi skriva $f(x)$ på formen $f(x) = (x - \alpha)q(x) + f(\alpha) = (x - \alpha)q(x) + 0$. Vi får alltså att $f(x) = q(x)(x - \alpha)$ och att $f(x)$ är delbart med $x - \alpha$. □

Om $\alpha$ är en rot till polynomet $f$, kan vi skriva $f = (x - \alpha)f_1$ för något polynom $f_1$. Om $\alpha$ också är en rot till $f_1$, så kan vi upprepa processen och får att $f_1 = (x-\alpha)f_2$ för något polynom $f_2(x)$. Därmed gäller $f = (x-\alpha)^2 f_2$. Vi kan fortsätta med detta tills vi kommer till $f = (x - \alpha)^m f_m$ för något $m$ och något polynom $f_m(x)$ där $f_m(\alpha) \neq 0$. Notera att $(x - \alpha)^m$ inte kan dela $f$ för något $m > \deg f$ på grund av Sats 2.2.3, dvs efter högst $\deg f$ gånger måste vi komma till ett $f_m$ med $f_m(\alpha) \neq 0$.

**Definition 2.4.4.** Talet $\alpha$ kallas en *rot av multiplicitet $m$* till polynomet $f$ om vi kan skriva $f$ på formen $f = (x - \alpha)^m q$ för något polynom $q$ med $q(\alpha) \neq 0$.

Notera att en rot till ett polynom som vi definierade tidigare är en rot av multiplicitet 1 eller högre enligt denna definition. Det är också vad vi menar i framtiden när vi skriver att något tal är en rot till något polynom utan att nämna multipliciteten.

**Exempel 2.4.5.** Betrakta polynomet $f(x) = x^3 + x^2 - x - 1$. Vi ser att $x = 1$ och $x = -1$ är rötter till $f$ eftersom $f(1) = f(-1) = 0$. För att beräkna multipliciteten av roten $x = 1$, utför vi polynomdivision och delar $f$ med $x - 1$ vilket ger $f(x) = (x - 1)q_1(x)$ där $q_1(x) = x^2 + 2x + 1$. Eftersom $q_1(-1) \neq 0$, är $x = -1$ en rot av multiplicitet 1. För roten $x = -1$ finner vi att $f(x) = (x + 1)q_2(x)$ där $q_2(x) = x^2 - 1$. Nu gäller det att $q_2(-1) = 0$ igen och vi utför polynomdivision en gång till för att få $q_2(x) = (x + 1)(x - 1)$ och därmed $f(x) = (x+1)^2 q_3(x)$ där $q_3(x) = x - 1$. Nu är $q_3(-1) \neq 0$ och $x = -1$ är en rot av multiplicitet 2. ▲

I avsnitt 3.3 ska vi se att vi alltid kan bryta ut faktorna på formen $(x - \alpha)^m$ för alla olika rötter och respektive multipliciteter samtidigt.

## Övningar

**Övning 2.1.** Visa att

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{2n^3 + 3n^2 + n}{6} \tag{2.2}$$

gäller för alla $n \in \mathbb{N}$ med hjälp av induktionsprincipen.

**Övning 2.2.** Visa de Moivres formel $(e^{i\theta})^k = e^{ik\theta}$, där $k \in \mathbb{N}$, med hjälp av induktion.

**Övning 2.3.** Visa Lemma 2.2.3: Låt $f$ och $g$ vara polynom.

1. Visa att $\deg(fg) = \deg f + \deg g$.
2. Visa att $\deg(f + g) \leqslant \max\{\deg f, \deg g\}$.
3. Ange två polynom $f$ och $g$ sådana att $\deg(f + g) < \max\{\deg f, \deg g\}$.

**Övning 2.4.** Beräkna kvoten och resten vid

1. division av $f(x) = x^4 - 5x^2 + 4x^2 - 14x + 4$ med $g(x) = x^2 + 3$. (Använd polynomdivison.)
2. division av $f(x) = x^n - 1$ med $g(x) = x - 1$ för alla $n > 0$. (Beräkna lösningen med polynomdivision för små $n$ och gissa den allmänna formeln. Visa sedan den allmänna lösningen med induktionsprincipen.)

**Övning 2.5.** Om två polynom $f$ och $g$ båda är delbara med polynomet $h$, kallas $h$ en *gemensam delare* av $f$ och $g$. Uppgiften leder dig genom beviset att det finns ett unikt moniskt polynom av maximal grad som är gemensam delare till $f$ och $g$. Detta polynom kallas *största gemensamma delare* av $f$ och $g$ och betecknas med $\operatorname{sgd}(f, g)$. En bra metod att beräkna $\operatorname{sgd}(f, g)$ är Euklides algoritm som vi nu ska förklara: Låt $f$ och $g$ vara två polynom. Om $\deg f < \deg g$, byt namn på polynomen. Skriv $f_0 = f$ och $f_1 = g$. Beräkna kvoten $q_2$ och resten $f_2$ vid division av $f_0$ med $f_1$. Om inte $f_2 = 0$, beräkna kvoten $q_3$ och resten $f_3$ vid division av $f_1$ med $f_2$. Fortsätt tills du får att $f_{k+1} = 0$.

1. Visa att $f_k$ är en gemensam delare av $f$ och $g$. (Visa det mer allmäna påståendet att $f_k$ delar alla $f_i$.)
2. Visa att om $h$ är en gemensam delare av $f$ och $g$, så är $h$ även en delare av $f_k$. (Visa mer allmänt att $h$ delar alla $f_i$.)

Vi har nu visat att $f_k$ som beräknat i Euklides algoritm är ett polynom med maximal grad som delar $f$ och $g$. Vi delar $f_k$ med första koefficienten så att polynomet blir moniskt. Resultatet kallar vi *största gemensamma delaren* och skriver $\operatorname{sgd}(f, g)$.

(c) Använd Euklides algoritm för att beräkna $\text{sgd}(2x^4 - 5x^3 + 2x^2 + 4x - 5, 2x^3 - 3x^2 - 2x + 3)$.

**Övning 2.6.** Låt $f$ vara ett *reellt* polynom.

1. Visa att $f(\overline{z}) = \overline{f(z)}$ för alla $z \in \mathbb{C}$. (Använd räknereglerna för komplexa tal och deras konjugat.)

2. Visa att om $\alpha \in \mathbb{C}$ är en rot till $f$, så är även $\overline{\alpha}$ en rot till $f$.

**Övning 2.7.** Ekvationen $x^4 + 2x^3 + 3x^2 + 2x + 2 = 0$ har en rot $x = -1 + i$. Bestäm samtliga rötter.

**Övning 2.8.** Låt $\alpha \in \mathbb{C}$ vara en rot till polynomet $f$. Visa att $\alpha$ har multiplicitet större än ett om och endast om $\alpha$ är en rot till derivatan $f'$. (Använd definitionen av multiplicitet och produktregeln för derivatan.)

# 3 Irreducibilitet

I detta kapitel kommer vi att studera hur polynom kan faktoriseras som produkter av polynom av lägre grad, och specifikt kommer vi att studera hur de möjliga faktoriseringarna beror på vilka koefficienter man tillåter sig att använda. Låt oss motivera detta med ett exempel.

**Exempel 3.0.6.** Betrakta polynomet

$$f(x) = x^4 - 2,$$

som har rationella koefficienter (till och med heltalskoefficienter). En gång i tiden kände man inte till irrationella tal (det vill säga, man trodde att alla tal kunde skrivas som en kvot av heltal), och i så fall hade man fått svårt att faktorisera polynomet ovan. Det visar sig att så fort vi försöker faktorisera polynomet kommer vi att behöva introducera irrationella koefficienter. För att faktorisera polynomet kan vi till exempel först använda konjugatregeln:

$$f(x) = (x^2 - \sqrt{2})(x^2 + \sqrt{2}),$$

och $\sqrt{2}$ är ett känt exempel på ett irrationellt tal. I nästa kapitel kommer vi också att visa att $\sqrt{2}$ är irrationellt.

Denna faktorisering kan dock tas ett steg längre: den första faktorn, $(x^2 - \sqrt{2})$, är noll när $x = \pm\sqrt[4]{2}$. Vi kan alltså faktorisera polynomet som

$$f(x) = (x + \sqrt[4]{2})(x - \sqrt[4]{2})(x^2 + \sqrt{2}).$$

Om vi vill faktorisera polynom vidare kommer vi dock att behöva gå ännu ett steg längre än att införa irrationella koefficienter: vi behöver komplexa tal, som också en gång i tiden var okända. Ty $x^2$ är alltid positivt om $x$ är reellt, $\sqrt{2}$ är alltid positivt, så den sista faktorn kan aldrig vara noll för reella $x$. Introducerar vi komplexa tal kan även sista faktorn faktoriseras, och man finner att

$$f(x) = (x + \sqrt[4]{2})(x - \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2}).$$

Längre än så här kan polynomet uppenbarligen inte faktoriseras. ▲

I detta kapitel ska vi försöka formalisera flera saker som beskrivits på ett vagt sätt i exemplet ovan: vad menar vi när vi pratar om vilken sorts koefficienter vi ”tillåter” i en faktorisering? Vad betyder det att faktorisera ett polynom ”så långt som möjligt”? Är en faktorisering i ”minsta möjliga delar” unik — hade vi kunnat få en annan faktorisering genom att först dividera bort $(x + \sqrt[4]{2})$ i stället för att först använda konjugatregeln? Och hur visar man egentligen att det måste behövas irrationella tal för att faktorisera $x^4 - 2$?

Det första vi gör är att specificera vad vi menar med en ”sorts” koefficienter som vi använder i en faktorisering. Vi vill inte tillåta koefficienter ur en godtycklig delmängd av komplexa talen, utan för kunna säga något intressant

måste vi kräva att koefficienterna tas från en *delkropp* av de komplexa talen. Sedan definierar vi vad vi menar med att ett polynom är irreducibelt över en delkropp, vilket svarar mot att polynomet har faktoriserats i så små faktorer som möjligt när vi endast tillåter koefficienter i delkroppen. Den viktiga satsen vi visar i detta kapitel är att polynom kan faktoriseras på ett unikt sätt i irreducibla faktorer.

## 3.1 Delkroppar och irreducibilitet

**Definition 3.1.1.** Låt $\mathbb{K} \subseteq \mathbb{C}$ vara en delmängd. Vi säger att $\mathbb{K}$ är en *delkropp till* $\mathbb{C}$ om följande villkor är uppfyllda:

1. $0 \in \mathbb{K}$;
2. $1 \in \mathbb{K}$;
3. Om $x, y \in \mathbb{K}$, kommer även $x + y \in \mathbb{K}$ och $xy \in \mathbb{K}$;
4. Om $x \in \mathbb{K}$ kommer $1/x \in \mathbb{K}$ och $-x \in \mathbb{K}$.

**Anmärkning 3.1.2.** Det definitionen ovan säger är att en delkropp är en delmängd där vi kan använda alla fyra räknesätten — addition och multiplikation enligt villkor 3, och eftersom division med $x$ är multiplikation med $1/x$ och subtraktion med $x$ är addition med $-x$, ger villkor 4 att även dessa räknesätt inte kan få oss att hamna utanför delkroppen.

**Anmärkning 3.1.3.** Oftast kommer vi endast att skriva *delkropp* när vi menar delkropp till $\mathbb{C}$.

**Exempel 3.1.4.** Följande delmängder till $\mathbb{C}$ är viktiga exempel på delkroppar: delmängden $\mathbb{Q}$ av rationella tal, delmängden $\mathbb{R}$ av reella tal, och delmängden $\mathbb{C}$ av alla komplexa tal. I övningarna i slutet av kapitlet kommer vi att se fler exempel på delkroppar. ▲

**Definition 3.1.5.** Låt $f$ vara ett polynom med koefficienter i en delkropp $\mathbb{K}$. Vi säger att $f$ är *irreducibelt över* $\mathbb{K}$ om det inte går att skriva $f$ som en produkt av två polynom med koefficienter i $\mathbb{K}$, $f = gh$, där både $g$ och $h$ har strikt lägre grad än $f$.

**Exempel 3.1.6.** Varje polynom av grad 0 eller 1 är irreducibelt över varje delkropp över huvud taget. Ty om $f = gh$ är $\deg f = \deg g + \deg h$. Om $\deg f = 0$ måste då $\deg g = \deg h = 0$, så ingen av dem kan ha strikt lägre grad. Om $\deg f = 1$ måste den ena av $g$ och $h$ ha grad 1, och den andra grad 0, och alltså har inte heller i detta fall bägge lägre grad. ▲

**Exempel 3.1.7.** Det är viktigt i definitionen ovan att man anger över vilken delkropp ett polynom skall vara irreducibelt. Tag till exempel polynomet

$$x^2 + 1.$$

Detta polynom är irreducibelt över $\mathbb{R}$, men inte över $\mathbb{C}$. Ty om man skall skriva polynomet som en produkt av två polynom av lägre grad, måste bägge faktorerna ha grad ett. Men att hitta en förstagradsfaktor till ett polynom är samma sak som att hitta en rot, och vi vet att polynomet inte har några reella rötter eftersom $x^2 \geqslant 0$ för reella värden på $x$. Dock är det inte irreducibelt när vi arbetar över $\mathbb{C}$, ty vi har faktoriseringen

$$x^2 + 1 = (x + i)(x - i).$$

▲

**Exempel 3.1.8.** I allmänhet är det klurigt att avgöra om ett polynom är irreducibelt eller inte, även om föregående exempel var enkelt. Till exempel går det att visa att polynomet

$$f(x) = x^5 + x + 1$$

är irreducibelt över $\mathbb{Q}$, men detta är inte så enkelt. ▲

**Anmärkning 3.1.9.** Låt $f$ vara ett polynom med koefficienter i delkroppen $\mathbb{K}$, och låt $c$ vara koefficienten till högstagradstermen. Då är $g = (1/c) \cdot f$ också ett polynom med koefficienter i $\mathbb{K}$, och $f$ är irreducibelt om och endast om $g$ är irreducibelt. När vi skall avgöra om ett polynom är irreducibelt kan vi alltså anta att polynomet är moniskt.

**Hjälpsats 3.1.10.** *Antag att $f$ och $g$ bägge har koefficienter i delkroppen $\mathbb{K}$, och att $g \neq 0$. Enligt divisionsalgoritmen kan vi nu skriva*

$$f = qg + r$$

*med* $\deg r < \deg g$. *Då har även $q$ och $r$ sina koefficienter i $\mathbb{K}$.*

*Bevis.* Genom att betrakta beviset av divisionsalgoritmen (Sats 2.3.1) ses att man hittar koefficienterna till $q$ och $r$ endast genom att addera, subtrahera, multiplicera och dividera koefficienter till $f$ och $g$. Om alla koefficienter till $f$ och $g$ ligger i $\mathbb{K}$, kommer även alla tal man kan få fram på detta sätt också att göra det, enligt Anmärkning 3.1.2. □

Ovanstående hjälpsats är för oss i princip hela poängen med att betrakta delkroppar: en delkropp är en delmängd av komplexa talen där divisionsalgoritmen för polynom fungerar.

**Exempel 3.1.11.** I fallet $\mathbb{K} = \mathbb{R}$ så säger hjälpsatsen ovan att om vi har två polynom $f$ och $g \neq 0$ med reella koefficienter, och vi räknar ut kvoten och resten vid division av $f$ med $g$, så kommer vi inte att behöva använda komplexa koefficienter varken i kvoten eller resten. ▲

En liknelse som det kan hjälpa att ha i huvudet när man läser detta kapitel är att mängden av alla polynom med koefficienter i någon fix delkropp $\mathbb{K}$

är som heltalen $\mathbb{Z}$, och de moniska irreducibla polynomen är som primtalen. Kom ihåg att ett primtal är ett heltal som inte kan skrivas som en produkt av två mindre heltal, vilket definitivt liknar vår definition av irreducibilitet. Oftast definierar man endast vad det betyder för ett *positivt* heltal att vara ett primtal, och detta liknar vår anmärkning i 3.1.9 att det räcker att titta på moniska polynom när vi talar om irreducibilitet.

Den här "gloslistan" säger hur man skall tänka på de olika begreppen på polynomsidan och heltalssidan.

| | |
|---|---|
| Alla polynom med koefficienter i $\mathbb{K}$ | Mängden av alla heltal |
| Moniska polynom med koefficienter i $\mathbb{K}$ | Positiva heltal |
| Nollskilda konstanta polynom | $\pm 1$ |
| Graden av ett polynom | Absolutbeloppet av ett heltal |
| Moniska irreducibla polynom | $\pm$ Primtal |

Absolutbeloppet kan verka konstigt i tabellen ovan om man bara tänker på beloppet av ett tal som att man tar bort ett eventuellt minustecken. Anledningen att det dyker upp är att både beloppet av ett tal och graden av ett polynom är det sätt man mäter "storleken" av det.

Till exempel gäller att varje heltal kan skrivas som $\pm 1$ gånger ett positivt heltal; på samma sätt kan varje polynom skrivas som en nollskild konstant gånger ett moniskt polynom. En annan likhet är att de nollskilda konstanta polynomen är exakt de polynom $f$ för vilka även $1/f$ är ett polynom, och på samma sätt är $\pm 1$ exakt de heltalen $x$ för vilka $1/x$ också är ett heltal.

Den viktigaste egenskapen hos primtal är att varje positivt heltal kan skrivas på ett unikt sätt som en produkt av primtal. Den sats vi skall visa i detta kapitel är motsvarigheten för polynom: varje moniskt polynom med koefficienter i delkroppen $\mathbb{K}$ kan skrivas på ett unikt sätt som en produkt av moniska irreducibla polynom som har koefficienter i $\mathbb{K}$.

## 3.2 Unik faktorisering

Fixera nu en delkropp $\mathbb{K}$, vilken som helst — i hela detta avsnitt kommer vi att arbeta med en och samma delkropp. För att bli lite mindre långrandiga kommer vi i detta avsnitt att mena "polynom med koefficienter i $\mathbb{K}$" när vi skriver "polynom", och vi kommer att mena "polynom som är irreducibelt över $\mathbb{K}$" när vi skriver "irreducibelt polynom".

Ofta när man vill bevisa att något kan göras på exakt ett sätt, delar man upp beviset i två delar: först visar man att detta kan göras på minst ett sätt, och sedan visar man att det kan göras på högst ett sätt. Så kommer vi att göra även nu.

**Hjälpsats 3.2.1.** *Låt $f$ vara ett moniskt polynom. Det finns minst ett sätt att skriva $f$ som en produkt av moniska irreducibla polynom.*

*Bevis.* Vi använder induktion över $\deg f$. Om $f$ har grad 1 är vi klara, för $f$ är då irreducibelt. Låt graden till $f$ vara $d$, och antag att alla moniska polynom av grad mindre än $d$ kan skrivas som en produkt av irreducibla moniska polynom.

Antag först att $f$ självt är irreducibelt. I så fall kan vi använda produkten som endast innehåller $f$. Så antag att $f$ är reducibelt. I så fall kan vi skriva $f = gh$, där $g$ och $h$ är moniska polynom av lägre grad. Men enligt induktionsantagandet är nu både $g$ och $h$ produkter av moniska irreducibla polynom: genom att skriva dessa produkter efter varandra, ser vi att även $f$ är det. □

Att faktoriseringen är entydig är den kluriga biten. Kom ihåg att vi hela tiden i detta kapitel menar polynom *med koefficienter i vår fixa delkropp* $K$ när vi endast skriver "polynom".

**Sats 3.2.2.** *Varje moniskt polynom $f$ kan skrivas på ett entydigt sätt som en produkt av moniska irreducibla polynom, upp till ordningen av faktorerna, och varje irreducibelt polynom som delar $f$ ingår i denna faktorisering.*

*Bevis.* Vi använder induktion över $\deg f$. Om $\deg f = 1$ är $f$ själv irreducibelt, och kan uppenbarligen inte skrivas som en produkt av irreducibla polynom på mer än ett sätt.

Så antag att $f$ har grad $d$, och att satsen gäller för alla polynom av lägre grad. Antag nu att $f$ har två faktoriseringar i irreducibla polynom:

$$f = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m.$$

Vi delar in i två fall. Antag först att $p_1 = q_1$. I så fall är

$$p_2 p_3 \cdots p_n = q_2 \cdots q_m,$$

och eftersom dessa produkter har gradtal lägre än $d$ måste faktoriseringarna vara lika (upp till ordningen av faktorer). I detta fall är vi klara. Så antag att $p_1 \neq q_1$. Antag utan inskränkning att $\deg p_1 \leqslant \deg q_1$. Enligt divisionsalgoritmen kan vi skriva

$$q_1 = ap_1 + b,$$

där $\deg b < \deg p_1$. Alltså gäller att

$$f = (ap_1 + b)q_2 q_3 \cdots q_m.$$

Vi vet att $p_1$ delar både $f$ och produkten $ap_1 q_2 q_3 \cdots q_m$. Alltså är även deras differens, det vill säga

$$bq_2 q_3 \cdots q_m,$$

delbar med $p_1$. Observera nu att $b$ har strikt lägre grad än $p_1$, och vi antog att $\deg p_1 \leqslant \deg q_1$. Det följer att

$$\begin{aligned} d = \deg(q_1 q_2 \cdots q_m) &= \deg q_1 + \deg(q_2 q_3 \cdots q_m) \\ &> \deg b + \deg(q_2 q_3 \cdots q_m) = \deg(bq_2 q_3 \cdots q_m). \end{aligned}$$

Enligt induktionsantagandet finns det alltså en *unik* faktorisering av produkten $bq_2q_3\cdots q_m$ i irreducibla polynom. Vi ser ett uppenbart sätt att hitta en faktorisering av produkten, nämligen att faktorisera $b$ i irreducibla polynom och sedan multiplicera med faktorerna $q_2, ..., q_m$, som vi vet är irreducibla. Detta är alltså den unika faktoriseringen. Eftersom $p_1$ delar $bq_2q_3\cdots q_m$ vet vi igen enligt induktionsantagandet att $p_1$ är lika med en av dessa irreducibla faktorer. Men vi vet också att $\deg p_1 > \deg b$, så $p_1$ kan inte vara någon av de irreducibla faktorer som vi fick genom att faktorisera $b$. Alltså är $p_1$ lika med någon av $q_2, ..., q_m$, och genom att byta ordning på faktorerna $q_i$ hamnar vi återigen i fallet $p_1 = q_1$. Beviset är klart. □

**Exempel 3.2.3.** Betrakta polynomet $f(x) = x^4 + 2x^3 - x - 2$. Vi har två olika faktoriseringar:

$$f(x) = (x^2 + x + 1)(x^2 + x - 2) = (x^3 - 1)(x + 2).$$

Eftersom det skall finnas en unik faktorisering av $f$ i irreducibla faktorer över $\mathbb{Q}$, så kan inte alla polynomen som ingår i faktoriseringen ovan vara irreducibla över $\mathbb{Q}$. Uppenbarligen är $(x + 2)$ irreducibelt. Polynomet $(x^3 - 1)$ är definitivt inte irreducibelt över $\mathbb{Q}$, eftersom högerledet då skulle vara den unika faktoriseringen i irreducibla polynom.

Mycket riktigt kan man snabbt hitta roten $x = 1$ till $x^3 - 1$, och dividerar vi $x^3 - 1$ med $x - 1$, som vi vet är möjligt enligt Sats 2.4.3, finner vi $x^2 + x + 1$, vilket är en av faktorerna i vänsterledet. Dividerar vi bägge sidor med $x^2+x+1$ kvarstår alltså

$$x^2 + x - 2 = (x - 1)(x + 2).$$

Dessutom är polynomet $x^2 + x + 1$ irreducibelt över $\mathbb{Q}$, så att den unika faktoriseringen av $f$ blir

$$f(x) = (x^2 + x + 1)(x - 1)(x + 2).$$

För att se att $x^2 + x + 1$ är irreducibelt, så noterar vi att om polynomet vore reducibelt skulle det vara en produkt av förstagradsfaktorer, vilket skulle ge polynomet två rationella rötter. Men vi kan enkelt hitta polynomets rötter; de är

$$-\frac{1}{2} \pm \sqrt{\frac{3}{4}} = \frac{-1 \pm \sqrt{3}}{2}$$

enligt $pq$-formeln. Men $\sqrt{3}$ är inte ett rationellt tal. Vi kommer att ge ett bevis av att $\sqrt{3}$ är irrationellt i nästa kapitel. ▲

## 3.3 Multiplicitet av rötter

**Sats 3.3.1.** *Om $\alpha_1, \alpha_2, \ldots, \alpha_k$ är olika rötter till polynomet $f$ av respektive multiplicitet $m_1, m_2, \ldots, m_k$ (det vill säga, $\alpha_1$ har multiplicitet $m_1$, och så vidare), kan vi skriva $f$ på formen*

$$f(x) = (x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \ldots (x - \alpha_k)^{m_k} q(x)$$

*för något polynom $q(x)$.*

*Bevis.* Låt $\mathbb{K}$ vara någon kropp som innehåller koefficienterna till $f$ och alla rötterna $\alpha_i$, till exempel $\mathbb{K} = \mathbb{C}$. Att $f$ har $\alpha_i$ som rot med multiplicitet $m_i$ säger precis att $f$ är delbart med $(x-\alpha_i)^{m_i}$. Eftersom $(x-\alpha_i)$ uppenbarligen är irreducibelt, måste $(x-\alpha_i)^{m_i}$ vara en faktor i den unika faktoriseringen av $f$ i irreducibla polynom över $\mathbb{K}$ som vi vet existerar enligt Sats 3.2.2. Eftersom detta gäller för varje $i$, och polynomen $(x-\alpha_i)$ och $(x-\alpha_j)$ är olika för $i \neq j$, följer satsen. □

Sats 3.3.1 har bland annat som konsekvens att det bara kan finnas ett ändligt antal rötter till ett nollskilt polynom.

**Följdsats 3.3.2.** *Låt $f$ vara ett nollskilt polynom av grad $\deg f = n \geqslant 0$ och låt $\alpha_1, \alpha_2, \ldots, \alpha_k$ vara rötter till $f$ av multiplicitet $m_1, m_2, \ldots, m_k$. Det gäller att*

$$m_1 + m_2 + \ldots + m_k \leqslant n.$$

*Det vill säga, summan av alla multipliciteter av de olika rötterna är högst $n$.*

*Bevis.* Sats 3.3.1 säger att vi kan skriva $f$ på formen

$$f = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\ldots(x-\alpha_k)^{m_k}q(x)$$

för något polynom $q$. Eftersom $f$ var nollskilt, så kan inte heller $q$ vara nollpolynomet och därmed är $\deg q \geqslant 0$. Det följer nu direkt från Sats 2.2.3 att

$$n = \deg f = m_1 + m_2 + \ldots + m_k + \deg q \geqslant m_1 + m_2 + \ldots + m_k. \qquad \square$$

**Följdsats 3.3.3.** *Låt $f$ vara ett nollskilt polynom av grad $n \geqslant 0$. Då har $f$ högst $n$ olika rötter.*

*Bevis.* Antag att $\alpha_1, \alpha_2, \ldots, \alpha_k$ är olika rötter till $f$ med multipliciteter $m_1$, $m_2, \ldots, m_k$. Då gäller $m_i \geqslant 1$ för multipliciteter $m_i$. Vi använder Följdsats 3.3.2 och får

$$n \geqslant m_1 + m_2 + \ldots + m_k \geqslant 1 + 1 + \ldots + 1 = k$$

Alltså är $k \leqslant n$ och det kan inte finnas mer än $n$ olika rötter till $f$. □

## 3.4 Irreducibilitet över $\mathbb{C}$ och $\mathbb{R}$

För att exemplifiera teorin från detta kapitel beskriver vi vilka komplexa respektive reella polynom som är irreducibla. I dessa fall visar det sig vara enkelt att avgöra vilka polynom som är irreducibla. Dock måste man nu känna till den så kallade *algebrans fundamentalsats*:

*Varje polynom med komplexa koefficienter har minst en rot i $\mathbb{C}$.*

Denna sats kommer att visas i detta kompendiums sista kapitel. Det är värt att poängtera att inga resultat i resten av kompendiet kommer att bero på de vi visar i detta avsnitt. Speciellt kommer vi inte att använda dessa resultat i beviset av algebrans fundamentalsats, då detta skulle leda till ett cirkelbevis.

**Sats 3.4.1.** *De enda polynom som är irreducibla över* $\mathbb{C}$ *är de som har grad högst* 1*.*

*Bevis.* Låt $f$ vara ett moniskt irreducibelt icke-konstant polynom med komplexa koefficienter. Enligt algebrans fundamentalsats existerar minst en rot $r \in \mathbb{C}$, och enligt faktorsatsen är $f$ delbart med $(x - r)$. Men $f$ är inte delbart med något polynom av grad minst ett utom sig självt, så $f$ är lika med $(x - r)$. □

Det följer att om $f$ är ett godtyckligt moniskt polynom över $\mathbb{C}$ så kommer den unika faktoriseringen i irreducibla polynom, som vi vet existerar enligt Sats 3.2.2, att se ut som

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_d),$$

där $d = \deg f$. Speciellt har polynomet exakt $d$ rötter räknat med multiplicitet.

**Sats 3.4.2.** *De enda irreducibla polynomen över* $\mathbb{R}$ *är de som har grad högst* 1*, och de andragradspolynom som har två komplexkonjugerade (icke-reella) rötter.*

*Bevis.* Låt $f$ vara ett moniskt irreducibelt polynom med reella koefficienter. Enligt algebrans fundamentalsats har $f$ minst en rot; låt oss kalla den $r$. Vi delar upp i två fall: antingen är $r$ reellt, eller så är $r$ icke-reellt.

I det första fallet vet vi enligt Sats 2.4.3 (Faktorsatsen) att $f$ är delbart med polynomet $(x - r)$. Men eftersom $f$ var irreducibelt över $\mathbb{R}$ är det inte delbart med något annat reellt polynom än sig självt, så $f(x) = (x - r)$.

I det andra fallet vet vi igen att $f$ är delbart med $(x - r)$, och enligt Övning 2.6 och faktorsatsen är det även delbart med $(x - \overline{r})$. Alltså är $f$ även delbart med produkten av dessa, det vill säga

$$(x - r)(x - \overline{r}) = x^2 - (r + \overline{r})x + r\overline{r}.$$

Men detta polynom har *reella* koefficienter! Ty $r + \overline{r} = 2\mathrm{Re}(r)$, och $r\overline{r} = |r|^2$, vilka alltid är rella tal. Eftersom $f$ är delbart med $(x - r)(x - \overline{r})$, som har reella koefficienter, och $f$ var irreducibelt över $\mathbb{R}$, måste

$$f(x) = (x - r)(x - \overline{r}) = x^2 - (r + \overline{r})x + r\overline{r}.$$

Vi har nu visat att $f$ måste ha grad ett eller vara ett andragradspolynom utan reella rötter. Omvändningen, att alla dessa polynom är irreducibla över $\mathbb{R}$, är enkelt. □

## Övningar

**Övning 3.1.** Bevisa aritmetikens fundamentalsats: *Varje heltal $n \geqslant 2$ kan skrivas unikt som en produkt av primtal, upp till ordningen av faktorerna*, genom att imitera beviset för polynom.

**Övning 3.2.** Låt $D$ vara ett rationellt tal, och $\sqrt{D}$ en av dess kvadratrötter. Vi antar inte nödvändigtvis att $D$ är positivt. Låt $\mathbb{Q}[\sqrt{D}]$ beteckna mängden

$$\{a + b\sqrt{D} \mid x, y \in \mathbb{Q}\} \subset \mathbb{C}.$$

Visa att $\mathbb{Q}[\sqrt{D}]$ är en delkropp. Ledning: för att se att man kan utföra division i $\mathbb{Q}[\sqrt{D}]$, jämför med hur man dividerar två komplexa tal.

**Övning 3.3.** Faktorisera

$$f(x) = x^4 + 3x^3 - 2x^2 - 10x - 12$$

i irreducibla reella faktorer, givet att $-1 + i$ är en rot till $f$.

**Övning 3.4.** Låt $f$ vara ett polynom med reella koefficienter. Visa att antalet icke-reella rötter till $f$, räknat med multiplicitet, är jämnt. Visa speciellt att alla reella polynom av udda grad har en reell rot.

**Övning 3.5.** Antag att ett reellt polynom $f$ har egenskapen att $f(x)$ och $f(x^2)$ har samma antal irreducibla faktorer över $\mathbb{R}$. Vad kan man säga om rötterna till $f$?

# 4 Gauss Lemma

I förra kapitlet diskuterades faktorisering av polynom i irreducibla faktorer över någon delkropp till $\mathbb{C}$. Vi studerade fallen $\mathbb{K} = \mathbb{R}$ och $\mathbb{K} = \mathbb{C}$, och såg att det fanns en enkel beskrivning av exakt hur de irreducibla polynomen ser ut. I detta kapitel fokuserar vi på delkroppen $\mathbb{Q}$ i stället, och vi kommer se att det finns en mycket rikare teori i detta fall.

Det första vi kommer att göra är att jämföra två olika problem: faktorisering med heltalskoefficienter och faktorisering med rationella koefficienter. Även om heltalen inte är en delkropp till $\mathbb{C}$, visar det sig att detta fall passar väl in i teorin som presenterades i föregående kapitel. Det finns nämligen en känd sats som brukar kallas *Gauss lemma*, och med hjälp av den kan man visa att så fort ett polynom med heltalskoefficienter kan skrivas som en produkt av polynom med rationella koefficienter, kan polynomet också skrivas som en produkt av polynom med heltalskoefficienter. Irreducibilitet över rationella talen är därför "samma sak" som irreducibilitet över heltalen.

Med hjälp av detta kan vi också hitta en enkel algoritm med vars hjälp man kan hitta alla rationella rötter till ett godtyckligt polynom med rationella koefficienter.

Efter detta kommer vi att visa Eisensteins kriterium, som förvånande ofta är användbart om man är given ett polynom som man vill bevisa är irreducibelt över $\mathbb{Q}$.

## 4.1 Primitiva polynom och Gauss lemma

Vi börjar med några observationer om hur polynom med rationella koefficienter kan skrivas om som polynom med heltalskoefficienter, och vice versa.

**Exempel 4.1.1.** Polynomet

$$f(x) = x^2 + \frac{1}{6}x - \frac{1}{3} = \left(x - \frac{1}{2}\right)\left(x + \frac{2}{3}\right)$$

har rationella koefficienter, och är reducibelt över de rationella talen. Dock är det inte särskilt meningsfullt att fråga sig om $f$ kan faktoriseras över heltalen: eftersom koefficienterna till $f$ inte är heltal, kan man omöjligen hitta två polynom $g$ och $h$ med heltalskoefficienter som uppfyller $f = g \cdot h$. Däremot blir frågan meningsfull om man först sätter alla termer i polynomet $f$ på ett gemensamt bråkstreck. Den minsta gemensamma nämnaren till alla termer i $f$ är 6, och multiplicerar vi med 6 får vi en faktorisering även över heltalen:

$$6 \cdot f(x) = 6x^2 + x - 2 = (2x - 1)(3x + 2).$$

Dock hade vi inte nödvändigtvis behövt multiplicera med minsta gemensamma nämnaren. Hade vi multiplicerat med en godtycklig multipel av 6 hade vi fortfarande fått ett polynom med heltalskoefficienter och en faktorisering över heltalen. ▲

I föregående kapitel var det smidigt att slippa oroa sig över tvetydigheter som kommer från att man kan multiplicera hela polynomet med en konstant genom att begränsa sig till moniska polynom. Motsvarigheten för polynom med heltalskoefficienter är att begränsa sig till så kallade primitiva polynom:

**Definition 4.1.2.** Låt $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ vara ett polynom med alla koefficienter $a_i$ heltal. Vi säger att $f$ är *primitivt* om det inte existerar något heltal $N > 1$ sådant att $N$ delar varje koefficient $a_i$.

I vårt exempel ovan var polynomet $6f$ primitivt, men (exempelvis) $42f$ är inte det.

**Hjälpsats 4.1.3.** *För varje polynom $f$ med rationella koefficienter finns ett rationellt tal $a$ sådant att $a \cdot f$ har heltalskoefficienter och är primitivt. Om $a'$ är något annat sådant tal, är $a' = \pm a$.*

*Bevis.* Genom att multiplicera $f$ med en gemensam multipel till varje tal som ingår i nämnarna till koefficienterna till $f$, fås ett polynom $pf$ med heltalskoefficienter. Delar vi sedan $pf$ med den största gemensamma delaren $q$ till de resulterande heltalskoefficienterna fås ett primitivt polynom, ty om det resulterande polynomet inte vore primitivt skulle vi kunna hitta en ännu större gemensam delare. Alltså fungerar $a = p/q$.

Antag att talet $a' = p'/q'$ också skulle uppfylla villkoret i hjälpsatsen. Antag också att $p/q$ respektive $p'/q'$ är reducerade bråk, det vill säga, att täljare och nämnare saknar gemensamma faktorer. Eftersom $p'qa = pq'a'$, är också

$$p'qaf = pq'a'f.$$

Bägge led är polynom med heltalskoefficienter. Notera nu att $p'$ delar alla koefficienter i högerledet. Eftersom $p'$ saknar gemensamma delare med $q'$, och $a'f$ är ett primitivt polynom och därför inte har några tal som delar varje koefficient, följer det att $p'$ delar $p$. På samma sätt delar $p$ talet $p'$, $q$ delar $q'$, och $q'$ delar $q$. Det följer att $p = \pm p'$ och $q = \pm q'$. □

**Exempel 4.1.4.** För polynomet

$$f(x) = x^2 + \frac{1}{6}x - \frac{1}{3}$$

som vi såg i ett tidigare exempel, ska talet $a$ i Hjälpsats 4.1.3 väljas till $\pm 6$. ▲

Den centrala observationen i beviset av Gauss lemma formulerar vi som en egen hjälpsats.

**Hjälpsats 4.1.5.** *Låt $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $g(x) = b_m x^m + \ldots + b_0$. Skriv $f(x)g(x) = c_{n+m}x^{n+m} + c_{n+m-1}x^{n+m-1} + \ldots + c_0$. Fixera ett primtal $p$, och antag att inte varje koefficient till $f$ eller $g$ är delbar med $p$. Om $a_i$ är den koefficient till $f$ som har lägst grad av de som ej är delbara med $p$, och $b_j$ är motsvarande koefficient till $g$, så kommer $c_{i+j}$ inte heller att vara delbar med $p$.*

*Bevis.* Låt oss först tänka på hur den $(i+j)$:te koefficienten till $fg$ ser ut. För att få en $x^{i+j}$-term vid multiplikationen av $f$ med $g$, så måste man multiplicera en term $a_k x^k$ och en term $b_l x^l$, där $k+l = i+j$. Alltså kan vi ha $(k,l) = (0, i+j)$, $(k,l) = (1, i+j-1)$, och så vidare, vilket ger att

$$c_{i+j} = a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_i b_j + \cdots + a_{i+j-1} b_1 + a_{i+j} b_0.$$

Nu gäller det att alla termer i denna summa *utom* $a_i b_j$ är delbar med $p$. För att se detta, notera att alla $a_k$ för $k < i$ enligt antagande är delbara med $p$ — vi har ju sagt att $a_i$ ska vara den lägsta koefficienten som ej är delbar med $p$ — och alla termer som kommer före $a_i b_j$ i summan är delbar med någon av dessa. Analogt vet vi att alla $b_k$ för $k < j$ är delbara med $p$, och alla termer som kommer efter $a_i b_j$ är delbara med någon av dessa. Men eftersom varken $a_i$ eller $b_j$ var delbara med $p$, är deras produkt inte det heller. (Här är enda stället vi använder att $p$ är ett primtal!)

Alltså är $c_{i+j}$ en summa av ett tal som är delbart med $p$ (nämligen summan av alla termer utom $a_i b_j$) och ett tal som ej är delbart med $p$ (den återstående termen, $a_i b_j$ självt). En sådan summa kan aldrig själv vara delbar med $p$. □

**Sats 4.1.6.** *(Gauss lemma.) Låt $f$ och $g$ vara två primitiva polynom. Då är även deras produkt $fg$ primitiv.*

*Bevis.* Låt oss anta motsatsen, att $fg$ inte är primitivt. Då existerar ett tal $N > 1$ som delar varje koefficient till $fg$. Låt $p$ vara ett primtal som delar $N$: då gäller att även $p$ delar varje koefficient till $fg$. Dock vet vi att både $f$ och $g$ var primitiva, så det kan inte gälla att $p$ delar varje koefficient till vare sig $f$ eller $g$. Alltså måste det existera någon koefficient $a_i$ till $f$ av lägsta gradtal som ej är delbar med $p$, och någon minsta koefficient $b_j$ till $g$ som ej är delbar med $p$. Men enligt föregående hjälpsats är i så fall den $(i+j)$:te koefficienten till $fg$ inte delbar med $p$, vilket är en motsägelse. Beviset är klart. □

Följande sats ger tillämpningen till irreducibilitet. Låt oss säga att ett polynom $f$ med heltalskoefficienter är *irreducibelt över $\mathbb{Z}$* om det inte existerar polynom $g, h$, av strikt lägre grad med heltalskoefficienter, sådana att $f = gh$.

**Följdsats 4.1.7.** *(Gauss lemma, alternativ form.) Ett polynom $f$ med heltalskoefficienter är irreducibelt över $\mathbb{Z}$ om och endast om det är $f$ irreducibelt över $\mathbb{Q}$.*

*Bevis.* Det är klart att om $f$ är irreducibelt över $\mathbb{Q}$ är det även irreducibelt över $\mathbb{Z}$.

Att dela bort en konstant påverkar inte irreducibilitet, så vi kan utan inskränkning anta att $f$ är primitivt. Antag att $f$ är reducibelt över $\mathbb{Q}$, så att det existerar en faktorisering

$$f = gh$$

där $g$ och $h$ har rationella koefficienter. Nu existerar det som i Hjälpsats 4.1.3 $c$ och $d$ sådana att $cg$ och $dh$ är primitiva polynom med heltalskoefficienter. Men i så fall är enligt Sats 4.1.6 även

$$cdf = (cg)(dh)$$

ett primitivt polynom! Eftersom både $f$ och $(cd)f$ är primitiva polynom med heltalskoefficienter, ger Hjälpsats 4.1.3 att $cd = \pm 1$. Alltså är

$$f = \pm(ag)(bh)$$

en faktorisering över heltalen. □

**Följdsats 4.1.8.** *(Kriterium för rationella rötter.) Låt $f(x) = a_n x^n + \cdots + a_0$ vara ett polynom med heltalskoefficienter. Antag att det rationella talet $x_0$ är en rot till $f$, och att*

$$x_0 = \frac{p}{q}$$

*där $p$ och $q$ saknar gemensam faktor. Då gäller att $q$ delar $a_n$ och $p$ delar $a_0$.*

*Bevis.* Enligt Faktorsatsen 2.4.3 är $f$ delbart med $(x - x_0)$. Vi får alltså en faktorisering över de rationella talen:

$$f(x) = (x - x_0) \cdot \frac{f(x)}{(x - x_0)}.$$

Som i beviset för föregående sats får vi en faktorisering över heltalen genom att multiplicera bägge faktorer med en konstant för att göra bägge faktorerna primitiva. Faktorn $(x - x_0)$ blir primitiv genom att multiplicera med $q$, så det finns en faktorisering

$$f(x) = (qx - p)g(x),$$

där $g$ har heltalskoefficienter. Men multiplicerar man ut högerledet ses nu att högstagradskoefficienten till $f$ är $q$ gånger högstagradskoefficienten till $g$, och konstanttermen till $f$ är $p$ gånger konstanttermen till $g$. Speciellt gäller alltså $q|a_n$ och $p|a_0$. □

**Anmärkning 4.1.9.** Ett användbart specialfall av 4.1.8 är när polynomet $f$ faktiskt är moniskt. I så fall skall nämnaren till en eventuell rationell rot dela termen $a_n$, som är 1, så nämnaren kan endast vara 1 och roten är faktiskt ett heltal. Detta ger följande användbara regel: *om ett moniskt polynom med heltalskoefficienter har en rationell rot, är denna rot ett heltal, och polynomets konstantterm är jämnt delbar med roten.*

**Exempel 4.1.10.** En omedelbar konsekvens är att det existerar reella tal som inte är rationella. Till exempel kan inte $\sqrt{2}$ vara rationellt, det vill säga, det existerar inte heltal $p$ och $q$ med

$$\frac{p}{q} = \sqrt{2}.$$

Ett sådant tal skulle nämligen vara en rationell lösning till ekvationen $x^2 - 2 = 0$, och enligt föregående anmärkning måste $p/q$ vara ett heltal som delar 2, alltså $\pm 1$ eller $\pm 2$, vilket är absurt. ▲

**Anmärkning 4.1.11.** Följdsats 4.1.8 ger en enkel algoritm för att hitta alla rationella rötter till ett polynom med rationella koefficienter. Man börjar med att sätta koefficenterna på en minsta gemensam nämnare, för att få ett polynom med heltalskoefficienter. Sedan vet man att varje rationell rot måste ha egenskapen att dess täljare delar konstanttermen och dess nämnare delar högstagradstermen. Men det finns bara ändligt många olika rationella tal med denna egenskap, och i praktiken går det ofta snabbt att helt enkelt testa alla dessa alternativ för att se om något av dem fungerar. Hittar man ingen rot på detta sätt saknar polynomet rationella rötter.

## 4.2 Eisensteins kriterium

Det är i allmänhet svårt att avgöra huruvida ett polynom med rationella koefficienter är irreducibelt över $\mathbb{Q}$. (Eller, vilket enligt Korollarium 4.1.7 är ett ekvivalent problem, om ett polynom med heltalskoefficienter är irreducibelt över $\mathbb{Q}$.) En enkel metod som fungerar ibland är det så kallade Eisensteins kriterium, som vi nu visar. Den viktiga observationen man behöver göra för att bevisa Eisensteins kriterium är densamma som i beviset av Gauss lemma, som vi tidigare isolerade i Lemma 4.1.5.

**Sats 4.2.1.** *(Eisensteins kriterium) Låt $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ vara ett polynom med heltalskoefficienter. Antag att det existerar ett primtal $p$ med följande tre egenskaper: (i) $p$ delar alla koefficienter $a_i$ för $i < n$; (ii) $p$ delar inte $a_n$; (iii) $p^2$ delar inte $a_0$. Då är $f$ irreducibelt över $\mathbb{Q}$.*

*Bevis.* Antag motsatsen, så $f(x) = g(x)h(x)$, där både $g$ och $h$ har grad minst ett och har heltalskoefficienter. (För att se att $g$ och $h$ kan antas ha heltalskoefficienter måste vi använda Korollarium 4.1.7.) Notera först att $a_n$ är produkten av högstagradskoefficienterna till $g$ och $h$. Eftersom $a_n$ ej är delbart med $p$, är inte heller högstagradskoefficenterna till $g$ eller $h$ det.

Dock hävdar vi nu att alla återstående koefficienter till $g$ och $h$ *är* delbara med $p$, det vill säga, alla koefficienter till $g$ och $h$ utom de högsta är delbara med $p$. Ty antag att det fanns koefficienter till $g$ eller $h$ av lägre grad som ej var delbara med $p$ — i så fall skulle, enligt Lemma 4.1.5, det också existera någon koefficient till $f$ av lägre grad än den högsta som inte var delbart med $p$. Men alla koefficienter utom $a_n$ var delbara med $p$.

Speciellt är konstanttermen till både $g$ och $h$ delbar med $p$. Men konstanttermen till $f$ är produkten av konstanttermerna till $g$ och $h$, så om båda dessa är delbara med $p$ måste $p^2$ dela konstanttermen $a_0$, vilket vi har antagit inte gäller. Denna motsägelse visar att $f$ måste ha varit irreducibelt. □

**Exempel 4.2.2.** Betrakta polynomet $f(x) = 15x^3 - 12x^2 + 98$. Detta polynom kan man visa är irreducibelt över $\mathbb{Q}$ med hjälp av Eisensteins kriterium.

Faktoriserar man koefficienterna i primtal finner man att

$$15 = 3 \cdot 5$$
$$12 = 2 \cdot 2 \cdot 3$$
$$98 = 2 \cdot 7 \cdot 7.$$

Alltså uppfyller $f$ Eisensteins kriterium för primtalet 2, vilket visar att det är irreducibelt. ▲

## Övningar

**Övning 4.1.** Antag att $n$ är ett heltal och att $x^5 + nx + 1$ har minst en rationell rot. Vad kan $n$ ha för värden?

**Övning 4.2.** Visa att $\sqrt{4 + \sqrt{3}}$ är ett irrationellt tal.

**Övning 4.3.** I beviset till Hjälpsats 4.1.5 använder vi att om ett primtal $p$ delar en produkt av heltal $ab$, måste $p$ dela antingen $a$ eller $b$. Varför är det viktigt att $p$ är ett primtal?

**Övning 4.4.** Visa att polynomet $f(x) = x^3 + 3x^2 - 5x + 4$ är irreducibelt över $\mathbb{Q}$. Ledning: om $f = gh$, vilka gradtal kan $g$ och $h$ ha? Vad säger detta om rötter till $f$?

**Övning 4.5.** Använd variabelbytet $y = x - 1$ och Eisensteins kriterium för att visa att polynomet $1 + x + x^2 + x^3 + x^4$ är irreducibelt över $\mathbb{Q}$.

**Övning 4.6.** Låt $f$ vara ett polynom med heltalskoefficienter av grad $d$. Visa att om det finns fler än $2d$ stycken olika heltal $n$ sådana att $f(n)$ är ett primtal, så måste $f$ vara irreducibelt över $\mathbb{Z}$. Ledning: om $f = gh$, hur många lösningar kan det finnas till $g(n) = \pm 1$ respektive $h(n) = \pm 1$?

# 5 Gauss-Lucas sats

I detta kapitel definierar vi först vad vi menar med att en delmängd av $\mathbb{C}$ är *konvex*, och vad som menas med konvexa höljet till en delmängd av punkter i planet. En svårighet när man definierar konvexitet är att det finns ett visst glapp mellan den formella definitionen av en konvex mängd, och den intuitiva bilden av konvexitet. Vi ger därför flera olika definitioner av konvexitet, och vi ger två olika karaktäriseringar av det konvexa höljet, en utifrån snittet av oändligt många konvexa mängder, och en utifrån konvexkombinationer.

Efter allt detta återvänder vi till polynomen. Den sats som detta kapitel fokuserar på, den så kallade Gauss-Lucas sats, säger att rötterna till ett polynoms derivata ligger i det konvexa höljet av rötterna till polynomet självt. Innan vi visar denna sats studerar vi också ett enkelt specialfall, nämligen om man väljer ett polynom $f$ som endast har reella rötter. I detta fall säger Gauss-Lucas sats att $f'$ också endast har reella rötter, och att varje rot till $f'$ ligger mellan två rötter till $f$.

## 5.1 Konvexa mängder i $\mathbb{C}$

I detta kapitel ska vi undersöka begreppet konvexitet och dess egenskaper. Vi kommer att arbeta med delmängder av $\mathbb{C}$, men vi påpekar att alla definitioner fungerar även i andra mängder som t.ex. $\mathbb{R}$. Egenskaperna som vi använder oss av är att man kan bilda summor av element, och multiplicera element med reella tal.

**Definition 5.1.1.** En mängd $K \subseteq \mathbb{C}$ kallas *konvex* om det för alla $z_1$ och $z_2$ i $K$ och $\lambda \in [0,1]$ även gäller att $z = \lambda z_1 + (1-\lambda)z_2$ ligger i $K$.

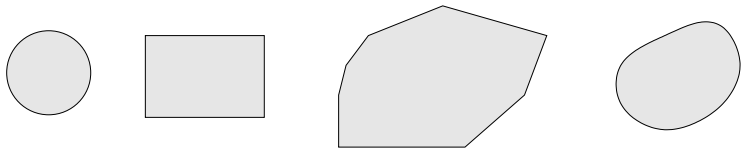
Geometriskt betyder definitionen följande: om man väljer två godtyckliga tal $z_1$ och $z_2$ i en konvex mängd, så är man garanterad att alla punkter som ligger på linjesegmentet mellan $z_1$ och $z_2$ också tillhör mängden $K$. Detta beror på att ekvationen

$$z = \lambda z_1 + (1-\lambda)z_2,$$

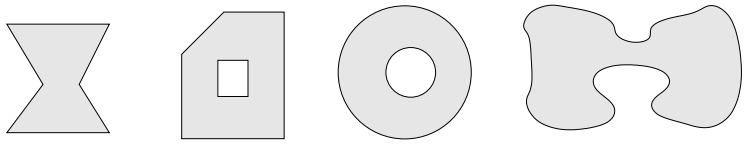
där $\lambda$ varierar över de reella talen, är en parametrisering av linjen som passerar genom $z_1$ och $z_2$. For $\lambda \in [0,1]$ får man precis alla punkter på linjen som ligger mellan $z_1$ och $z_2$. Parametern $\lambda$ bestämmer hur nära punkten $z$ ska ligga $z_1$ eller $z_2$: när $\lambda = 0$ fås $z = z_1$, och när $\lambda = 1$ fås $z = z_2$.

Här är några exempel på konvexa och icke-konvexa mängder i $\mathbb{C}$.

**Exempel 5.1.2.** Betrakta nu följande situation: givet är en konvex mängd $K$, och tre punkter $z_1, z_2$ och $z_3$ som alla tre tillhör $K$ och som bildar hörnen av en triangel. Eftersom $K$ är konvex, tillhör alla punkter på triangelns kanter också $K$. Men vad händer med punkterna som ligger i det inre av triangeln? Låt oss välja en godtycklig punkt $z$ i triangelns inre, och bilda linjen genom $z$ och hörnet $z_1$. Denna linje skär den motstående kanten i någon punkt $x$.

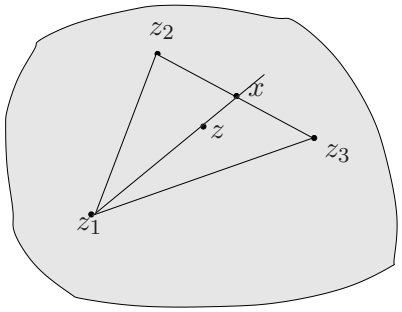


Figur 5.1: Några konvexa mängder



Figur 5.2: Några icke-konvexa mängder

Eftersom $K$ är konvex, och $x$ ligger på segmenten mellan $z_2$ och $z_3$, så vet vi att $x$ är ett element av $K$. Men nu ligger $z$ på segmentet mellan $x$ och $z_1$ och eftersom $K$ är konvex, så ligger även $z$ i mängden $K$. Detta visar att hela triangeln är en delmängd av $K$. ▲




Figur 5.3: Triangeln i $K$

Intuitivt skulle vi kunna säga att en konvex mängd innehåller alla punkter som ligger "någonstans i mitten" mellan ett visst antal av punkter i mängden. Detta ska vi formalisera genom att införa begreppet konvexkombination:

**Definition 5.1.3.** Låt $z_1, z_2, \ldots, z_n$ vara $n$ punkter i $\mathbb{C}$. En summa på formen

$$a_1 z_1 + a_2 z_2 + \ldots + a_n z_n,$$

där $a_1, a_2, \ldots, a_n$ är icke-negativa reella tal som uppfyller att

$$a_1 + a_2 + \ldots + a_n = 1$$

kallas för en *konvexkombination* av punkterna $z_1, z_2, \ldots, z_n$.

**Exempel 5.1.4.** Vi kan tänka på en konvexkombination som ett viktat medelvärde av punkterna $z_1, z_2$ upp till $z_n$. Här är två specialfall:

1. Vi har två punkter $z_1$ och $z_2$ och sätter $a_1 = a_2 = 1/2$. Då blir
$$z = a_1 z_1 + a_2 z_2 = \frac{z_1 + z_2}{2}$$
precis mittpunkten av segmenten mellan $z_1$ och $z_2$.

2. Vi har tre punkter $z_1$, $z_2$ och $z_3$ och sätter $a_1 = a_2 = a_3 = 1/3$. I detta fall blir
$$z = a_1 z_1 + a_2 z_2 + a_3 z_3 = \frac{z_1 + z_2 + z_3}{3}$$
precis mittpunkten (tyngdpunkten) av triangeln som har hörnen $z_1$, $z_2$ och $z_3$.

▲

Det finns även en fysikalisk tolkning: Kom ihåg att vi kan tänka oss $\mathbb{C}$ som planet. Låt oss föreställa oss att detta plan $\mathbb{C}$ är en stor men viktlös skiva och att vi ställer en vikt som väger $a_1$ viktenheter i punkten $z_1$, en vikt med $a_2$ viktenheter i punkten $z_2$, och så vidare. I så fall blir punkten $z = a_1 z_1 + a_2 z_2 + \ldots + a_n z_n$ precis tyngdpunkten av denna konstruktion, det vill säga, att skivan skulle kunna balansera på ett nålshuvud som var placerat i exakt denna punkt.

**Sats 5.1.5.** *En mängd $K \subseteq \mathbb{C}$ är konvex om och endast om $K$ innehåller alla konvexkombinationer av punkter som ligger i $K$.*

*Bevis.* Om en mängd $K$ innehåller alla konvexkombinationer av element i $K$, så innehåller den speciellt alla konvexkombinationer av *två* element:
$$a_1 z_1 + a_2 z_2.$$
För dessa vet vi att $a_1 + a_2 = 1$. Om vi kallar $a_1$ för $\lambda$ så blir $a_2$ lika med $1 - \lambda$, och vi har återfått definitionen av en konvex mängd.

Vi visar nu andra riktningen med induktion. Som basfall tar vi fallet med två punkter. Första delen av beviset visar exakt att en mängd är konvex precis när den innehåller konvexkombinationer av två punkter. Antag att påståendet är sant för $n$ punkter. Antag också att $z$ är en konvexkombination av $z_1, \ldots, z_{n+1} \in K$:
$$z = a_1 z_1 + \cdots + a_{n+1} z_{n+1}.$$
Låt $A = a_1 + a_2 + \cdots + a_n = 1 - a_{n+1}$. Om $A = 0$ är $z = z_{n+1}$ och ligger i $K$. Antag istället att $A \neq 0$ och betrakta elementet
$$\widetilde{z} = \frac{1}{A}\left(a_1 z_1 + \cdots + a_n z_n\right).$$
Denna är en konvexkombination av $z_1, \ldots, z_n$ eftersom summan av koefficienterna är
$$\frac{1}{A}\left(a_1 + a_2 + \cdots + a_n\right) = 1,$$

så enligt induktionsantagandet är $\widetilde{z} \in K$. Låt nu $\lambda = A$. I så fall är

$$\lambda\widetilde{z} + (1-\lambda)z_{n+1} = \frac{A}{A}(a_1z_1 + \cdots + a_nz_n) + (1-(1-a_{n+1}))z_n = z.$$

Eftersom $K$ antogs konvex, följer att $z \in K$. □

Antag nu att vi har ett visst antal punkter $z_1, z_2, \ldots, z_n$ i $\mathbb{C}$ givna. Vi vill hitta en konvex mängd som innehåller alla punkterna och är så "liten" som möjligt. Vi ska klargöra vad vi menar med "liten". För det behöver vi följande hjälpsats:

**Hjälpsats 5.1.6.** *Låt $\Gamma$ vara en godtycklig mängd, och antag att vi för varje $\gamma \in \Gamma$ är givna en konvex mängd $K_\gamma \subseteq \mathbb{C}$. Vi definierar snittet*

$$K = \bigcap_{\gamma\in\Gamma} K_\gamma$$

*som mängden av de element som ligger i alla $K_\gamma$. I denna situation är även $K$ konvex.*

*Bevis.* Antag att $z_1$ och $z_2$ är två punkter i $K$ och att $\lambda \in [0,1]$. Vi behöver visa att även $\lambda z_1 + (1-\lambda)z_2$ tillhör $K$.

Tag ett godtyckligt $\gamma \in \Gamma$. Då innehåller $K_\gamma$ både $z_1$ och $z_2$ enligt definitionen av snitt. Nu är $K_\gamma$ konvex och innehåller därmed även $\lambda z_1 + (1-\lambda)z_2$. Detta gäller alltså för alla $\gamma \in \Gamma$ och det följer att $\lambda z_1 + (1-\lambda)z_2$ är ett element av snittet av alla $K_\gamma$, det vill säga $K$. Beviset är klart. □

Låt oss betrakta mängden av alla konvexa mängder som innehåller våra givna punkter $z_1, z_2, \ldots, z_n$. Uppenbarligen så innehåller snittet av dessa också de givna punkterna, och är dessutom enligt föregående lemma konvex. Framför allt är snittet innehållen i varje konvex mängd som innehåller $z_1, ..., z_n$, och på så sätt kan vi tänka på det som den minsta sådana mängden. Detta motiverar följande definition:

**Definition 5.1.7.** Låt $z_1, z_2, \ldots, z_n$ vara punkter i $\mathbb{C}$. Det *konvexa höljet* av punkterna är definierat som snittet av alla konvexa mängder som innehåller alla punkter $z_1, z_2, \ldots, z_n$, och betecknas $\text{conv}(z_1, z_2, \ldots, z_n)$.

Man känner kanske att den givna definitionen av det konvexa höljet av ett antal punkter inte säger så mycket om hur det konvexa höljet faktiskt ser ut i praktiken. Vi ska nu se att man kan beskriva $\text{conv}(z_1, z_2, \ldots, z_n)$ på ett annat sätt med hjälp av konvexkombinationer:

**Sats 5.1.8.** *Låt $x_1, \ldots, x_n$ vara punkter i det komplexa planet. Det konvexa höljet* $\text{conv}(x_1, \ldots, x_n)$ *är lika med mängden av alla konvexkombinationer av punkterna $x_1, x_2, \ldots, x_n$.*

*Bevis.* Vi ska visa att $\text{conv}(x_1, x_2, \ldots, x_n)$ och mängden av alla konvexkombinationer av punkterna $x_1, x_2, \ldots, x_n$ är samma mängd. Låt oss kalla den senare mängden för $L$.

Vi har i Sats 5.1.5 visat att en konvex mängd innehåller alla konvexkombinationer av dess punkter. Eftersom $\text{conv}(x_1, x_2, \ldots, x_n)$ innehåller alla punkter $x_1, x_2, \ldots, x_n$ och är konvex, så följer det att den innehåller även alla konvexkombinationer. Alltså är $L$ en delmängd av mängden $\text{conv}(x_1, x_2, \ldots, x_n)$. Vi fortsätter med att visa att $L$ är konvex. Detta är lite tekniskt att visa. Låt oss välja två godtyckliga punkter $z$ och $z'$ i $L$. Enligt defintionen av $L$ kan de skrivas på formen

$$z = a_1x_1 + a_2x_2 + \ldots + a_nx_n \text{ och } z' = a_1'x_1 + a_2'x_2 + \ldots + a_n'x_n$$

för vissa $a_1, \ldots, a_n, a_1', \ldots, a_n' \in [0, 1]$ som uppfyller att

$$a_1 + a_2 + \ldots + a_n = a_1' + a_2' + \ldots + a_n' = 1.$$

Låt oss dessutom välja ett godtyckligt $\lambda \in [0, 1]$. Vi ska nu visa att $\lambda z + (1-\lambda)z'$ är ett element av $L$. Vi beräknar

$$\begin{aligned}\lambda z + (1-\lambda)z' &= \lambda\left(a_1x_1 + a_2x_2 + \ldots + a_nx_n\right) \\ &\quad + (1-\lambda)\left(a_1'x_1 + a_2'x_2 + \ldots + a_n'x_n\right) \\ &= \left(\lambda a_1 + (1-\lambda)a_1'\right)x_1 + \ldots + \left(\lambda a_n + (1-\lambda)a_n'\right)x_n\end{aligned}$$

Om vi definierar $b_i = \lambda a_i + (1-\lambda)a_i'$ kan vi skriva ekvationen som

$$\lambda z + (1-\lambda)z' = b_1x_1 + b_2x_2 + \ldots + b_nx_n$$

Detta ser ut som att det är en konvexkombination av $x_1, x_2, \ldots, x_n$. Man behöver dock nu kontrollera att alla $b_i$ ligger i intervallet $[0, 1]$ och att deras summa $b_1 + b_2 + \ldots + b_n$ är lika med 1. Detta ger vi som övningsuppgift åt läsaren.

Därmed har vi visat att $L$ är konvex och per definition innehåller $L$ alla punkter $z_1, \ldots, z_n$. Eftersom $\text{conv}(z_1, \ldots, z_n)$ är snittet av alla konvexa mängder som innehåller $z_1, \ldots, z_n$, måste $\text{conv}(z_1, \ldots, z_n)$ vara en delmängd av $L$. Som vi visade i början av beviset är tvärtom $L$ en delmängd av $\text{conv}(z_1, \ldots, z_n)$. Därmed är mängderna lika. □

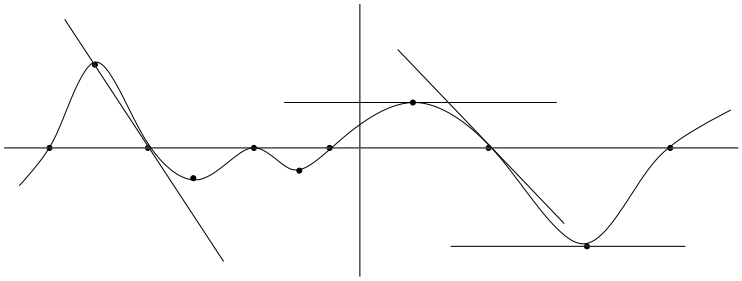
## 5.2 Gauss-Lucas sats

Vi ska i denna kapitel studera hur rötterna till ett polynom ger villkor på rötterna till dess derivata. Låt oss börja med att definiera vad derivatan av ett polynom är.

**Definition 5.2.1.** Derivatan av ett polynom $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ är polynomet $f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2x^2 + a_1$.

**Exempel 5.2.2.** Polynomet $f(x) = 2x^3 + x^2 - 5x + 4$ har derivatan $f'(x) = 6x^2 + 2x - 5$. Varje konstant polynom $f(x) = c$ för något $c \in \mathbb{C}$ har derivata $f'(x) = 0$. ▲

**Exempel 5.2.3.** Läsaren känner kanske till att derivatan av en funktion i någon punkt anger lutningen av tangenten till funktionens graf i den punkten. Betrakta följande bild som visar funktionsgrafen till ett reellt polynom. Vi



Figur 5.4: Funktionsgrafen till ett reellt polynom med några tangenter

ser från bilden att polynomet har antingen ett *lokalt minimum* eller ett *lokalt maximum* mellan varje par av konsekutiva nollställen. Vi kommer att gå in mer i detalj om minimumpunkter och maximumpunkter i Kapitel 7. Tangenten i ett lokalt minimum eller maximum har alltid lutning 0. Annars sagt, har derivatan av funktionen alltid en rot i ett lokalt minimum eller maximum. Det följer att derivatan av ett polynom alltid måste ha en rot mellan två punkter som båda är rötter till polynomet själv. ▲

För att visa påståendena i föregående paragraf på ett matematiskt korrekt sätt, kan vi använda oss av Rolles sats. Den är formulerad för en godtycklig kontinuerlig funktion och vi använder oss av faktumet att alla polynom är kontinuerliga funktioner. Vi ger inget bevis för satsen, eftersom detta skulle kräva en djupare bakgrund i analys.

**Sats 5.2.4** (Rolles sats)**.** *Om $f\colon \mathbb{R} \to \mathbb{R}$ är en kontinuerlig funktion och $f(x_1) = f(x_2) = 0$ för två olika reella tal $x_1$ och $x_2$, så finns det ett tal $\xi$ som uppfyller $x_1 < \xi < x_2$ och $f'(\xi) = 0$.*

Rolles sats har en intressant konsekvens för polynom som bara har reella rötter.

**Följdsats 5.2.5.** *Låt $f(x)$ vara ett polynom av grad $n$ som har $n$ olika reella rötter. Då har dess derivata $f'(x)$ exakt $n-1$ olika reella rötter.*

*Bevis.* Låt $x_1 < x_2 < \ldots < x_n$ vara de $n$ olika rötterna av $f(x)$. Enligt Rolles sats finns det för varje $i = 1, \ldots, n-1$ ett reellt tal $\xi_i$ som uppfyller $x_i < \xi_i < x_{i+1}$ och $f'(\xi_i) = 0$. Alltså har $f'(x)$ de $n-1$ olika rötterna $\xi_1, \xi_2, \ldots, \xi_{n-1}$. □

Låt oss nu betrakta ett polynom $f$ med komplexa koefficienter. Om polynomet inte bara har reella rötter, så skulle vi ändå vilja säga något om var rötterna

av derivatan ligger. Det visar sig att detta är möjligt: vi skall nu visa den så kallade Gauss-Lucas sats, som är en generalisering av föregående sats. I Gauss-Lucas sats arbetar vi med det konvexa höljet av rötterna till polynomet $f$, så vi får en tydlig bild av vad satsen innebär geometriskt i det komplexa planet.

**Sats 5.2.6** (Gauss-Lucas sats)**.** *Låt $f$ vara ett icke-konstant polynom. Då ligger alla rötter till $f'$ i det konvexa höljet av rötterna till $f$.*

*Bevis.* Låt oss kalla de $n$ rötterna till $f$ för $z_1, \ldots, z_n$, där $n = \deg f$. I övningsuppgift 5.4 visas identiteten

$$\frac{f'(z)}{f(z)} = \frac{1}{z - z_1} + \frac{1}{z - z_2} + \ldots + \frac{1}{z - z_n}$$

för alla polynom $f$ och alla $z \in \mathbb{C}$ där $f(z) \neq 0$.

Låt $z$ vara en rot till $f'$. Låt oss även anta att $f(z) \neq 0$, specialfall $f(z) = 0$ tar vi hand om i slutet av beviset. Vi förlänger alla bråk i den föregående ekvationen för att få reella nämnare. Enligt våra antaganden är $f'(z)/f(z) = 0$, vilket ger

$$0 = \frac{\bar{z} - \bar{z_1}}{|z - z_1|^2} + \frac{\bar{z} - \bar{z_2}}{|z - z_2|^2} + \ldots + \frac{\bar{z} - \bar{z_n}}{|z - z_n|^2}.$$

Låt oss definiera $\alpha_i := \frac{1}{|z - z_i|^2}$ för varje $i = 1, \ldots, n$, och låt $\alpha = \alpha_1 + \alpha_2 + \ldots + \alpha_n$. Om vi samlar ihop alla termer med $z$, så får vi

$$\alpha\bar{z} = \alpha_1\bar{z_1} + \alpha_2\bar{z_2} + \ldots + \alpha_n\bar{z_n}.$$

Vi noterar att alla talen $\alpha_1, \ldots, \alpha_n$ samt deras summa $\alpha$ är reella. Vi konjugerar ekvationen och får

$$\alpha z = \alpha_1 z_1 + \alpha_2 z_2 + \ldots + \alpha_n z_n.$$

Vi definierar $a_i := \alpha_i/\alpha$ och noterar att alla $a_i$ är positiva reella tal vars summa är 1. Om vi nu delar förra ekvationen med $\alpha$, så får vi

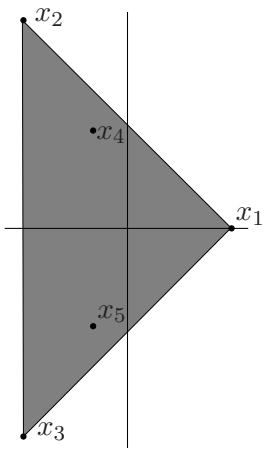
$$z = a_1 z_1 + a_2 z_2 + \ldots + a_n z_n.$$

Detta visar att $z$ ligger i det konvexa höljet av $z_1, z_2, \ldots, z_n$.

Vi ska inte glömma specialfallet när både $f'(z) = 0$ och $f(z) = 0$. I detta fall kan vi skriva $z = 1 \cdot z$, och eftersom $z$ själv är en rot till $f$ så ligger alltså $z$ i det konvexa höljet av alla rötter till $f$. □

Korollarium 5.2.5 är ett specialfall av Gauss-Lucas sats: Om $f$ endast har reella rötter, kommer det konvexa höljet av rötterna att bli ett intervall på reella linjen. Alltså har dess derivata också endast reella rötter.

**Exempel 5.2.7.** Betrakta polynomet $f(x) = x^3 + x^2 + 3x - 5$. Rötterna till $f$ är $x_1 = 1$, $x_2 = -1+2i$ och $x_3 = -1-2i$ och alla har multiplicitet 1. Derivatan av $f$ är polynomet $f'(x) = 3x^2 + 2x + 3$ och har rötterna $x_4 = (-1 + 2\sqrt{2}i)/3$ och $x_5 = (-1 - 2\sqrt{2}i)/3$. I Figur 5.5 kan vi se att $x_4$ och $x_5$ ligger i triangeln som har hörnen $x_1$, $x_2$ och $x_3$. ▲




Figur 5.5: Rötterna till polynomet $x^3 + x^2 + 3x - 5$ och dess derivata

## Övningar

**Övning 5.1.** Visa Carathéodorys sats för det komplexa planet $\mathbb{C}$ som säger följande: Om $z$ ligger i det konvexa höljet $K$ av punkterna $z_1, z_2, \ldots, z_n \in \mathbb{C}$, så finns det tre punkter $z_i, z_j, z_k$ bland $z_1, z_2, \ldots, z_n$ så att $z$ även ligger i $\text{conv}(z_i, z_j, z_k)$. (Använd ett geometriskt resonemang: Vilken form har $K$? Om du drar en rak linje genom $z$ och t.ex. punkten $z_1$, så skär den linjen mellan två andra av punkterna. Använd det för att konstruera en konvexkombination.)

**Övning 5.2.** Visa medelvärdessatsen för kontinuerliga funktioner som säger följande: Om $f$ är en kontinuerlig funktion och $a < b$ är två reella tal, så finns det något reellt tal $c \in (a, b)$ så att

$$f'(c) = \frac{f(b) - f(a)}{b - a}$$

(Konstruera en kontinuerlig funktion $g$ som uppfyller att $g(a) = g(b) = 0$. Du kan göra ansatsen $g(x) = f(x)+kx+l$ och bestämma lämpliga konstanter $k$ och $l$. Använd räknelagarna för derivatan och Rolles sats för $g$.) Vad beskrivs av talen $\frac{f(b)-f(a)}{b-a}$ samt $f'(c)$? Gör en geometrisk tolkning av medelvärdessatsen.

**Övning 5.3.** Låt $a_1, \ldots, a_n, a'_1, \ldots, a'_n \in [0, 1]$ vara så att

$$a_1 + \ldots + a_n = a'_1 + \ldots + a'_n = 1$$

och låt $\lambda \in [0, 1]$. Definiera $b_i = \lambda a_i + (1 - \lambda)a'_i$ som i beviset av Sats 5.1.8. Visa att

1. $b_i \in [0, 1]$,
2. $b_1 + \ldots + b_n = 1$.

**Övning 5.4.** Visa att om ett icke-konstant polynom $f$ av grad $d$ har rötterna $z_1, z_2, \ldots, z_d$ så gäller det att

$$\frac{f'(z)}{f(z)} = \frac{1}{z - z_1} + \frac{1}{z - z_2} + \ldots + \frac{1}{z - z_d}$$

för alla $z \in \mathbb{C}$ där $f(z) \neq 0$. (För $z$ där $f(z) = 0$ får vi ett odefinierat uttryck.)

**Övning 5.5.** Låt $p$ vara ett andragradspolynom, dvs $\deg p = 2$, som har rötterna $\alpha$ och $\beta$. Beräkna roten av $p'$ och skriv den som konvexkombination av $\alpha$ och $\beta$. Visa att Gauss-Lucas sats stämmer för $p$.

# 6 Symmetriska funktioner

I detta kapitel kommer vi att införa flera nya begrepp. Först introduceras polynom i flera variabler, vilket är exakt vad det låter som: i stället för endast en variabel, till exempel $x$, tillåter vi flera variabler, till exempel $x$, $y$ och $z$.

Dock kommer vi inte i detta kapitel att studera polynom i flera variabler i allmänhet, utan en väldigt speciell sorts polynom, de så kallade symmetriska polynomen. Symmetriska polynom är viktiga även när man studerar polynom i en variabel, på grund av Sats 6.4.1 som vi visar i detta kapitel. Denna sats säger att sambandet mellan rötterna till ett polynom och polynomets koefficienter enklast uttrycks med hjälp av symmetriska polynom.

Den enskilt viktigaste satsen om symmetriska polynom är den så kallade fundamentalsatsen för symmetriska polynom. Denna beskriver hur varje symmetriskt polynom, oavsett hur komplicerat, är uppbyggt av enkla byggstenar. Dessa enkla byggstenar är de *elementära symmetriska polynomen*.

Slutligen ger vi ett bevis av Newtons identiteter, som relaterar de elementära symmetriska polynomen till en annan familj av symmetriska polynom, potenssummorna.

## 6.1 Polynom i flera variabler

Tidigare i kursen har vi endast arbetat med polynom i *en* variabel, som ju är ett uttryck liknande

$$17 + 5x + 10x^3 - \pi x^5.$$

I detta kapitel kommer vi dock att behöva tala om polynom i *flera* variabler. Med detta menar vi ett uttryck såsom

$$5xy + 4xz^3 - y^2 - 2x^2yz.$$

Formellt gör vi följande definition. För att kunna arbeta med ett godtyckligt antal variabler (och inte bara tre) så betecknar vi variablerna med $x_1, x_2, ..., x_n$ i stället för $x, y, z$.

**Definition 6.1.1.** Ett *polynom i flera variabler* är en ändlig summa av termer på formen

$$ax_1^{r_1}x_2^{r_2}\cdots x_n^{r_n},$$

där $a \in \mathbb{C}$ är en *koefficient*, $x_1, ..., x_n$ är *variablerna*, och $r_1, ..., r_n$ är *exponenterna*. Varje tal $r_i$ är ett heltal större än eller lika med 0.

Vi ser t.ex. att $x_1^3x_2^5 + 5x_1x_2^2$ är ett polynom i variablerna $x_1$ och $x_2$ och att $x_1^3x_2^5 + 5x_1x_2^2 - 2x_2^{-3}$ inte är ett polynom eftersom exponenten till $x_2$ är negativ.

Många, men inte alla, av egenskaperna för polynom i en variabel går fortfarande att formulera för polynom i flera variabler.

## 6.2 Symmetriska funktioner

Vi ska i detta avsnitt betrakta polynom i flera variabler som inte förändras av att man byter ordning på variablerna. Sådana polynom ska vi kalla för *symmetriska*.

Vi ska klargöra vad vi menar med att "byta ordning på variabler" med ett exempel. Funktionen

$$f(x, y, z) = x^2y + y^2z + z^2x + 3xyz$$

är en symmetrisk funktion eftersom

$$f(x, y, z) = f(y, x, z) = f(x, z, y) = f(z, y, x) = f(z, x, y) = f(y, z, x).$$

Å andra sidan är

$$x^2y + y^2x + xz + yz$$

inte en symmetrisk funktion. Den förändras inte av att man byter $x$ och $y$ med varandra, men om man byter $x$ mot $z$ eller $y$ mot $z$ ändras uttrycket.

För att kunna formalisera definitionen av en symmetrisk funktion, behöver vi göra en till definition.

**Definition 6.2.1.** Låt $X$ vara en mängd. En funktion $\sigma\colon X \to X$ kallas en *permutation* om det existerar en funktion $\sigma^{-1}\colon X \to X$ med egenskapen att $\sigma^{-1} \circ \sigma$ och $\sigma \circ \sigma^{-1}$ är identitetsfunktionen, d.v.s. funktionen som avbildar alla element av $X$ på sig själv.

Om $X = \{x_1, x_2, \ldots, x_n\}$, tänker vi på $\sigma$ som en funktion som byter plats på variablerna $x_1, x_2, \ldots, x_n$, och $\sigma^{-1}$ som funktionen som byter tillbaka dem igen. Kravet att $\sigma^{-1}$ ska existera är nödvändigt för att utesluta "dåliga" funktioner, som den som avbildar alla variabler på $x_1$.

**Definition 6.2.2.** Låt $f$ vara en funktion i variablerna $x_1, ..., x_n$. Vi säger att $f$ är en *symmetrisk funktion* om det för varje permutation

$$\sigma\colon \{x_1, x_2, ..., x_n\} \to \{x_1, x_2, ..., x_n\},$$

gäller att

$$f(x_1, x_2, ..., x_n) = f(\sigma(x_1), \sigma(x_2), ..., \sigma(x_n)).$$

Om $f$ är ett polynom och en symmetrisk funktion, säger vi att $f$ är ett *symmetriskt polynom*.

Vi ska senare använda oss av följande hjälpsats.

**Hjälpsats 6.2.3.** *Låt $f$ vara en symmetrisk funktion i $x_1, x_2, \ldots, x_n$. Definiera funktionen $g$ i variablerna $x_1, x_2, \ldots, x_{n-1}$ genom*

$$g(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 0).$$

*Då är $g$ en symmetrisk funktion.*

*Bevis.* Låt $\sigma\colon \{x_1, \ldots, x_{n-1}\} \to \{x_1, \ldots, x_{n-1}\}$ vara en permutation. Vi ska visa att

$$g(x_1, \ldots, x_{n-1}) = g(\sigma(x_1), \ldots, \sigma(x_{n-1})).$$

Vi definierar $\tau\colon \{x_1, \ldots, x_{n-1}, x_n\} \to \{x_1, \ldots, x_{n-1}, x_n\}$ genom $\tau(x_i) = \sigma(x_i)$ för alla $i = 1, \ldots, n-1$ och $\tau(x_n) = x_n$, då är $\tau$ en permutation. Eftersom $f$ är symmetrisk, gäller det att

$$\begin{aligned} f(x_1, \ldots, x_{n-1}, x_n) &= f(\tau(x_1), \ldots, \tau(x_{n-1}), \tau(x_n)) \\ &= f(\sigma(x_1), \ldots, \sigma(x_{n-1}), x_n). \end{aligned}$$

Detta ger oss

$$\begin{aligned} g(x_1, \ldots, x_{n-1}) &= f(x_1, \ldots, x_{n-1}, 0) \\ &= f(\sigma(x_1), \ldots, \sigma(x_{n-1}), 0) \\ &= g(\sigma(x_1, \ldots, \sigma(x_{n-1})). \end{aligned}$$

vilket skulle visas. □

## 6.3 Elementära symmetriska polynom

**Definition 6.3.1.** Låt $1 \leqslant k \leqslant n$. Vi definierar det $k$:te *elementära symmetriska polynomet* av variablerna $x_1, ..., x_n$ som summan av alla möjliga produkter av $k$ olika variabler. Vi betecknar det med $e_k(x_1, ..., x_n)$, eller $e_k^{(n)}$ om vi vill framhäva antalet variabler, eller bara $e_k$ om antalet variabler framgår från kontexten. Om $k > n$ definierar vi $e_k = 0$.

**Exempel 6.3.2.** För $n = 4$ finns exakt fyra olika elementära symmetriska polynom som inte är noll.

$$\begin{aligned} e_1 &= x_1 + x_2 + x_3 + x_4 \\ e_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ e_3 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ e_4 &= x_1x_2x_3x_4. \end{aligned}$$

▲

Att vi använder samma namn $e_k$ för den $k$:te elementära symmetriska funktionen oavsett vilket antal variabler vi använder kan verka förvirrande först, men visar sig vara mycket bekvämt. I praktiken leder inte detta till förvirring på grund av följande användbara lemma.

**Hjälpsats 6.3.3.** *Det gäller att*

$$e_k^{(n)}(x_1, ..., x_n) = e_k^{(n+1)}(x_1, ..., x_n, 0).$$

*Bevis.* Termerna i högerledet är alla möjliga produkter av $k$ stycken av variablerna $x_1, ..., x_n, x_{n+1}$. Sätter vi $x_{n+1} = 0$ försvinner exakt de termer där $x_{n+1}$ ingår, och resten är oförändrade. Kvar blir alltså exakt alla möjliga produkter av $k$ stycken av $x_1, ..., x_n$. □

Nästa hjälpsats säger att om vi ersätter variablerna i ett polynom med andra symmetriska polynom i samma antal variabler, så får vi igen ett symmetriskt polynom.

**Hjälpsats 6.3.4.** *Om $p$ är ett polynom i $k$ variabler och om $f_1, \ldots, f_k$ är symmetriska polynom i $n$ variabler, så är polynomet*

$$p(f_1, f_2, \ldots, f_k)$$

*ett symmetriskt polynom i $n$ variabler.*

*Bevis.* Låt $\sigma\colon \{x_1, \ldots, x_n\} \to \{x_1, \ldots, x_n\}$ vara en permutation. Vi ska visa att

$$\begin{aligned} &p(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n)) \\ &\qquad = p(f_1(\sigma(x_1), \ldots, \sigma(x_n)), \ldots, f_k(\sigma(x_1), \ldots, \sigma(x_n))). \end{aligned}$$

Detta följer direkt från vårt antagande att alla $f_i$ är symmetriska funktioner. □

**Exempel 6.3.5.** Låt $p(z_1, z_2) = z_1 + 2z_2^2 + z_1 z_2$. Vi noterar att $p(z_1, z_2)$ inte är symmetriskt i variablerna $z_1$ och $z_2$. Låt $f_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$ och $f_2(x_1, x_2, x_3) = x_1 x_2 x_3$. Vi beräknar

$$\begin{aligned} p(f_1, f_2) &= f_1 + 2f_2^2 + f_1 f_2 \\ &= (x_1 + x_2 + x_3) + 2(x_1 x_2 x_3)^2 + (x_1 + x_2 + x_3)(x_1 x_2 x_3) \\ &= x_1 + x_2 + x_3 + 2x_1^2 x_2^2 x_3^2 + x_1^2 x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2 \end{aligned}$$

och ser att detta är ett symmetriskt polynom i variablerna $x_1, x_2$ och $x_3$. ▲

Hjälpsats 6.3.4 har ett intressant specialfall: Låt $p$ vara ett godtyckligt polynom i variablerna $x_1, ..., x_n$, och låt $e_1, ..., e_n$ vara de elementära symmetriska polynomen i dessa variabler. Vi kan bilda polynomet

$$p(e_1, e_2, ..., e_n)$$

genom att sätta in var och ett av de symmetriska polynomen $e_k$ där variablerna $x_k$ var förut. Hjälpsatsen säger att $p(e_1, e_2, ..., e_n)$ är ett symmetriskt polynom.

Det visar sig att *varje* symmetriskt polynom kan konstrueras på detta sätt för ett unikt polynom $p$: de elementära symmetriska polynomen är de enkla atomer av vilka varje komplicerat symmetriskt polynom är uppbyggt.

Innan vi formulerar och visar detta precist behöver vi ett lemma till.

**Hjälpsats 6.3.6.** *Låt $p$ vara ett polynom i variablerna $x_1, ..., x_n$. Antag att*

$$p(x_1, ..., x_{n-1}, 0) = 0.$$

*Då finns ett polynom $q$ i variablerna $x_1, \ldots, x_n$ med*

$$p = x_n \cdot q.$$

*Bevis.* Att sätta $x_n$ till noll är detsamma som att stryka alla termer från $p$ där variabeln $x_n$ ingår. Att man får nollpolynomet kvar efteråt säger precis att alla termer försvunnit, så att varje term i polynomet $p$ var delbara med $x_n$. Alltså kan $x_n$ brytas ut, vilket skulle visas. □

**Sats 6.3.7** (Fundamentalsatsen för symmetriska funktioner)**.** *Låt $p$ vara ett symmetriskt polynom i $x_1, ..., x_n$. Det existerar ett unikt polynom $\widetilde{p}$ i $n$ variabler sådant att*

$$p = \widetilde{p}(e_1, ..., e_n).$$

*Bevis.* Vi använder ett lite knepigt induktionsargument. Det som gör det här beviset lite mer komplicerat är att vi inte använder induktion över ett tal, utan induktion över *två*: både graden till polynomet och antalet variabler. Vi måste därför också ha två olika bassteg. Det första är fallet att $p$ har grad noll, d.v.s. är en konstant. I så fall får vi helt enkelt välja $\widetilde{p}$ till samma konstant. Det andra är fallet att $n = 1$, där $p$ är ett vanligt polynom i en variabel. I så fall är $e_1 = x_1$, alla polynom är symmetriska, och vi måste även i detta fall välja $p = \widetilde{p}$.

Antag att satsen är bevisad för: (i) alla symmetriska funktioner av högst $n - 1$ variabler, och (ii) alla symmetriska funktioner av grad mindre än $\deg p$. Betrakta polynomet

$$q = p(x_1, x_2, ..., x_{n-1}, 0). \tag{6.1}$$

Enligt Hjälpsats 6.2.3 är $q$ en symmetrisk funktion av variablerna $x_1, \ldots, x_n$. Enligt antagande (i) finns det ett unikt polynom $\widetilde{q}$ i $n - 1$ variabler, sådant att

$$q = \widetilde{q}(e_1^{(n-1)}, e_2^{(n-1)}, ..., e_{n-1}^{(n-1)}). \tag{6.2}$$

Betrakta nu polynomet

$$r = p(x_1, ..., x_n) - \widetilde{q}(e_1^{(n)}, e_2^{(n)}, ..., e_{n-1}^{(n)}) \tag{6.3}$$

i $n$ variabler. Enligt Hjälpsats 6.3.4 är $q(e_1^{(n)}, e_2^{(n)}, ..., e_{n-1}^{(n)})$ symmetriskt. Dessutom är differensen av två symmetriska funktioner symmetrisk. Därmed är $r$ en symmetrisk funktion i $n$ variabler. Dessutom är

$$r(x_1, ..., x_{n-1}, 0) = 0.$$

För att se detta, notera att när vi sätter in $x_n = 0$ i ekvation (6.3) blir enligt ekvation (6.1) första termen lika med $q$, och andra termen blir enligt Lemma 6.3.3 exakt

$$\widetilde{q}(e_1^{(n-1)}, e_2^{(n-1)}, ..., e_{n-1}^{(n-1)}),$$

Ekvation (6.2) säger att dessa två termer tar ut varandra. Enligt Hjälpsats 6.3.6 är därför varje term i $r$ delbar med $x_n$. Eftersom $r$ är symmetriskt är varje term till och med delbar med $x_1x_2\cdots x_n = e_n$. Vi kan alltså skriva

$$r = e_n \cdot s.$$

för något polynom $s$ i $n$ variabler. Eftersom $r$ och $e_n$ är symmetriska funktioner är även $s$ det. Dessutom har $s$ lägre grad än $p$, så enligt det *andra* induktionsantagandet kan vi skriva

$$s = \widetilde{s}(e_1, ..., e_n)$$

på ett unikt sätt. Det följer att

$$p = \widetilde{q}(e_1, ..., e_{n-1}) + e_n\widetilde{s}(e_1, ..., e_n),$$

så $p$ är ett polynom i de elementära symmetriska funktionerna. Eftersom både $\widetilde{q}$ och $\widetilde{s}$ var unikt bestämda av induktionsantaganden är denna representation unik. □

**Exempel 6.3.8.** Betrakta det symmetriska polynomet från Exempel 6.3.5,

$$p(x_1, x_2, x_3) = x_1 + x_2 + x_3 + 2x_1^2x_2^2x_3^2 + x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^3.$$

Vi sätter $q(x_1, x_2) = p(x_1, x_2, 0) = x_1 + x_2$ vilket är ett symmetriskt polynom i två variabler. Vi ser direkt att $q(x_1, x_2)$ är det första elementära symmetriskta polynomet. Om vi definierar $\widetilde{q}(x_1, x_2) = x_1$, får vi därmed att

$$q(x_1, x_2) = x_1 + x_2 = e_1 = \widetilde{q}(e_1, e_2).$$

Vi beräknar nu

$$\begin{aligned} r(x_1, x_2, x_3) &= p(x_1, x_2, x_3) - \widetilde{q}(e_1, e_2) \\ &= 2x_1^2x_2^2x_3^2 + x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^3 \\ &= x_1x_2x_3\left(2x_1x_2x_3 + x_1 + x_2 + x_3\right) \end{aligned}$$

och får $r = e_3s$ där $s = 2x_1x_2x_3 + x_1 + x_2 + x_3$. Om vi sätter $\widetilde{s}(x_1, x_2, x_3) = 2x_3 + x_1$, får vi $s = \widetilde{s}(e_1, e_2, e_3)$. Vi sätter ihop allt och får

$$p = \widetilde{q}(e_1, e_2) + e_3\widetilde{s}(e_1, e_2, e_3)$$

d.v.s. vi kan sätta

$$\widetilde{p} = \widetilde{q} + x_3\widetilde{s} = x_1 + x_3\left(2x_3 + x_1\right) = x_1 + 2x_3^2 + x_1x_3.$$

Detta ger oss

$$p(x_1, x_2, x_3) = \widetilde{p}(e_1, e_2, e_3) = e_1 + 2e_3^2 + e_1e_3.$$

Vi uppmanar läsaren att jämföra detta med Exempel 6.3.5. ▲

Vi ger även ett lite mer komplext exempel där man behöver använda idén från beviset av Sats 6.3.7 flera gånger.

**Exempel 6.3.9.** Betrakta det symmetriska polynomet

$$p(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3.$$

Vi ska uttrycka $p$ med hjälp av $e_1, e_2$ och $e_3$. Vi delar upp lösningen i flera steg för att inte tappa överblicken.

Steg 1: Vi betraktar $p(x_1, x_2, 0) = x_1^3 + x_2^3$ och ska uttrycka detta symmetriska polynom i två variabler med hjälp av $e_1(x_1, x_2)$ och $e_2(x_1, x_2)$. Eftersom det inte är uppenbart hur det går, så reducerar till en variabel i Steg 2.

Steg 2: Vi betraktar $p(x_1, 0, 0) = x_1^3$ och vill skriva detta med hjälp av $e_1(x_1) = x_1$. Detta är enkelt och vi får $p(x_1, 0, 0) = e_1(x_1)^3$.

Steg 3: Vi återgår till två variabler och betraktar

$$p(x_1, x_2, 0) - e_1(x_1, x_2)^3 = x_1^3 + x_2^3 - (x_1 + x_2)^3 = -3(x_1^2 x_2 + x_1 x_2^2).$$

vilket i enlighet med beviset av Sats 6.3.7 är delbart med $e_2(x_1, x_2) = x_1 x_2$. Vi ser att

$$-3(x_1^2 x_2 + x_1 x_2^2) = -3x_1 x_2 (x_1 + x_2) = -3e_2(x_1, x_2)e_1(x_1, x_2).$$

Vi får att

$$p(x_1, x_2, 0) = e_1(x_1, x_2)^3 - 3e_2(x_1, x_2)e_1(x_1, x_2).$$

Steg 4: Vi är nu beredda att hantera alla tre variabler. Vi beräknar

$$\begin{aligned} &p(x_1, x_2, x_3) - \big(e_1(x_1, x_2, x_3)^3 - 3e_2(x_1, x_2, x_3)e_1(x_1, x_2, x_3)\big) \\ &\quad = 3x_1 x_2 x_3 = 3e_3(x_1, x_2, x_3). \end{aligned}$$

och uppmanar läsaren att genomföra räkningen ovan själv. Detta ger oss slutligen att

$$x_1^3 + x_2^3 + x_3^3 = e_1^3 - 3e_2 e_1 + 3e_3.$$

▲

Vi ser att ett någorlunda enkelt exempel kan leda till mycket räkning för att komma fram till hur man kan uttrycka ett symmetriskt polynom med hjälp av de elementära symmetriska polynomen. Dock finns det ett sätt att förenkla några av räkningarna och just exemplet ovan blir mycket lättare om vi använder resultatet i Avsnitt 6.5.

## 6.4 Rötter och koefficienter av polynom

Betrakta nu polynom i en variabel över de komplexa talen. Kom ihåg att enligt algebrans fundamentalsats (som visas i nästa kapitel) har varje polynom av grad $n$ exakt $n$ stycken rötter, om vi räknar en rot av multiplicitet $m$ som $m$ upprepningar av samma rot.

**Sats 6.4.1.** *Låt $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ vara ett moniskt polynom i en variabel. Låt dess rötter vara $r_1, ..., r_n$. Det gäller att*

$$a_k = (-1)^{n-k} e_{n-k}(r_1, r_2, ..., r_n),$$

*så koefficienterna till $f$ ges (upp till ett teckenbyte) exakt av de elementära symmetriska funktionerna av rötterna.*

*Bevis.* Vi vet att

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n). \tag{6.4}$$

Begrunda nu vad som händer när man multiplicerar ut alla parenteserna. Varje term blir en produkt av $n$ faktorer. Man kommer att få en term $x^k$ precis när man multiplicerar ihop $k$ stycken $x$, och $n - k$ stycken faktorer på formen $(-r_i)$. Summan av alla sätt att multiplicera ihop $n - k$ olika av de $n$ talen $r_1, ..., r_n$ är enligt definitionen av elementära symmetriska funktioner exakt

$$e_{n-k}(r_1, ..., r_n),$$

och eftersom varje rot har ett minustecken vid sig i ekvation (6.4) får vi dessutom en faktor $(-1)^{n-k}$. Men eftersom detta gav precis summan av alla koefficienter som hör till $x^k$-termer, får vi just $a_k$ som koefficient för $x^k$. □

**Exempel 6.4.2.** Betrakta polynomet $f(x) = x^3 + a_2x^2 + a_1x + a_0$ och antag att $f$ har rötterna $r_1, r_2$ och $r_3$. Vi vet från Sats 3.3.1 att vi kan skriva $f(x) = c(x-r_1)(x-r_2)(x-r_3)$ där $c \in \mathbb{C}$ är en konstant. Men eftersom $f$ är moniskt, vet vi att $c = 1$. Vi multiplicerar ut och får

$$f(x) = x^3 - (r_1 + r_2 + r_3)x^2 + (r_1r_2 + r_1r_3 + r_2r_3)x - r_1r_2r_3.$$

Därmed gäller det att

$$\begin{aligned} a_2 &= -e_1(r_1, r_2, r_3) \\ a_1 &= e_2(r_1, r_2, r_3) \\ a_0 &= -e_3(r_1, r_2, r_3). \end{aligned}$$

▲

Kombinerar vi Sats 6.4.1 med Sats 6.3.7, får vi följande viktiga följdsats.

**Följdsats 6.4.3.** *Varje funktion av rötterna till ett polynom som inte förändras när vi byter ordning på rötterna kan uttryckas i polynomets koefficienter.*

**Exempel 6.4.4.** Betrakta det moniska polynomet $f(x) = x^3+a_2x^2+a_1x+a_0$ med rötter $r_1, r_2$ och $r_3$. Polynomet

$$p_3(r_1, r_2, r_3) = r_1^3 + r_2^3 + r_3^3$$

är ett symmetriskt polynom i variablerna $r_1, r_2$ och $r_3$ och enligt Följdsatsen ovan kan det skrivas som ett polynom i koefficienterna $a_2, a_1$ och $a_0$.

Vi påminner oss om Exempel 6.3.9 där vi beräknade att $p_3 = e_1^3 - 3e_2e_1 + 3e_3$. Enligt Exempel 6.4.2 är $e_1 = -a_2$, $e_2 = a_1$ och $e_3 = -a_0$ vilket ger oss att

$$r_1^3 + r_2^3 + r_3^3 = -a_2^3 + 3a_1a_2 - 3a_0.$$

▲

## 6.5 Newtons identiteter

**Definition 6.5.1.** Låt $k \geqslant 1$ och $n \geqslant 1$. Vi definierar den *k:te potenssumman* som den symmetriska funktionen

$$p_k = x_1^k + x_2^k + \cdots + x_n^k.$$

Precis som med $e_k$ har vi valt en notation för dessa funktioner som inte visar antalet variabler. Motsvarigheten till Lemma 6.3.3 för potenssummor kan visas, och det följer att det inte leder till förvirring att använda samma namn oavsett antalet variabler. Eftersom dessa är symmetriska funktioner, så vet vi enligt Sats 6.3.7 att det går att uttrycka varje $p_k$ i de elementära symmetriska funktionerna $e_1, ..., e_n$. Följande sats ger ett sätt att räkna ut hur varje $p_k$ kan uttryckas i $e_i$.

**Sats 6.5.2** (Newtons identiteter)**.** *Betrakta symmetriska funktioner i n variabler. För varje k gäller att*

$$0 = p_k - e_1p_{k-1} + e_2p_{k-2} - e_3p_{k-3} - \cdots + (-1)^{k-1}e_{k-1}p_1 + (-1)^k ke_k$$

*(Kom ihåg att vi har definierat $e_k = 0$ om $k > n$.)*

*Bevis.* Det första och viktigaste steget är att inse att det förbluffande nog räcker att bevisa påståendet i det väldigt speciella fallet $k = n$. Om $k > n$ kan vi bara lägga till $k - n$ extra variabler, bevisa påståendet i detta fall, och sedan sätta alla extra variabler till 0. Enligt Lemma 6.3.3 får vi kvar exakt detta påstående.

Om $k < n$ krävs lite mer. Först noterar vi att alla termer är symmetriska, och kan därför uttryckas i $e_1, ..., e_n$ enligt Sats 6.3.7. Men eftersom varje term har grad högst $k$, kan endast $e_1, ..., e_k$ ingå. Om vi sätter alla variabler $x_{k+1}, x_{k+2}, ..., x_n$ till noll får vi en symmetrisk funktion av $x_1, ..., x_k$, och enligt Sats 6.3.7 kan vi därför skriva uttrycket vi får då på ett *unikt* sätt som en funktion av $e_1, ..., e_k$. Men det finns ett uppenbart sätt att skriva uttrycket som en funktion av $e_1, ..., e_k$, nämligen att ta det uttryck som vi vet fungerar för $n$ variabler. Det räcker alltså att visa påståendet efter att de sista $n - k$ variablerna satts till noll, och igen har vi reducerat till fallet $n = k$.

Som i Proposition 6.4.1 gäller att

$$(t - x_1)(t - x_2)\cdots(t - x_n) = t^n - e_1t^{n-1} + e_2t^{n-2}\cdots + (-1)^n e_n.$$

Sätt in $t = x_1$. Högerledet försvinner, och vi får

$$0 = x_1^n - e_1 x_1^{n-1} + e_2 x_1^{n-2} \cdots + (-1)^n e_n.$$

Gör nu samma sak för $t = x_2$, $t = x_3$, och så vidare, och summera alla ekvationerna man får. Vi ser att summan första termen i varje uttryck blir exakt

$$x_1^n + x_2^n + \cdots + x_n^n = p_n,$$

och summan av andra termen i varje uttryck blir

$$-e_1 x_1^{n-1} - e_1 x_2^{n-1} - \cdots - e_1 x_n^{n-1} = -e_1 p_{n-1},$$

och så vidare. Beviset är klart. □

**Exempel 6.5.3.** Vi kommer ihåg Exempel 6.3.9 där vi beräknade att $p_3 = e_1^3 - 3e_2e_1 + 3e_3$ med hjälp av flera långa räkningar. Vi ska istället använda 6.5.2. Newtons identitet för $k = 3$ säger att

$$0 = p_3 - e_1 p_2 + e_2 p_1 - 3e_3.$$

Vi ser att vi behöver uttrycka även $p_2$ och $p_1$ med hjälp av $e_1, e_2$ och $e_3$. Det är klart från definitionen att $p_1 = e_1$. För att uttrycka $p_2$ använder vi Newtons identitet för $k = 2$ och får

$$0 = p_2 - e_1 p_1 + 2e_2.$$

Därmed är $p_2 = e_1^2 - 2e_2$ och

$$p_3 = e_1 p_2 - e_2 p_1 + 3e_3 = e_1(e_1^2 - 2e_2) - e_2 e_1 + 3e_3 = e_1^3 - 3e_1 e_2 + 3e_3.$$

Vi tycker att denna räkning var mycket smidigare än i Exempel 6.3.9. ▲

**Följdsats 6.5.4.** *Varje elementärt symmetriskt polynom $e_k$ kan uttryckas med hjälp av potenssummorna $p_1, \ldots, p_k$.*

*Bevis.* Detta följer direkt från Sats 6.5.2 och induktionsprincipen. Som basfall kan vi uttrycka $e_1$ med hjälp av $p_1$ eftersom $e_1 = p_1$ per definition. Antag att vi kan uttrycka $e_1, \ldots, e_{k-1}$ med hjälp av $p_1, \ldots, p_{k-1}$. Betrakta Newtons identitet

$$0 = p_k - e_1 p_{k-1} + e_2 p_{k-2} - e_3 p_{k-3} - \cdots + (-1)^{k-1} e_{k-1} p_1 + (-1)^k k e_k.$$

Vi ser att den sista termen i högerledet är $e_k$ med en koefficient och att alla andra termer innehåller $e_1, \ldots, e_{k-1}$ samt potentsummorna $p_1, \ldots, p_k$. Enligt vårt induktionsantagande kan vi uttrycka alla andra de termerna med hjälp av $p_1, \ldots, p_{k-1}$ och $p_k$. Det ger oss ett uttryck för $e_k$, vilket skulle visas. □

**Exempel 6.5.5.** Vi ska uttrycka $e_3$ med hjälp av $p_1, p_2$ och $p_3$. För detta behöver vi även uttrycka $e_1$ och $e_2$ genom $p_1$ och $p_2$. Vi vet att $e_1 = p_1$. Newtons identitet för $k = 2$ ger oss att

$$0 = p_2 - e_1 p_1 + 2e_2.$$

och därmed är $e_2 = \frac{1}{2}(e_1 p_1 - p_2) = \frac{1}{2}\left(p_1^2 - p_2\right)$. Vi använder Newtons identitet för $k = 3$

$$0 = p_3 - e_1 p_2 + e_2 p_1 - 3e_3$$

och får att

$$\begin{aligned} e_3 &= \frac{1}{3}(p_3 - e_1 p_2 + e_2 p_1) \\ &= \frac{1}{3}\left(p_3 - p_1 p_2 + \frac{1}{2}\left(p_1^2 - p_2\right) p_1\right) \\ &= \frac{1}{6}\left(2p_3 - 3p_1 p_2 + p_1^3\right) \end{aligned}$$

▲

## Övningar

**Övning 6.1.** Uttryck det symmetriska polynomet

$$x_1 x_2^3 + x_1 x_3^3 + x_2 x_1^3 + x_2 x_3^3 + x_3 x_1^3 + x_3 x_2^3$$

med hjälp av de elementära symmetriska polynomen $e_1, e_2$ och $e_3$.

**Övning 6.2.** Uttryck potenssumman $p_4$ med hjälp av de elementära symmetriska polynomen $e_1, e_2, e_3$ och $e_4$.

**Övning 6.3.** Uttryck det elementära symmetriska polynomet $e_4$ med hjälp av potenssummorna $p_1, p_2, p_3$ och $p_4$.

**Övning 6.4.** Låt $p(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$ vara ett reellt polynom med rötterna $x_1, x_2, x_3$ och $x_4$.

1. Uttryck potenssummorna $x_1^2 + x_2^2 + x_3^2 + x_4^2$ och $x_1^4 + x_2^4 + x_3^4 + x_4^4$ med hjälp av koefficienterna $a_3, a_2, a_1$ och $a_0$.

2. Förklara på vilket sätt man kan testa om polynomet $p$ bara har reella rötter med hjälp av potenssummorna $x_1^2 + x_2^2 + x_3^2 + x_4^2$ och $x_1^4 + x_2^4 + x_3^4 + x_4^4$ - utan att beräkna rötterna. Är testet tillräckligt för att veta att polynomet bara har reella rötter?

3. Utför testet på polynomen $f_1(x) = x^4 - x^3 + x^2 - x + 1$, $f_2(x) = x^4 - 2x^3 + x^2 + x + 1$ och $f_3(x) = x^4 - 2x^3 + x^2 - x + 1$.

**Övning 6.5.** Antag att polynomet $p(x) = x^3 + a_2x^2 + a_1x + a_0$ har rötterna $r_1, r_2$ och $r_3$. Bestäm koefficienterna av polynomet $q(x) = x^3 + b_2x^2 + b_1x + b_0$ som har rötterna $r_1^2, r_2^2$ och $r_3^2$ på följande sätt:

1. Uttryck $b_2, b_1$ och $b_0$ med hjälp av de elementära symmetriska polynomen $e_1(r_1^2, r_2^2, r_3^2), e_2(r_1^2, r_2^2, r_3^2)$ och $e_3(r_1^2, r_2^2, r_3^2)$. (Använd Exempel 6.4.2.)

2. Skriv $e_1(r_1^2, r_2^2, r_3^2), e_2(r_1^2, r_2^2, r_3^2)$ och $e_3(r_1^2, r_2^2, r_3^2)$ med hjälp av de elementära symmetriska polynomen i variablerna $r_1, r_2$ och $r_3$.

3. Skriv $e_1(r_1, r_2, r_3), e_2(r_1, r_2, r_3)$ och $e_3(r_1, r_2, r_3)$ med hjälp av $a_2, a_1$ och $a_0$. (Använd Exempel 6.4.2.)

4. Uttryck $b_2, b_1$ och $b_0$ med hjälp av $a_2, a_1$ och $a_0$.

5. Givet att polynomet $p(x) = x^3 - 2x^2 - 5x + 6$ har rötterna 1, $-2$ och 3, bestäm polynomet som har rötterna $1, 4$ och 9.

# 7 Algebrans fundamentalsats

I detta kapitel bevisar vi till sist den berömda *algebrans fundamentalsats:* varje polynom med komplexa koefficienter har minst en komplex rot. Vi börjar med att ge en översiktsbild av strategin vi kommer att använda i beviset. Efter detta kommer ett avsnitt där vi diskuterar maximum- och minimumpunkter av reellvärda funktioner, något som kommer att vara centralt i bevisföringen. Efter detta kommer själva beviset för satsen. Vi visar flera hjälpsatser som har att göra med vilka termer i ett polynom som är stora och vilka termer som är små, sett till beloppet. Man kan säga att när $|z|$ är nära noll, kommer polynomets beteende att avgöras av hur lägstagradstermen ser ut, och när $|z|$ är mycket stort kommer polynomets beteende att avgöras av hur högstagradstermen ser ut. När alla hjälpsatser är samlade får man ut beviset med förvånansvärt liten ansträngning.

Vi rekommenderar att läsaren växlar mellan översiktsbilden i avsnitt 7.1 och det utförliga beviset i avsnitt 7.3. Bevisskissen kan vara svårläst för att den känns för pratig och oprecis, medan det fullständiga beviset kanske kan kännas omotiverat eller så detaljerat att man inte ser skogen för alla träd.

## 7.1 Bevisskiss

Den grundläggande idén i beviset för algebrans fundamentalsats är att studera lokala minimipunkter till polynom över de komplexa talen. Över de reella talen är läsaren antagligen bekant med vad en minimum- och maximumpunkt till en funktion är för något, och hur man hittar dem: till exempel är $x = 0$ en (global) minimumpunkt till polynomet $x^2 + 1$, och $x = -1$ är ett (lokalt) maximum till polynomet $x^3 - 3x + 2$. (Vi avstår från att gå in i detaljer om uträkningarna som visar detta.)

Över de komplexa talen måste man först fundera över vad man menar med ett minimum eller ett maximum. Det är ju odefinierat huruvida ett komplext tal är större än ett annat. Dock kan vi jämföra beloppen av komplexa tal med varandra, så man kan säga att ett tal $z_0$ är ett lokalt minimum till $|f(z)|$ om det för alla tal $z$ som ligger tillräckligt nära $z_0$ i komplexa planet gäller att $|f(z)| \geqslant |f(z_0)|$.

Det som visar sig med denna definition är att de punkter som var minimi- och maximipunkter till polynom över de reella talen generellt slutar vara det när man tittar över de komplexa talen. Till exempel så var $x = 0$ ett minimum till $x^2 + 1$, som vi anmärkte förut. Men detta beror endast på att $x^2$ alltid är positivt när $x$ är reellt: när $x$ tillåts ta komplexa värden kan $x^2$ mycket väl vara negativt, så att vi inte längre har ett minimum i origo. (Tag t.ex. $x = i/10$, eller $x = i/1000$, eller...)

Den mycket viktiga hjälpsats vi visar i detta kapitel är följande: om $f$ är ett polynom och $z_0$ är en punkt i komplexa planet, så kan $|f(z)|$ endast ha ett lokalt minimum i denna punkt av den triviala anledningen att $f(z_0)$ faktiskt

är lika med noll. Med denna hjälpsats i vår arsenal räcker det alltså att visa att $|f(z)|$ har något lokalt minimum om vi vill visa att $f$ har ett nollställe.

För att visa existensen av ett lokalt minimum kommer vi faktiskt att visa ett starkare påstående, nämligen att det existerar ett globalt minimum. Det är inte sant att alla funktioner har ett globalt minimum, så det är verkligen något vi måste bevisa här! I vårt fall är vi intresserade av funktionen $|f|\colon \mathbb{C} \to \mathbb{R}$, som är sammansättningen av $f\colon \mathbb{C} \to \mathbb{C}$, och absolutbeloppsfunktionen $\mathbb{C} \to \mathbb{R}$. Det som dock gäller för funktionen $|f|\colon \mathbb{C} \to \mathbb{R}$ är följande egenskaper, som kommer att preciseras i kapitlet: (i) funktionen är *kontinuerlig*; (ii) när $|z|$ är tillräckligt stort kommer även $|f(z)|$ vara stort. Av dessa kommer vi endast att visa egenskap (ii). Intuitivt gäller påståendet eftersom att när $|z|$ är stort är högstagradstermen $z^n$ mycket större till beloppet än alla andra termerna.

Dessa två egenskaper visar sig vara tillräckliga för att garantera existensen av ett globalt minimum till en funktion $\mathbb{C} \to \mathbb{R}$. För att visa detta i detalj behövs det en lite djupare studie av egenskaper hos de reella och komplexa talen. Vi kommer därför att förpassa detta till ett appendix, och i kapitlet kommer vi endast att citera det resultat vi behöver.

## 7.2 Lokala och globala minima

Vi börjar med att definiera de termer vi kommer att tala om i detta kapitel. Vi nöjer oss med att definiera minimipunkter, och överlåter åt läsaren att formulera motsvarande definitioner av maximumpunkter. Låt oss börja med att definiera vad vi menar med ett globalt minimum.

**Definition 7.2.1.** Låt $X$ vara en godtycklig mängd, och $f\colon X \to \mathbb{R}$ en funktion. Vi säger att ett element $x_0 \in X$ är ett *globalt minimum till* $f$ om olikheten $f(x_0) \leqslant f(x)$ gäller för alla $x \in X$.

**Definition 7.2.2.** Låt $X$ vara en godtycklig mängd, och $f\colon X \to \mathbb{R}$ en funktion. Vi säger att $f$ är *nedåt begränsad* om det existerar en konstant $K$ sådan att $f(x) \geqslant K$ för alla $x \in X$.

En funktion som har ett globalt minimum är också nedåt begränsad, eftersom vi kan ta $K = f(x_0)$.

Vi kommer också att behöva tala om *lokala* minimipunkter. Detta skall tolkas som att funktionen inte antar några mindre värden än $f(x_0)$ så länge man tittar tillräckligt *nära* punkten $x_0$. Men för en godtycklig mängd $X$ är det meningslöst att tala om att två element är nära varandra, så i nästa definition måste vi vara lite specifikare angående vad för slags mängd funktionen $f$ är definierad på.

**Definition 7.2.3.** Låt $S$ vara en delmängd av $\mathbb{C}$, och $f\colon S \to \mathbb{R}$ en funktion. Vi säger att ett element $x_0 \in S$ är ett *lokalt minimum* till $f$ om det existerar ett tal $r > 0$ sådant att för alla $x \in S$ vars avstånd till $x_0$ (alltså $|x - x_0|$) är högst $r$, gäller att $f(x_0) \leqslant f(x)$.

Låt oss betrakta två exempel.

**Exempel 7.2.4.** Betrakta funktionen $f\colon \mathbb{C} \to \mathbb{R}$ som definieras genom $f(z) = e^{-|z|}$. Denna funktion antar ett största värde: vi har $f(0) = 1$, och om $z \neq 0$ är $|z| > 0$, så $e^{-|z|} < 1$. Funktionen är därför uppåt begränsad. Den är också nedåt begränsad, eftersom exponentialfunktionen aldrig är negativ. Dock saknar funktionen ett globalt minimum! Anledningen är att funktionen antar värden godtyckligt nära noll, men den antar aldrig värdet noll självt. När $|z|$ väljs stort nog kan $f(z)$ fås att vara mindre än vilken konstant $r > 0$ som helst. ▲

**Exempel 7.2.5.** Låt $S$ vara cirkelskivan

$$\{z \in \mathbb{C} \mid |z| < 1\},$$

och betrakta funktionen $f\colon S \to \mathbb{R}$ som ges av $f(x+iy) = y$, det vill säga, tar ut imaginärdelen. Denna funktion saknar både globalt och lokalt minimum. Funktionen antar alla värden i intervallet $-1 < r < 1$, men den antar aldrig randvärdena 1 och $-1$. Om vi ändrar mängden $S$ till

$$T = \{z \in \mathbb{C} \mid |z| \leqslant 1\},$$

det vill säga, vi lägger till randen på cirkelskivan, så finns det dock både ett globalt minimum och maximum, nämligen i punkterna $z = -i$ respektive $z = i$. ▲

Problemet i föregående exempel som förhindrade existensen av globala minima var att funktionen kunde anta mindre och mindre värden när variabeln $z$ togs närmre och närmre randen på definitionsmängden. På ett ganska liknande sätt var problemet i exemplet innan dess att funktionen antog mindre och mindre värden när variabeln $z$ togs närmre och närmre oändligheten.

Om man vill garantera att en kontinuerlig funktion har ett globalt minimum räcker det dock att utesluta dessa två möjligheter. Låt för varje $R \geqslant 0$

$$D_R = \{z \in \mathbb{C} \mid |z| \leqslant R\}.$$

Mänden $D_R$ har de viktiga egenskaperna att den är ändligt stor och *sluten*, vilket vi inte kommer att definiera precist men som ungefär innebär att den innehåller sin egen rand. Följande sats kommer vi att använda utan bevis.

**Sats 7.2.6.** *Varje kontinuerlig funktion $D_R \xrightarrow{f} \mathbb{R}$ har ett globalt minimum respektive maximum, det vill säga, antar ett största och minsta värde.*

Att definiera exakt vad en kontinuerlig funktion är skulle ta oss för långt från ämnet. En något omatematisk definition av kontinuitet är att så länge man har en tillräckligt liten störning i funktionens indata, kan man se till att skillnaden i funktionens utdata blir godtyckligt liten. Funktionerna i exemplen ovan är

kontinuerliga. Ett exempel på en icke kontinuerlig funktion är $f\colon \mathbb{C} \to \mathbb{R}$ som ges av

$$f(z) = \begin{cases} 1 & \text{om } z \in D_R \\ 0 & \text{annars.} \end{cases}$$

Denna funktion har en så kallad *diskontinuitet* i varje punkt på randen till cirkelskivan $D_R$. För oss räcker det att veta att när $f$ är ett polynom är $|f(z)|$ en kontinuerlig funktion, så att satsen ovan är tillämpbar i detta fall. Mer detaljer finns i appendixet.

## 7.3 Algebrans fundamentalsats

**Hjälpsats 7.3.1.** *Varje tal $a \in \mathbb{C}$ har en $k$:te rot för alla positiva heltal $k$, det vill säga, det existerar något $z$ som uppfyller $z^k = a$.*

*Bevis.* Skriv $a$ på polär form: $a = re^{i\theta}$. Låt nu $z = (\sqrt[k]{r})e^{i\theta/k}$. (Notera att eftersom $r$ är positivt och reellt, har det en positiv och reell $k$:te rot $\sqrt[k]{r}$ — vi behöver alltså inte använda hjälpsatsen vi försöker visa för att definiera $z$, vilket skulle leda till ett otrevligt cirkelbevis.) Nu gäller att

$$z^k = (\sqrt[k]{r})^k (e^{i\theta/k})^k = re^{i\theta} = a,$$

vilket visar påståendet. □

Denna hjälpsats är ett specialfall av algebrans fundamentalsats, eftersom det kan formuleras som att polynomet $z^k - a$ har minst en rot.

Vi påminner om triangelolikheten (Övning 1.5) eftersom den kommer att användas på flera ställen i resten av detta avsnitt. Olikheten säger att om $z$ och $w$ är komplexa tal, gäller att

$$|z \pm w| \leqslant |z| + |w|.$$

Vi kommer också att använda den omvända triangelolikheten,

$$|z \pm w| \geqslant |z| - |w|.$$

**Hjälpsats 7.3.2.** *Låt $f$ och $g$ vara polynom, och antag att* $\deg f > \deg g$. *Då existerar ett positivt tal $R$ sådant att*

$$|f(z)| > |g(z)|$$

*om $|z| > R$.*

*Bevis.* Den intuitiva förklaring till hjälpsatsen är mycket enkel: när $|z|$ är mycket stort, kommer högstagradstermen att vara mycket större än alla andra termer, så att beloppet av $|f(z)|$ i princip bestäms av beloppet av termen med högst grad. Alltså växer $|f|$ snabbare än $|g|$ om $f$ har högre gradtal. För att

visa hjälpsatsen rigoröst krävs dock en del räkning. Dock kan vi göra riktigt grova uppskattningar, eftersom vi inte är intresserade av att hitta ett speciellt litet $R$ — vi vill bara veta att det existerar *något* tal $R$ med egenskapen i hjälpsatsen.

Låt $f(z) = a_0 + a_1 z + \ldots + a_n z^n$, och $g(z) = b_0 + b_1 z + \ldots + b_m z^m$. Genom att använda triangelolikheten flera gånger fås att

$$|g(z)| \leqslant |b_0| + |b_1||z| + \ldots + |b_m||z^m|.$$

Om dessutom $|z| \geqslant 1$ (och eftersom vi får välja $R$ hur stort vi vill är det ju tillåtet att anta detta) kommer $|z^m| > |z|$, så vi får en ännu grövre uppskattning genom att ta

$$|g(z)| \leqslant (|b_0| + |b_1| + \ldots + |b_m|)\,|z^m|.$$

För att förenkla notationen, låt $b = |b_0| + |b_1| + \ldots + |b_m|$. Vi kan alltså ersätta $g$ med

$$\widetilde{g}(z) = bz^m,$$

eftersom detta polynom kommer att ha större belopp än $g$ när $|z|$ är stort. Vi kan dessutom anta att $m = n - 1$, eftersom

$$|bz^{n-1}| = |bz^m| \cdot |z^{n-1-m}| \geqslant |bz^m|,$$

då $|z| \geqslant 1$ och $n - 1 - m \geqslant 0$. Nu är

$$\left|\frac{f(z)}{\widetilde{g}(z)}\right| = \left|\frac{a_0 + \ldots + a_n z^n}{bz^{n-1}}\right| = \frac{1}{b}\left|\frac{a_0}{z^{n-1}} + \frac{a_1}{z^{n-2}} + \ldots + a_{n-1} + a_n z\right|. \quad (7.1)$$

Antag att $|z|$ är större än den största av koefficienterna $a_0, \ldots, a_{n-2}$. I så fall har var och en av termerna

$$\frac{a_0}{z^{n-1}}, \frac{a_1}{z^{n-2}}, \ldots, \frac{a_{n-2}}{z}$$

belopp mindre än 1. Eftersom det är $n - 1$ stycken termer, följer det ur triangelolikheten att

$$\left|\frac{a_0}{z^{n-1}} + \frac{a_1}{z^{n-2}} + \ldots + \frac{a_{n-2}}{z} + a_{n-1}\right| \leqslant n - 1 + |a_{n-1}|.$$

Låt nu $a = n - 1 + |a_{n-1}|$. Använder vi omvända triangelolikheten på ekvation (7.1) fås

$$\left|\frac{f(z)}{\widetilde{g}(z)}\right| \geqslant= \frac{1}{b}\left(|a_n z| - \left|\frac{a_0}{z^{n-1}} + \frac{a_1}{z^{n-2}} + \ldots + a_{n-1}\right|\right) \geqslant \frac{1}{b}\left(|a_n z| - a\right). \quad (7.2)$$

Antag nu att

$$|z| > \frac{a+b}{|a_n|}.$$

Insättning i ekvation (7.2) ger att

$$\left|\frac{f(z)}{\widetilde{g}(z)}\right| > \frac{1}{b}\left(|a_n| \cdot \frac{a+b}{|a_n|} - a\right) = 1,$$

eller ekvivalent att $|f(z)| > |\widetilde{g}(z)| > |g(z)|$. □

I beviset ansträngde vi oss inte för att hitta en speciellt *bra* undre gräns för vad $R$ ska väljas till, utan nöjde oss med att veta att något sådant $R$ existerar. I beviset antog vi på olika ställen att $|z| \geqslant 1$, att $|z|$ är större än var och en av koefficienterna $a_0, a_1, \cdots a_{n-2}$, och slutligen att $|z| \geqslant (a+b)/|a_n|$, där både $a$ och $b$ var stora uttryck som berodde på koefficienterna till $f$ och $g$. Beviset säger alltså att $R$ skall väljas större än vart och ett av dessa villkor.

Nästa hjälpsats är en variation på den föregående. Nu vill vi i stället studera beteendet nära origo. I förra hjälpsatsen var intuitionen att när $|z|$ är stort kommer bara högstagradstermen att avgöra polynomets beteende, och att högstagradstermen växer snabbare ju högre gradtal den har. Här behöver vi i stället att när $|z|$ är litet så kommer lägstagradstermen att vara dominerande, och ju lägre gradtal denna term har desto större blir den nära origo. För att bevisa denna hjälpsats kommer vi att använda resultatet av föregående hjälpsats och variabelbytet $w = 1/z$; att $|z|$ är nära noll blir då exakt samma sak som att $w$ har stort absolutbelopp.

**Definition 7.3.3.** Låt $f$ vara ett polynom. Vi definierar *kograden* av $f$ som exponenten till den term som har *lägst* gradtal. Kograden till nollpolynomet definieras som $+\infty$. Vi betecknar kograden med $\operatorname{codeg} f$.

**Hjälpsats 7.3.4.** *Låt $f$ och $g$ vara nollskilda polynom. Antag att* $\operatorname{codeg} f < \operatorname{codeg} g$. *I så fall existerar ett positivt tal $r$ sådant att*

$$|f(z)| > |g(z)|$$

*inuti den punkterade disken* $\{z \in \mathbb{C} \mid 0 < |z| < r\}$.

*Bevis.* Om $g = 0$ är antagandet i hjälpsatsen sant, och påståendet uppenbart. Så antag att $g \neq 0$.

Låt $w = 1/z$. Vi kan inte direkt tillämpa föregående hjälpsats på uttrycken $f(1/w)$ och $g(1/w)$, eftersom dessa inte är polynom i $w$. Det vi dock kan göra är detta: låt $N$ vara ett tal större än eller lika med både $\deg(f)$ och $\deg(g)$. Betrakta

$$w^N f(1/w) \text{ och } w^N g(1/w).$$

Uttrycket $f(1/w)$ innehåller bara negative exponenter av $w$. Den lägsta exponenten som ingår är $-\deg(f)$ och den högsta exponenten blir $-\operatorname{codeg}(f)$. Eftersom $N - \deg(f) \geqslant 0$ blir $w^N f(1/w)$ verkligen ett polynom i $w$, och dess grad är $N - \operatorname{codeg}(f)$. Motsvarande påstående gäller för $g$. Alltså är

$$\deg(w^N f(1/w)) = N - \operatorname{codeg}(f) > N - \operatorname{codeg}(g) = \deg(w^N g(1/w)),$$

så enligt föregående hjälpsats finns det ett tal $R$ sådant att när $|w| > R$ är

$$|w^N f(1/w)| > |w^N g(1/w)|.$$

Delar vi olikheten med $|w^N|$ (som ju måste vara positivt och nollskilt!) fås i stället att

$$|f(1/w)| > |g(1/w)|$$

då $|w| > R$, vilket efter att byta tillbaks till variabeln $z$ är ekvivalent med att

$$|f(z)| > |g(z)|$$

då $0 < |z| < 1/R$. □

**Hjälpsats 7.3.5.** *Låt $f$ vara ett icke-konstant polynom, och antag att $f(z_0) \neq 0$. I så fall har $|f(z)|$ inte ett lokalt minimum i punkten $z_0$.*

*Bevis.* Vi gör först några förenklande antaganden. Att visa att $f(z)$ inte har ett minimum i $z_0$ är ekvivalent med att visa att polynomet $f(z + z_0)$ inte har ett minimum i origo. Genom att byta ut vårt ursprungliga $f$ mot $f(z + z_0)$ kan vi alltså anta att $z_0 = 0$. Vi kommer inte heller att förändra huruvida polynomet har ett minimum eller inte genom att dividera $f$ med $f(0)$ (som vi vet är nollskilt), så vi kan anta att $f(0) = 1$.

Låt $b$ vara polynomets nästa nollskilda koefficient efter konstanttermen, så att vi kan skriva

$$f(z) = 1 + bz^k + z^{k+1}g(z),$$

där $k \geqslant 1$ är något heltal och $g(z)$ är något polynom. Enligt Hjälpsats 7.3.1 kan vi välja ett tal $a$ sådant att $a^k = -1/b$. Genom att ersätta $z$ med $az$, kan vi dessutom anta att $b = -1$, eftersom $b(az)^k = -z^k$. För att sammanfatta kan vi alltså anta att $z_0 = 0$, och att $f$ har den speciella formen

$$f(z) = 1 - z^k + z^{k+1}g(z).$$

Det vi vill visa nu är att om man väljer $z$ till ett tillräckligt litet positivt reellt tal kommer

$$|f(z)| < |f(0)|.$$

Speciellt kan då inte $|f(0)|$ ha varit ett lokalt minimum, eftersom $z$ kan väljas godtyckligt nära origo. Uppenbarligen gäller det att

$$\operatorname{codeg}(z^k) < \operatorname{codeg}(z^{k+1}g(z)).$$

Enligt Hjälpsats 7.3.4 existerar det ett tal $r > 0$ sådant att för alla $z$ med $0 < |z| < r$ gäller

$$|z^k| > |z^{k+1}g(z)|.$$

Om $|z| < r$ ger denna olikhet tillsammans med triangelolikheten (Övning 1.5) att

$$|f(z)| = |1 - z^k + z^{k+1}g(z)| \leqslant |1 - z^k| + |z^{k+1}g(z)| < |1 - z^k| + |z^k|.$$

Antag nu att $z$, utöver att vara mindre i belopp än $r$, dessutom är positivt, reellt och mindre än 1. I så fall är $|1 - z^k| = 1 - z^k$ och $|z^k| = r^k$. Olikheten ovan blir därav

$$|f(z)| < 1 - z^k + z^k = 1 = |f(0)|.$$

Eftersom det går att hitta reella tal $z$ godtyckligt nära origo som uppfyller de givna villkoren ($0 < z < r$, $z < 1$) visar detta att $|f(z)|$ inte kan ha haft origo som lokalt minimum. □

**Sats 7.3.6.** *Varje polynom av grad minst ett har minst en rot i komplexa planet.*

*Bevis.* Betrakta $f(0)$ som ett polynom av grad noll. Enligt Hjälpsats 7.3.2 existerar en konstant $R$ sådan att $|f(z)| > |f(0)|$ om $|z| > R$, det vill säga, om $z \notin D_R$. Enligt Sats 7.2.6 finns det en punkt $z_0 \in D_R$ som minimerar den kontinuerliga funktionen $|f(z)| : D_R \to \mathbb{R}$. Vi vet alltså att

$$|f(z)| \geqslant |f(z_0)|$$

för alla $z \in D_R$. Men vi vet också att $|f(z)| \geqslant |f(0)|$ för alla $z \notin D_R$, och att $|f(0)| \geqslant |f(z_0)|$ eftersom $0 \in D_R$. Det följer att olikheten

$$|f(z)| \geqslant |f(z_0)|$$

gäller för alla $z \in \mathbb{C}$ över huvud taget. Alltså är $z_0$ ett globalt minimum och speciellt även ett *lokalt* minimum. Men i så fall ger Hjälpsats 7.3.5 att $f(z_0) = 0$, och vi har funnit en rot. □

## Övningar

**Övning 7.1.** Låt $f(x) = a_0 + a_k x^k + a_{k+1} x^k + \cdots + a_n x^n$ vara ett polynom med reella koefficienter, så att $f$ definierar en funktion $\mathbb{R} \to \mathbb{R}$. Här är $k \geqslant 1$ gradtalet på första nollskilda koefficienten efter konstanttermen. Visa att huruvida $f$ har ett lokalt minimum eller maximum i origo endast bestäms av $a_k$. Mer specifikt: om $k$ är udda har $f$ varken ett minimum eller maximum, men om $k$ är jämnt kommer $f$ att ha ett lokalt minimum om $a_k > 0$ och ett lokalt maximum om $a_k < 0$.

**Övning 7.2.** Förklara vad föregående uppgift har att göra med det så kallade ”andraderivata-testet”, om ni har sett det tidigare.

**Övning 7.3.** Låt $f$ vara ett icke-konstant polynom. Visa att $f$ antar alla värden i det komplexa planet minst en gång.

**Övning 7.4.** Låt $f$ vara ett polynom av grad $n > 0$. Visa att $f$ antar alla utom ändligt många värden i det komplexa planet exakt $n$ gånger.

Ledning: Använd resultatet från Övning 2.8, att polynomet $f$ har en upprepad rot i punkten $z_0$ om och endast om $z_0$ också är en rot till derivatan till $f$.

**Övning 7.5.** Visa att följande två påståenden är ekvivalenta: (i) Varje polynom med koefficienter i $\mathbb{C}$ har minst en rot; (ii) De enda polynom med koefficienter i $\mathbb{C}$ som är irreducibla över $\mathbb{C}$ har de vars grad är högst 1.

**Övning 7.6.** Låt $f$ vara ett polynom, och $R > 0$ ett tal. Funktionen

$$|f| : D_R \to \mathbb{R}$$

har enligt Sats 7.2.6 ett största och minsta värde. Visa att maximum antas på randen till mängden, det vill säga då $|z| = R$. Ledning: bevisa först en motsvarighet till Sats 7.3.5 för lokala maximum, i stället för lokala minimum.

**Övning 7.7.** Låt $D$ vara enhetsdisken $D_1 = \{z \in \mathbb{C} \mid |z| \leqslant 1\}$. Låt $f$ vara ett polynom som har egenskapen att $f(z) \in D$ om $z \in D$. Antag också att $f(0) = 0$. Visa att olikheten $|f(z)| \leqslant |z|$ gäller på hela $D$. Ledning: använd resultatet från föregående uppgift på ett listigt sätt.

## Lösningar till udda övningsuppgifter

**Övning 0.1.**

1. $B \cup C = A$.
2. $B \cap C = \emptyset$.
3. $D \cap C = \{4, 36\}$.
4. $\{x \in D \mid x \in B\} = D \cap B = \{1, 19, 101\}$.
5. $\{x \in A \mid x = y + 1 \text{ för något } y \in D\} = \{2, 5, 20, 37, 102\}$.
6. $\{x + 1 \mid x \in D\} = \{2, 5, 20, 37, 102\}$.

**Övning 0.3.** Tag $x \in ((A \cap C) \cup (B \cap C^c))^c$. Det betyder att $x \in \Omega$ och $x \notin (A \cap C) \cup (B \cap C^c)$. Alltså har vi att $x \notin A \cap C$ och $x \notin B \cap C^c$. Det finns nu två möjligheter: $x \in C$ och $x \notin C$.

I det första fallet, det vill säga $x \in C$, måste $x \notin A$ eftersom om $x \in A$ så skulle $x \in A \cap C$ vilket är falskt. Alltså gäller $x \in A^c$, vilket tillsammans med $x \in C$ ger att $x \in A^c \cap C$ i detta fall. I synnerhet har vi att $x \in (A^c \cap C) \cup (B^c \cap C^c)$.

I det andra fallet gäller $x \in C^c$ och då måste $x \in B^c$ eftersom om $x \in B$ så skulle $x \in B \cap C^c$ vilket är falskt. Alltså gäller $x \in B^c \cap C^c$, och i synnerhet $x \in (A^c \cap C) \cup (B^c \cap C^c)$.

I båda fallen gäller alltså $x \in (A^c \cap C) \cup (B^c \cap C^c)$, och eftersom $x$ var godtycklig så visar detta att $((A \cap C) \cup (B \cap C^c))^c \subseteq (A^c \cap C) \cup (B^c \cap C^c)$.

Omvänt, tag $x \in (A^c \cap C) \cup (B^c \cap C^c)$. Då gäller $x \in A^c \cap C$ eller $x \in B^c \cap C^c$ (eller båda). Vi har alltså dessa två fall.

I det första fallet, det vill säga $x \in A^c \cap C$, har vi att $x \notin A$ och $x \notin C^c$. I synnerhet har vi att $x \notin A \cap C$ (eftersom $x \notin A$) och att $x \notin B \cap C^c$ (eftersom $x \notin C^c$). Alltså tillhör $x$ varken $A \cap C$ eller $B \cap C^c$, vilket betyder att $x \in ((A \cap C) \cup (B \cap C^c))^c$.

I det andra fallet, det vill säga $x \in B^c \cap C^c$ har vi att $x \notin B$ och att $x \notin C$. Det följer att $x \notin A \cap C$ och att $x \notin B \cap C^c$. Alltså gäller $x \notin (A \cap C) \cup (B \cap C^c)$, vilket betyder att $x \in ((A \cap C) \cup (B \cap C^c))^c$.

I båda fallen har det alltså visats att $x \in ((A \cap C) \cup (B \cap C^c))^c$, och eftersom $x$ var godtycklig visar detta att $(A^c \cap C) \cup (B^c \cap C^c) \subseteq ((A \cap C) \cup (B \cap C^c))^c$.

Vi har alltså visat att $((A \cap C) \cup (B \cap C^c))^c \subseteq (A^c \cap C) \cup (B^c \cap C^c)$ och att $(A^c \cap C) \cup (B^c \cap C^c) \subseteq ((A \cap C) \cup (B \cap C^c))^c$ och därmed att

$$((A \cap C) \cup (B \cap C^c))^c = (A^c \cap C) \cup (B^c \cap C^c).$$

**Övning 1.1.**

1. Vi beräknar först summan $z + w = 3 + (-1) + (1 + 4)i = 2 + 5i$ och differensen $z - w = 3 - (-1) + (1 - 4)i = 4 - 3i$. Produkten av $z$ och $w$ blir
$$zw = 3 \cdot (-1) - 4 \cdot 1 + i(3 \cdot 4 + 1 \cdot (-1)) = -7 + 11i.$$
Eftersom $|-1 + 4i|^2 = 4^2 + 1^2 = 17$ får vi
$$\frac{z}{w} = \frac{(3+i)(-1-4i)}{(-1+4i)(1-4i)} = \frac{-3+4+i(-12-1)}{17} = \frac{1}{17} - \frac{13}{17}i.$$

2. Vi har $z + w = 0 + 2 + i(-\sqrt{2} - 5) = 2 - (5 + \sqrt{2})i$, och differensen blir $z - w = 0 - 2 + i(-\sqrt{2} - (-5)) = -2 + (5 - \sqrt{2})i$. Vi får vidare
$$zw = 0 \cdot 2 - (-\sqrt{2})(-5) + i(0 \cdot (-5) - 2 \cdot \sqrt{2}) = -5\sqrt{2} - 2\sqrt{2}i,$$
och kvoten av $z$ och $w$ blir
$$\frac{z}{w} = \frac{-\sqrt{2}i \cdot (2 + 5i)}{4 + 25} = \frac{5\sqrt{2}}{29} - \frac{2\sqrt{2}}{29}i.$$

**Övning 1.3.** Om $z = x + iy$ är $\overline{z} = x - iy$. Så
$$z + \overline{z} = x + iy + x - iy = 2x,$$
och
$$z - \overline{z} = x + iy - x + iy = 2iy.$$
Delar vi ekvationerna ovan med 2 respektive $2i$ finner vi att
$$x = \mathrm{Re}(z) = \frac{z + \overline{z}}{2}$$
och
$$y = \mathrm{Im}(z) = \frac{z - \overline{z}}{2i}.$$

**Övning 1.5.** Vi ska visa att $|x + y| \leqslant |x| + |y|$. Eftersom bägge sidor är ickenegativa, är detta ekvivalent med att visa att
$$|x + y|^2 \leqslant (|x| + |y|)^2 = |x|^2 + |y|^2 + 2|x||y|,$$
vilket i sin tur är ekvivalent med att
$$(x + y)(\overline{x} + \overline{y}) \leqslant x\overline{x} + y\overline{y} + 2|x||y|.$$
Men $(x + y)(\overline{x} + \overline{y}) = x\overline{x} + y\overline{y} + x\overline{y} + y\overline{x}$. Subtraherar vi $x\overline{x} + y\overline{y}$ från bägge sidor finner vi alltså att det är ekvivalent att visa olikheten
$$x\overline{y} + y\overline{x} \leqslant 2|x||y|.$$
Låt nu $z = x\overline{y}$. Då är $|z| = |x||\overline{y}| = |x||y|$, så vi kan skriva om olikheten som
$$z + \overline{z} \leqslant 2|z|.$$

Eftersom $z + \overline{z} = 2\mathrm{Re}(z)$, återstår enbart att visa olikheten $\Re(z) \leqslant |z|$. Om $z = a + bi$ skall vi alltså visa att $a \leqslant \sqrt{a^2 + b^2}$. Men eftersom $b^2 \geqslant 0$ är $\sqrt{a^2 + b^2} \geqslant \sqrt{a^2} = |a| \geqslant a$. och olikheten är visad.

För att visa den omvända triangelolikheten, låt $z = x - y$. Vi har enligt triangelolikheten att $|z + y| \leqslant |z| + |y|$. Men detta är samma sak som att $|x| \leqslant |x - y| + |y|$, eller $|x| - |y| \leqslant |x - y|$.

**Övning 1.7.** Vi skriver $e^{i\theta}$ med hjälp av sinus och cosinus

$$\frac{d}{d\theta} e^{i\theta} = \frac{d}{d\theta} (\cos\theta + i \sin\theta)$$

och deriverar real- och imaginärdel var för sig, vilket ger oss

$$\begin{aligned} \frac{d}{d\theta} e^{i\theta} &= \frac{d}{d\theta} \cos\theta + i \frac{d}{d\theta} \sin\theta \\ &= -\sin\theta + i\cos\theta \\ &= i\,(i\sin\theta + \cos\theta) \\ &= ie^{i\theta} \end{aligned}$$

**Övning 2.1.** Vi börjar med basfallet $n = 1$: ekvation 2.2 är uppfyllt för $n = 1$ eftersom $1^2 = \frac{2\cdot 1^3 + 3 1^2 + 1}{6} = 1$.

Antag att ekvation (2.2) gäller för något $n \in \mathbb{N}$. Vi ska visa att det då gäller för $n + 1$. Betrakta vänsterledet i ekvation (2.2) för $n + 1$.

$$1^2 + 2^2 + 3^2 + \ldots + n^2 + (n+1)^2 = \left(1^2 + 2^2 + 3^2 + \ldots + n^2\right) + (n+1)^2$$

Vi använder induktionsantagandet att ekvation (2.2) gäller för $n$ och ersätter den kortare summan. Det ger oss att

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \ldots + n^2 &= \frac{2n^3 + 3n^2 + n}{6} + (n+1)^2 \\ &= \frac{2n^3 + 3n^2 + n + 6(n+1)^2}{6} \\ &= \frac{2n^3 + 9n^2 + 13n + 6}{6} \end{aligned}$$

Vi beräknar högerledet i Ekvation 2.2 där vi ersätter $n$ med $n + 1$

$$\begin{aligned} &\frac{2(n+1)^3 + 3(n+1)^2 + (n+1)}{6} \\ &\quad = \frac{2(n^3 + 3n^2 + 3n + 1) + 3(n^2 + 2n + 1) + (n+1)}{6} \\ &\quad = \frac{2n^3 + 9n^2 + 13n + 6}{6} \end{aligned}$$

Vi ser att vänster- och högerledet blir samma och därmed stämmer ekvation 2.2 även för $n + 1$.

Nu ger induktionsprincipen att ekvation (2.2) gäller för alla $n \in \mathbb{N}$.

**Övning 2.3.** Antag att $\deg f = n$ och $\deg g = m$. Då kan vi skriva $f(x) = a_n x^n + \ldots + a_1 x + a_0$ och $g(x) = b_m x^m + \ldots + b_1 x + b_0$ för några $a_0, \ldots, a_n \in \mathbb{C}$ och $b_0, \ldots, b_n \in \mathbb{C}$ där $a_n \neq 0$ och $b_m \neq 0$.

(i). Vi beräknar produkten

$$\begin{aligned}(fg)(x) &= (a_n x^n + \ldots + a_1 x + a_0) + (b_m x^m + \ldots + b_1 x + b_0) \\ &= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m)\, x^{n+m-1} + \ldots\end{aligned}$$

Vi ser att termen med den högsta exponenten är lika med $a_n b_m x^{n+m}$ och att $a_n b_m \neq 0$. Därmed är $\deg(fg) = n + m$.

(ii). Vi beräknar summan

$$(f+g)(x) = (a_n x^n + \ldots + a_1 x + a_0) + (b_m x^m + \ldots + b_1 x + b_0)\,.$$

Vi betraktar olika möjliga fall.

Fall 1: $n > m$. Termen med den högsta exponenten i $f + g$ är lika med $a_n x^n$ och därmed är $\deg(f + g) = \deg f$.

Fall 2: $n < m$. Då är $b_m x^m$ termen med den högsta exponenten och vi får $\deg(f + g) = \deg g$.

Fall 3: $n = m$ och $a_n + b_n \neq 0$. I detta fall är termen med den högsta exponenten lika med $(a_n + b_n)x^n$ och eftersom $a_n + b_n \neq 0$ får vi $\deg(f+g) = \deg f = \deg g$.

Fall 4: $n = m$ och $a_n + b_n = 0$. Det är det intressanta fallet, eftersom termen $(a_n + b_n)x^n$ är lika med 0 och försvinner. Då har termen med den högsta exponenten som inte försvinner en exponent som är mindre än $n$ och vi får att $\deg(f + g) < \deg f = \deg g$.

Vi ser att i alla fyra fall blir $\deg(f + g) \leqslant \max(\deg f, \deg g)$.

(iii) Tag till exempel $f(x) = x + 1$ och $g(x) = -x + 2$ där $\deg f = 1$ och $\deg g = 1$. Vi får att $f + g = 3$ och $\deg(f + g) = 0$. Alltså är i detta fall $\deg(f + g) < \max(\deg f, \deg g)$.

**Övning 2.5.** Vi har enligt uppgiften följande situation:

$$\begin{aligned} f &= q_2 g + f_2 \\ g &= q_3 f_2 + f_3 \\ f_2 &= q_4 f_3 + f_4 \\ &\ldots \\ f_{k-2} &= q_k f_{k-1} + f_k \\ f_{k-1} &= q_{k+1} f_k + 0. \end{aligned}$$

(a). Om vi betraktar den sista ekvationen ovan, ser vi att $f_{k-1}$ är delbart med $f_k$. Enligt den näst sista ekvationen är $f_{k-2}$ summan av två polynom som båda är delbara med $f_k$ och därmed är $f_{k-2}$ delbart med $f_k$. Det följer att $f_{k-3} = q_{k-1} f_{k-2} + f_{k-1}$ också är delbart med $f_k$. Vi fortsätter stegvis med

samma metod och får att $f_{k-4}, f_{k-5}, \ldots, f_2$ och slutligen $f_1 = g$ och $f_0 = f$ är delbara med $f_k$. Därmed är $f_k$ en gemensam delare av $f$ och $g$.

*Anmärkning.* Vi använde oss av följande två egenskaper: (i) Om polynomet $f$ är delbart med polynomet $p$, så är även $fg$ delbart med $p$. (ii) Om två polynom $f$ och $g$ är delbara med polynomet $p$, så är även $f + g$ delbart med $p$.)

(b). Låt $h$ vara en gemensam delare till $f$ och $g$. Eftersom $f_2 = f - q_2 g$ och $f$ och $g$ är delbara med $h$, så är även $f_2$ delbart med $h$. På samma sätt är $f_3 = g - q_3 f_2$ och därmed är $f_3$ delbart med $h$. Vi fortsätter och får succesivt att $f_4, f_5, \ldots, f_k$ är delbara med $h$.

(c). Vi använder polynomdivision för att beräkna kvoten och resten vid division av $x^5 - x^5 + 4x^2 - 2x - 8$ med $x^3 + x^2 - 2x - 2$ samt kvoter och rester i de följande stegen av Euklides algoritm. Vi får följande resultat:

$$\begin{aligned} 2x^4 - 5x^3 + 2x^2 + 4x - 5 &= (x-1)(2x^3 - 3x^2 - 2x + 3) + (x^2 - x - 2) \\ 2x^3 - 3x^2 - 2x + 3 &= (2x-1)(x^2 - x - 2) + (x+1) \\ x^2 - x - 2 &= (x-2)(x+1) \end{aligned}$$

Den sista resten som vi fick innan resten blev 0, var $x + 1$ vilket redan är ett moniskt polynom. Därmed är $\mathrm{sgd}(2x^4 - 5x^3 + 2x^2 + 4x - 5, x^3 + x^2 - 2x - 2) = x + 1$.

**Övning 2.7.** Polynomet har reella koefficienter och enligt Övning 2.6 är då även $\overline{x} = -1 - i$ en rot. Vi vet från Sats 2.4.3 (Faktorsatsen) att vi kan skriva $x^4 + 2x^3 + 3x^2 + 2x + 2$ på formen $(x - (-1 - i))(x - (-1 + i))p = (x^2 + 2x + 2)p$ för något polynom $p$. Vi utför polynomdivision för att bestämma $p$ och får $p = x^2 + 1$. Vi ser att $p$ har rötterna $x = i$ och $x = -i$. Därmed har ekvationen $x^4 + 2x^3 + 3x^2 + 2x + 2 = 0$ rötterna $-1 + i, -1 - i, i$ och $-i$. Eftersom $x^4 + 2x^3 + 3x^2 + 2x + 2 = 0$ är av grad 4 kan det inte finnas fler än fyra rötter och vi har bestämt samtliga rötter.

**Övning 3.1.** Vi visar först att varje positivt heltal är en produkt av primtal med induktion över $n$. När $n = 2$ är $n$ själv ett primtal. Antag att alla tal mindre än eller lika med $n$ kan skrivas som en produkt av primtal. Vi delar in i två fall: antingen är $n + 1$ ett primtal, och vi är klara. Eller så är $n + 1$ inte ett primtal, och vi kan skriva

$$n + 1 = n_1 \cdot n_2$$

där $n_1$ och $n_2$ båda är mindre än $n$. Induktionsantagandet ger att både $n_1$ och $n_2$ kan faktoriseras i primtal.

Vi visar sedan att denna faktorisering är unik med hjälp av induktion. Basfallet $n = 2$ är klart. Antag att alla tal mindre än eller lika med $n$ har en unik faktorisering i primtal. Antag att $n + 1$ har två faktoriseringar i primtal:

$$n + 1 = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m.$$

Vi vill visa att dessa är lika upp till ordningen av faktorerna. Om $p_1 = q_1$, dela med dessa och använd induktionsantagandet på

$$p_2 p_3 \cdots p_n = q_2 \cdots q_m.$$

Om inte, antag att $p_1 < q_1$. Eftersom vi kan dividera heltal med varandra med rest, existerar heltal $a$ och $b$ sådana att

$$q_1 = ap_1 + b,$$

där $b < p_1$. Alltså gäller att

$$n + 1 = (ap_1 + b)q_2 q_3 \cdots q_m.$$

Vi vet att $p_1$ delar både $n + 1$ och produkten $ap_1 q_2 q_3 \cdots q_m$. Alltså är även deras differens, det vill säga

$$bq_2 q_3 \cdots q_m,$$

delbar med $p_1$. Observera nu att $b < p_1$, och vi antog att $p_1 < \deg q_1$. Det följer att

$$n + 1 = q_1 q_2 \cdots q_m > p_1 q_2 q_3 \cdots q_m > bq_2 q_3 \cdots q_m.$$

Enligt induktionsantagandet finns det alltså en *unik* faktorisering av produkten $bq_2 q_3 \cdots q_m$ i primtal. Men eftersom alla $q_i$ redan är primtal, måste denna faktorisering fås genom att dela upp $b$ i primtalsfaktorer.

Eftersom $p_1$ delar $bq_2 q_3 \cdots q_m$ vet vi igen enligt induktionsantagandet att $p_1$ är ett av primtalen som ingår i denna faktorisering. Eftersom $p_1 > b$ kan inte $p_1$ vara en av primtalsfaktorerna vi fick när vi faktoriserade $b$, så $p_1$ är lika med någon $q_i$. Genom att byta ordning på faktorerna hamnar vi återigen i fallet att $p_1 = q_1$.

**Övning 3.3.** Vi vet att om $z$ är en icke-reell rot till $f$, så kommer $(x-z)(x-\overline{z})$ att vara en irreducibel faktor, som i beviset av Sats 3.4.2. Alltså är polynomet $f$ delbart med

$$(x + 1 + i)(x + 1 - i) = (x + 1)^2 - i^2 = x^2 + 2x + 2.$$

Vi beräknar kvoten av $f$ med $x^2 + 2x + 2$ med hjälp av liggande stolen:

$$\begin{array}{rrrrrrrrrrrrr}
 & x^2 & + & x & - & 6 & & & & & & \multicolumn{2}{|r}{x^2+2x+2} \\
\cline{2-13}
 & (x^4 & + & 3x^3 & - & 2x^2 & - & 10x & - & 12) & & \multicolumn{2}{|r}{} \\
- & (x^4 & + & 2x^3 & + & 2x^2) & & & & & & \multicolumn{2}{|r}{} \\
\cline{2-10}
 & & & x^3 & - & 4x^2 & - & 10x & - & 12 & & \multicolumn{2}{|r}{} \\
 & & - & (x^3 & + & 2x^2 & + & 2x) & & & & \multicolumn{2}{|r}{} \\
\cline{3-10}
 & & & & - & 6x^2 & - & 12x & - & 12 & & \multicolumn{2}{|r}{} \\
 & & & - & (- & 6x^2 & - & 12x & - & 12) & & \multicolumn{2}{|r}{} \\
\cline{4-13}
 & & & & & & & & & 0 & & \multicolumn{2}{|r}{}
\end{array}$$

Vi finner alltså att

$$x^4 + 3x^3 - 2x^2 - 10x - 12 = (x^2 + 2x + 2)(x^2 + x - 6).$$

Det återstår att ta hand om faktorn $x^2 + x - 6$. Om den saknar reella rötter är den irreducibel, men annars är den en produkt av två andragradare. Med hjälp av kvadratkomplettering eller $pq$-formeln finner man dock att $x^2 + x - 6$ har de två rötterna 2 och $-3$, så den fullständiga faktoriseringen i irreducibla faktorer blir

$$f(x) = (x^2 + 2x + 2)(x - 2)(x + 3).$$

**Övning 3.5.** Om $f(x) = f_1(x) \cdots f_n(x)$, är också $f(x^2) = f_1(x^2) \cdots f_n(x^2)$. Alltså ger varje irreducibel faktor till $f(x)$ upphov till minst en irreducibel faktor till $f(x^2)$. Vi har samma antal irreducibla faktorer endast om för varje irreducibel faktor $f_i(x)$ till $f(x)$, $f_i(x^2)$ också är irreducibel.

Vi vet enligt Sats 3.4.2 att $f_i(x)$ antingen är en andragradare utan reella rötter, eller en förstagradare. Antag att $\deg f_i(x) = 2$. I så fall är $\deg f_i(x^2) = 4$, som aldrig kan vara irreducibelt. Vi får alltså inte ha några sådana faktorer.

Antag därför att $f_i(x) = (x - r)$, där $r \in \mathbb{R}$. Om $r \geqslant 0$ får vi en faktorisering

$$f_i(x^2) = (x - \sqrt{r})(x + \sqrt{r}),$$

över $\mathbb{R}$, eftersom $r$ har en reell kvadratrot i detta fall. Om $r < 0$ fås istället

$$f_i(x^2) = (x^2 - r)$$

som saknar reella rötter eftersom $x^2 \geqslant 0$ och $-r > 0$. Det följer att $f$ endast kan ha strikt negativa reella rötter.

**Övning 4.1.** Enligt Sats 4.1.8 måste varje rationell rot $p/q$ uppfylla att $p$ delar 1 och $q$ delar 1. Alltså är enda möjligheten att $\pm 1$ är en rot. Om 1 är en rot, är

$$1 + n + 1 = 0,$$

så $n = -2$. Om $-1$ är en rot, är

$$-1 - n + 1 = 0,$$

så $n = 0$. Dessa är enda möjligheterna.

**Övning 4.3.** Denna egenskap gäller inte längre om $p$ inte är ett primtal. Tag till exempel $p = 6$, $a = 3$, $b = 4$.

**Övning 4.5.** Vi gör variabelbytet $x = y + 1$. Formellt betyder detta att vi inför polynomet

$$g(y) = 1 + (y + 1) + (y + 1)^2 + (y + 1)^3 + (y + 1)^4.$$

Då är $f(x) = g(x - 1)$. Dessutom är $f$ irreducibelt om och endast om $g$ är det, ty om vi har en faktorisering

$$f(x) = f_1(x) f_2(x)$$

är också

$$g(x) = f(x + 1) = f_1(x + 1) f_2(x + 1).$$

Men multiplicerar vi ut definitionen av $g$, fås att

$$g(y) = 5 + 10y + 10y^2 + 5y^3 + y^4.$$

Eftersom $g$ uppfyller Eisensteins kriterium för primtalet 5, så är det irreducibelt över $\mathbb{Q}$.

**Övning 5.1.** Vi noterar att $\text{conv}(z_1, z_2, \ldots, z_n)$ är en $m$-hörning för något $m \leqslant n$. Vi antar att $z_1$ är ett av hörnen, annars byter vi namn på några av punkterna så att det blir så.

Betrakta linjen som går genom $z_1$ och $z$. Om vi bara betrakta den delen av linjen som ligger på samma sida av $z_1$ som $z$, så går den antingen genom ett annat hörn av månghörningen eller genom en kant. Om den går genom ett annat hörn $z_k$, så ligger alltså $z$ på linjesegmentet mellan $z_1$ och $z_k$ och kan därmed skrivas som konvexkombination av $z_1$ och $z_k$. Om linjen skär kanten mellan hörnen $z_k$ och $z_l$, så ligger $z$ i det innersta av triangeln med hörnen $z_1, z_k$ och $z_l$ och kan enligt Exempel 5.1.2 skrivas som linjärkombination av $z_1, z_k$ och $z_l$.

**Övning 5.3.**

1. $b_i$ är en konvexkombination av $a_i$ och $a_i'$ och ligger därmed i $\text{conv}(a_i, a_i')$ vilket är lika med intervallet $[a_i, a_i']$ om $a_i \leqslant a_i'$ eller $[a_i', a_i]$ om $a_i > a_i'$. Eftersom $0 \leqslant a_i \leqslant 1$ och $0 \leqslant a_i' \leqslant 1$ får vi att $b_i \in \text{conv}(a_i, a_i') \subseteq [0, 1]$. Alltså gäller $b_i \in [0, 1]$.

2. Vi beräknar

$$\begin{aligned} b_1 + \ldots + b_n &= \left(\lambda a_1 + (1-\lambda)a_1'\right) + \ldots + \left(\lambda a_n + (1-\lambda)a_n'\right) \\ &= \lambda\left(a_1 + \ldots + a_n\right) + (1-\lambda)\left(a_1' + \ldots + a_n'\right) \\ &= \lambda \cdot 1 + (1-\lambda)\cdot 1 = 1 \end{aligned}$$

**Övning 5.5.** Enligt Sats 3.3.1 kan vi skriva $p(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$. Vi deriverar och får $p'(x) = 2x - (\alpha+\beta)$. Alltså har $p'$ som enda rot $x = \frac{\alpha+\beta}{2}$, eller skriven som konvexkombination

$$x = \frac{1}{2}\alpha + \frac{1}{2}\beta,$$

och enligt Sats 5.1.8 ligger roten till $p'$ i det konvexa höljet av $\alpha$ och $\beta$. Detta visar Gauss-Lucas sats för polynom av grad 2.

**Övning 6.1.** Vi använder samma metod som i Exempel 6.3.9. Skriv

$$p(x_1, x_2, x_3) = x_1x_2^3 + x_1x_3^3 + x_2x_1^3 + x_2x_3^3 + x_3x_1^3 + x_3x_2^3.$$

Vi reducerar till två variabler först:

$$p(x_1, x_2, 0) = x_1x_2^3 + x_1^3x_2 = x_1x_2((x_1+x_2)^2 - 2x_1x_2) = e_2^{(2)}\left((e_1^{(2)})^2 - 2e_2^{(2)}\right).$$

Sen återgår vi till tre variabler, ersätter alla $e_i^{(2)}$ med $e_i^{(3)}$ och bildar differensen:

$$p(x_1, x_2, x_3) - e_2^{(3)}\left((e_1^{(3)})^2 - 2e_2^{(3)}\right) = -x_1x_2x_3(x_1+x_2+x_3) = -e_3^{(3)}e_1^{(3)}.$$

Det ger oss resultatet

$$x_1x_2^3 + x_1x_3^3 + x_2x_1^3 + x_2x_3^3 + x_3x_1^3 + x_3x_2^3 = e_2\left(e_1^2 - 2e_2\right) - e_3e_1.$$

**Övning 6.3.** Newtons identitet från Sats 6.5.2 för $k = 4$ ger att

$$0 = p_4 - e_1p_3 + e_2p_2 - e_3p_1 + 4e_4.$$

och från Exempel 6.5.5 vet vi att $e_2 = \frac{1}{2}\left(p_1^2 - p_2\right)$ och $e_3 = \frac{1}{6}\left(2p_3 - 3p_1p_2 + p_1^3\right)$ samt att $e_1 = p_1$. Det ger att

$$\begin{aligned} e_4 &= \frac{1}{4}\left(-p_4 + e_1p_3 - \frac{1}{2}\left(p_1^2 - p_2\right)p_2 + \frac{1}{6}\left(2p_3 - 3p_1p_2 + p_1^3\right)p_1\right) \\ &= \frac{1}{24}\left(-6p_4 + 8p_1p_3 - 6p_1^2p_2 + 3p_2^2 + p_1^4\right). \end{aligned}$$

**Övning 6.5.** 1. $b_2 = -e_1(r_1^2, r_2^2, r_3^2), b_1 = e_2(r_1^2, r_2^2, r_3^2), b_0 = -e_3(r_1^2, r_2^2, r_3^2)$

2.

$$\begin{aligned} e_3(r_1^2, r_2^2, r_3^2) &= r_1^2r_2^2r_3^2 = (r_1r_2r_3)^2 = e_3(r_1, r_2, r_3)^2 \\ e_2(r_1^2, r_2^2, r_3^2) &= r_1^2r_2^2 + r_1^2r_3^2 + r_2^2r_3^2 \\ &= (r_1r_2 + r_1r_3 + r_2r_3)^2 - 2r_1r_2r_3(r_1 + r_2 + r_3) \\ &= e_2(r_1, r_2, r_3)^2 - 2e_3(r_1, r_2, r_3)e_1(r_1, r_2, r_3) \\ e_1(r_1^2, r_2^2, r_3^2) &= r_1^2 + r_2^2 + r_3^2 = p_2(r_1, r_2, r_3) \\ &= e_1(r_1, r_2, r_3)^2 - 2e_2(r_1, r_2, r_3) \end{aligned}$$

3. $e_1(r_1, r_2, r_3) = -a_2$, $e_2(r_1, r_2, r_3) = a_1$, $e_3(r_1, r_2, r_3) = -a_0$

4.

$$\begin{aligned} b_2 &= -e_1(r_1^2, r_2^2, r_3^2) = -\left(e_1(r_1, r_2, r_3)^2 - 2e_2(r_1, r_2, r_3)\right) = -a_2^2 + 2a_1 \\ b_1 &= e_2(r_1^2, r_2^2, r_3^2) = e_2(r_1, r_2, r_3)^2 - 2e_3(r_1, r_2, r_3)e_1(r_1, r_2, r_3) = a_1^2 - 2a_0a_2 \\ b_0 &= -e_3(r_1^2, r_2^2, r_3^2) = -e_3(r_1, r_2, r_3)^2 = -a_0^2 \end{aligned}$$

5. Om $a_2 = -2, a_1 = -5$ och $a_0 = 6$, så blir $b_2 = -(-2)^2 + 2 \cdot (-5) = -14$, $b_1 = (-5)^2 - 2 \cdot 6 \cdot (-2) = 49$ och $b_0 = -6^2 = -36$.

**Övning 7.1.** Vi påverkar inte huruvida $f$ har ett lokalt minimum eller maximum genom att subtrahera en konstant från $f$, så vi kan anta att $a_0 = 0$. Vi ser att

$$\operatorname{codeg}(a_kx^k) < \operatorname{codeg}(a_{k+1}x^k + \cdots + a_nx^n),$$

så enligt Hjälpsats 7.3.4 existerar ett tal $r$ sådant att

$$|a_kx^k| > |a_{k+1}x^k + \cdots + a_nx^n|$$

om $0 < |x| < r$. Det följer att tecknet till $f(x)$, alltså huruvida $f(x)$ är större eller mindre än noll, är detsamma som tecknet till $a_k x^k$ om $0 < |x| < r$.

Antag att $k$ är udda och $a_k > 0$. I så fall är $a_k x^k > 0$ när $x > 0$ och $a_k x^k < 0$ när $x < 0$. Alltså är $f(x) > 0$ för $0 < x < r$, och $f(x) < 0$ för $0 > x > -r$. Samma argument fungerar när $a_k < 0$. Alltså har $f$ varken lokalt minimum eller maximum när $k$ är udda.

Om $k$ är jämnt och $a_k > 0$, är $a_k x^k > 0$ för alla $x \neq 0$. Alltså är $f(x) > 0$ för $0 < |x| < r$, vilket innebär att $f$ har ett lokalt minimum i origo eftersom $f(0) = 0$. Samma argument, men omvänt, fungerar när $a_k < 0$.

**Övning 7.3.** Låt $\alpha \in \mathbb{C}$. Polynomet $f$ antar värdet $\alpha$ om och endast om ekvationen

$$f(x) - \alpha = 0$$

har någon lösning $x$. Men detta är en polynomekvation i $x$ med komplexa koefficienter, så enligt algebrans fundamentalsats finns minst en lösning.

**Övning 7.5.** Att algebrans fundamentalsats innebär att de enda irreducibla polynomen är förstagradare eller konstanta visades redan i Sats 3.4.1. Vi visar omvändningen.

Vi använder induktion för att visa att alla icke-konstanta polynom har en rot. Som basfall använder vi polynomen med grad 1. Alla dessa kan skrivas som $(x - r)$, så de har roten $r$. Antag att varje polynom av grad $n$ har en rot, och låt $f$ vara ett polynom av grad $n + 1$. Enligt antagande är inte $f$ irreducibelt, så vi kan skriva

$$f = gh$$

där både $g$ och $h$ har strikt lägre grad, och därför grad minst 1. Enligt induktionsantagandet har då både $g$ och $h$ minst en rot, och därför har även $f$ det.

**Övning 7.7.** Enligt faktorsatsen är $f(z)$ delbart med $z$, så $f(z)/z$ är ett polynom. Alltså antar enligt förra uppgiften funktionen

$$\left| \frac{f(z)}{z} \right|$$

sitt största värde på skivan $D$ i någon punkt $z_0$ med $|z_0| = 1$, enligt förra uppgiften. Men dessutom är $f(z_0) \in D$, så $|f(z_0)| \leqslant 1$. Alltså gäller olikheten

$$\left| \frac{f(z)}{z} \right| \leqslant \frac{|f(z_0)|}{|z_0|} = |f(z_0)| \leqslant 1$$

för alla $z \in D$, det vill säga,

$$|f(z)| \leqslant |z|$$

vilket skulle bevisas.

# A Kontinuitet och kompakthet

I detta appendix ska vi definiera och precisera vissa begrepp som använts utan precisa definitioner i Kapitel 7 av detta kompendium. Framför allt kommer vi att definiera vad det betyder att en funktion är *kontinuerlig*, vilket är ett fundamentalt begrepp i den högre matematiken. Framställningen i detta appendix är något mer kortfattad än framställningen i resten av kompendiet. I avsnittet med förslag till vidare läsning ges tips

## A.1 Talföljder och delföljder

**Definition A.1.1.** En *talföljd* är en funktion $x\colon \mathbb{N} \to \mathbb{C}$. Om $x$ är en talföljd så brukar man skriva $x_n$ i stället för $x(n)$.

Ofta skriver vi en talföljd som en oändlig sekvens av tal, vilket är hur man bör tänka på en talföljd. Till exempel har vi följden

$$\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots.$$

**Definition A.1.2.** Låt $x_n$ vara en talföljd. Vi säger att $x_n$ *konvergerar mot* $x \in \mathbb{C}$, om det för varje $r > 0$ finns ett tal $N$ sådant att $|x_n - x| \leqslant r$ om $n \geqslant N$.

Med andra ord kan elementen i talföljden fås att ligga godtyckligt nära talet $x$, så länge vi tittar tillräckligt långt fram i talföljden. Vi använder följande notation för att visa att talföljden $x_n$ konvergerar mot $x$:

$$\lim_{n\to\infty} x_n = x$$

Notera att inte alla talföljder konvergerar mot något tal över huvud taget.

**Definition A.1.3.** En talföljd är *konvergent* om det existerar ett tal den konvergerar mot.

**Exempel A.1.4.** Talföljden $x_n = 1/n$ konvergerar mot 0: för varje $r > 0$ finns ett tal $N$ sådant att $|x_n - 0| = 1/n \leqslant r$ om $n \geqslant N$. ▲

**Övning A.1.** Om en talföljd konvergerar mot $x$ och konvergerar mot $y$, måste $x = y$.

**Definition A.1.5.** En talföljd $x_n$ kallas för en *Cauchyföljd* om det för varje $r \geqslant 0$ finns ett tal $N$ sådant att

$$|x_n - x_m| < r$$

för alla möjliga par av $n, m \geqslant N$.

**Exempel A.1.6.** Varje konvergent talföljd är en Cauchyföljd. Ty antag att $x_n$ konvergerar mot $x$. Tag något $r > 0$. Enligt definitionen av konvergens finns ett tal $N$ sådant att

$$|x_n - x| \leqslant \frac{r}{2}$$

om $n \geqslant N$. Om nu både $n$ och $m$ är tal större än $N$, så gäller att

$$|x_n - x_m| = |x_n - x + x - x_m| \leqslant |x_n - x| + |x - x_m| \leqslant \frac{r}{2} + \frac{r}{2}$$

där vi använt triangelolikheten (Övning 1.5). Alltså är följden en Cauchyföljd. ▲

**Sats A.1.7** (Fullständighet av de komplexa talen)**.** *Varje Cauchyföljd är konvergent.*

Vi kommer inte att ge ett bevis av denna sats eftersom detta skulle kräva en rigorös definition av vad ett reellt tal är, vilket vi inte har givit. Man kan i stället acceptera satsen som ett axiom.

**Anmärkning A.1.8.** Satsen uttrycker att de komplexa talen är *fullständiga*, vilket man kan tänka på som att det inte finns tal som "saknas"; det finns inga glapp bland de komplexa talen. Ett exempel på något som inte är fullständigt är mängden av alla rationella tal $\mathbb{Q}$. Tag till exempel talföljden

$$3, 3.1, 3.14, 3.141, 3.1415, \ldots$$

som lägger till fler och fler decimaler av $\pi$. Detta är en talföljd i $\mathbb{Q}$. Den är en Cauchyföljd och konvergerar alltså i de *komplexa talen* mot $\pi$. Men det finns inget tal den konvergerar mot bland de *rationella talen*.

**Definition A.1.9.** Låt $x\colon \mathbb{N} \to \mathbb{C}$ vara en talföljd. Vi säger att $y\colon \mathbb{N} \to \mathbb{C}$ är en *delföljd* till $x_n$ om det finns en växande funktion $\sigma : \mathbb{N} \to \mathbb{N}$, alltså en funktion för vilken $\sigma(1) < \sigma(2) < \sigma(3) < \ldots$, sådan att $y = x \circ \sigma$.

I klarspråk betyder föregående definition att talföljden $y_n$ fås genom att stryka termer ur följden $x_n$. Vi tänker på $\sigma(1)$ som den första av termerna ur $x_n$ som är kvar, $\sigma(2)$ är den andra termen, och så vidare.

**Exempel A.1.10.** Betrakta återigen talföljden $x_n = 1/n$. Ett exempel på en delföljd till denna är följden

$$\frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11} \qquad \text{(alla primtal)}.$$

En annan delföljd är

$$\frac{1}{1}, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \frac{1}{25} \qquad \text{(alla jämna kvadrater)}.$$

▲

**Övning A.2.** Antag att $x_n$ konvergerar mot $x$. Då konvergerar också varje delföljd till $x_n$ mot $x$.

**Exempel A.1.11.** Om en talföljd inte är konvergent, kan man ibland ändå hitta en delföljd som konvergerar. Tag till exempel talföljden

$$1, -1, 1, -1, 1, \ldots.$$

Denna följd är uppenbarligen inte konvergent. Dock kan vi ta delföljden som består av alla ettor, och få en delföljd som konvergerar (nämligen mot 1). Det finns också flera möjliga delföljder som konvergerar mot $-1$. ▲

**Exempel A.1.12.** Ett exempel på en talföljd som saknar konvergenta delföljder är

$$1, 2, 3, 4, \ldots.$$

Varje delföljd kommer att ha egenskapen att elementen i följden blir obegränsat stora, och delföljden kan därför inte konvergera mot ett ändligt värde. ▲

**Övning A.3.** Låt $x_n$ vara en talföljd med egenskapen att för varje tal $K$ finns det minst ett element som uppfyller $|x_n| \geqslant K$. Visa att $x_n$ inte är konvergent.

Föregående exempel är i någon mening den enda möjliga sortens exempel på en talföljd som saknar konvergenta delföljder. Det enda problemet som kan förhindra existensen av konvergenta delföljder är att följden består av termer som växer obegränsat stora.

**Sats A.1.13** (Bolzano-Weierstrass sats)**.** *Låt $x_n$ vara en talföljd. Antag att det existerar ett tal $K$ sådant att $|x_n| \leqslant K$ för alla $n$. Då har $x_n$ en delföljd som konvergerar mot något tal $x \in \mathbb{C}$.*

*Bevis.* Antagandet säger att talföljden ligger i disken

$$D_K = \{z \in \mathbb{C} \mid |z| \leqslant K\}.$$

Täck över $D_K$ med ändligt många diskar vars diameter är 1. Eftersom talföljden har oändligt många termer, måste det finnas en delföljd $x_n^1$ som endast består av element från *en* av diskarna. Välj en sådan cirkelskiva och delföljd. Täck nu på samma sätt över denna skiva med diskar av diameter $1/2$, och tag en delföljd $x_n^2$ som endast befinner sig någon av dessa diskar. Täck nu i sin tur över denna disk med skivor vars diameter är $1/3$, tag en delföljd $x_n^3$, och så vidare.

Det vi nu gör är att vi konstruerar den *diagonala* delföljden. Denna har som sitt första element det första elementet ur den första följden; som sitt andra element det andra elementet ur den andra delföljden, och så vidare. Med andra ord betraktar vi följden $x_n^n$. Vi hävdar att denna följd är en Cauchyföljd. Tag $r > 0$, och välj ett heltal $N > 0$ sådant att $1/N \leqslant r$. Om nu $n$ och $m$ är större än $N$, så kommer

$$|x_n^n - x_m^m| \leqslant \frac{1}{N} \leqslant r.$$

Detta eftersom både $x_n^n$ och $x_m^m$ ligger inuti en cirkelskiva av diameter $1/N$ enligt vår konstruktion.

Eftersom $x_n^n$ är en delföljd av $x_n$, och den är konvergent enligt Sats A.1.7, är vi klara. □

## A.2 Kompakthet

**Definition A.2.1.** En delmängd $S \subseteq \mathbb{C}$ sägs vara *sluten* om det för varje konvergent talföljd $x_n$ av element i $S$ även gäller att

$$\lim_{n\to\infty} x_n$$

är ett element av $S$.

**Hjälpsats A.2.2.** *Cirkelskivan $D_K$ är sluten för alla $K \geqslant 0$.*

*Bevis.* Antag att $x \notin D_K$. Vi skall visa att det inte finns en talföljd av element i $D_K$ som konvergerar mot $x$. Låt $x_n$ vara en talföljd i $D_K$. Vi vet att $|x| > K$. Låt

$$r = |x| - K > 0.$$

Då kan det inte existera något $x_n$ med egenskapen att

$$|x - x_n| < r,$$

eftersom

$$|x - x_n| \geqslant |x| - |x_n| \geqslant |x| - K = r$$

enligt omvända triangelolikheten. Alltså är $D_K$ sluten. □

**Exempel A.2.3.** Mängden $S = \{z \in \mathbb{C} \mid |z| < 1\}$ är inte sluten. Vi kan till exempel ta följden

$$0, \frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \frac{15}{16}, \dots$$

som konvergerar mot $1 \notin S$, trots att alla element i följden ligger i $S$. ▲

**Definition A.2.4.** En delmängd $S \subseteq \mathbb{C}$ sägs vara *begränsad* om $S \subseteq D_K$ för något $K$.

**Definition A.2.5.** En delmängd $S \subseteq \mathbb{C}$ sägs vara *kompakt* om det för varje talföljd $x_n$ av element i $S$ existerar en delföljd $y_n$ som konvergerar mot ett element av $S$.

**Sats A.2.6.** *En delmängd $S \subseteq \mathbb{C}$ som är sluten och begränsad är kompakt.*

*Bevis.* Eftersom $S$ är begränsad, har varje följd av element i $S$ en konvergent delföljd enligt Sats A.1.13. Eftersom $S$ är sluten vet vi dessutom att det element delföljden konvergerar mot faktiskt ligger i $S$. □

**Följdsats A.2.7.** *Varje cirkelskiva $D_K$ är kompakt.*

## A.3 Kontinuitet, maxima och minima

Vi är nu redo att definiera vad det betyder att en funktion är kontinuerlig.

**Definition A.3.1.** Låt $S$ vara någon delmängd av $\mathbb{C}$. En funktion $f\colon S \to \mathbb{C}$ kallas *kontinuerlig* om det för varje talföljd $x_n$ i $S$ som konvergerar mot något $x \in S$, gäller att

$$\lim_{n\to\infty} f(x_n) = f(x).$$

Om $f$ inte är kontinuerlig kallas den *diskontinuerlig*.

**Exempel A.3.2.** Funktionen $f : \mathbb{R} \to \mathbb{R}$ som ges av

$$f(x) = \begin{cases} 0 & \text{om } x \leqslant 0 \\ 1 & \text{annars} \end{cases}$$

är inte kontinuerlig. Om vi tar följden $x_n = 1/n$ från tidigare, så har vi att

$$\lim_{n\to\infty} x_n = 0.$$

Men $f(x_n) = 1$ för alla $n$, och $f(0) = 0$. Så

$$\lim_{n\to\infty} f(x_n) = 1 \neq 0 = f(0).$$

Alltså har det "skutt" som funktionen gör i punkten $x = 0$ hindrat den från att vara kontinuerlig. ▲

**Exempel A.3.3.** Alla "vanliga" funktioner, såsom polynom och trigonometriska funktioner, är kontinuerliga. Att visa detta i detalj skulle dock ta ganska lång tid. ▲

Vi har redan i Kapitel 7 definierat vad ett minimum och ett maximum av en funktion $f\colon S \to \mathbb{R}$ är för något, där $S$ är en godtycklig mängd.

**Sats A.3.4.** *Låt $S$ vara en kompakt delmängd av $\mathbb{C}$, och $f\colon S \to \mathbb{C}$ en kontinuerlig funktion. Då är även*

$$f(S) = \{f(x) \mid x \in S\}$$

*en kompakt mängd.*

*Bevis.* Eftersom varje element i $f(S)$ kan skrivas som $f(x)$, kan varje talföljd i $f(S)$ skrivas som

$$f(x_n),$$

där $x_n$ är en talföljd i $S$. Eftersom $S$ är kompakt har $x_n$ en delföljd $y_n$ som konvergerar mot något $y \in S$. Nu vet vi enligt definitionen av kontinuitet att

$$\lim_{n\to\infty} f(y_n) = f(y) \in f(S).$$

Eftersom $f(y_n)$ är en delföljd till $f(x_n)$ som konvergerar mot ett element i $f(S)$, är $f(S)$ kompakt. □

**Hjälpsats A.3.5.** *Varje nedåt begränsad delmängd $X$ av $\mathbb{Z}$ har ett minsta element.*

*Bevis.* Låt $n$ vara ett element av $X$, och låt $N$ vara ett tal sådant att

$$m \geqslant N$$

för alla $m \in X$. Att $N$ existerar säger exakt att $X$ är nedåt begränsad. Nu är

$$S \cap \{m \in \mathbb{Z} \mid N \leqslant m \leqslant n\}$$

en ändlig mängd, eftersom det bara finns ändligt många heltal i intervallet. Dessutom är den icke-tom, eftersom $n$ ingår. Alltså har den ett minsta element. Eftersom inga element av $X$ kan vara mindre än $N$, är detta element ett minsta element av $X$. □

**Definition A.3.6.** Låt $S$ vara en delmängd av $\mathbb{R}$. Vi säger att $\alpha \in \mathbb{R}$ är ett *infimum* till $S$ om

- för alla $x \in S$ gäller $x \geqslant \alpha$,
- det existerar en talföljd $x_n$ i $S$ som konvergerar mot $\alpha$.

Om samma villkor gäller men med omvänd olikhet, säger vi att $\alpha$ är ett *supremum* till $S$.

**Sats A.3.7.** *Varje begränsad delmängd $S \subset \mathbb{R}$ har ett infimum och ett supremum.*

*Bevis.* Vi visar existensen av ett infimum; beviset av existensen av supremum är i princip likadant. Tag något $x_1 \in S$. Om $x_1$ är det minsta elementet av $S$ är det också ett infimum. Antag därför att det finns minst ett mindre element av $S$. Det existerar då något heltal $k$ sådant att det finns ett element i $S$ mindre än

$$x_1 - 2^{-k},$$

eftersom $2^{-k}$ blir godtyckligt litet när $k$ väljs godtyckligt stort. Mängden av alla sådana heltal är nedåt begränsad, eftersom $2^{-k}$ blir obegränsat stort när $k$ väljs obegränsat litet, och $S$ var begränsad. Alltså finns ett minsta sådant tal $k_1$. Låt $x_2$ vara ett element av $S$ sådant att

$$x_2 \leqslant x_1 - 2^{-k_1}.$$

Eftersom $k_1$ valdes så litet som möjligt, vet vi att

$$x_1 - 2^{-k_1+1} < x_2 \leqslant x_1 - 2^{-k_1}.$$

Om $x_2$ är det minsta elementet av $S$ är vi klara. Annars kan vi låta $k_2$ vara det minsta heltalet sådant att det existerar element i $S$ mindre än eller lika

med $x_2 - 2^{-k_2}$. På detta sätt kan vi konstruera en talföljd $x_n$ med egenskapen att

$$x_i - 2^{-k_n+1} < x_{n+1} \leqslant x_n - 2^{-k_n}.$$

Det följer ur konstruktionen att olikheten

$$x_i - 2^{-k_n+1} < x_m \leqslant x_n - 2^{-k_n}.$$

gäller för *alla* $m > n$. Vi har nämligen att $x_m \leqslant x_n - 2^{-k_n}$ eftersom $x_m \leqslant x_{n+1} \leqslant x_n - 2^{-k_n}$. Vi har att $x_n - 2^{-k_n+1} < x_m$ eftersom vi har valt vårt $k_n$ sådant att alla element i $S$ är större än $x_n - 2^{-k_n+1}$.

Vi hävdar att $k_1 < k_2 < k_3 < \ldots$. Ty antag motsatsen, att $k_n = k_{n+1}$. I så fall är

$$x_{n+2} \leqslant x_{n+1} - 2^{-k_{n+1}} \leqslant x_n - 2^{-k_n} - 2^{-k_{n+1}} = x_n - 2^{-k_n+1},$$

vilket säger emot att $k_n$ valdes så litet som möjligt eftersom $x_{n+2} \in S$. Vi använde ovan att

$$2^k + 2^k = 2^{k+1}$$

för alla $k$.

Det följer att talföljden $x_n$ är en Cauchyföljd. Tag något $r > 0$. Eftersom $k_n$ är en strikt växande följd av heltal är den obegränsad, så vi kan hitta ett tal $N$ sådant att

$$2^{-k_N} < r.$$

Eftersom alla $x_n$ för $n > N$ ligger i intervallet

$$x_N - 2^{-k_N+1} < x_n \leqslant x_N - 2^{-k_N},$$

som har längd $2^{-k_N}$, kommer vi ha att $|x_n - x_n| < r$ om $n, m \geqslant N$. Talföljden konvergerar mot ett element $x$. Vi hävdar att $x$ är ett infimum till $S$.

Uppenbarligen finns det en talföljd i $S$ som konvergerar mot $x$. Det räcker alltså att visa olikheten

$$x \leqslant x_n$$

för alla $n$. Antag motsatsen, att $x > x_N$ för något $N$. Tag $r = x - x_N > 0$. Eftersom följden $x_n$ är avtagande, måste alla $x_n$ för $n > N$ uppfylla

$$x > x_N > x_n,$$

så $|x - x_n| = |x - x_N| + |x_N - x_n| = r + |x_N - x_n| < r$ vilket säger emot att $x_n$ konvergerar mot $x$. Beviset är klart. □

**Sats A.3.8.** *Låt $S$ vara en kompakt delmängd av $\mathbb{R}$. Då innehåller $S$ ett största och ett minsta element.*

*Bevis.* Vi visar först att $S$ är begränsad. Antag motsatsen. Då kan vi för varje heltal $n$ hitta ett element $x_n \in S$ sådant att $|x_n| \geqslant n$. Denna talföljd kan inte ha en konvergent delföljd, vilket är en motsägelse. Så $S$ är begränsad, och har ett infimum enligt Sats A.3.7. Tag en talföljd i $S$ som konvergerar mot $x$. Varje delföljd konvergerar också till $x$. Av kompakthet måste någon delföljd konvergera mot ett element i $S$, så $x \in S$. Alltså är $x$ ett minsta element till $S$. På samma sätt hittas ett största element. □

**Sats A.3.9.** *Låt $S$ vara en kompakt delmängd av $\mathbb{C}$. Varje kontinuerlig funktion $f\colon S \to \mathbb{R}$ har ett globalt minimum och ett globalt maximum.*

*Bevis.* Enligt Sats A.3.4 är $f(S)$ kompakt. Enligt Sats A.3.8 innehåller $f(S)$ ett största och ett minsta element. Låt $y$ vara det minsta elementet. Eftersom $y \in f(S)$ vet vi att $y = f(x)$. Då är $x$ ett globalt minimum till $f$. På samma sätt hittar vi ett globalt maximum. □

Vi har därmed visat påståendet från Kapitel 7 att varje kontinuerlig funktion $f : D_K \to \mathbb{R}$ antar ett största och minsta värde.

Eftersom *polynom* är ett så brett ämne, finns det många olika böcker som kan läsas efter detta kompendium, beroende på vilken aspekt man är mest intresserad av.

## Förslag till vidare läsning


[1] E.J. Barbeau *Polynomials.* Springer Problem Books in Mathematics, 1989.

En hel lärobok om polynom. Antagligen kan nästan allt i detta kompendium hittas någonstans i denna bok. Framställningen är lite speciell — boken innehåller inga bevis, utan i stället presenteras all teori genom mer eller mindre kluriga problem. Problemen är dels bevis för viktiga satser som delats in i mindre delar, eller fristående problem som bara valts för att de är eleganta.

[2] David Sharpe: *Rings and factorization* Cambridge University Press, 1987.

Läsaren som tyckte att Kapitel 3 i detta kompendium var intressant kan med fördel läsa denna korta lilla bok. Boken ger en abstrakt behandling av *ringar* och *kroppar*. Exempel på kroppar är $\mathbb{C}$, $\mathbb{R}$ och $\mathbb{Q}$. Ett exempel på en ring är mängden av alla polynom med koefficienter i någon kropp. Denna bok sätter in resultaten från Kapitel 3 i ett större sammanhang.

[3] Ian Stewart *Galois Theory, 2nd ed.* Chapman and Hall, 1989

Galoisteori kan sammanfattas som det allmänna studiet av sambandet mellan *symmetri* och *lösbarhet av polynomekvationer i olika kroppar*. Denna lärobok kan med fördel läsas efter Sharpes bok, men även fristående. Boken visar bland annat det mest kända resultatet inom Galoisteori, Abel-Ruffinis sats: Det finns ingen formel med vars hjälp man kan hitta rötterna till ett godtyckligt polynom av grad minst 5 endast uttryckt i räkneoperationerna plus, gånger, minus, division, och rotutdragning. Jämför detta med *pq*-formeln, som är en sådan formel för andragradspolynom. Boken är också en guldgruva för historisk information om Galoisteori.

[4] Carl Friedrich Gauss *Disquisitiones Arithmeticae, English ed.* Yale University Press, 1966.

Lärobok i talteori, skriven av den store matematikern Gauss år 1798 när han var 24 år gammal. Boken sammanfattar och ger eleganta bevis av nära nog all talteori som var känd innan dess, och mer än halva boken är egna resultat. Boken börjar systematiskt från grunden och kan fortfarande läsas med behållning trots den ibland omoderna framställningen. Gauss lemma formulerades första gången i denna bok (§42).

[5] Walter Rudin *Principles of Mathematical Analysis, 3rd ed.* McGraw-Hill, 1976.

Denna bok är en riktig matematisk klassiker (första utgåvan kom ut 1953). På ett mycket elegant och koncist sätt definierar den vad de reella och komplexa talen är, olika typer av konvergens, kontinuitet, deriverbarhet, integration, och så vidare. Läsaren som fick mersmak av kompendiets appendix kommer att hitta mer i samma stil i denna bok.

[6] Benjamin Fine, Gerhard Rosenberger *The Fundamental Theorem of Algebra* Springer Undergraduate Texts in Mathematics, 1997.

Denna lärobok handlar som titeln antyder enbart om algebrans fundamentalsats. Bokens mål är att ge så många olika bevis av detta resultat som möjligt. På vägen introduceras flera tyngre matematiska ämnen, såsom komplex analys, Galoisteori och algebraisk topologi. Kan läsas efter Persson-Böiers.

[7] Arne Persson & Lars-Christer Böiers: *Analys i en variabel,* Studentlitteratur, 2001

Standardbok i analys för nybörjare på högskolan.

Böckerna ovan, och många andra böcker, finns att låna på Matematikbiblioteket, Lindstedtsvägen 25 (bottenvåningen). Biblioteket är öppet för alla.