SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Kvadratiska talkroppar och entydig faktorisering

av

Ulrika Nyström Aanstad

2021 - No K25

Kvadratiska talkroppar och entydig faktorisering

Ulrika Nyström Aanstad

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Håkan Granath

2021

Sammanfattning

I detta arbete studeras algebraiska tal, algebraiska heltal och entydig faktorisering i kvadratiska talkroppar. Vi inleder med de ”vanliga” heltalen där vi genom Aritmetikens fundamentalsats visar att faktorisering i primtalsfaktorer är entydig. Vidare undersöker vi om satsen går att tillämpa på andra talstrukturer, som algebraiska talkroppar, där vi begränsar oss till att undersöka de kvadratiska talkropparna. Huvudresultatet i detta arbete är att entydig faktorisering i kvadratiska talkroppar snarare är undantag än regel och vi kommer visa att då den kvadratiska heltalsringen är euklidisk får vi entydig faktorisering. Avslutningsvis tillämpar vi det vi lärt oss om entydig faktorisering i kvadratiska talkroppar och löser den diofantiska ekvationen $y^2 + 49 = z^3$.

Förord

Detta arbete utgör ett examensarbete om 15 hp i matematik på kandidatnivå vid Matematiska Institutionen vid Stockholms Universitet under handledning av Håkan Granath. Jag vill rikta ett stort och hjärtligt tack till Håkan för all hjälp och stöd under arbetets gång.

Innehåll

1 Introduktion

I årtusenden har människan fascinerats av tal och människan har nog alltid räknat på fingrarna $1, 2, 3, ...$ o.s.v. för att beräkna *antal*, så de positiva heltalen $\mathbb{Z}^+$ var dem som introducerades först. Efter många hundra år införde man talet 0 och på så sätt fick man de naturliga talen $\mathbb{N} = \{0, 1, 2, 3, ...\}$ [7, s. 67]. Pythagoréerna, som var ett filosofiskt brödraskap och bildades av Pythagoras (år 500 f.Kr.), studerade många egenskaper hos de naturliga talen. En av de mest kända satserna inom matematiken är Pythagoras sats $x^2 + y^2 = z^2$, där x och y utgör sidorna i en rätvinklig triangel och z hypotenusan [9]. Fastän att satsen bygger på geometri så fångade den talteoretikernas intresse. Babylonierna visade på Pythagoreiska tripplar, d.v.s. tripplar av naturliga tal som uppfyller Pythagoras sats. Exempel på detta är $(3, 4, 5)$ och $(5, 12, 13)$ som alla är naturliga tal (x, y, z) där $x^2 + y^2 = z^2$ [1, s. 1]. Även i det antika Grekland ägnade man sig åt att lösa ekvationer som endast hade heltalslösningar, s.k. *diofantiska ekvationer* efter den grekiska talteoretikern Diofantos som levde ca 250 f.Kr. [7, s. 77]. Genom århundraden utvecklades algebran och talområdet utvidgades med de negativa heltalen $\mathbb{Z}^-$, de rationella talen $\mathbb{Q}$ och så småningom de reella talen $\mathbb{R}$ samt de komplexa talen $\mathbb{C}$ [7, s. 67]. I denna uppsats kommer vi att studera de *algebraiska talen* som är en ytterligare utvidgning av talområdet. Ett algebraiskt tal är ett komplext tal som är ett nollställe till ett nollskilt polynom $a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ där samtliga koefficienter a_i är heltal. Om vi sen tillför kravet att högstagradskoefficienten ska vara 1 får vi de *algebraiska heltalen* [1, s. 4]. Exempelvis är $\sqrt{2}$ ett algebraiskt heltal eftersom det är ett nollställe till polynomet $x^2 - 2$ där högstagradskoefficienten är 1 och koefficienten -2 är ett heltal. Däremot är inte talet π algebraiskt, eftersom det inte är ett nollställe till något nollskilt polynom med heltalskoefficienter [8].

En av de största talteoretikerna var Pierre de Fermat (1601-1665), som efter sin död efterlämnade många matematiska påståenden, som flertalet saknade nedskrivna bevis. De flesta av Fermats påståenden, kunde efter hans död, bevisas av andra matematiker [1, s. 2]. Men en av satserna, som senare fick namnet Fermats stora sats, kom att gäcka matematiker över hela världen i över 300 år. Fermat hävdade, i kontrast till de oändliga antal fall av de Pythagoreiska tripplarna [1, s. ix], att den diofantiska ekvationen $x^n + y^n = z^n$ saknade lösningar för $n \geq 3$ bland de positiva heltalen [1, s. 2]. Detta påstående, så enkelt att ange men ändå så komplex, inspirerade många matematiker till att försöka framlägga ett bevis. Otaliga försök av välkända matematiker som Gabriel Lamé, Ernst Kummer, Adrien-Marie Legendre m.fl. bidrog i sig till en betydande utveckling av den abstrakta matematiken [1]. Flera av bevisen visade sig felaktigt bygga på antagandet om att Aritmetikens fundamentalsats om entydig faktorisering för ”vanliga” heltal också kunde tillämpas på de algebraiska heltalen. Det var först i 1995 som Andrew Wiles presentera-

de ett bevis som efter mycket kritiskt granskande godkändes av det matematiska samfundet [1, s. xii]. I denna uppsats kommer vi ta upp denna förargade men avgörande fråga om huruvida faktorisering i andra talstrukturer är entydig eller ej. Vi kommer titta på en viss typ av talkroppar, de kvadratiska, där vi kommer visa att faktoriseringen inte alltid är entydig.

Vi inleder i kapitel 2 med de ”vanliga” heltalen och visar genom Euklides lemma och Aritmetikens fundamentalsats att alla heltal större än 1 har entydig faktorisering i primtal, bortsett från ordningen. I kapitel 3 går vi över till den abstrakta matematiken och inleder med lite allmän teori om algebraiska strukturer, som ringar och kroppar. Vi pratar om kroppsutvidgning och detta leder oss in på en definition av den kvadratiska talkroppen. I kapitel 4 definierar vi de algebraiska talen och några viktiga egenskaper som normen och spåret för att sen i kapitel 5 visa en mycket central sats som säger vilka de algebraiska heltalen är i kvadratiska talkroppar. Detta blir en viktig grund för vårt vidare arbete i kapitel 6 som handlar om entydig faktorisering där vi genom exempel visar att faktorisering i vissa kvadratiska talkroppar inte är entydig. Vi avslutar kapitlet med att titta på en alldeles egen klass av ringar, de så kallade norm-euklidiska ringarna, där vi visar att faktorisering i dessa ringar alltid är entydig. Lite kort nämner vi Gauss eftersom han var den första som bevisade att faktorisering i heltalsringen $\mathbb{Z}[i]$ är entydig. Avslutningsvis tillämpar vi det vi lärt oss om entydig faktorisering och med hjälp av de Gaussiska heltalen löser vi den diofantiska ekvationen $y^2 + 49 = z^3$.

2 Entydig faktorisering i heltalen

Entydig faktorisering innebär att ett heltal större än 1 endast kan faktoriseras på ett *unikt* sätt, om man bortser från ordningen på faktorerna. Historiskt sett tog man detta länge för givet utan närmare bevis. Det har även hänt att man presenterade matematiska bevis som då felaktigt byggde på antaganden om unik faktorisering [1, s. 75]. Vi kommer i detta kapitel att titta på heltalsringen $\mathbb{Z}$ där vi genom Aritmetikens fundamentalsats visar att faktoriseringen i primtal är entydig.

2.1 Primtal

Vi börjar först med att definiera vad ett primtal är för något.

Definition 2.1. [7, s. 68] Ett *primtal* är ett naturligt tal, som är större än 1 och som inte har några andra positiva delare än 1 eller talet självt.

Ett naturligt tal, större än 1, som inte är ett primtal kallas ett *sammansatt tal*. Ett sammansatt tal n kan skrivas som en produkt av två naturliga tal $a, b > 1$ där $n = ab$. Av detta följer att $1 < a < n$ och $1 < b < n$. [7, s. 68]

Exempel 2.2. Talet 15 är ett sammansatt heltal ty $15 = 3 \cdot 5$. Talet 3 är ett primtal eftersom det inte kan skrivas på ett icke-trivialt sätt som en produkt av två naturliga tal $3 = ab$. Med samma resonemang får vi att talet 5 också är ett primtal.

2.2 Euklides lemma

Innan vi går in på beviset av Aritmetikens fundamentalsats behöver vi känna till Bézouts identitet samt Euklides lemma. Bézouts identitet kommer vi använda i beviset av Euklides lemma så vi inleder med den.

Sats 2.3 (Bézouts identitet)**.** *[7, sats 5.15] Största gemensamma delaren $SGD(a, b)$ till två heltal a och b kan skrivas som en linjärkombination av a och b, d.v.s. det finns heltal x och y, sådana att $SGD(a, b) = ax + by$.*

Bevis. Beviset av Bézouts identitet bygger på att man utför Euklides algoritm och på så sätt finner $SGD(a, b)$. Sen gör man Euklides algoritm baklänges och på så sätt får man $SGD(a, b)$ som en linjärkombination av a och b sådan att $SGD(a, b) = ax + by$. Vi kommer senare i uppsatsen att göra ett motsvarande bevis när vi bevisar sats 6.24 så vi nöjer oss här med att illustrera bevisidén av Bézouts identitet med hjälp av ett exempel.

Vi väljer $a = 69$ och $b = 15$. För att finna $SGD(69, 15)$ tillämpar vi Euklides algoritm:

$$\begin{aligned} 69 &= 4 \cdot 15 + 9 \\ 15 &= 1 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 \end{aligned}$$

Då den sista nollskilda resten är 3 är alltså $SGD(69, 15) = 3$. Vi gör nu Euklides algoritm baklänges genom att börja från den nästsista raden och jobbar oss uppåt:

$$\begin{aligned} 3 &= 9 - 1 \cdot 6 \\ &= 9 - 1 \cdot (15 - 1 \cdot 9) = 2 \cdot 9 - 1 \cdot 15 \\ &= 2 \cdot (69 - 4 \cdot 15) - 1 \cdot 15 = 2 \cdot 69 - 9 \cdot 15. \end{aligned}$$

Därmed har vi skrivit $3 = SGD(69, 15)$ som en linjärkombination av 69 och 15 med $x = 2$ och $y = -9$. □

Lemma 2.4 (Euklides lemma)**.** *[7, lemma 5.16] Låt p vara ett primtal och $a, b \in \mathbb{Z}$. Om $p \mid ab$ då gäller det att $p \mid a$ eller $p \mid b$.*

Bevis. Om $p \mid a$ så är vi klara. Därför tittar vi på fallet då $p \nmid a$ och visar att $p \mid b$. Om $p \nmid a$ så är $SGD(p, a) = 1$ eftersom p endast har delarna ± 1 och $\pm p$. Enligt Bézouts identitet (sats 2.3) får vi

$$SGD(p, a) = px + ay = 1.$$

Vi multiplicerar båda sidor med b och får

$$\begin{aligned} pxb + ayb &= b \\ \Leftrightarrow (pb)x + (ab)y &= b. \end{aligned}$$

Eftersom vi antog att $p \mid ab$ kan vi skriva $ab = qp$ där $q \in \mathbb{Z}$. Vi sätter in i ekvationen och får

$$(pb)x + (pq)y = b.$$

Slutligen bryter vi ut p ur vänsterledet

$$p(bx + qy) = b$$

och vi ser att vänsterledet är delbart med p så därmed är också högerledet delbart med p och vi har visat att $p \mid b$. □

2.3 Aritmetikens fundamentalsats

Vi kommer nu gå in på Aritmetikens fundamentalsats som är en mycket viktig sats inom talteorin som ligger till grund för många andra satser och bevis inom matematiken.

Sats 2.5 (Aritmetikens fundamentalsats)**.** *[7, sats 5.4] Varje heltal $n > 1$ kan skrivas som en produkt av primtal på ett och endast ett sätt (bortsett från faktorernas ordning).*

Det satsen säger är att ett sammansatt tal endast kan faktoriseras på *ett* unikt sätt bortsett från ordningen på faktorerna och att vi på så sätt får en entydig faktorisering. Vi visar här exempel på några primtalsfaktoriseringar,

$$\begin{aligned} 35 &= 5 \cdot 7, \\ 156 &= 2 \cdot 2 \cdot 3 \cdot 13, \\ 2145 &= 3 \cdot 5 \cdot 11 \cdot 13. \end{aligned}$$

Det är relativt lätt att övertyga sig om att primtalsfaktoriseringarna ovan inte kan göras på några andra sätt bortsett från att ändra ordningen på faktorerna. Nedanstående bevis visar att så också är fallet.

Bevis. [7, s. 81] Vi gör ett motsägelsebevis där vi antar att talet n har två *olika* primtalsfaktoriseringar, nämligen

$$p_1p_2p_3.....p_r = n = q_1q_2q_3.....q_s \quad \text{där alla } p_i, q_i \text{ är primtal.}$$

Då p_1 delar vänsterledet, så är p_1 också en delare till högerledet, $q_1q_2q_3.....q_s$. Enligt Euklides lemma måste p_1 dela någon av $q_1q_2q_3.....q_s$, säg q_i. Eftersom q_i är ett primtal vet vi från definition 2.1 att q_i endast har delarna 1 eller sig självt vilket medför att $p_1 = q_i$. Om vi ändrar om på ordningen och indexerar $q_1 = p_1$ kan vi reducera likheten till

$$p_2p_3.....p_r = n = q_2q_3.....q_s.$$

Om vi nu upprepar ovan förfarande tills samtliga faktorer är matchade ser vi att faktoriseringen är entydig bortsett från ordningen på faktorerna och vi har således bevisat Aritmetikens fundamentalsats. □

Vi kommer nu visa ett exempel på hur man med hjälp av entydig faktorisering i heltalen $\mathbb{Z}$ kan lösa en diofantisk ekvation.

Exempel 2.6. Vi vill lösa den diofantiska ekvationen $x^2 - 35 = y^2$ som är ekvivalent med $(x+y)(x-y) = 35$. Vi använder oss av primtalsfaktoriseringen av 35 och får dessa möjliga faktoriseringar

$$\begin{aligned} 35 &= 7 \cdot 5 = (-7) \cdot (-5) = 5 \cdot 7 = (-5) \cdot (-7) \\ &= 1 \cdot 35 = 35 \cdot 1 = (-1) \cdot (-35) = (-35) \cdot (-1) \end{aligned}$$

Vi ställer upp ekvationssystemen

$$\begin{cases} x+y=7 \\ x-y=5 \end{cases}, \begin{cases} x+y=-7 \\ x-y=-5 \end{cases}, \begin{cases} x+y=5 \\ x-y=7 \end{cases}, \begin{cases} x+y=-5 \\ x-y=-7 \end{cases},$$

$$\begin{cases} x+y=1 \\ x-y=35 \end{cases}, \begin{cases} x+y=35 \\ x-y=1 \end{cases}, \begin{cases} x+y=-1 \\ x-y=-35 \end{cases} \text{ och } \begin{cases} x+y=-35 \\ x-y=-1 \end{cases}$$

vilket ger oss de enda åtta möjliga lösningarna

$$(x,y) = (\pm 6, \pm 1) \text{ och } (x,y) = (\pm 18, \pm 17).$$

Vi kommer nu lämna den elementära algebran och gå vidare till den abstrakta algebran. Som tidigare nämnts, är syftet med denna uppsats är att undersöka huruvida Aritmetikens fundamentalsats kan tillämpas på andra talstrukturer än heltalen $\mathbb{Z}$.

3 Algebraiska strukturer

När vi talar om algebraiska strukturer är vi i den abstrakta delen av matematiken. En algebraisk struktur består av en mängd tillsammans med en eller flera operationer som är definierade för elementen i mängden och ett antal axiom för dessa operationer. En operation kan t.ex. vara addition eller multiplikation och beroende på vilka axiom operationerna uppfyller så delas de in i olika algebraiska strukturer. Vi kommer i denna uppsats att titta på två algebraiska strukturer, ringar och kroppar, och då främst kvadratiska ringar och kroppar. Vi inleder detta kapitel med lite teori om dessa strukturer och börjar med ringar.

3.1 Ringar

Först en definition av begreppet *kommutativ ring med en etta*.

Definition 3.1. [2, s. 296] En *kommutativ ring med en etta* är en mängd R med två operationer, addition och multiplikation, som uppfyller nedanstående villkor:

1. Mängden R är sluten under addition och multiplikation.
2. Mängden R är associativ och kommutativ för både addition och multiplikation samt att lagen om distributivitet gäller.
3. Mängden R innehåller ett additativt och ett multiplikativt enhetselement, 0 respektive 1.
4. Alla element i R har en additativ invers.

Exempel 3.2. Heltalen $\mathbb{Z}$ är en kommutativ ring med en etta då den är sluten under addition och multiplikation, innehåller det additativa och det multiplikativa enhetselementen 0 och 1 samt har en additativ invers. Räknereglerna som associativ, kommutativ och distributiv är också uppfyllda i $\mathbb{Z}$.

3.2 Kroppar

Den andra algebraiska strukturen vi kommer använda oss av är kroppar. Även här består en kropp av en mängd K med de båda operationerna, addition och multiplikation.

Definition 3.3. [2, s. 299] En *kropp* är en kommutativ ring med en etta där alla nollskilda element har en multiplikativ invers.

Vi undersöker huruvida heltalen $\mathbb{Z}$ också är en kropp och ser då att kravet om att alla nollskilda element ska ha en multiplikativ invers inte är uppfyllt, så därmed är

heltalen $\mathbb{Z}$ inte en kropp. Om vi istället utvidgar mängden till de rationella talen $\mathbb{Q}$ är kravet om en multiplikativ invers uppfyllt, så de rationella talen $\mathbb{Q}$ är en kropp.

En kroppsutvidgning innebär att man utgår från en kropp och utökar den med fler element. Man säger att en kroppsutvidgning är en kropp som innehåller en annan kropp eller uttryckt på ett annat sätt, det omvända till en delkropp [4].

Som exempel är de komplexa talen $\mathbb{C}$ en kroppsutvidgning av de reella talen $\mathbb{R}$.

3.3 Kvadratiska talkroppar

Innan vi går in på vad kvadratiska talkroppar är för något behöver vi känna till begreppet *kvadratfritt heltal*. Ett kvadratfritt heltal d är ett heltal som inte är delbart med ett primtal i kvadrat [1, s. 50]. Som exempel är 15 kvadratfritt men inte 18, eftersom 18 är delbart med 9 som är lika med 3^2.

Definition 3.4. Låt $d \neq 1$ vara ett kvadratfritt heltal. Vi definierar mängden

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

Eftersom $d \neq 1$ och kvadratfritt så medför det att $\sqrt{d}$ inte är ett rationellt tal och på så sätt får vi en äkta kroppsutvidgning. Att $\sqrt{d}$ inte är rationellt visas enklast med ett motsägelsebevis där vi antar att $\sqrt{d} = \frac{a}{b}$ där $a, b \in \mathbb{Z}$. Vi skriver om uttrycket som $b^2 d = a^2$ och eftersom för ett primtal p med $p \mid d$ får vi ett udda antal faktorer p i primtalsfaktoriseringen av vänsterledet medan ett jämnt antal i högerledet. Således har vi med hjälp av entydig faktorisering visat att $\sqrt{d}$ inte är ett rationellt tal om d har minst en primtalsfaktor, d.v.s. om $d \neq -1$. I fallet då $d = -1$ har vi $\sqrt{-1} = i$ som är ett komplext tal och således inte ett rationellt tal.

I nästa sats kommer vi se att mängden $\mathbb{Q}(\sqrt{d})$, med operationerna addition och multiplikation, är en kropp.

Sats 3.5. *$\mathbb{Q}(\sqrt{d})$ är en kroppsutvidgning av $\mathbb{Q}$.*

Bevis. Det är relativt enkelt att visa att $\mathbb{Q}(\sqrt{d})$ är en kommutativ ring med en etta då $\mathbb{Q}(\sqrt{d})$ är en delmängd till de komplexa talen där villkoren i definition 3.1 är uppfyllda. Vi väljer att visa ett av villkoren i definition 3.1, det att $\mathbb{Q}(\sqrt{d})$ är sluten under multiplikation. Vi väljer två godtyckliga element $a+b\sqrt{d}, c+e\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Vi får

$$(a + b\sqrt{d}) \cdot (c + e\sqrt{d}) = \underbrace{(ac + bed)}_{\mathbb{Q}} + \underbrace{(ae + bc)}_{\mathbb{Q}} \sqrt{d} \ \in \mathbb{Q}(\sqrt{d})$$

och vi har således visat att $\mathbb{Q}(\sqrt{d})$ är sluten under multiplikation.

För att $\mathbb{Q}(\sqrt{d})$ ska vara en kropp måste även villkoret i definition 3.3, att alla nollskilda element i $\mathbb{Q}(\sqrt{d})$ har en multiplikativ invers, vara uppfyllt. Vi väljer ett godtyckligt nollskilt element $a+b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ och undersöker om det existerar en invers x sådan att

$$\begin{aligned}(a+b\sqrt{d}) \cdot x &= 1 \\ \Leftrightarrow x &= \frac{1}{a+b\sqrt{d}}.\end{aligned}$$

Vi förlänger med konjugatet och förenklar uttrycket, så

$$x = \frac{1}{a+b\sqrt{d}} \cdot \frac{a-b\sqrt{d}}{a-b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-db^2} = \frac{a}{a^2-db^2} + \frac{-b}{a^2-db^2}\sqrt{d}.$$

Vi har $\frac{a}{a^2-db^2}, \frac{-b}{a^2-db^2} \in \mathbb{Q}$, där $a^2-db^2 \neq 0$ eftersom d är ett kvadratfritt heltal, så x är ett element i $\mathbb{Q}(\sqrt{d})$ och vi har således visat att alla nollskilda element är inverterbara och därmed att $\mathbb{Q}(\sqrt{d})$ är en kropp. □

3.4 Homomorfier

Definition 3.6. [1, s. 13] En *homomorfi* $\sigma : K \to F$ där K, F är kroppar, är en funktion så att

$$\begin{aligned}\sigma(1) &= 1 \\ \sigma(a+b) &= \sigma(a) + \sigma(b) \\ \sigma(a \cdot b) &= \sigma(a) \cdot \sigma(b)\end{aligned}$$

för alla $a, b \in K$.

Om funktionen σ är bijektiv kallas den isomorfi, om surjektiv för epimorfi och slutligen för monomorfi om den är injektiv. En homomorfi mellan kroppar är alltid en monomorfi.

Lemma 3.7. *Låt $K = \mathbb{Q}(\sqrt{d})$ och $\sigma : K \to \mathbb{C}$ en monomorfi. Då gäller att $\sigma(\alpha) = \alpha$ för alla $\alpha \in \mathbb{Q}$.*

Bevis. Vi visar först att $\sigma(0) = 0$ och utgår från

$$0 + 0 = 0.$$

Vi låter funktionen σ verka på båda sidor om likhetstecknet och får

$$\sigma(0) + \sigma(0) = \sigma(0).$$

Slutligen subtraherar vi $\sigma(0)$ från båda sidor och vi har då visat att

$$\sigma(0) = 0.$$

Vidare visar vi att $\sigma(1) = 1$ och utgår från

$$1 \cdot 1 = 1.$$

Vi låter funktionen σ verka på båda sidor om likhetstecknet igen och får

$$\sigma(1 \cdot 1) = \sigma(1).$$

Då strukturen bevaras har vi att

$$\sigma(1) \cdot \sigma(1) = \sigma(1).$$

Vi förkortar med $\sigma(1)$ och har således visat att

$$\sigma(1) = 1.$$

Vi fortsätter genom att visa att $\sigma(2) = 2$ där

$$\sigma(2) = \sigma(1 + 1) = \sigma(1) + \sigma(1) = 1 + 1 = 2.$$

På detta sätt kan man fortsätta och med induktion visa att $\sigma(n) = n$ för alla positiva heltal n.

För negativa heltal, $-n$, har vi

$$n + \sigma(-n) = \sigma(n) + \sigma(-n) = \sigma(n + (-n)) = \sigma(0) = 0$$

så $\sigma(-n) = -n$.

Avslutningsvis, när $\alpha = \frac{a}{b}$ där $a, b \in \mathbb{Z}$ och $b \neq 0$ får vi

$$\sigma(\alpha) = \frac{\sigma(a)}{\sigma(b)} = \frac{a}{b} = \alpha.$$

□

4 Algebraiska tal

Vi kommer i detta kapitel utvidga talområdet med de algebraiska talen. Vi inleder med en definition av vad ett algebraiskt tal är för något för att sen gå in på tre viktiga begrepp; normen, spåret och minimalpolynom. Vi kommer se att om α är ett algebraiskt tal så har det ett unikt minimalpolynom och vi kommer visa hur man kan beräkna minimalpolynomet till ett godtyckligt element i en kvadratisk talkropp med hjälp av normen och spåret.

4.1 Definition av algebraiska tal

Definition 4.1. [1, s. 38] [6] Ett komplext tal α är *algebraiskt* om det är algebraiskt över $\mathbb{Q}$, d.v.s. att det är ett nollställe till ett nollskilt polynom med koefficienter i $\mathbb{Q}$.

Man kan även förlänga polynomekvationen så att nämnarna försvinner vilket då ger oss en polynomekvation med koefficienter i $\mathbb{Z}$ på formen

$$a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0, \quad a_k \in \mathbb{Z} \quad k = 0, 1, ...n, \ a_n \neq 0.$$

Vi ger här två exempel på algebraiska tal.

Exempel 4.2. $\frac{1}{4}$ är ett algebraiskt tal eftersom det är en lösning till polynomekvationen $x - \frac{1}{4} = 0$ där vi ser att koefficienterna är i $\mathbb{Q}$.

Exempel 4.3. $1 + \sqrt{3}$ är ett algebraiskt tal eftersom det är en lösning till polynomekvationen $x^2 - 2x - 2 = 0$.

Ett *transcendent tal*, är ett tal som inte kan definieras som ett nollställe till ett polynom med koefficienter i $\mathbb{Q}$, det är motsatsen till ett algebraiskt tal. Ett exempel på ett transcendent tal är talet π [1, s. 22] [8].

Definition 4.4. [1, s. 38] En delkropp till $\mathbb{C}$ som fås genom att utvidga $\mathbb{Q}$ med ett ändligt antal algebraiska tal kallas en *talkropp*.

Vi såg tidigare exempel på kvadratiska talkroppar som är en kroppsutvidgning av $\mathbb{Q}$ genom att man lägger till det algebraiska talet $\sqrt{d}$.

4.2 Normen och spåret

Normen och spåret är ett sätt att tilldela varje element i en talkropp ett rationellt tal, något som vi kommer ha stor användning av senare i uppsatsen. Vi betecknar normen med N och spåret med T från det engelska ordet *trace*. Vi inleder med en definition av begreppen.

Definition 4.5. [1, s. 51] Om K är en talkropp och $\sigma_1, ..., \sigma_n : K \to \mathbb{C}$ är alla monomorfier så definieras normen respektive spåret för något $\alpha \in K$ som

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

och

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Innan vi går vidare in på vad normen och spåret är i kvadratiska talkroppar så ska vi först bestämma samtliga monomorfier $\sigma : K \to \mathbb{C}$ då $K = \mathbb{Q}(\sqrt{d})$.

För ett godtyckligt element $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ får vi

$$\sigma(a + b\sqrt{d}) = \sigma(a) + \sigma(b)\sigma(\sqrt{d}).$$

Enligt lemma 3.7 får vi därför

$$\sigma(a + b\sqrt{d}) = a + b\sigma(\sqrt{d}).$$

Eftersom $(\sqrt{d})^2 = d$ får vi $\sigma(\sqrt{d})^2 = d$ vilket medför att $\sigma(\sqrt{d}) = \pm\sqrt{d}$. Därmed har vi visat följande sats.

Sats 4.6. *[1, s. 40] För $\mathbb{Q}(\sqrt{d})$ ges alla monomorfier $\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{C}$ av:*

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d},$$
$$\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

Bevis. Det återstår att visa att σ_1 och σ_2 är homomorfier genom att visa att de är additativa och multiplikativa funktioner enligt definition 3.6. Båda, σ_1 och σ_2, visas på samma sätt och eftersom σ_1 avbildar element på sig själva väljer vi att visa σ_2 och hänvisa till samma förfarande för σ_1.

För $x = a + b\sqrt{d}$ och $y = c + e\sqrt{d}$ där $x, y \in \mathbb{Q}\sqrt{d}$ får vi

$$\begin{aligned}\sigma_2(x + y) = \sigma_2(a + b\sqrt{d} + c + e\sqrt{d}) = a - b\sqrt{d} + c - e\sqrt{d} = \\ = \sigma_2(a + b\sqrt{d}) + \sigma_2(c + e\sqrt{d}) = \sigma_2(x) + \sigma_2(y),\end{aligned}$$

och

$$\begin{aligned}\sigma_2(x \cdot y) = \sigma_2((a + b\sqrt{d})(c + e\sqrt{d})) = \sigma_2(ac + bc\sqrt{d} + ae\sqrt{d} + bde) = \\ = ac - bc\sqrt{d} - ae\sqrt{d} + bde = (a - b\sqrt{d})(c - e\sqrt{d}) = \sigma_2(x) \cdot \sigma_2(y).\end{aligned}$$

Vi har härmed visat att σ_2 är en additiv och multiplikativ funktion och σ_2 är således en homomorfi. □

För varje talkropp K finns det bara ett ändligt antal monomorfier $\sigma_i : K \to \mathbb{C}$ $(i = 1, ..., n)$ [1, sats 2.4]. Alltså är definition 4.5 meningsfull för alla talkroppar.

4.3 Normen och spåret i kvadratiska talkroppar

Vi inleder med normen i kvadratiska talkroppar. Då $K = \mathbb{Q}(\sqrt{d})$ får vi enligt definition 4.5 och sats 4.6 att normen av ett element $\alpha \in K$ är

$$N(\alpha) = \sigma_1(\alpha) \cdot \sigma_2(\alpha). \tag{4.7}$$

För $\alpha = a + b\sqrt{d}$ är normen därmed

$$N(a + b\sqrt{d}) = (a + b\sqrt{d}) \cdot (a - b\sqrt{d}) = a^2 - db^2,$$

så $N(\alpha) \in \mathbb{Q}$ för alla $\alpha \in K$. Vi noterar att α har samma norm som sitt konjugat.

Vi kommer nu visa en viktig egenskap hos normen, nämligen att den är multiplikativ.

Sats 4.8. *[1, s. 51] Normen är multiplikativ d.v.s.* $N(\alpha\beta) = N(\alpha)N(\beta)$ *då* $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$.

Bevis. Ekvation (4.7) ger

$$\begin{aligned} N(\alpha\beta) &= \sigma_1(\alpha\beta)\sigma_2(\alpha\beta) = \sigma_1(\alpha)\sigma_1(\beta)\sigma_2(\alpha)\sigma_2(\beta) \\ &= \sigma_1(\alpha)\sigma_2(\alpha)\sigma_1(\beta)\sigma_2(\beta) = N(\alpha)N(\beta), \end{aligned}$$

så normen är multiplikativ. □

Vi fortsätter med spåret i kvadratiska talkroppar. Då $K = \mathbb{Q}(\sqrt{d})$ får vi enligt definition 4.5 och sats 4.6 att spåret till ett element $\alpha \in K$ är

$$T(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha). \tag{4.9}$$

För $\alpha = a + b\sqrt{d}$ är spåret alltså

$$T(a + b\sqrt{d}) = (a + b\sqrt{2}) + (a - b\sqrt{2}) = 2a,$$

så $T(\alpha) \in \mathbb{Q}$ för alla $\alpha \in K$.

På motsvarande sätt som att normen är multiplikativ visar vi här att spåret är additativt för samtliga element i en kvadratisk kropp.

Sats 4.10. *[1, s. 51] Spåret är additivt d.v.s.* $T(\alpha + \beta) = T(\alpha) + T(\beta)$ *då* $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$.

Bevis. Ekvation (4.9) ger att

$$\begin{aligned} T(\alpha+\beta) &= \sigma_1(\alpha+\beta)+\sigma_2(\alpha+\beta) = \sigma_1(\alpha)+\sigma_2(\alpha)+\sigma_2(\alpha)+\sigma_2(\beta) \\ &= \sigma_1(\alpha)+\sigma_2(\alpha)+\sigma_1(\beta)+\sigma_2(\beta) = T(\alpha)+T(\beta), \end{aligned}$$

så spåret är additivt. □

I sats 4.8 och 4.10 visade vi att normen och spåret är multiplikativ respektive additivt i kvadratiska talkroppar men man inser enkelt att detta även är sant för godtyckliga talkroppar.

4.4 Minimalpolynom

När vi nu vet hur man beräknar både normen och spåret till ett element ska vi i detta kapitel se hur vi kan använda dessa för att beräkna minimalpolynomet. Men först börjar vi med att definiera vad ett minimalpolynom är för något.

Definition 4.11. [1, s. 22] Ett *minimalpolynom* $p_\alpha(x) \in \mathbb{Q}[x]$ för ett element α i en talkropp K, är det unika moniska polynomet av minimal grad så att $p_\alpha(\alpha) = 0$. Graden av α är definierad som graden av $p_\alpha(x)$.

Att det existerar ett minimalpolynom beror på att elementet α är algebraiskt och därmed, enligt definition 4.1, är ett nollställe till ett nollskilt polynom $f(x) \in \mathbb{Q}[x]$. Detta medför att det måste finnas ett sådant polynom med lägsta grad. Att minimalpolynomet sen är unikt inses enklast genom att förutsätta det motsatta, att det finns två minimalpolynom $f(x)$ och $g(x)$. Om så är fallet medför det att vi kan få ett nytt polynom $h(x)$ genom att ta differensen $h(x) = f(x) - g(x)$ och eftersom minimalpolynomen är moniska medför det att $h(x)$ har lägre grad än $f(x)$ och $g(x)$ samt uppfyller $h(\alpha) = 0$. Det innebär att vi måste ha $h(x) = 0$ vilket medför att $f(x) = g(x)$ och således är minimalpolynomet unikt.

4.5 Minimalpolynom för kvadratiska talkroppar

Vi kommer nu visa hur man med hjälp av normen och spåret kan beräkna minimalpolynomet till ett godtyckligt element i en kvadratisk talkropp.

Vi låter $K = \mathbb{Q}(\sqrt{d})$ där $d \neq 1$ och kvadratfritt. Vi väljer elementet $\alpha = a + b\sqrt{d}$, där $a, b \in \mathbb{Q}$ och $b \neq 0$. Enligt sats 4.6 får vi därför

$$\begin{aligned} \sigma_1(\alpha) &= a + b\sqrt{d} \\ \sigma_2(\alpha) &= a - b\sqrt{d}. \end{aligned}$$

Vi söker ett nollskilt polynom $f(x) \in \mathbb{Q}[x]$ så att $f(\alpha) = 0$. Om vi sätter

$$\begin{aligned} f(x) &= (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) = x^2 - (\sigma_1(\alpha) + \sigma_2(\alpha))x + \sigma_1(\alpha)\sigma_2(\alpha) \\ &= x^2 - T(\alpha)x + N(\alpha) \end{aligned}$$

ser vi att $f(\alpha) = 0$ och $T(\alpha), N(\alpha) \in \mathbb{Q}$ så är $f(x) \in \mathbb{Q}[x]$. Vi noterar att $f(x)$ är moniskt och av minimal grad eftersom α består av det irrationella talet $\sqrt{d}$ och således inte kan ha ett minimalpolynom av lägre grad än 2. Alltså är $f(x) = p_\alpha(x)$, minimalpolynomet för α.

I fallen då $b = 0$ har vi att $\alpha \in \mathbb{Q}$ och vi får minimalpolynomet $p_\alpha(x) = x - \alpha$ som är av grad 1. Så beroende på om α är rationellt eller irrationellt får vi ett minimalpolynom av grad 1 eller 2 på formen

$$p_\alpha(x) = \begin{cases} x - \alpha & \text{om } \alpha \in \mathbb{Q} \\ x^2 - T(\alpha)x + N(\alpha) & \text{om } \alpha \in \mathbb{Q}(\sqrt{d})\backslash\mathbb{Q} \end{cases} \tag{4.12}$$

Vi illustrerar båda fallen genom att beräkna minimalpolynomen till två element.

Exempel 4.13. Låt $\alpha = \frac{1}{3}$. Eftersom $\alpha \in \mathbb{Q}$ får vi minimalpolynomet enligt ekvation (4.12) på formen

$$p_\alpha(x) = x - \frac{1}{3}.$$

Exempel 4.14. Låt $\alpha = \frac{2+3\sqrt{2}}{5}$. Eftersom $\alpha \in \mathbb{Q}(\sqrt{2})\backslash\mathbb{Q}$ får vi minimalpolynomet enligt ekvation (4.12) på formen

$$p_\alpha(x) = x^2 - T(\alpha)x + N(\alpha).$$

Vi beräknar spåret och normen

$$\begin{aligned} T(\alpha) &= \sigma_1(\alpha) + \sigma_2(\alpha) = \Big(\frac{2+3\sqrt{2}}{5}\Big) + \Big(\frac{2-3\sqrt{2}}{5}\Big) = \frac{4}{5}, \\ N(\alpha) &= \sigma_1(\alpha) \cdot \sigma_2(\alpha) = \Big(\frac{2+3\sqrt{2}}{5}\Big) \cdot \Big(\frac{2-3\sqrt{2}}{5}\Big) = -\frac{14}{25}. \end{aligned}$$

Detta ger oss minimalpolynomet $p_\alpha(x) = x^2 - \frac{4}{5}x - \frac{14}{25}$.

5 Algebraiska heltal

I detta kapitel introducerar vi de algebraiska heltalen. Dessa heltal kommer vara en viktig del när vi senare i uppsatsen tittar på entydig faktorisering. Vi inleder med att definiera vad ett algebraiskt heltal är för något för att sen undersöka vilka de algebraiska heltalen är i kvadratiska talkroppar.

5.1 Definition av algebraiska heltal

Definition 5.1. [1, s. 43] Ett komplext tal α är ett *algebraiskt heltal* om det är ett nollställe till ett moniskt polynom (högstagradskoefficienten är 1) där koefficienterna är heltal, d.v.s.

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0 \quad \text{där } a_i \in \mathbb{Z} \text{ för alla } i.$$

Enligt rationella rotsatsen [7] har ett moniskt heltalspolynom endast rationella heltalslösningar vilket innebär att de algebraiska heltalen i $\mathbb{Q}$ endast är heltalen $\mathbb{Z}$.

Vi ger här ytterligare ett exempel på ett algebraiskt heltal.

Exempel 5.2. I ekvationen $x^2 - 2 = 0$ där koefficienterna är heltalen 1 och -2 har vi nollställena $\pm\sqrt{2}$, så således är $\pm\sqrt{2}$ algebraiska heltal.

Nedanstående lemma och sats visar hur de algebraiska talen förhåller sig till de algebraiska heltalen. För bevisen av dessa hänvisar vi till [1, lemma 2.13 och sats 2.9]

Lemma 5.3. *Ett algebraiskt tal α är ett algebraiskt heltal om och endast om dess minimalpolynom över $\mathbb{Q}$ har koefficienter i $\mathbb{Z}$.*

Om K är en delkropp till $\mathbb{C}$ som består av algebraiska tal så definierar vi $\mathcal{O}_K$ som mängden $\{\alpha \in K \mid \alpha \text{ algebraiskt heltal}\}$.

Sats 5.4. *$\mathcal{O}_K$ är en delring till K.*

I och med sats 5.4 innebär det att de algebraiska heltalen är slutna under addition och multiplikation. Ett exempel på detta som vi tidigare sett är ringen av heltalen $\mathbb{Z}$ (som är algebraiska heltal) som är en delring till talkroppen $\mathbb{Q}$ (som består av algebraiska tal) och är en delkropp till $\mathbb{C}$.

Vi avslutar detta delkapitel med ett lemma som säger vilken ring som genereras av ett algebraiskt heltal.

Lemma 5.5. *[1] Om $p(\alpha) = 0$ och $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ är ett moniskt heltalspolynom av grad n, så är*

$$\mathbb{Z}[\alpha] = \{a_0 + a_1\alpha + ...a_{n-1}\alpha^{n-1} \mid a_k \in \mathbb{Z},\ k = 0, 1, ..n-1\}.$$

Vi påminner om att ringen $\mathbb{Z}[\alpha]$ består av alla heltalspolynom i α och är av godtycklig grad. Vi noterar att den högsta graden på α i högerledet är $n-1$ och det beror på att termer av grad $\geq n$ kan reduceras med hjälp av $\alpha^n = -a_{n-1}\alpha^{n-1} - ... - a_0$. Vi illustrerar ovanstående resonemang med ett exempel.

Exempel 5.6. Låt $\alpha = 2 + \sqrt{3}$. Vi beräknar först minimalpolynomet $p_\alpha(\alpha) = \alpha^2 - 4\alpha + 1 = 0$ och noterar att det är av grad 2. Det innebär att t.ex. α^3 kan reduceras med hjälp av $\alpha^2 = 4\alpha - 1$ där

$$\alpha^3 = \alpha(\alpha)^2 = \alpha(4\alpha - 1) = 4\alpha^2 - \alpha = 4(4\alpha - 1) - \alpha = 15\alpha - 4.$$

Så med hjälp av minimalpolynomet har vi reducerat graden av polynomuttrycket α^3 från 3 till 1.

5.2 De algebraiska heltalen i kvadratiska talkroppar

Vi kommer nu visa en sats som säger vilka de algebraiska heltalen i kvadratiska talkroppar är. Ett av målen för mig med denna uppsats har varit att förstå detta bevis och kunna skriva beviset med egna ord. Men först en definition:

Definition 5.7. Låt $d \neq 1$ vara ett kvadratfritt heltal. Den *kvadratiska heltalsringen* $\mathcal{O}_d$ är ringen av algebraiska heltal $\alpha \in \mathbb{Q}(\sqrt{d})$.

Sats 5.8. *[1, sats 3.2] Låt $d \neq 1$ vara ett kvadratfritt heltal. Då är ringen av algebraiska heltal i $\mathbb{Q}(\sqrt{d})$:*

1. $\mathbb{Z}[\sqrt{d}]$ *om* $d \not\equiv 1 \pmod 4$,
2. $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ *om* $d \equiv 1 \pmod 4$.

Bevis. Ett godtyckligt element $\alpha \in \mathbb{Q}(\sqrt{d})$ kan skrivas på den generella formen $a + b\sqrt{d}$ där $a, b \in \mathbb{Q}$. Vi skriver om α som

$$\alpha = \frac{x + y\sqrt{d}}{z} \quad \text{där } x, y, z \in \mathbb{Z} \text{ och } z > 0.$$

Vi antar att det inte finns något primtal p som delar x, y och z samtidigt, d.v.s. att x, y och z är förkortade så långt det är möjligt. Det innebär att x, y och z är relativt prima, d.v.s. att $SGD(x, y, z) = 1$.

Vi noterar i fallet då $y = 0$ att $\alpha \in \mathbb{Q}$, som vi i kapitel 5.1 såg endast är ett algebraiskt heltal då $\alpha \in \mathbb{Z}$, d.v.s. då $z = 1$.

I fallet då $y \neq 0$ är $\alpha \notin \mathbb{Q}$ och vi får enligt (4.12) ett minimalpolynom som är kvadratiskt. Vi beräknar minimalpolynomet $p_\alpha(t)$ med hjälp av spåret och normen där $p_\alpha(t) = t^2 - T(\alpha)t + N(\alpha)$.

Vi beräknar först

$$N(\alpha) = \sigma_1(\alpha) \cdot \sigma_2(\alpha) = \left(\frac{x + y\sqrt{d}}{z}\right)\left(\frac{x - y\sqrt{d}}{z}\right) = \frac{x^2 - y^2 d}{z^2}$$
$$T(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = \left(\frac{x + y\sqrt{d}}{z}\right) + \left(\frac{x - y\sqrt{d}}{z}\right) = \frac{2x}{z}$$

och minimalpolynomet till α blir således

$$p_\alpha(t) = t^2 - \frac{2x}{z}t + \frac{x^2 - y^2 d}{z^2}.$$

Enligt lemma 5.3 är ett element ett algebraiskt heltal om koefficienterna i minimalpolynomet är heltal. Detta ger oss två villkor på x, y, z som båda måste vara uppfyllda för att elementet α i $\mathbb{Q}(\sqrt{d})$ ska vara ett algebraiskt heltal, nämligen

$$\frac{x^2 - y^2 d}{z^2} \in \mathbb{Z} \tag{5.9}$$

och

$$\frac{2x}{z} \in \mathbb{Z}. \tag{5.10}$$

Vi börjar med villkoret (5.10) och undersöker om x och z kan ha någon gemensam primtalsfaktor p. Om så är fallet existerar $k, l \in \mathbb{Z}$ så att $x = l \cdot p$ och $z = k \cdot p$. Enligt villkor (5.9) får vi då att p också måste dela y. Vi visar detta med hjälp av moduloräkning och Euklides lemma 2.4. Villkor (5.9) medför då att $p^2 \mid x^2 + y^2 d$ så

$$x^2 - y^2 d \equiv 0 \pmod{p^2}$$

som är ekvivalent med

$$l^2 \cdot p^2 - y^2 d \equiv 0 \pmod{p^2}$$

och vi får

$$-y^2 d \equiv 0 \pmod{p^2}.$$

Om $p \nmid d$ så $p \mid y^2$ enligt Euklides lemma. Om $p \mid d$ så existerar ett $n \in \mathbb{Z}$ så att $d = n \cdot p$ men eftersom d är kvadratfritt så $p \nmid n$ så $p \mid y^2 n$ och Euklides lemma ger att $p \mid y^2$ även i detta fall. Med Euklides lemma ytterligare en gång får vi att $p \mid y$. Vi har alltså kommit fram till att $p \mid x$, $p \mid y$ och $p \mid z$ men detta blir en motsägelse till vårt ursprungsantagande om att $SGD(x, y, z) = 1$. Går vi tillbaka till villkor (5.10) när vi nu vet att $SGD(x, z) = 1$ och åter igen använder oss av Euklides lemma innebär det att z måste dela 2 och därmed endast kan anta värdet 1 eller 2.

I fallet då $z = 1$ är båda villkoren (5.9) och (5.10) uppfyllda för alla $x, y \in \mathbb{Z}$ och vi får de algebraiska heltal i $\mathbb{Q}(\sqrt{d})$ på formen $\alpha = x + y\sqrt{d}$ där $x, y \in \mathbb{Z}$.

I fallet då $z = 2$ ser vi att villkor (5.10) är uppfyllt för alla $x \in \mathbb{Z}$ medan villkor (5.9) behöver undersökas lite närmare.

Vi börjar med att sätta in $z = 2$ i villkor (5.9) och får då

$$\frac{x^2 - y^2 d}{4} \in \mathbb{Z}.$$

Vi går nu över till att räkna i modulo 4 och kan då skriva om villkoret på formen

$$x^2 - y^2 d \equiv 0 \pmod 4. \tag{5.11}$$

Låt oss nu undersöka för vilka värden på x, y och d som ekvation 5.11 är uppfylld. Vi skriver ett udda tal på den generella formen $2k+1$ där $k \in \mathbb{Z}$. Kvadraten av detta blir $4k^2 + 4k + 1 \equiv 1 \pmod 4$. På motsvarande sätt kan vi skriva ett jämnt tal som $2k$ och får att $4k^2 \equiv 0 \pmod 4$. För att ekvation (5.11) ska vara uppfylld är en möjlighet att båda x och y är jämna tal men eftersom $z = 2$ och vi har antagit att $SGD(x, y, z) = 1$ blir det en motsägelse. Eftersom att $d \neq 0$ kvarstår enda möjligheten för att ekvation (5.11) ska vara uppfylld att x och y båda är udda, och att $d \equiv 1 \pmod 4$. Detta ger oss ytterligare en möjlighet till att båda villkoren (5.9) och (5.10) blir uppfyllda och vi kan därmed utöka mängden av algebraiska heltal i fallet då $d \equiv 1 \pmod 4$ med elementen $\alpha = \frac{x+y\sqrt{d}}{2}$ där båda x, y är udda heltal.

Sammanfattningsvis har vi alltså visat att de algebraiska heltalen i $\mathbb{Q}(\sqrt{d})$ då $d \not\equiv 1 \pmod 4$ är

$$\{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\}$$

och att när $d \equiv 1 \pmod 4$ kan mängden utökas till

$$\{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\} \cup \{\frac{x + y\sqrt{d}}{2} \mid x, y \text{ udda heltal}\}.$$

I det senare fallet skriver vi om mängden och får

$$\mathcal{O}_d = \left\{\frac{x + y\sqrt{d}}{2} \mid x, y \text{ jämna heltal}\right\} \cup \left\{\frac{x + y\sqrt{d}}{2} \mid x, y \text{ udda heltal}\right\}.$$

Vi noterar att både x och y, antingen är jämna eller udda, och skriver det som $x \equiv y \pmod 2$. Slutligen kan vi skriva mängden av algebraiska heltal som

$$\mathcal{O}_d = \left\{\frac{x + y\sqrt{d}}{2} \mid x, y \in \mathbb{Z} \text{ och } x \equiv y \pmod 2\right\}. \tag{5.12}$$

Vi avslutar beviset med att återföra mängden (5.12) på formen $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ där vi med hjälp av lemma 5.5 kan skriva

$$\mathbb{Z}[\tfrac{1+\sqrt{d}}{2}] = \left\{ a + b\tfrac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z} \right\}.$$

Vi får att $\alpha = \frac{x+y\sqrt{d}}{2} \in \mathcal{O}_d$ kan skrivas som $\alpha = a + b\frac{1+\sqrt{d}}{2}$ med $a = \frac{x-y}{2} \in \mathbb{Z}$ och $b = y \in \mathbb{Z}$. Omvänt, $\alpha = a + b\frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ kan skrivas som $\alpha = \frac{x+y\sqrt{d}}{2}$ med $x = 2a + b \in \mathbb{Z}$ och $y = b \in \mathbb{Z}$ så $x \equiv y \pmod 2$. Vi har därmed visat att $\mathcal{O}_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. □

6 Entydig faktorisering

Vi inleder kapitlet med några viktiga definitioner och satser som vi kan behöva för att bättre förstå entydig faktorisering i det allmänna fallet. Sen går vi in på de kvadratiska talkropparna där vi genom exempel visar att faktorisering i dessa talkroppar inte alltid är entydig. Vi fortsätter sen med en alldeles egen grupp av ringar, de så kallade Euklidiska ringarna, där vi kommer se att faktoriseringen alltid är entydig. Avslutningsvis visar vi hur man med hjälp av entydig faktorisering kan lösa en diofantisk ekvation.

6.1 Entydig faktorisering i generella ringar

Vi kommer här att definiera några viktiga begrepp som delbarhet, enheter, associerade element, irreducibelt element och primelement för att sen avsluta kapitlet med en allmän definition av entydig faktorisering i kommutativa ringar med en etta. Vi vill också anmärka att de ringar R vi tittar på saknar nolldelare eftersom R är en delmängd till en kropp. Att R saknar nolldelare innebär att produkten av två element i R endast kan bli noll om minst ett av elementen i sig är noll.

Definition 6.1. Låt α och β vara två element i ringen R. Då delar β elementet α om $\alpha = \gamma\beta$ för något $\gamma \in R$. Vi skriver då $\beta \mid \alpha$.

Definition 6.2. [1, s. 12] En *enhet* u (eng. unit) i ringen R är ett element med multiplikativ invers, så att

$$u \cdot x = 1 \quad \text{för något } x \in R.$$

Bland heltalen $\mathbb{Z}$ så har vi endast två enheter, 1 och -1, medan bland de rationella talen $\mathbb{Q}$ är alla nollskilda element en enhet [1, s. 79].

Begreppet enhet används bland annat när man pratar om associerade element och trivial faktorisering. Låt oss titta på en definition av begreppet associerade.

Definition 6.3. [1, s. 79] Två nollskillda element x och y i en kommutativ ring med en etta är *associerade* om $x = uy$ där u är en enhet.

För heltalen $\mathbb{Z}$ innebär definition 6.3 att bland de nollskilda elementen är de parvis associerade eftersom det endast finns två enheter i $\mathbb{Z}$. Exempelvis är 3 associerad med -3 då elementen endast skiljer sig åt med en faktor -1, som är en enhet i $\mathbb{Z}$.

En faktorisering av $x \in R$ där $x = yz$ kallas *äkta* om varken y eller z är en enhet, i annat fall kallas den *trivial* och då är en av faktorerna en enhet och den andra associerad med x [1, s. 79].

I nästa definition kommer vi se att enheter också spelar en viktig roll när man pratar om irreducibla element.

Definition 6.4. [1, s. 75] Elementet p i ringen R säger vi är ett *irreducibelt element* om $p \neq 0$ och ej en enhet samt om $p = ab$ medför att antingen a eller b är en enhet.

Definitionen innebär att det enda sättet att skriva ett irreducibelt element som en produkt av två element är att låta den ena faktorn vara en enhet. Bland heltalen $\mathbb{Z}$ är de irreducibla elementen på formen p och $-p$ där p är ett primtal. Som exempel visar vi den triviala faktoriseringen av talet 3 i heltalen $\mathbb{Z}$ där vi ser att vi får fyra faktoriseringar men där de endast skiljer sig åt i ordingen på faktorerna samt enheterna ± 1 framför faktorerna

$$1 \cdot 3 = 3 \cdot 1 = (-1) \cdot (-3) = (-3) \cdot (-1).$$

För att bättre förstå när en faktorisering är unik behöver vi känna till begreppet primelement.

Definition 6.5. [1, s. 89] Elementet p i ringen R säger vi är ett *primelement* om $p \neq 0$ och ej en enhet samt om

$$p \mid ab \text{ medför att } p \mid a \text{ eller } p \mid b.$$

Vi illustrerar definition 6.5 med hjälp av ett exempel.

Exempel 6.6. I talkroppen $\mathbb{Q}(\sqrt{-6})$ kan vi faktorisera talet 6 på följande sätt $6 = 2 \cdot 3 = \sqrt{-6} \cdot (-\sqrt{-6})$. Enligt definition av delbarhet (def. 6.1) ser vi att $2 \mid 6$ men $2 \nmid (\pm\sqrt{-6})$ eftersom $\frac{\pm\sqrt{-6}}{2} \notin \mathcal{O}_{-6}$ så därmed är 2 inte ett primelement i $\mathcal{O}_{-6}$.

Nästa sats säger något om hur de irreducibla elementen förhåller sig till primelementen.

Sats 6.7. *[1, sats 4.13] Ett primelement i ringen R är alltid ett irreducibelt element.*

Bevis. Vi antar att R är en ring och att $x \in R$ och är ett primelement, och $x = ab$. Eftersom x är ett primelement har vi från definition 6.5 att $x \mid a$ eller $x \mid b$. Om $x \mid a$ kan vi skriva $a = xc$ där $c \in R$ och insättning ger $x = xcb$ och eftersom R saknar nolldelare kan vi använda oss av kanselleringslagen och får $1 = cb$, så b är således en enhet. På samma sätt kan vi visa att a är en enhet om $x \mid b$. Därmed har vi visat att primelementet x även är ett irreducibelt element. □

Det omvända, att ett irreducibelt element är ett primelement, gäller inte. Detta kunde vi se i exempel 6.6.

Vi kommer nu gå in på en sats som listar några egenskaper hos enheter, associerade element och irreducibla element:

Sats 6.8. *[1, sats 4.4] För en ring R gäller att:*
a) Ett element x är en enhet om och endast om $x \mid 1$.
b) Två godtyckliga enheter är associerade och ett associerat element till en enhet är en enhet.
c) Elementen x och y är associerade om och endast om $x \mid y$ och $y \mid x$.
d) Ett element x är irreducibelt om och endast om varje delare till x är associerad med x eller är en enhet.
e) Ett associerat element till ett irreducibelt element är irreducibel.

Bevis. a) och b) följer från definition 6.2.

c) Vi antar att $x \mid y$ och $y \mid x$. Då existerar $a, b \in R$ så att $y = ax$ och $x = by$. Insättning av y i x ger

$$x = bax.$$

Om nu $x = 0$ får vi att $y = 0$ och de är associerade. I annat fall när $x \neq 0$ kan vi använda oss av kanselleringslagen och får då

$$1 = ba,$$

vilket innebär att både a och b är enheter och därav är x och y associerade.

d) och e) följer från definition 6.4. □

När vi nu lärt oss om enheter, associerade element, irreducibla element och primelement kan vi gå in på själva definitionen av begreppet entydig faktorisering.

Definition 6.9. [1, s. 84] Faktorisering i ringen R är entydig om, närhelst

$$p_1 ... p_r = q_1 ... q_s$$

och varje p_i och q_j är irreducibla i R, följande är uppfyllt:
(a) $r = s$.

(b) Det finns en permutation π av $1, ..., r$ sådan att p_i och $q_{\pi(i)}$ är associerade för alla $i = 1, ..., r$.

Villkor (a) innebär att det är lika många irreducibla element som ingår i faktoriseringen medan villkor (b) innebär att ordningen de står i inte spelar någon roll samt att faktorerna kan modifieras genom att multipliceras med enheter.

6.2 Entydig faktorisering i kvadratiska talkroppar

I detta kapitel kommer vi genom exempel visa att faktorisering i vissa kvadratiska talkroppar *inte* är entydig. För en ökad förståelse av exemplerna inleder vi med att först titta på två satser som säger något om enheter, associerade element och irreducibla element i kvadratiska talkroppar. Innan vi sätter igång vill vi bara lite kort ge ett exempel på hur definition 6.1 om delbarhet i ringar kan användas på kvadratiska heltalsringar $\mathcal{O}_d$.

Exempel 6.10. Vi ser att $1 + i \mid 2$ eftersom $2 = (1 - i)(1 + i)$ där samtliga element tillhör $\mathcal{O}_{-1}$.

Sats 6.11. *[1, sats 4.10]*
Låt $\mathcal{O}_d$ vara ringen av heltal i $\mathbb{Q}(\sqrt{d})$ och låt $x, y \in \mathcal{O}_d$, då gäller
(a) Ett element $x \in \mathcal{O}_d$ är en enhet om och endast om $N(x) = \pm 1$.
(b) Om x och y är associerade så är $N(x) = \pm N(y)$.
(c) Om $N(x)$ är ett primtal så är x irreducibel.

Bevis. (a) Från definitionen av en enhet (se def. 6.2) har vi att $xu = 1$. Vi tar normen på båda sidor och får $N(x)N(u) = 1$. Eftersom $N(x), N(u) \in \mathbb{Z}$ medför detta att $N(x) = \pm 1$. Omvänt, vi antar att $N(x) = \pm 1$ och eftersom vi är i den kvadratiska heltalsringen fås normen genom

$$N(x) = \sigma_1(x) \cdot \sigma_2(x) = x \cdot \sigma_2(x) = \pm 1$$

som vi kan skriva om som

$$x \cdot (\pm \sigma_2(x)) = 1.$$

Det innebär att x har en multiplikativ invers i $\mathcal{O}_d$ och således är en enhet enligt definition 6.2, vilket skulle visas.

(b) Om x, y är associerade ger definition 6.2 att $x = uy$ där u är en enhet. Då har vi

$$N(x) = N(uy) = N(u) \cdot N(y).$$

Från (a) vet vi att $N(u) = \pm 1$ vilket ger att $N(x) = \pm 1 \cdot N(y) = \pm N(y)$.

(c) Låt $x = yz$ och anta att $N(x) = p$ där p är ett primtal. Då har vi $N(x) = N(yz) = N(y) \cdot N(z) = p$ vilket medför att $N(y)$ eller $N(z)$ är $\pm p$ medan den andra är ± 1. Så enligt (a) är y eller z en enhet och enligt definition 6.4 är således x irreducibel. □

Sats 6.12. *[1, s. 82] Varje nollskilt element $\alpha \in \mathcal{O}_d$ kan skrivas som en produkt av irreducibla faktorer.*

Bevis. Om α inte är ett irreducibelt element så innebär det att α kan faktoriseras som $\alpha = ab$ där varken a eller b är enheter. Från sats 6.11 vet vi att absolutbeloppet av normen av en enhet är 1 vilket medför att $1 < |N(a)| < |N(\alpha)|$ och $1 < |N(b)| < |N(\alpha)|$. Eftersom normen av faktorerna är heltal får vi genom upprepande av ovan förfarande en avtagande norm som efter ett ändligt antal upprepningar ger en ändlig faktorisering i irreducibla element. □

Vi kommer nu genom exempel på olika kvadratiska talkroppar $\mathbb{Q}(\sqrt{d})$ visa att faktorisering inte alltid är entydig. Vi inleder med två satser, där vi i den första kommer se några kvadratiska talkroppar $\mathbb{Q}(\sqrt{d})$ då $d < 0$ (imaginära kvadratiska talkroppar), där faktoriseringen ej är unik. I den andra satsen ser vi på motsvarande men då i kvadratiska talkroppar $\mathbb{Q}(\sqrt{d})$ då $d > 0$ (reella kvadratiska talkropparna). Observera att satserna inte täcker alla värden på d utan endast intervallet -30 till 30, därav ordet ”åtminstone” i satserna.

Sats 6.13. *[1, sats 4.11] Faktorisering i irreducibla faktorer är ej unik i den kvadratiska heltalsringen $\mathcal{O}_d$ för (åtminstone) dessa värden på d:*

$$-5, -6, -10, -13, -14, -15, -17, -21, -22, -23, -26, -29, -30.$$

Vi väljer att visa satsen i fallet då $d = -10$ men beviset kan göras på motsvarande sätt för de övriga värdena på d.

Bevis. I $\mathbb{Q}(\sqrt{-10})$ kan talet 14 faktoriseras på följande sätt:

$$14 = 2 \cdot 7 = (2 + \sqrt{-10})(2 - \sqrt{-10}).$$

Vi inleder genom att visa med hjälp av normen, att elementen $2, 7$ och $(2 \pm \sqrt{-10})$ är irreducibla i $\mathcal{O}_{-10}$. Eftersom $-10 \not\equiv 1 \pmod 4$ ger sats 5.8 att elementen i $\mathcal{O}_{-10}$ kan skrivas på formen $a + b\sqrt{-10}$ där $a, b \in \mathbb{Z}$. Vi får normen

$$N(a + b\sqrt{-10}) = a^2 + 10b^2.$$

Vi beräknar $N(2) = 4, N(7) = 49$ och $N(2 \pm \sqrt{-10}) = 14$. Vidare antar vi att $2, 7$ och $(2 \pm \sqrt{-10})$ *inte* är irreducibla, vilket innebär att vi kan skriva $2 = xy$

där $x, y \in \mathcal{O}_{-10}$ och ej är enheter. Vi får då $N(2) = 4 = N(x)N(y)$ så $N(x) = 2$ och $N(y) = 2$ eftersom normen är positiv i detta fall. Vi använder samma typ av resonemang på de andra elementen vilket innebär att 7 måste ha icke-triviala delare med norm 7 och $(2 \pm \sqrt{-10})$ måste ha icke-triviala delare med norm 2 och 7. Sammantaget innebär det att

$$a^2 + 10b^2 = 2 \text{ eller } 7 \quad (a, b \in \mathbb{Z}).$$

Om $|b| \geq 1$ medför det att $a^2 + 10b^2 \geq 10$ som är mer än både 2 och 7 så enda möjligheten är att $|b| = 0$ och vi får att $a^2 = 2$ eller 7 vilket innebär att $a \notin \mathbb{Z}$. Således existerar inga icke-triviala delare och de fyra elementen är alla irreducibla. Eftersom $N(2) = 4$ och $N(2 \pm \sqrt{-10}) = 14$ ger sats 6.11 att 2 och $(2 \pm \sqrt{-10})$ ej är associerade så därmed är faktoriseringen ej unik. □

Sats 6.14. *[1] Faktorisering i irreducibla faktorer är ej unik i den kvadratiska heltalsringen $\mathcal{O}_d$ för (åtminstone) dessa värden på d:*

$$10, 15, 26, 30.$$

Bevis. I $\mathbb{Q}(\sqrt{15})$ kan talet 10 faktoriseras på följande sätt:

$$10 = 2 \cdot 5 = (5 + \sqrt{15})(5 - \sqrt{15}).$$

Genom att använda samma resonemang som i beviset innan (sats 6.13), kan vi bevisa att $2, 5$ och $(5 \pm \sqrt{15})$ är irreducibla genom att visa att

$$a^2 - 15b^2 = \pm 2 \text{ eller } \pm 5$$

inte har några heltalslösningar, $a, b \in \mathbb{Z}$. På grund av minustecknet är det inte lika lätt att säga något om värdet på $|b|$ som vi gjorde i förra beviset så istället tittar vi på fallen separat. Vi börjar med fallet

$$a^2 - 15b^2 = \pm 5. \tag{6.15}$$

Vi ser att $5 \mid a^2$ så enligt Euklides lemma får vi att $5 \mid a$ och vi kan skriva $a = 5 \cdot k$ där $k \in \mathbb{Z}$. Insättning i (6.15) ger

$$25k^2 - 15b^2 = \pm 5$$

som är ekvivalent med

$$5k^2 - 3b^2 = \pm 1.$$

Vi övergår till att räkna modulo 5 och får

$$-3b^2 \equiv \pm 1 \pmod 5.$$

Vidare undersöker vi om ekvationen har några heltalslösningar genom att sätta upp tabellen för modulo 5:

b	0	1	2	3	4
$-3b^2$	0	2	3	3	2

och vi ser att $-3b^2 \not\equiv \pm 1 \pmod 5$ vilket innebär att ekvation (6.15) saknar heltalslösningar.

Vidare undersöker vi det andra fallet,

$$a^2 - 15b^2 = \pm 2. \tag{6.16}$$

Med hjälp av samma resonemang som i första fallet får vi att $a = 2k$ där $k \in \mathbb{Z}$. Insättning i (6.16) ger

$$4k^2 - 15b^2 = \pm 2$$

som är ekvivalent med

$$-15b^2 \equiv \pm 2 \pmod 4.$$

Vi sätter upp tabellen för modulo 4:

b	0	1	2	3
$-15b^2$	0	1	0	1

och ser att $-15b^2 \not\equiv \pm 2 \pmod 4$ vilket innebär att ekvation (6.16) även i detta fallet saknar heltalslösningar. Således existerar inga icke-triviala delare och $2, 5$ och $(5 \pm \sqrt{15})$ är alla irreducibla element. Eftersom $N(2) = 4$ och $N(5 \pm \sqrt{15}) = 10$ ger sats 6.11 att 2 och $(5 \pm \sqrt{15})$ ej är associerade så därmed är faktoriseringen ej unik. □

6.3 Euklidiska ringar

Vi kommer nu titta på en alldeles egen klass av ringar, de så kallade euklidiska ringarna, där faktorisering i dessa ringar alltid är entydig. Euklidiska ringar är en klass av ringar där Euklides algoritm kan tillämpas. Vi kommer senare i kapitlet att påminna oss om vad Euklides algoritm är för något samt titta på vilka kvadratiska heltalsringar som är euklidiska. I denna uppsats begränsar vi oss till de norm-euklidiska ringarna så låt oss inleda med en definition av begreppet norm-euklidisk.

Definition 6.17. [1, definition 4.15] $\mathcal{O}_d$ är norm-euklidisk om det för varje $\alpha, \beta \in \mathcal{O}_d \backslash \{0\}$ existerar $q, r \in \mathcal{O}_d$ så att $\alpha = q\beta + r$ med $|N(r)| < |N(\beta)|$.

Man säger att absolutbeloppet av normen, $|N|$, utgör den euklidiska värderingen på $\mathcal{O}_d$.

Vi kommer nu titta på en sats som säger vilka kvadratiska heltalsringar $\mathcal{O}_d$ som är norm-euklidiska i fallet då $d < 0$.

Sats 6.18. *[1, sats 4.19] Den kvadratiska heltalsringen $\mathcal{O}_d$ är norm-euklidisk när $d = -1, -2, -3, -7, -11$.*

Bevis. Vi väljer två godtyckliga element $\alpha, \beta \in \mathcal{O}_d \backslash \{0\}$ och kommer här visa att det existerar $q, r \in \mathcal{O}_d$ så att $\alpha = q\beta + r$ med $|N(r)| < |N(\beta)|$ (jmf definition 6.17).

Vi börjar med att dividerar elementen och får

$$\frac{\alpha}{\beta} = s + t\sqrt{d}, \text{ där } s, t \in \mathbb{Q}.$$

I fallet då $d \not\equiv 1 \pmod 4$ skriver vi heltalen i $\mathcal{O}_d$ (enligt sats 5.8) på formen $\kappa = x + y\sqrt{d}$ där $x, y \in \mathbb{Z}$. Vi låter nu x och y vara närmaste heltalen till s respektive t, så

$$\begin{cases} s = x + u \\ t = y + v \end{cases}$$

där $x, y \in \mathbb{Z}$ och $|u|, |v| \leq |\frac{1}{2}|$.

Vi får

$$\frac{\alpha}{\beta} = (x + u) + (y + v)\sqrt{d} = (x + y\sqrt{d}) + (u + v\sqrt{d}).$$

Då

$$\alpha = \underbrace{(x + y\sqrt{d})}_{q}\beta + \underbrace{(u + v\sqrt{d})\beta}_{r}$$

och eftersom $\alpha, \beta, q \in \mathcal{O}_d$ medför det att $r = \alpha - q\beta \in \mathcal{O}_d$.

Slutligen har vi att

$$N(r) = N(u + v\sqrt{d}) \cdot N(\beta)$$

där

$$N(u + v\sqrt{d}) = u^2 - dv^2 \leq (\tfrac{1}{2})^2 - d(\tfrac{1}{2})^2 = (\tfrac{1}{4}) - d(\tfrac{1}{4}) < 1$$

i fallen då $d = -1$ eller -2, vilket ger att $N(r) < N(\beta)$.

I de resterande tre fallen är $d \equiv 1 \pmod 4$ och vi skriver heltalen i $\mathcal{O}_d$ (enligt sats 5.8) på formen $\kappa = x + y\left(\frac{1+\sqrt{d}}{2}\right)$ där $x, y \in \mathbb{Z}$. Vi väljer y som närmaste heltalet

till $2t$ och x som närmaste heltalet till $s - \frac{1}{2}y$, så

$$\begin{cases} s - \frac{1}{2}y = x + u \\ 2t = y + v \end{cases} \quad \Leftrightarrow \quad \begin{cases} s = x + \frac{1}{2}y + u \\ t = \frac{1}{2}y + \frac{1}{2}v \end{cases}$$

där $x, y \in \mathbb{Z}$ och $|u|, |v| \leq |\frac{1}{2}|$.

Vi får

$$\frac{\alpha}{\beta} = x + \tfrac{1}{2}y + u + \big(\tfrac{1}{2}y + \tfrac{1}{2}v\big)\sqrt{d} = x + y\Big(\frac{1+\sqrt{d}}{2}\Big) + \big(u + \tfrac{1}{2}v\sqrt{d}\big)$$

Då

$$\alpha = \underbrace{\Big(x + y\Big(\frac{1+\sqrt{d}}{2}\Big)\Big)}_{q}\beta + \underbrace{\big(u + \tfrac{1}{2}v\sqrt{d}\big)\beta}_{r}$$

och eftersom $\alpha, \beta, q \in \mathcal{O}_d$ medför det att $r = \alpha - q\beta \in \mathcal{O}_d$.

Slutligen har vi att

$$N(r) = N(u + \tfrac{1}{2}v\sqrt{d}) \cdot N(\beta)$$

där

$$N(u + \tfrac{1}{2}v\sqrt{d}) = u^2 - \tfrac{1}{4}dv^2 \leq (\tfrac{1}{2})^2 - \tfrac{1}{4}d(\tfrac{1}{2})^2 = (\tfrac{1}{4}) - d(\tfrac{1}{16}) < 1$$

i fallen då $d = -3, -7$ eller -11, vilket ger att $N(r) < N(\beta)$. □

Vi ger nu två exempel, det första när $d = -1$ och det andra när $d = -3$.

Exempel 6.19. Låt $\alpha = 2 + 5\sqrt{-1}$ och $\beta = 1 + \sqrt{-1}$. Vi börjar med att dividera elementen och förlänger sen med konjugatet. Vi får

$$\frac{\alpha}{\beta} = \frac{2 + 5\sqrt{-1}}{1 + \sqrt{-1}} = \frac{2 + 5\sqrt{-1}}{1 + \sqrt{-1}} \cdot \frac{1 - \sqrt{-1}}{1 - \sqrt{-1}} = \frac{7 + 3\sqrt{-1}}{2} = \frac{7}{2} + \frac{3}{2}\sqrt{-1}.$$

Vi väljer $x = 4$ och $y = 2$ som närmaste heltalen till $\frac{7}{2}$ respektive $\frac{3}{2}$ och kan skriva

$$\frac{\alpha}{\beta} = 4 + 2\sqrt{-1} + \Big(-\frac{1}{2} - \frac{1}{2}\sqrt{-1}\Big)$$

som är ekvivalent med

$$\alpha = \underbrace{(4 + 2\sqrt{-1})}_{q}\beta \underbrace{-\sqrt{-1}}_{r}.$$

Vi beräknar $N(r)$ och $|N(\beta)|$ till 1 respektive 2 och således har vi att $N(r) < |N(\beta)|$.

Vi noterar att vi även kunde ha valt $x = 3$ och $y = 1$ som närmaste heltal och då hade vi istället fått q' och r' där

$$\alpha = \underbrace{(3 + \sqrt{-1})}_{q'}\beta + \underbrace{\sqrt{-1}}_{r'}.$$

Vi noterar att $N(r) = N(r')$ så därmed är även $N(r') < |N(\beta)|$.

Exempel 6.20. I fallet när $d = -3$ har vi $-3 \equiv 1 \pmod 4$ vilket innebär att q och r skrivs på formen $x + y\big(\frac{1+\sqrt{-3}}{2}\big)$ där $x, y \in \mathbb{Z}$. Vi låter $\alpha = 2 + 5\sqrt{-3}$ och $\beta = 1 + \sqrt{-3}$ och följer samma tillvägagångssätt som i föregående exempel där

$$\frac{\alpha}{\beta} = \frac{2 + 5\sqrt{-3}}{1 + \sqrt{-3}} = \frac{17 + 3\sqrt{-3}}{4}.$$

Vi väljer y som närmaste heltalet till $2 \cdot \frac{3}{4}$, alltså 2. Slutligen väljer vi x som närmaste heltalet till $\frac{17}{4} - \frac{2}{2}$, alltså 3. Därmed kan vi skriva

$$\frac{\alpha}{\beta} = 3 + 2\big(\frac{1 + \sqrt{-3}}{2}\big) + \big(\frac{1}{4} - \frac{1}{4}\sqrt{-3}\big)$$

som är ekvivalent med

$$\alpha = \underbrace{\Big(3 + 2\big(\frac{1 + \sqrt{-3}}{2}\big)\Big)}_{q}\beta + \underbrace{1}_{r}.$$

Avslutningsvis beräknar vi $|N(r)|$ och $|N(\beta)|$ till 1 respektive 10 och således har vi $|N(r)| < |N(\beta)|$.

Vi kommer i slutet av detta kapitel visa en mycket viktig sats som säger att varje norm-euklidisk heltalsring har entydig faktorisering, men för att kunna göra det behöver vi först känna till två andra satser, ett lemma och följande definition:

Definition 6.21. [7, s.75] Om $\alpha, \beta \in \mathcal{O}_d$ och $\alpha, \beta \neq 0$ då är η största gemensamma delare, $SGD(\alpha, \beta)$, till α och β förutsatt att:

1. $\eta \mid \alpha$ och $\eta \mid \beta$,
2. om $\kappa \mid \alpha$ och $\kappa \mid \beta$ för något $\kappa \in \mathcal{O}_d$ så gäller att $\kappa \mid \eta$.

Det första villkoret i definitionen säger att η är en gemensam delare till α och β medan det andra villkoret säger att η även är den största delaren, därav namnet största gemensamma delare.

Om η_1 och η_2 båda är $SGD(\alpha, \beta)$ så är η_1 och η_2 associerade, d.v.s. de skiljer med en enhet. Vi visar detta påstående genom att använda oss av villkor 1 och 2

i definition 6.21. Om både η_1 och η_2 är $SGD(\alpha, \beta)$ så har vi enligt villkor 1 att $\eta_1 \mid \alpha$ och $\eta_1 \mid \beta$. Eftersom η_2 är en största gemensam delare ger villkor 2 att $\eta_1 \mid \eta_2$ och enligt definition 6.1 om delbarhet kan vi skriva $\eta_2 = x\eta_1$ där $x \in R$. På samma sätt får vi att $\eta_2 \mid \eta_1$ och vi kan skriva $\eta_1 = y\eta_2$ där $y \in R$. Sammantaget har vi då att $\eta_2 = x\eta_1 = xy\eta_2$ som medför att $n_2(1 - xy) = 0$. Eftersom R inte har några nolldelare så måste $1 - xy = 0$ som i sin tur ger att $xy = 1$, så enligt definition 6.2 är både x och y enheter. Eftersom $\eta_1 = x\eta_2$ och x är en enhet får vi enligt definition 6.3 att η_1 och η_2 är associerade.

Anmärkning 6.22. Vi låter $SGD(\alpha, \beta)$ beteckna mängden av alla största delare till α och β. Som vi precis visade i avsnittet innan så är samtliga element i denna mängd associerade med varandra.

Lemma 6.23. *Låt $\alpha, \beta \in \mathcal{O}_d$. Om $\alpha = q\beta + r$ där $q, r \in \mathcal{O}_d$ så är $SGD(\alpha, \beta) = SGD(\beta, r)$.*

Bevis. Låt $\eta \in \mathcal{O}_d$. Om η_1 delar α och β så delar η_1 även r eftersom r kan skrivas som en linjärkombination av α och β, där $r = \alpha - q\beta$. Omvänt, om η_2 delar r och β så delar η_2 även α eftersom $\alpha = q\beta + r$. Så de gemensamma delarna till α och β respektive β och r är alltså desamma, d.v.s. $SGD(\alpha, \beta) = SGD(\beta, r)$. □

Sats 6.24. *Om $\mathcal{O}_d$ är norm-euklidisk och $\alpha, \beta \in \mathcal{O}_d$ och $\alpha, \beta \neq 0$, så finns en största gemensam delare η som kan skrivas som en linjärkombination av α och β, d.v.s. det finns $x, y \in \mathcal{O}_d$, sådana att $\eta = \alpha x + \beta y$.*

Vårt bevis av ovanstående sats kommer följa samma upplägg som motsvarande bevis för heltalen $\mathbb{Z}$, jämför [7, s. 79] som bygger på Euklides algoritm.

Bevis. Låt $\alpha, \beta \in \mathcal{O}_d$ och $\alpha, \beta \neq 0$. För att finna $\eta \in SGD(\alpha, \beta)$ tillämpar vi divisionsalgoritmen i definition 6.17 upprepade gånger och på så sätt utför vi Euklides algoritm:

$$
\begin{aligned}
\alpha &= q_1\beta + r_1 && |N(r_1)| < |N(\beta)| \\
\beta &= q_2 r_1 + r_2 && |N(r_2)| < |N(r_1)| \\
r_1 &= q_3 r_2 + r_3 && |N(r_3)| < |N(r_2)| \\
&\vdots && \vdots \\
r_{m-3} &= q_{m-1} r_{m-2} + r_{m-1} && |N(r_{m-1})| < |N(r_{m-2})| \\
r_{m-2} &= q_m r_{m-1} + r_m && |N(r_m)| < |N(r_{m-1})| \\
r_{m-1} &= q_{m+1} r_m
\end{aligned}
$$

Processsen slutar med resten 0 efter ett ändligt antal steg eftersom resterna bildar en avtagande följd av heltal där

$$|N(\beta)| > |N(r_1)| > |N(r_2)| > ... > |N(r_{m-1}| > |N(r_m)| \geq 0.$$

Enligt lemma 6.23 gäller att

$$SGD(\alpha, \beta) = SGD(\beta, r_1) = SGD(r_1, r_2) = ... = SGD(r_{m-1}, r_m) = SGD(r_m, 0).$$

Så den sista nollskilda resten är r_m så alltså är $\eta = r_m \in SGD(\alpha, \beta)$.

För att visa att r_m kan skrivas som en linjärkombination av α och β gör vi Euklides algoritm baklänges. Vi utgår från näst sista raden och jobbar oss uppåt:

$$r_m = r_{m-2} - q_m r_{m-1} = x_m r_{m-2} + y_m r_{m-1} \quad \text{där } x_m = 1 \text{ och } y_m = -q_m.$$

Använder vi nu $r_{m-1} = r_{m-3} - q_{m-1} r_{m-2}$ får vi

$$r_m = x_{m-1} r_{m-3} + y_{m-1} r_{m-2} \quad \text{där } x_{m-1} = -q_m \text{ och } y_{m-1} = 1 + q_m q_{m-1}.$$

Genom att upprepade gånger sätta in ekvationerna i varandra på detta sätt får vi slutligen r_m som en linjärkombination av α och β

$$r_m = x_1 \alpha + y_1 \beta$$

där $x_1, y_1 \in \mathcal{O}_d$. □

Sats 6.25. *Om $\mathcal{O}_d$ är norm-euklidisk är varje irreducibelt element p ett primelement.*

Vi kommer följa samma upplägg som i beviset av Euklides lemma (sats 2.4) med den skillnaden att vi nu låter p vara ett irreducibelt element istället för ett primtal.

Bevis. Vi antar att p är ett irreducibelt element. Vi vill visat att p är ett primelement, d.v.s. om $p \mid \alpha\beta$ där $\alpha, \beta \in \mathcal{O}_d$ så medför det att $p \mid \alpha$ eller $p \mid \beta$. Om $p \mid \alpha$ så är vi klara. Därför tittar vi på fallet då $p \nmid \alpha$ och visar att $p \mid \beta$. Om $p \nmid \alpha$ så är en största gemensam delare till p och α lika med 1 eftersom p endast har delare associerade med p och enheter. Sats 6.24 ger att

$$xp + y\alpha = 1 \text{ där } x, y \in \mathcal{O}_d.$$

Multiplikation med β på båda sidor ger

$$xp\beta + y\alpha\beta = \beta.$$

Eftersom vi antog att $p \mid \alpha\beta$ ger det att vänsterledet är delbart med p och således måste även högerledet vara det, vilket i sin tur ger att $p \mid \beta$ och vi har således visat att varje irreducibelt element $p \in \mathcal{O}_d$ är ett primelement då $\mathcal{O}_d$ är norm-euklidisk. □

Vi närmar oss slutet på kapitlet och är nu redo att visa nedanstående mycket viktiga sats.

Sats 6.26. *[1, sats 4.16 och 4.17] Om $\mathcal{O}_d$ är norm-euklidisk så har $\mathcal{O}_d$ unik faktorisering.*

För beviset av ovan sats kommer vi följa samma upplägg som i beviset av Aritmetikens fundamentalsats 2.5 för heltalen $\mathbb{Z}$, även här med den skillnaden att vi låter p vara ett irreducibelt element istället för ett primtal.

Bevis. Från sats 6.25 har vi att varje irreducibelt element, då $\mathcal{O}_d$ är norm-euklidisk, är ett primelement. Vi gör ett motsägelsebevis och antar att elementet $\alpha \in \mathcal{O}_d$ kan faktoriseras på följande två sätt:

$$p_1p_2p_3...p_r = \alpha = q_1q_2q_3...q_s \quad \text{där alla } p_i, q_i \text{ är primelement.}$$

Eftersom p_1 är ett primelement medför det att p_1 delar någon av $q_1, q_2, ..., q_s$, säg q_i. Och eftersom q_i endast har delare associerade med q_i eller enheter medför det att p_1 är associerad med q_i. Om vi ändrar om på ordningen och modifierar faktorerna med lämplig enhet samt indexerar så att $q_1 = p_1$ kan vi anta att $p_1 \mid q_1$ och division med p_1 reducerar likheten till

$$p_2p_3...p_r = \alpha = q_2q_3...q_s.$$

Med upprepad användning av Euklides lemma tills samtliga faktorer är matchade ser vi att faktorisering i $\mathcal{O}_d$ är entydig då $\mathcal{O}_d$ är norm-euklidisk. □

Vi kommer nu lite kort nämna den euklidiska heltalsringen $\mathbb{Z}[i]$, även kallad de Gaussiska heltalen, uppkallad efter matematikern Carl Friedrich Gauss som mycket grundligt och rigoröst bevisade att $\mathbb{Z}[i]$ har entydig faktorisering.

Definition 6.27. [1, s. 4] Ett Gaussiskt heltal är ett komplext tal z på formen $z = x + iy$ där $x, y \in \mathbb{Z}$.

Eftersom $i = \sqrt{-1}$ motsvarar den Gaussiska heltalsringen $\mathbb{Z}[i]$ den kvadratiska heltalsringen $\mathbb{Z}[\sqrt{-1}]$. Sats 6.18 och sats 6.26 ger oss följande sats:

Sats 6.28. *Den Gaussiska heltalsringen $\mathbb{Z}[i]$ har unik faktorisering.*

Vi ger här ett exempel på en faktorisering i irreducibla element i de Gaussiska heltalen.

Exempel 6.29. Vi har t.ex. följande faktorisering i $\mathbb{Z}[i]$

$$-6 + 58i = (1 + i)^3(2 - i)^2(4 + i).$$

Eftersom $N(1+i) = 2, N(2-i) = 5$ och $N(4+i) = 17$, där samtliga är primtal, ger sats 6.11 att faktorerna är irreducibla. Så detta är ett exempel på en faktorisering i irreducibla element i $\mathbb{Z}[i]$.

6.4 Tillämpning på en diofantisk ekvation

Vi kommer nu visa hur vi med hjälp av entydig faktorisering hos de Gaussiska heltalen kan lösa den diofantiska ekvationen

$$y^2 + 49 = z^3. \tag{6.30}$$

Ekvation (6.30) kan inte faktoriseras i $\mathbb{Z}$ och därmed inte lösas på samma sätt som vi tidigare gjorde i exempel 2.6 där vi löste en diofantisk ekvation med hjälp av entydig faktorisering. Istället väljer vi att faktorisera vänsterledet i $\mathbb{Z}[i]$ där

$$(y + 7i)(y - 7i) = z^3.$$

Vi undersöker om det finns en gemensam faktor $a + bi$ där $a, b \in \mathbb{Z}$ till $y + 7i$ och $y - 7i$. En sådan gemensam faktor är även en faktor till dess summa och differens och vi skriver

$$\begin{cases} a + bi \mid 2y \\ a + bi \mid 14i \end{cases}.$$

Vi använder oss av normen och får

$$\begin{cases} a^2 + b^2 \mid 4y^2 \\ a^2 + b^2 \mid 14^2 \end{cases}. \tag{6.31}$$

Primtalsfaktorisering ger att $14^2 = 2^2 \cdot 7^2$ så vi börjar med att undersöka om 7 kan vara en faktor till $a^2 + b^2$. Om $7 \mid y$ medför det att $y = 7k$ där $k \in \mathbb{Z}$. Insättning i ekvation (6.30) ger att vänsterledet är delbart med 7 och således måste också högerledet vara det, vilket medför att $7 \mid z$. Vi låter $z = 7m$ där $m \in \mathbb{Z}$ och insättning i (6.30) ger

$$(7k)^2 + 49 = (7m)^3.$$

Vi förkortar med 49 på båda sidor och får

$$k^2 + 1 = 7m^3$$

som medför att

$$k^2 + 1 \equiv 0 \pmod 7.$$

Vi undersöker möjliga värden på k modulo 7

k	0	1	2	3	4	5	6
$k^2 + 1$	1	2	5	3	3	5	2

och noterar att $k^2 + 1 \not\equiv 0 \pmod 7$ vilket innebär att $7 \nmid y$. Vi återgår till (6.31) och enligt Euklides lemma (sats 2.4) innebär det att $a^2 + b^2 \mid 4$ vilket medför att $a^2 + b^2 = 1, 2$ eller 4. Vi kommer nu undersöka dessa tre fallen.

Om $a^2 + b^2 = 2$ har vi att $a = \pm 1$ och $b = \pm 1$ där lösningarna endast skiljer sig åt med en enhet så det räcker att vi tittar på en av lösningarna, säg $1 + i$. Vi undersöker om $1+i \mid z^3$ och använder oss av normen och får att $2 \mid z^6$ vilket innebär att z måste vara ett jämnt tal. Det medför att högerledet i (6.30) är delbart med 8 och således även vänsterledet och vi får

$$y^2 + 1 \equiv 0 \pmod 8.$$

Vi undersöker möjliga värden på y modulo 8

y	0	1	2	3	4	5	6	7
y^2+1	1	2	5	2	1	2	5	2

och ser att $y^2 + 1 \not\equiv 0 \pmod 8$. Alltså kan inte $a^2 + b^2 = 2$.

I fallet då $a^2 + b^2 = 4$ har vi lösningarna $a = 0, b = \pm 2$ och $a = \pm 2, b = 0$ som samtliga också har en norm som är delbar med 2 och med samma resonemang som ovan kan alltså inte $a^2 + b^2 = 4$.

Då kvarstår enda möjligheten, att $a^2 + b^2 = 1$. I detta fall får vi lösningarna $a = \pm 1, b = 0$ och $a = 0, b = \pm 1$ som samtliga har normen 1, så sats 6.11 ger att $a^2 + b^2$ är en enhet vilket innebär att $y + 7i$ och $y - 7i$ är relativt prima.

Eftersom vi enligt sats 6.28 har unik faktorisering i $\mathbb{Z}[i]$ måste produkten av $y+7i$ och $y - 7i$ vara en kub så en av faktorerna måste vara $u\alpha^3$ och den andra $u^{-1}\beta$ där u är en enhet och $\alpha, \beta \in \mathbb{Z}[i]$.

Vi antar att $y + 7i = u\alpha^3$ och låter $\alpha = c + di$ där $c, d \in \mathbb{Z}$. Eftersom samtliga $u = \pm 1, \pm i$ är jämna kuber kan vi i själva verket skriva

$$y + 7i = (c + di)^3.$$

Vi jämför realdel och imaginärdel och får

$$\begin{cases} y = c(c^2 - 3d^2) \\ 7 = d(3c^2 - d^2) \end{cases}$$

där vi från andra ekvationen ser att $d = \pm 1$ och ± 7. Vi beräknar c i dessa fyra fallen och får endast heltalslösningarna $c = \pm 4$ i fallet då $d = -7$. Med hjälp av första ekvationen beräknar vi $y = \pm 524$ och insättning i ekvation (6.30) ger

$$\begin{aligned} (\pm 524)^2 + 49 &= z^3 \\ \Leftrightarrow z &= 65. \end{aligned}$$

Vi har alltså med hjälp av entydig faktorisering hos de Gaussiska heltalen visat följande sats:

Sats 6.32. *De enda heltalslösningarna till ekvationen*

$$y^2 + 49 = z^3$$

är $y = \pm 524$, $z = 65$.

7 Avslutning

Avslutningsvis kan vi konstatera att vi genom Aritmetikens fundamentalsats har entydig faktorisering i heltalen $\mathbb{Z}$ men att satsen *inte* gäller allmänt för heltalsringar i talkroppar. Detta kunde vi visa genom exempel i de kvadratiska talkropparna där vi såg att entydig faktorisering snarare var ett undandag än en regel. Slutligen tittade vi på de norm-euklidiska heltalsringarna, där faktoriseringen alltid är unik, där vi genom tillämpning av entydig faktorisering hos de Gaussiska heltalen kunde lösa en diofantisk ekvation.

Referenser

[1] Ian Stewart & David Tall, *Algebraic Number Theory and Fermat's Last Theorem,* 4:th edition, CRC Press Taylor & Francis Group, 2016.

[2] Norman L. Biggs, *Discrete Mathematics,* 2:nd edition, Oxford University Press, 2002.

[3] Wikipedia, Ring (matematik), hämtad 2021-02-10.

[4] Wikipedia, Kroppsutvidgning, hämtad 2021-02-10.

[5] John R. Durbin, *Modern Algebra An Introduction*, 6:th edition, John Wiley & Sons, 2009.

[6] Wikipedia, Algebraiska tal, hämtad 2021-02-10.

[7] Rikard Bøgvad, Qimh Xantcha & Håkan Granath, *Algebra 1*, Matematiska institutionen, Stockholms universitet, 2018.

[8] Wikipedia, Transcendenta tal, hämtad 2021-04-06.

[9] Wikipedia, Pythagoras sats, hämtad 2021-05-06.