SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Skevkroppar

av

Lisa Nicklasson

2012 - No 11

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Skevkroppar

Lisa Nicklasson

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Rikard Bögvad

2012

Sammanfattning

Kroppar har många trevliga egenskaper, bland annat att varje element har en invers. Men man kräver också att multiplikationen ska vara kommutativ och associativ. I denna uppsats ska vi undersöka vad som händer om man inte längre kräver att multiplikationen är kommutativ. Då får vi, som titeln lovar, vad som kallas en skevkropp. Men finns det sådana? Och hur ser de i så fall ut?

Innehåll

1 Inledning

Denna uppsats behandlar ämnet skevkroppar.
Som bekant har kroppar trevliga egenskaper, så som att varje element har en multiplikativ invers.
I kroppar som $\mathbb{R}$ och $\mathbb{C}$ är det lätt att bestämma inversen till ett tal. Men även i ändliga kroppar kan vi vara säkra på att varje element har en multiplikativ invers. Till exempel har elementet 5 i den ändliga kroppen $\mathbb{Z}_7$ inversen 3, eftersom $5 \cdot 3 = 15 \equiv 1(mod\ 7)$.
I en kropp gäller att multiplikation är både kommutativ och associativ.
Låt oss säga att vi vill behålla egenskapen att varje element har en invers, men släppa kravet på kommutativitet. Då får vi vad som kallas en skevkropp, eller divisionsring.
Det första man bör fråga sig är om detta ens är möjligt: Finns det skevkroppar? När vi visat att så faktiskt är fallet, genom att se på ett exempel, kan vi gå vidare och studera skevkropparnas egenskaper. Bland annat ska vi visa att varje ändlig skevkropp måste vara kommutativ.

En annan känd egenskap hos kroppar är att man för varje nolldelarfri ring R kan konstruera en minsta kropp, en så kallad fraktionskropp, som har R som delring. Till exempel kan man på så sätt konstuera de rationella talen med hjälp av heltalen.
Vi ska visa att en liknande konstruktion är möjlig även för skevkroppar.

2 Grundläggande begrepp

Innan vi börjar studera skevkroppar och deras egenskaper behöver vi några grundläggande resultat. Bland annat denna sats från gruppteorin.

Sats 1. *(**Lagrange**) Låt H vara en delgrupp av en ändlig grupp G, och låt $|H| = m$, $|G| = n$. Då är $m|n$.*

För bevis, se [1].

Tag till exempel den additiva gruppen $\mathbb{Z}_{100}$ som har 100 element. Följande tabell visar alla delgrupper av denna.

delgrupp	antal element
$2\mathbb{Z}_{100} = \{0, 2, 4, \dots 98\}$	50
$4\mathbb{Z}_{100} = \{0, 4, 8 \dots 96\}$	25
$5\mathbb{Z}_{100} = \{0, 5, 10 \dots 95\}$	20
$10\mathbb{Z}_{100} = \{0, 10, 20, \dots 90\}$	10
$20\mathbb{Z}_{100} = \{0, 20, 40, 60, 80\}$	5
$25\mathbb{Z}_{100} = \{0, 25, 50, 75\}$	4
$50\mathbb{Z}_{100} = \{0, 50\}$	2

Antalet element i varje delgrupp delar 100, precis som Lagranges sats lovar.

Antalet sidoklasser av en delgrupp H av G kallas *index* av H i G och betecknas $[G : H]$.
Om $|H| = m$ och $|G| = n$ är $[G : H] = \frac{n}{m}$.
Tag till exempel delgruppen $4\mathbb{Z}_{100}$ av $\mathbb{Z}_{100}$. Denna har sidoklasserna

$$1 + 4\mathbb{Z}_{100} = \{1, 5, 9, \dots 97\}$$

$$2 + 4\mathbb{Z}_{100} = \{2, 6, 10, \dots 98\}$$

$$3 + 4\mathbb{Z}_{100} = \{3, 7, 11, \dots 99\}$$

och $4\mathbb{Z}_{100}$ själv, alltså fyra stycken. Vi har

$$[\mathbb{Z}_{100} : 4\mathbb{Z}_{100}] = \frac{100}{25} = 4.$$

Vi behöver också följande resultat om kroppar.
Låt K vara en kropp och F en delkropp av K. Då kan K beskrivas som ett

vektorrum över F. [6, s. 131]
Till exempel är ju $\mathbb{C}$ ett vektorrum med basen $\{1, i\}$ över $\mathbb{R}$.
Om K och F är ändliga är förstås dimensionen av K som vektorrum över F också ändlig. Låt säga att dimensionen är n, och att F har q element, för heltal n och q. Då har K q^n element:
Låt $v_1, v_2, \ldots, v_n \in K$ utgöra en bas i vektorrummet. Då kan varje element i K på ett entydigt sätt skrivas som

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n.$$

F har q element, så för varje α_i finns q val. Alltså är $|K| = q^n$.

Nu kan det vara på sin plats med definitionen av en skevkropp.

Definition 1. *En **skevkropp** är en mängd K tillsammans med två binära operationer $+$ och $\cdot$ som uppfyller följande villkor.*
Låt $a, b, c \in K$.

- *Addition är associativ:* $a + (b + c) = (a + b) + c$
- *Addition är kommutativ:* $a + b = b + a$
- *Det finns ett element 0 så att $x + 0 = 0 + x = x$ för varje $x \in K$.*
- *För varje element $x \in K$ finns en additiv invers $-x$, det vill säga $x + (-x) = (-x) + x = 0$.*
- *Multiplikation är associativ:* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- *Det finns ett element 1 sådant att $1 \neq 0$ och $x \cdot 1 = 1 \cdot x = x$ för varje $x \in K$.*
- *För varje element $x \in K$ finns en multiplikativ invers x^{-1}, det vill säga $x \cdot x^{-1} = x^{-1} \cdot x = 1$.*
- *Multiplikation distribuerar över addition:* $a \cdot (b + c) = a \cdot b + a \cdot c$ *och* $(a + b) \cdot c = a \cdot c + b \cdot c$.

En skevkropp uppfyller alltså alla villkoren för en kropp, förutom just kommutativa lagen för multiplikation.
Man kan också säga att en skevkropp är en ring där 1 existerar (och ej är 0) och varje element har en multiplikativ invers. Därav den ekvivalenta benämningen *divisionsring*.

3 Kvaternioner

Det första kända exemplet på en icke kommutativ skevkropp är kvaternionerna. Dessa introducerades av William Rowan Hamilton. Hamilton hade länge försökt komma på ett sätt att multiplicera tredimensionella vektorer. När han, under en promenad den 16 oktober 1843, slutligen insåg att han behövde en fjärde dimension kunde han inte motstå impulsen att ta fram sin kniv och rista in

$$i^2 = j^2 = k^2 = ijk = -1$$

i bron han just passerade.
Denna ekvation beskriver hur baselementen multipliceras med varandra i Hamiltons fyrdimensionella algebra.

Mängden av kvaternioner betecknas $\mathbb{H}$ (efter Hamilton), och utgörs av vektorer i $\mathbb{R}^4$. Låt

$$1 = (1,0,0,0) \quad i = (0,1,0,0) \quad j = (0,0,1,0) \quad k = (0,0,0,1)$$

och

$$a_1 = (a_1,0,0,0) \quad a_2 i = (0,a_2,0,0) \quad a_3 j = (0,0,a_3,0) \quad a_4 k = (0,0,0,a_4).$$

Addition i $\mathbb{H}$ definieras, som i $\mathbb{R}^4$, av komponentvis addition. Vi har alltså att

$$a_1 + a_2 i + a_3 j + a_4 k = (a_1, a_2, a_3, a_4)$$

och

$$(a_1+a_2 i+a_3 j+a_4 k)+(b_1+b_2 i+b_3 j+b_4 k) = (a_1+b_1, a_2+b_2, a_3+b_3, a_4+b_4) =$$

$$= (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k.$$

Multiplikation med ett reellt tal r definieras också som för vektorer i $\mathbb{R}^4$:

$$r(a_1 + a_2 i + a_3 j + a_4 k) = r(a_1, a_2, a_3, a_4) = (ra_1, ra_2, ra_3, ra_4) =$$

$$= ra_1 + ra_2 i + ra_3 j + ra_4 k$$

$\mathbb{H}$ är en abelsk grupp under addition, och ett reellt vektorrum av dimension 4.

Multiplikation av baselementen definieras av att

$$1a = a1 = a \quad \text{för alla } a \in \mathbb{H},$$

$$i^2 = j^2 = k^2 = -1$$

och

$$ij = k, \quad jk = i, \quad ki = j, \quad ik = -j, \quad kj = -i, \quad ji = -k.$$

Multiplikation i $\mathbb{H}$ är alltså inte kommutativ, t.ex. är $ij \neq ji$.
Mängden $\{1, -1, i, -i, j, -j, k, -k\}$ bildar en grupp under multiplikation. Denna brukar kallas Q eller Q_8.
Lägg märke till att i här har precis samma egenskaper som $i \in \mathbb{C}$. Mängden av kvaternioner på formen $a_1 + a_2 i$ kan alltså identifieras med de komplexa talen.

För att distributiva lagen ska hålla måste multiplikation i $\mathbb{H}$ definieras som

$$(a_1 + a_2 i + a_3 j + a_4 k) \cdot (b_1 + b_2 i + b_3 j + b_4 k) =$$

$$= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) i +$$

$$+ (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) j + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) k.$$

Notera att $(a_1 + a_2 i + a_3 j + a_4 k) = (a_1 + a_2 i) + (a_3 + a_4 i) j$. Varje element i $\mathbb{H}$ kan alltså skrivas som $a + bj$ där $a, b \in \mathbb{C}$. Detta kan användas för att visa att multiplikation i $\mathbb{H}$ är associativ.
Låt $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{C}$.

$$((a_1 + a_2 j)(b_1 + b_2 j))(c_1 + c_2 j) =$$

$$= (a_1 b_1 + a_1 b_2 j + a_2 j b_1 + a_2 j b_2 j)(c_1 + c_2 j) =$$

$$= a_1 b_1 c_1 + a_1 b_2 j c_1 + a_2 j b_1 c_1 + a_2 j b_2 j c_1 + a_1 b_1 c_2 j + a_1 b_2 j c_2 j + a_2 j b_1 c_2 j + a_2 j b_2 j c_2 j =$$

$$= a_1 (b_1 c_1 + b_2 j c_1 + b_1 c_2 j + b_2 j c_2 j) + a_2 j (b_1 c_1 + b_2 j c_1 + b_1 c_2 j + b_2 j c_2 j) =$$

$$= (a_1 + a_2 j)((b_1 + b_2 j)(c_1 + c_2 j))$$

Det återstår nu att visa att varje element i $\mathbb{H}$ har en invers för att konstatera att $\mathbb{H}$ är en skevkropp.
Låt $a = a_1 + a_2 i + a_3 j + a_4 k$ vara en godtycklig kvaternion. Definiera *konjugatet* av a som

$$\overline{a} = a_1 - a_2 i - a_3 j - a_4 k$$

och *normen* som

$$|a| = \sqrt{a_1^2 + a_2^2 + a_3^2 + a_4^2}.$$

Då är

$$a\overline{a} = \overline{a}a = a_1^2 + a_2^2 + a_3^2 + a_4^2 = |a|^2.$$

Notera att $\frac{1}{|a|^2}$ är ett reellt tal och därmed också en kvaternion.

$$a \cdot \frac{\overline{a}}{|a|^2} = \frac{\overline{a}}{|a|^2} \cdot a = 1$$

så

$$\frac{\overline{a}}{|a|^2} \quad \text{är inversen till } a.$$

Detta är samma princip som för komplexa tal. Inversen till ett komplext tal $a + bi$ är ju just

$$\frac{a - bi}{a^2 + b^2} \ .$$

$\mathbb{H}$ är alltså en icke kommutativ skevkropp.

Skevkroppar uppför sig annorlunda jämfört med kroppar. Till exempel har ett polynom av grad n i $K[x]$, som bekant, högst n nollställen om K är en kropp. Detta är inte sant i $\mathbb{H}[x]$.
Till exempel är $i,\ j$ och k nollställen till polynomet $x^2 + 1$.
Vidare, om $x = a + bi + cj + dk$ är

$$x^2 = (a^2 - b^2 - c^2 - d^2) + (2ab)i + (2ac)j + (2ad)k,$$

så

$$x^2 = -1 \ \Rightarrow \ a = 0, \quad b^2 + c^2 + d^2 = 1$$

och därmed har polynomet $x^2 + 1$ oändligt många nollställen.

4 Oktonioner

Sats 2. *Om det finns en bilinjär produkt*

$$p : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$$

utan nolldelare måste n vara en potens av 2.

(Att produkten är bilinjär betyder att den distribuerar över addition, och om $\lambda \in \mathbb{R}$ och $a, b \in \mathbb{R}^n$ så är $p(\lambda a, b) = p(a, \lambda b) = \lambda p(a, b)$.)
För bevis, se [7].
För $n = 1$ har vi förstås vanlig multiplikation av reella tal. För $n = 2$ har vi multiplikation av komplexa tal.
Vi har även sett att en sådan produkt existerar för $n = 4$, nämnligen multiplikation av kvaternioner. Men då är produkten ej längre kommutativ.
Man kan då fråga sig hur det är med $n = 8$.
Som bekant kan komplexa tal skrivas som par av reella tal, och kvaternioner som par av komplexa tal. Om vi går vidare på samma sätt och konstruerar en ny algebra där varje element är ett par av kvaternioner får vi oktonionerna, eller Cayleytalen, som betecknas $\mathbb{O}$.
Varje oktonion är ett tal på formen

$$x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 + x_4 i_4 + x_5 i_5 + x_6 i_6 + x_7 i_7 \qquad x_0, \dots x_7 \in \mathbb{R}.$$

Eller som par av kvaternioner:

$$x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 + (x_6 + x_5 i_1 - x_7 i_2 + x_4 i_3) i_6$$

Multiplikation av baselementen ges här av följande tabell.

$\cdot$	1	i_1	i_2	i_3	i_4	i_5	i_6	i_7
1	1	i_1	i_2	i_3	i_4	i_5	i_6	i_7
i_1	i_1	-1	i_4	i_7	$-i_2$	i_6	$-i_5$	$-i_3$
i_2	i_2	$-i_4$	-1	i_5	i_1	$-i_3$	i_7	$-i_6$
i_3	i_3	$-i_7$	$-i_5$	-1	i_6	i_2	$-i_4$	i_1
i_4	i_4	i_2	$-i_1$	$-i_6$	-1	i_7	i_3	$-i_5$
i_5	i_5	$-i_6$	i_3	$-i_2$	$-i_7$	-1	i_1	i_4
i_6	i_6	i_5	$-i_7$	i_4	$-i_3$	$-i_1$	-1	i_2
i_7	i_7	i_3	i_6	$-i_1$	i_5	$-i_4$	$-i_2$	-1

.

Denna tabell finns i flera varianter, men alla är isomorfa. Här kan man se att $i_l i_k = -i_k i_l$ om $k \neq l$, så multiplikation är ej kommutativ.
Värre är att den inte heller är associativ. Till exempel är $(i_1 i_2) i_3 = -i_4 i_3 = -i_6$ och $i_1(i_2 i_3) = -i_1 i_5 = i_6$.
Oktonionerna är alltså ingen skevkropp.
Däremot finns fortfarande inverser. Dessa kan bestämmas på samma sätt

som för komplexa tal och kvaternioner.
Konjugatet av en oktonion

$$x = x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 + x_4 i_4 + x_5 i_5 + x_6 i_6 + x_7 i_7$$

är som väntat

$$\overline{x} = x_0 - x_1 i_1 - x_2 i_2 - x_3 i_3 - x_4 i_4 - x_5 i_5 - x_6 i_6 - x_7 i_7.$$

$x\overline{x} = \overline{x}x$ blir då det reella talet

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2$$

så vi kan beräkna inversen till x

$$x^{-1} = \frac{\overline{x}}{x\overline{x}}$$

Man har också att

$$|xy| = |x||y|, \qquad \text{där} \quad |x| = \sqrt{x\overline{x}}$$

vilket även är sant i $\mathbb{R}, \mathbb{C}$ och $\mathbb{H}$. Detta gör $\mathbb{O}$ till en normerad (icke-associativ) divisionsalgebra (som inte definieras här). [4]

5 Frobenius sats

Vi vet nu att $\mathbb{R}, \mathbb{C}$ och $\mathbb{H}$ är exempel på skevkroppar. $\mathbb{O}$ däremot är inte en skevkropp. Man kan misstänka ett en skevkropp som är en algebra över de reella talen då måste vara av just dimension 1, 2 eller 4. Detta är precis vad Frobenius sats, som bevisades av Ferdinand Georg Frobenius år 1877, säger.

Definition 2. *Låt D vara en divisionsalgebra. Mängden*

$$\{x \in D \mid xa = ax \quad \forall a \in D\}$$

av element som kommuterar med alla andra element i D kallas ***centrum*** *av D.*

Definition 3. *Låt D vara en divisionsalgebra. D är* ***algebraisk*** *över en kropp F om*

- *F tillhör centrum av D.*
- *varje $a \in D$ är ett nollställe till ett polynom med koefficienter i F.*

Lemma 1. *Om en skevkropp D är algebraisk över $\mathbb{C}$ så är $D = \mathbb{C}$.*

Bevis. Antag att D är algebraisk över $\mathbb{C}$ och välj godtyckligt $a \in D$. Då finns något polynom $p(x)$ med koefficienter i $\mathbb{C}$ sådant att $p(a) = 0$. Om $p(x)$ är av grad n finns exakt n stycken nollställen, alla i $\mathbb{C}$. Vi kan alltså skriva

$$p(x) = \prod_{i=1}^{n}(x - \alpha_i) \qquad \alpha_i \in \mathbb{C} \quad \text{för } i = 1, \ldots, n.$$

Eftersom $p(a) = 0$ har vi

$$\prod_{i=1}^{n}(a - \alpha_i) = 0 \quad \Longleftrightarrow \quad a - \alpha_1 = 0 \quad \Longleftrightarrow \quad a = \alpha_i \quad \text{för något } i.$$

Det vill säga, $a \in \mathbb{C}$, och vi måste ha att $D = \mathbb{C}$. □

Sats 3. *(**Frobenius**) Låt D vara en skevkropp algebraisk över $\mathbb{R}$. Då är D isomorf till $\mathbb{R}$, $\mathbb{C}$ eller $\mathbb{H}$.*

Bevis. Antag först att D är kommutativ, och att $D \neq \mathbb{R}$.
Välj godtyckligt a sådant att $a \in D$, $a \notin \mathbb{R}$.
Eftersom D är algebraisk över $\mathbb{R}$ är a ett nollställe till något irreducibelt polynom med koefficienter i $\mathbb{R}$. Irreducibla polynom med reella koefficienter

är av grad 1 eller 2. Polynomet kan ej vara av grad 1 eftersom $a \notin \mathbb{R}$, så alltså måste det vara av grad 2. Ett sådant polynom kan skrivas som

$$a^2 - 2\alpha a + \beta = 0, \qquad \alpha, \beta \in \mathbb{R}$$

$$(a - \alpha)^2 = \alpha^2 - \beta.$$

Här är $\alpha^2 - \beta < 0$ eftersom a ej är reell (om $\alpha^2 - \beta > 0$ finns reell lösning för $a - \alpha$), alltså

$$\alpha^2 - \beta = -\gamma^2, \qquad \gamma \in \mathbb{R}.$$

Då har vi även

$$(a - \alpha)^2 = -\gamma^2 \quad \iff \quad \Big(\frac{a - \alpha}{\gamma}\Big)^2 = -1 = i^2.$$

Observera att regeln

$$x^2 = y^2 \quad \iff \quad x = \pm y$$

följer av kommutativitet:

$$(x - y)(x + y) = x^2 + xy - yx + y^2 = x^2 - y^2 \quad \text{ om } xy = yx.$$

Vi använder alltså att D är kommutativ och får

$$\frac{a - \alpha}{\gamma} = \pm i.$$

D är alltså algebraisk över $\mathbb{R}(i)$, det vill säga $\mathbb{C}$. Enligt lemma 1 har vi då att $D \cong \mathbb{C}$.
Om D är kommutativ är D alltså isomorf till antingen $\mathbb{R}$ eller $\mathbb{C}$.

Antag nu att D ej är kommutativ.
Då är $\mathbb{R}$ centrum av D:
$\mathbb{R}$ tillhör centrum eftersom D är algebraisk över $\mathbb{R}$.
Antag att det finns ett $a \notin \mathbb{R}$ i centrum av D. På samma sätt som tidigare finns då $\alpha, \gamma \in \mathbb{R}$ sådana att $(\frac{a-\alpha}{\gamma})^2 = -1$. Då innehåller centrum en delkropp C isomorf till $\mathbb{C}$, där i motsvaras av $\frac{a-\alpha}{\gamma}$. Men då är D algebraisk över C och därmed är $D \cong \mathbb{C}$ enligt lemma 1.
Men detta är en motsägelse eftersom D ej är kommutativ. Alltså måste $\mathbb{R}$ vara centrum av D.

Vi vill nu visa att D måste vara $\mathbb{H}$.
Välj något $a \in D$ sådant att $a \notin \mathbb{R}$. Som tidigare finns då några $\alpha, \gamma \in \mathbb{R}$ sådana att $i = \frac{a-\alpha}{\gamma}$ uppfyller $i^2 = -1$. Eftersom $i \notin \mathbb{R}$, tillhör i ej centrum, och det finns något $b \in D$ sådant att

$$c = bi - ib \neq 0$$

Från detta följer

$$ic + ci = i(bi - ib) + (bi - ib)i = ibi - i^2b + bi^2 - ibi = b - b = 0$$

$$\iff \quad ic = -ci.$$

Elementen c och i antikommuterar.
Vidare gäller att

$$ic^2 = (ic)c = (-ci)c = -c(ic) = -c(-ci) = c^2 i,$$

det vill säga c^2 kommuterar med i.
Eftersom c inte kommuterar med i kan c inte ligga i centrum, det vill säga $c \notin \mathbb{R}$. Men D är algebraisk över $\mathbb{R}$ så c måste lösa någon andragradsekvation med reella koefficienter.

$$c^2 + \lambda c + \mu = 0 \qquad \lambda, \mu \in \mathbb{R}$$

Elementen c^2 och μ kommuterar med i, därför måste λc också göra det.

$$\lambda ci = i\lambda c = \lambda ic = -\lambda ci \quad \iff \quad 2\lambda ci = 0$$

$$c, i \neq 0 \quad \Rightarrow \quad \lambda = 0$$

Alltså har vi

$$c^2 + \mu = 0 \quad \iff \quad c^2 = -\mu$$

Eftersom c ej reell måste c^2 vara negativ. μ är alltså positiv. Då är

$$\mu = v^2 \text{ för något } v \in \mathbb{R},$$

och därmed

$$c^2 = -v^2.$$

Låt nu $j = \frac{c}{v}$. Då är

$$j^2 = \frac{c^2}{v^2} = -1 \quad \text{och}$$

$$ji + ij = \frac{c}{v}i + i\frac{c}{v} = \frac{ci + ic}{v} = 0 \quad \iff \quad ji = -ij.$$

Låt till sist $k = ij$. Dessa i, j och k uppför sig nu precis som i, j och k i $\mathbb{H}$:

- $k^2 = (ij)^2 = ij(-ji) = -ij^2 i = i^2 = -1$ så
$$i^2 = j^2 = k^2 = -1.$$

- $jk = jij = j(-ji) = -j^2 i = i,$
$ki = iji = j,$
$ik = i^2 j = -j,$
$kj = ij^2 = -i$ och
$ji = -ij = -k$ så
$$ij = k, \quad jk = i, \quad ki = j, \quad ik = -j, \quad kj = -i, \quad ji = -k.$$

Alltså har vi att

$$H = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}\}$$

är en delskevkropp av D isomorf till $\mathbb{H}$. Det återstår att visa att $D = H$.

Välj ett godtyckligt $r \in D$ sådant att $r^2 = -1$. Vi ska först studera delringen

$$N(r) = \{x \in D \mid xr = rx\}$$

av element som kommuterar med r. Elementet r, och därmed alla element på formen $\alpha_0 + \alpha_1 r,\ \alpha_0, \alpha_1 \in \mathbb{R}$, tillhör centrum av $N(r)$.
Men $\{\alpha_0 + \alpha_1 r\} \cong \mathbb{C}$, så $N(r)$ är algebraisk över $\mathbb{C}$ och då är $N(r) \cong \mathbb{C}$ enligt lemma 1. Alltså är

$$N(r) = \{\alpha_0 + \alpha_1 r | \alpha_0, \alpha_1 \in \mathbb{R}\},$$

så om $xr = rx$ är $x = \alpha_0 + \alpha_1 r$ för några $\alpha_0, \alpha_1 \in \mathbb{R}$.

Antag nu att $u \in D,\ u \notin \mathbb{R}$. Vi vill visa att $u \in H$.
Som tidigare finns $\alpha, \beta \in \mathbb{R}$ sådana att $w = \frac{u-\alpha}{\beta}$ uppfyller $w^2 = -1$.
Elementet $wi + iw$ kommuterar med både i och w:

$$i(wi + iw) = iwi - w = iwi + w(-1) = iwi + wi^2 = (iw + wi)i$$

$$\text{och på samma sätt } \ w(wi + iw) = (iw + wi)w$$

så $wi+iw \in N(i)$ och $wi+iw \in N(w)$, och vi har alltså $wi+iw = \alpha_0' + \alpha_1' i = \alpha_0 + \alpha_1 w$.
Om $w \notin H$ måste $\alpha_1 = 0$, för annars är $w = \frac{\alpha_0' - \alpha_0 + \alpha_1' i}{\alpha_1} \in H$.
Alltså är $wi + iw = \alpha_0 \in \mathbb{R}$ och på samma sätt $wj + jw = \beta_0 \in \mathbb{R}$ och $wk + kw = \gamma_0 \in \mathbb{R}$.
Låt

$$z = w + \frac{\alpha_0}{2} i + \frac{\beta_0}{2} j + \frac{\gamma_0}{2} k.$$

Då är

$$zi + iz = wi + iw + \frac{\alpha_0}{2} i^2 + i\frac{\alpha_0}{2} i + \frac{\beta_0}{2} ji + i\frac{\beta_0}{2} j + \frac{\gamma_0}{2} ki + i\frac{\gamma_0}{2} k =$$

$$= \alpha_0 + \frac{\alpha_0}{2}(i^2 + i^2) + \frac{\beta_0}{2}(ij + ji) + \frac{\gamma_0}{2}(ik + ki) = \alpha_0 - \alpha_0 = 0$$

På samma sätt är $zj + jz = zk + kz = 0$. Av detta får vi

$$0 = zk + kz = zij + ijz = zij - izj = (zi - iz)j$$

eftersom $jz = -zj$.
Vi vet att $j \neq 0$, så $zi - iz = 0$. Men $zi + iz = 0$ så $(zi - iz) + (zi + iz) = 2iz = 0$. Eftersom $i \neq 0$ måste $z = 0$, vilket ger

$$z = w + \frac{\alpha_0}{2}i + \frac{\beta_0}{2}j + \frac{\gamma_0}{2}k = 0 \;\Rightarrow\; w \in H.$$

Detta motsäger antagandet att $w \notin H$.

Alltså gäller $w \in H$. Eftersom $w = \frac{u-\alpha}{\beta}$ är $u = \beta w + \alpha \in H$, vilket vi ville visa.
Varje element i D är alltså i H, och $H \subseteq D$, så $H = D$.
Nu har vi alltså visat att

$$D \cong \mathbb{H}$$

□

6 Wedderburns sats

Sats 4. *(**Wedderburn**) Varje ändlig skevkropp är kommutativ, och alltså en kropp.*

Detta är en känd sats av Joseph H. M. Wedderburn som bevisades av densamme år 1905.
För att bevisa satsen krävs dock några förberedelser.

Lemma 2. *Låt t, m och n vara heltal, $m \leq n$. Om $t^m - 1$ delar $t^n - 1$ så måste m dela n.*

Bevis. Låt $n = km + r$ där $0 \leq r < m$.
Då är

$$t^n - 1 = (t^{km+r} - t^r) + (t^r - 1) = t^r(t^{km} - 1) + (t^r - 1) =$$

$$= t^r q(t)(t^m - 1) + (t^r - 1) \quad \text{där} \quad q(t) = (t^{(k-1)m} + t^{(k-2)m} + \cdots + 1).$$

Eftersom

$$grad(t^r - 1) = r < m = grad(t^m - 1)$$

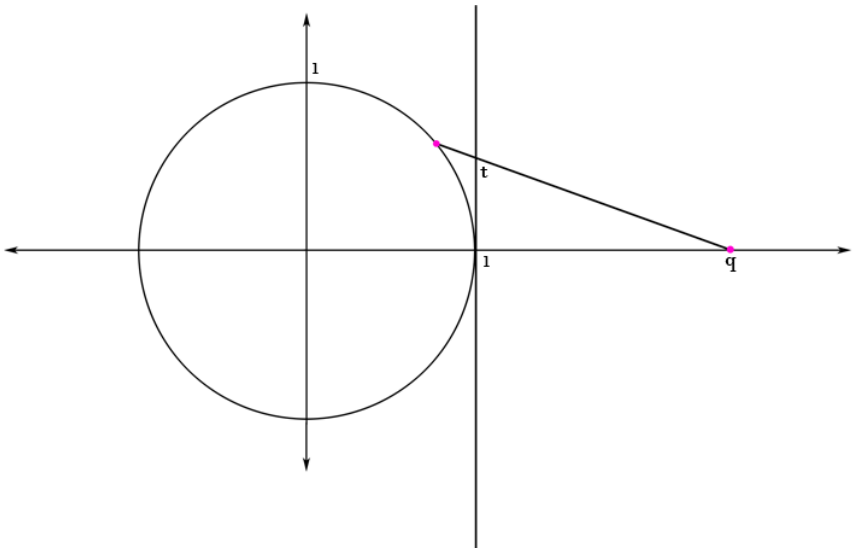
måste, enligt divisionsalgoritmen, $t^r - 1$ vara resten vid division av $t^n - 1$ med $t^m - 1$. Om $t^m - 1$ delar $t^n - 1$ måste då $t^r - 1 = 0$, så $r = 0$ och $n = km$. □

Definition 4. *En **n:te enhetsrot** är ett tal $x \in \mathbb{C}$ sådant att $x^n = 1$.*
*x är en **primitiv n:te enhetsrot** om $x^n = 1$ och $x^m \neq 1$ för alla $m < n$.*

Lemma 3. *Låt q vara ett positivt heltal och $\theta_i,\ i = 1, 2, ..., n$ de n:te enhetsrötterna. Då är $|q - \theta| > |q - 1|$ för $\theta \neq 1$.*

Bevis. Varje θ är på formen $\theta = cos\alpha + isin\alpha$ och ligger på enhetscirkeln i det komplexa talplanet. Det betyder att $Re\ \theta < 1$ då $\theta \neq 1$. Eftersom q är ett positivt heltal måste en rät linje från q till θ gå genom en punkt t med $Re\ t = 1$. Om $\theta \neq 1$ är alltså

$$|q - \theta| = |q - t| + |t - \theta| > |q - t| \geq |q - 1|.$$



□

Definition 5.

$$\Phi_n(x) = \prod_{\theta}(x - \theta)$$

där θ löper över alla primitiva n:te enhetsrötter, kallas det **n:te cyklotomiska polynomet**.

De fyra första cyklotomiska polynomen är:

$$\Phi_1(x) = x - 1$$

$$\Phi_2(x) = x + 1$$

$$\Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = x^2 + 1$$

Definition 6. *Låt G vara en grupp. Mängden*

$$Z(G) = \{x \in G \mid xg = gx \quad \forall g \in G\}$$

av element som kommuterar med alla andra element i G kallas ***centrum*** *av G.*

Till exempel är 1 och -1 de enda element som kommuterar med alla andra element i kvaterniongruppen $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Centrum av Q_8 är alltså

$$Z(Q_8) = \{1, -1\}.$$

Definition 7. *Låt G vara en grupp och $a, b \in G$. Elementet a kallas ett **konjugat** av b om det finns $x \in G$ så att $a = xbx^{-1}$. Man säger att a och b är **konjugerade**.*

Att vara konjugerade är en ekvivalensrelation:
Låt $a \sim b$ beteckna att a är ett konjugat av b, och låt $a, b, c, x, y \in G$.

- $a = 1a1^{-1}$, så $a \sim a$.
- $a = xbx^{-1} \Rightarrow b = x^{-1}a(x^{-1})^{-1}$, så $a \sim b \Rightarrow b \sim a$.
- $a = xbx^{-1} \quad b = ycy^{-1} \Rightarrow a = xycy^{-1}x^{-1} = (xy)c(xy)^{-1}$, så $a \sim b, \ b \sim c \Rightarrow a \sim c$.

Notera att en ekvivalensklass består av endast ett element a om och endast om a tillhör centrum:
Låt $[a]$ beteckna ekvivalensklassen som representeras av a.
Om a kommuterar med alla element i G och $a = xbx^{-1}$ så är $a = b$, så $[a]$ består av endast a.
Om $[a]$ består av endast a har vi $xax^{-1} = a$ för alla $x \in G$ (för om $xax^{-1} = g \neq a$ är $g \in [a]$). Alltså är $xa = ax$ för alla $x \in G$, det vill säga a tillhör centrum.

Definition 8. *Låt G vara en grupp och $x \in G$. Då kallas*

$$Z(x) = \{a \in G \mid ax = xa\}$$

centralisatorn *av x i G.*

Om g är ett konjugat av x sådant att $g = axa^{-1} = bxb^{-1}$ så är $b^{-1}ax = xb^{-1}a$, det vill säga $b^{-1}a \in Z(x)$. Då är $aZ(x) = bZ(x)$, a och b tillhör samma sidoklass av $Z(x)$.
Omvänt, om $aZ(x) = bZ(x)$ kan man lätt se att $axa^{-1} = bxb^{-1}$.
Ett konjugat av x motsvarar alltså en sidoklass av $Z(x)$. Antalet sidoklasser måste då vara samma som antalet element i konjugatklassen av x. Detta leder till den så kallade **klassekvationen**, [2, s. 294]:

Sats 5. *Låt G vara en ändlig grupp. Då är*

$$|G| = |Z(G)| + \sum [G : Z(x)]$$

där summan tas över ett x från varje icketrivial konjugatklass.

Bevis. $[G : Z(x)]$ är antalet sidoklasser av $Z(x)$, och alltså antalet element i konjugatklassen av x. Konjugatklasserna utgör en partition av G, så summan räknar antalet element i G, förutom de som tillhör en trivial konjugatklass. En trivial konjugatklass är en klass med bara ett element, och alla dessa element tillhör centrum av G. □

Nu till beviset av Wedderburns sats.

Bevis. Låt K vara en ändlig skevkropp med centrum

$$Z = \{z \in K \mid zx = xz \ \ \forall x \in K\}.$$

Vi har att $0, 1 \in Z$. Välj $x \in K$ och $y, z \in Z$. Då gäller:

- $(-z)x = -zx = -xz = x(-z)$, så $-z \in Z$.
- $(y + z)x = yx + zx = xy + xz = x(y + z)$, så $y + z \in Z$.
- $zx = xz \iff z^{-1}zxz^{-1} = z^{-1}xzz^{-1} \iff xz^{-1} = z^{-1}x$, så $z^{-1} \in Z$.
- $(yz)x = yxz = x(yz)$, så $yz \in Z$.

Z är alltså en delkropp av K. Det betyder att K kan beskrivas som ett vektorrum över Z. Det följer att K då har q^n element, där q är antalet element i Z och n dimensionen av vektorrummet.
Vi vill nu visa att $Z = K$, det vill säga att $n = 1$.
Välj ett godtyckligt $a \in K$. Centralisatorn

$$Z(a) = \{x \in K \mid xa = ax\}$$

av a är en delskevkropp av K (visas på liknande sätt som för Z) och innehåller Z. Även $Z(a)$ är alltså ett vektorrum över Z och har q^{m_a} element för något heltal $m_a \leq n$.
Vi ska nu betrakta de multiplikativa grupperna K^*, Z^* och $Z(a)^*$ (vilket betyder att man tar bort nollelementet ur mängden, t.ex är $K^* = K \setminus \{0\}$). Antalet element i K^* är $q^n - 1$ element, och $Z(a)^*$ har $q^{m_a} - 1$ element. Eftersom $Z(a)^* \subseteq K^*$ måste $q^{m_a} - 1 \mid q^n - 1$, enligt Lagranges sats. Lemma 2 ger då att $m_a \mid n$.

Klassekvationen för K^* är $|K^*| = |Z^*| + \sum[K^* : Z(a)^*]$ där summan tas över ett a från varje konjugatklass av K^*.

Antalet sidoklasser av $Z(a)^*$ är $\frac{q^n-1}{q^{m_a}-1}$, så vi får ekvationen

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^{m_a} - 1} \tag{1}$$

Det återstår att visa att denna ekvation endast håller då $n = 1$.

För att visa det tar vi hjälp av cyklotomiska polynom och visar att $\Phi_n(x)$ delar $x^n - 1$ och $\sum \frac{x^n-1}{x^{m_a}-1}$ i $\mathbb{Z}(x)$, och därmed även $x - 1$:
I $\mathbb{C}[x]$ har vi att

$$x^n - 1 = \prod_{i=1}^{n}(x - \lambda_i) \tag{2}$$

där $\lambda_1, \ldots \lambda_n$ är alla rötter till ekvationen, det vill säga alla n:te enhetsrötter. Varje n:te enhetsrot måste vara en primitiv m:te enhetsrot för något heltal m. Då måste $n = km$ för något heltal k, för annars får vi $x^n = x^{km}x^r = x^r = 1$ för ett heltal $r < m$. Vi har alltså att $m|n$.
Därför kan vi skriva (2) som

$$x^n - 1 = \prod_{i=1}^{n}(x - \lambda_i) = \prod_{d|n} \Phi_d(x). \tag{3}$$

$\Phi_n(x)$ är en av faktorerna, så $\Phi_n(x)|x^n - 1$. Men vi behöver också att cyklotomiska polynom endast har heltalskoefficienter.

$\Phi_1(x),\ \Phi_2(x),\ \Phi_3(x)$ är alla moniska polynom med heltalskoefficienter. Med stark induktion kan man visa att varje $\Phi_n(x)$ har denna egenskap.
Antag att detta är sant för varje $\Phi_d(x)$ med $d < n$. Då gäller påstendet speciellt för alla d sådana att $d|n$ utom $d = n$, så

$$x^n - 1 = \Phi_n(x)g(x)$$

där $g(x)$ är ett moniskt polynom med heltalskoefficienter. Divisionen

$$\Phi_n(x) = \frac{x^n - 1}{g(x)}$$

resulterar i ett polynom med den önskade egenskapen. Detta ser man enklast genom att tänka sig att man faktiskt utför divisionen.

Vi vill fortfarande visa att

$$\Phi_n(x)\Big|\frac{x^n - 1}{x^d - 1} \text{ för varje } d \text{ sådant att } d|n \text{ utom } d = n.$$

Men eftersom $x^d - 1 = \prod_{k|d} \Phi_k(x)$, och $k|d$, $d|n$ medför att $k|d$ kan (3) skrivas som

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x)(x^d - 1)f(x)$$

där $f(x) = \prod_{k|n,\ k\nmid d,\ k\neq n} \Phi_k(x)$ har heltalskoefficienter. Alltså har vi

$$\frac{x^n - 1}{x^d - 1} = \Phi_n(x) f(x).$$

Nu vet vi att $\Phi_n(q)$ är ett heltal och att

$$\Phi_n(q) | q^n - 1 \text{ och } \Phi_n(q) \Big| \sum \frac{q^n - 1}{q^{m_a} - 1}.$$

Enligt (1) måste då $\Phi_n(q) | q - 1$. Men $\Phi_n(q) = \prod_\theta (q - \theta)$ där produkten går över alla primitiva n:te enhetsrötter. Då är $|q - \theta| > |q - 1|$ för alla $\theta \neq 1$ enligt lemma 3. Att $\Phi_n(q) | q - 1$ kan därför endast gälla om $n = 1$, och därmed är satsen bevisad. □

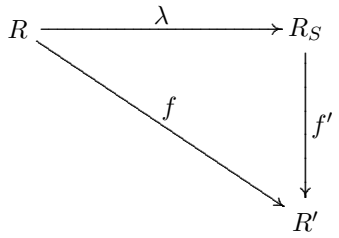
7 Fraktionskroppar

En fraktionskropp, för en ring R, är en minsta skevkropp K som innehåller R som en delring (minsta i den meningen att K inte innehåller någon mindre skevkropp som omfattar R). Elementen i fraktionskroppen är på formen $a \cdot b^{-1}$ där a och b är element i R. En metod för att konstruera en skevkropp är alltså att bestämma fraktionskroppen för en ring R. Det vill säga, skapa inverser till elementen i R. Denna konstruktion är unik.
Men är detta möjligt för alla ringar?

7.1 Konstruktion

Sats 6. *Givet en ring R och en delmängd S av R existerar en ring R_S med följande egenskaper:*

- *Det finns en homomorfi $\lambda : R \to R_S$ sådan att varje $\lambda(s)$, där $s \in S$, har invers.*
- *För varje homomorfi $f : R \to R'$ sådan att, för $s \in S$, $f(s)$ har invers, finns en unik homomorfi $f' : R_S \to R'$ sådan att $f = \lambda \circ f'$.*



Bevis. Låt R vara en ring och S en delmängd av R. Då kan R_S konstrueras genom att lägga till ett element s' för varje $s \in S$ sådant att $ss' = s's = 1$: Sätt

$$I = (s_1 s_1' - 1,\ s_1' s_1 - 1,\ s_2 s_2' - 1,\ s_2' s_2 - 1, \ldots) \quad \forall s_i \in S \ \text{ och}$$

$$R_S := R[s_1',\ s_2',\ \ldots]/I$$

(Här förutsätter vi att S är uppräknelig. Om S är överuppräknelig är $I = (ss' - 1\ ;\ s \in S)$, alltså idealet genererat av alla relationer $ss' - 1$ i ringen $R[s'\ ;\ s \in S]$.)
Låt $\lambda : R \to R_S$ avbilda varje element i R på motsvarande element i R_S. Då

har $\lambda(s)$ en invers, för varje $s \in S$. Dessutom bevarar λ multiplikation och addition, så λ är en homomorfi.

Antag nu att $f : R \to R'$ också är en homomorfi sådan att varje $f(s)$ har invers.
Definiera då $f' : R_S \to R'$ som

$$f'(\lambda(a)) = f(a) \qquad f'(s') = (f(s))^{-1}$$

där $a \in R$ och $s \in S$.
Då är $f = \lambda \circ f'$.
Låt $a, b \in R$ och $s_1, s_2 \in S$. Eftersom λ och f är homomorfier är

$$f'(\lambda(a)\lambda(b)) = f'(\lambda(ab)) = f(ab) = f(a)f(b) = f'(\lambda(a))f'(\lambda(b))$$

$$f'(s_1's_2') = (f(s_2s_1))^{-1} = (f(s_1))^{-1}(f(s_2))^{-1} = f'(s_1')f'(s_2').$$

Motsvarande gäller för addition.
Vi har

$$f'(r+ss'-1) = f'(r)+f'(s)f'(s')-f'(1) = f'(r)+f(s)(f(s))^{-1}-1 = f'(r).$$

Detta visar att f' är väldefinierad, så f' är en homomorfi.
För $a \in R$ är $f'(\lambda(a)) = f(a)$ unikt definierad av f. Även $f(s') = (f(s))^{-1}$ är unik eftersom inverser är unika. Vi har nu visat att f' är en unik homomorfi.

□

Ovanstående sats gäller för alla ringar, men den garanterar inte att R är en delring av R_S.
Till exempel, låt $R = \mathbb{Z}_4$ och $S = 2$. Då är R_S en ring där det existerar ett element s' sådant att $2s' = 1$. Då får vi

$$2s' - 1 = 0 \;\Rightarrow\; 2(2s' - 1) = 0 \;\Rightarrow\; 4s' - 2 = 0 \;\Rightarrow\; -2 = 2 = 0$$

$$2 = 0 \;\Rightarrow\; 0 = 2s' - 1 = -1 = 3$$

$$3 = 0 \;\Rightarrow\; 4 - 3 = 1 = 0$$

$$R_S = \{0\}$$

Det behövs alltså några restriktioner på R för att konstruktion av en fraktionskropp, med R som delring, ska vara möjlig.
Låt följande villkor gälla, för en ring R och en delmängd S av R:

1. S är sluten under multiplikation

2. För varje $a \in R,\ s \in S$ gäller $sR \cap aS \neq \emptyset$.

3. $a \in R,\ s \in S,\ sa = 0 \quad \Rightarrow \quad at = 0$ för något $t \in S$.

För att konstruera en fraktionskropp, med element på formen $a \cdot s^{-1}$ där $a \in R,\ s \in S$, börja med att definiera följande relation på $R \times S$.
$(a, s) \sim (a', s')$ om det finns $u, u' \in R$ så att

$$\begin{cases} au = a'u' \\ su = s'u' \in S. \end{cases}$$

Relationen $(a, s) \sim (a', s')$ ska motsvara $a \cdot s^{-1} = a' \cdot s'^{-1}$.

Denna relation är en ekvivalensrelation:
Det är klart att $\sim$ är reflexiv ($(a, s) \sim (a, s)$) och symmetrisk ($(a, s) \sim (a', s') \ \Rightarrow \ (a', s') \sim (a, s)$).
För att visa transitivitet, antag att $(a, s) \sim (a', s')$ och $(a', s') \sim (a'', s'')$. Då är, för några $u, u', v, v' \in R$,

$$\begin{cases} au = a'u' \\ su = s'u' \in S \end{cases} \quad \begin{cases} a'v = a''v' \\ s'v = s''v' \in S \end{cases} .$$

Enligt (2) är $s'u'R \cap s'vS \neq \emptyset$, det vill säga, det finns $r \in R$ och $t \in S$ så att

$$s'u'r = s'vt \quad \Longleftrightarrow \quad s'(u'r - vt) = 0.$$

Vi har inte antagit att R är nolldelarfri, så vi kan inte bara kancellera s'. Däremot ger villkor (3) att det finns $t' \in S$ så att

$$(u'r - vt)t' = 0 \quad \Longleftrightarrow \quad u'rt' = vtt'$$

Definiera

$$w = rt' \ \text{ och } \ w' = tt'.$$

Vi har då att

$$u'w = vw',$$

och då är också

$$\begin{cases} auw = a'u'w = a'vw' = a''v'w' \\ suw = s'u'w = s'vw' = s''v'w' \in S. \end{cases}$$

Alltså är $(a, s) \sim (a'', s'')$. Relationen $\sim$ är transitiv och därmed en ekvivalensrelation.

Nu kan vi införa operationer på mängden av ekvivalensklasser. Låt $[a, s]$ beteckna ekvivalensklassen som representeras av (a, s).

För två klasser $[a,b]$, $[c,d]$ finns, enligt (2), $m, r \in R$ och $s \in S$ så att $br = ds = m$. Eftersom $d, s \in S$ och S är sluten under multiplikation, enligt (1), måste $m \in S$.
Vi vill att

$$ab^{-1} + cd^{-1} = ar(br)^{-1} + cs(ds)^{-1} = (ar + cs)m^{-1}$$

så definiera addition som

$$[a,b] + [c,d] = [ar + cs, m].$$

Men m är inte unik, så vi måste visa att additionen ger samma resultat vid olika val av m.
Välj därför m' så att $br' = ds' = m'$ för $r' \in R$ och $s' \in S$.
Vi vill visa att $(ar + cs, m) \sim (ar' + cs', m')$.
(2) ger att $su = s'u'$ för något $u' \in S$. Då följer

$$su = s'u' \quad \Rightarrow \quad dsu = ds'u' \quad \text{och}$$

$$bru = br'u' \quad \Longleftrightarrow \quad b(ru - r'u') = 0.$$

Eftersom $b \in S$ ger (3) att det finns ett $t \in S$ så att

$$(ru - r'u')t = 0 \quad \Longleftrightarrow \quad rut = r'u't.$$

Nu har vi

$$\begin{cases} rut = r'u't \\ sut = s'u't \end{cases}$$

och därmed

$$\begin{cases} (ar + cs)ut = arut + csut = ar'u't + cs'u't = (ar' + cs')u't \\ mut = dsut = ds'u't = m'u't \in S. \end{cases},$$

så $(ar + cs, m) \sim (ar' + cs', m')$.
Additionen är alltså oberoende av valet av m. För att additionen ska vara väldefinierad måste vi också visa att den är oberoende av valet av representanter för ekvivalensklasserna $[a,b]$ och $[c,d]$.
Låt därför $(a,b) \sim (a',b')$ och $(c,d) \sim (c',d')$. Alltså

$$\begin{cases} au = a'u' \\ bu = b'u' \in S \end{cases} \quad \begin{cases} cv = c'v' \\ dv = d'v' \in S \end{cases}$$

Eftersom additionen är oberoende av valet av m kan vi välja m som

$$m = bur = dvs$$

($buR \cap dvS \neq \emptyset$ enligt (2).)

$$m = b'u'r = d'v's.$$

Då är

$$[a,b]+[c,d]=[aur+cvs,m]=[a'u'r+c'v's,m]=[a',b']+[c',d']$$

och additionen är väldefinierad.

Till två klasser $[a,b]$ och $[c,d]$ finns också $x \in R$ och $y \in S$ sådana att $bx = cy$ enligt (2).
Multiplikation bör då definieras som

$$[a,b]\cdot[c,d]=[ax,dy]$$

eftersom vi vill att

$$ab^{-1}\cdot cd^{-1}=ax(bx)^{-1}\cdot cy(dy)^{-1}=ax(bx)^{-1}bx(dy)^{-1}=ax(dy)^{-1}.$$

Notera att $dy \in S$ eftersom $d, y \in S$ och S är sluten under multiplikation.
Att multiplikationen är väldefinierad kan visas på liknande sätt som för addition:
Om $x' \in R$, $y' \in S$ och $bx' = cy'$, välj $u \in R$, $u' \in S$ så att $yu = y'u'$ enligt (2). Då har vi

$$yu=y'u' \quad \Rightarrow \quad cyu=cy'u' \quad \Longleftrightarrow \quad bxu=bx'u'.$$

Vi använder (3), som tidigare, och får att det finns ett $t \in S$ så att

$$xut=x'u't.$$

Nu har vi

$$\begin{cases} xut=x'u't \\ yut=y'u't \in S. \end{cases}$$

Ur detta följer

$$\begin{cases} axut=ax'u't \\ dyut=dy'u't \in S. \end{cases}$$

och $(ax, dy) \sim (ax', dy')$. Det vill säga $[ax, dy] = [ax', dy']$ och multiplikationen är oberoende av valet av x och y.

Om $(a,b) \sim (a',b')$ och $(c,d) \sim (c',d')$ så finns $u, u', v, v' \in R$ så att

$$\begin{cases} au=a'u' \\ bu=b'u' \in S \end{cases} \qquad \begin{cases} cv=c'v' \\ dv=d'v' \in S. \end{cases}$$

Det finns $r \in R$ och $s \in S$ så att

$$bur=cvs$$

och då även

$$b'u'r=c'v's.$$

Då är

$$[a,b]\cdot[c,d]=[aur,dvs]=[a'u'r,d'v's]=[a',b']\cdot[c',d']$$

Alltså är multiplikationen också väldefinierad.
Nu har vi två väldefinierade operationer. Notera att alla de tre villkoren var nödvändiga.
Att additionen är kommutativ är lätt att se.
Identitetselementet för addition är $[0,1]$:

$$[a,s]+[0,1]=[a+0s,s]=[a,s]$$

Den additiva inversen till $[a,s]$ är därför $[-a,s]$:

$$[a,s]+[-a,s]=[a+(-a),s]=[0,s]=[0,1]$$

För att mängden av ekvivalensklasser ska utgöra en ring krävs också att associativa lagen är uppfylld för båda operationerna, och att distributiva lagen gäller.
Vi börjar med att titta på summan

$$([a,b]+[c,d])+[e,f]=[ar+cs,m]+[e,f]=[(ar+cs)x+ey,n]$$

där $br=ds=m,\ \ mx=fy=n$ och därmed $brx=dsx=fy=n$.
Med dessa likheter får vi även

$$[a,b]+([c,d]+[e,f])=[a,b]+[csx+ey,n]=[arx+csx+ey,n]=$$

$$=[(ar+cs)x+ey,n]$$

så addition är associativ.

För produkten gäller

$$([a,b]\cdot[c,d])\cdot[e,f]=[ax,dy]\cdot[e,f]=[axz,fw]$$

där $bx=cy,\ \ dyz=ew$ och $bxz=cyz$.
De två sista likheter ger också

$$[a,b]\cdot([c,d]\cdot[e,f])=[a,b]\cdot[cyz,fw]=[axz,fw]$$

så även multiplikation är associativ.

Slutligen är

$$[a,b]\cdot[c,d]+[a,b]\cdot[e,f]=[ax,dy]+[az,fw]=[axr+azs,m]$$

där $bx=cy,\ \ bz=ew$ och $dyr=fws=m$. Detta ger också att

$[a,b]\cdot([c,d]+[e,f])=[a,b]\cdot[cyr+ews,m]=[a,b]\cdot[bxr+bzs,m]=[a(xr+zs),m]$.

Distributiva lagen gäller alltså vid vänstermultiplikation.
På liknande sätt kan man se att

$$[a,b]\cdot[e,f]+[c,d]\cdot[e,f]=([a,b]+[c,d])\cdot[e,f].$$

Distributiva lagen gäller både till höger och vänster, och vi har en ring.

Klassen $[1,1]$ utgör ett multiplikativt identitetselement eftersom

$$[a,s]\cdot[1,1]=[a,s]$$

$$[1,1]\cdot[a,s]=[a,s]$$

Notera också att alla element på formen $[s,1]$, där $s\in S$, har invers:

$$[1,s]\cdot[s,1]=[s,s]=[1,1]$$

$$[s,1]\cdot[1,s]=[s,s]=[1,1]$$

$R_S=R\times S/\sim$ är alltså en ring och elementen som motsvaras av S har inverser. Vi vill nu visa att R_S har egenskaperna i sats 6.

- $\lambda:R\to R_S$ definieras som $\lambda(x)=[x,1]$, och alla element $[s,1]$, där $s\in S$, har invers.
- Antag att det finns en ring R' och en homomorfi $f:R\to R'$ sådan att varje $f(s)$ har invers i R'. Definiera då $f':R_S\to R'$ som

  $$f'([a,s])=f(a)(f(s))^{-1}.$$

  Då är $f'(\lambda(x))=f'([x,1])=f(x)$, så $f=\lambda\circ f'$.
  Funktionen f' är unik: Antag att det finns en homomorfi $g:R_S\to R'$ sådan att $f=\lambda\circ g$. Då är $g([r,1])=g(\lambda(r))=f(r)$.
  För godtyckligt $[a,s]\in R_S$ gäller då

  $$f(a)=g([a,1])=g([a,s]\cdot[s,1])=g([a,s])g([s,1])=g([a,s])f(s)$$

  $$g([a,s])=f(a)(f(s))^{-1}$$

  så $g=f'$.

R_S är alltså en unik minsta ring med egenskapen att varje element i S har invers. Elementen i R_S är på formen rs^{-1}.

Tyvärr kan vi inte säga att vi R_S är en fraktionskropp ännu eftersom vi

inte visat att varje element har en invers, eller att R är en delring av R_S. Faktum är att mystiska saker kan inträffa eftersom R kan innehålla nolldelare. Antag att det finns element $a, b \in S$ sådana att $ab = 0$. Både a och b har inverser så $0 = a^{-1}abb^{-1} = 1$, men $0 \neq 1$ är ett av kraven på en skevkropp.
Om vi däremot antar att R är nolldelarfri kan vi visa att ekvivalensklasserna på formen $[r, 1]$, för alla $r \in R$, utgör en delring av R_S isomorf till R:
Vi har $\lambda(r) = [r, 1]$ från tidigare, och denna funktion är uppenbart surjektiv. Vi behöver visa att den även är injektiv. Om $\lambda(r_1) = \lambda(r_2)$, för några $r_1, r_2 \in R$ har vi

$$[r_1, 1] = [r_2, 1] \iff r_1 1^{-1} = r_2 1^{-1} \iff r_1 = r_2,$$

och λ är alltså injektiv.
Observera att om R skulle innehålla nolldelare är det inte säkert att λ är injektiv:
Antag att det finns $r \in R$, $s \in S$ sådana att $r, s \neq 0$ och $rs = 0$. Då är $[r, 1] = [0, 1]$ eftersom

$$\begin{cases} rs = 0s \\ 1s = 1s. \end{cases}$$

Vi har alltså $\lambda(r) = \lambda(0)$, men $r \neq 0$.

Tag som exempel den nolldelarfria ringen $\mathbb{C}[x]$, och välj $S = \{1, x, x^2, \ldots\}$. S är sluten under multiplikation så det första av våra tre villkor är uppfyllda.
$\mathbb{C}[x]$ är kommutativ så för ett godtyckligt polynom $p(x) \in \mathbb{C}[x]$ och något $x^t \in S$ har vi

$$p(x)x^t = x^t p(x) \in x^t\mathbb{C}[x] \cap p(x)S,$$

och det andra villkoret är uppfyllt. Det tredje villkoret följer direkt av att ringen är nolldelarfri.
Vi lägger till inverserna $\{1, x^{-1}, x^{-2}, \ldots\}$. Elementen i $\mathbb{C}[x]_S$ kommer då att vara på formen

$$\alpha_{-m}x^{-m} + \alpha_{-m+1}x^{-m+1} + \cdots + \alpha_{-1}x^{-1} + \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$$

för heltal m och n.
Denna ring innehåller mycket riktigt alla polynom i $\mathbb{C}[x]$.

7.2 Oredomän

Definition 9. *En nolldelarfri ring R som uppfyller*

$$\forall a, b \in R \quad aR \cap bR \neq \{0\} \qquad \textit{(höger Orevillkor)}$$

kallas en ***höger Oredomän****.*
Vänster Oredomän *definieras analogt.*

En Oredomän uppfyller villkoren (1),(2) och (3) om man sätter $S = R^*$. Eftersom R är nolldelarfri kan vi nu vara säkra på att $1 \neq 0$ i R_{R^*}:
Välj ett godtyckligt element $a \in R^*$. Då är $aa^{-1} = 1$. Om $1 = 0$ måste

$$aa^{-1} = 0 \iff aa^{-1}a = 0a \iff a = 0,$$

men det motsäger att $a \in R^*$.

Varje element ab^{-1} har en inversen ba^{-1}, så R_{R^*} är nu en skevkropp.
Därmed är R_{R^*} fraktionskroppen för R.

Omvänt, om vi har en skevkropp $K \supseteq R$ sådan att

$$K = \{xy^{-1} \mid x, y \in R\} \quad \text{för den nolldelarfria ringen R}$$

så måste ringen uppfylla Orevillkoret:
Låt $a, b \in K$. Eftersom K är en skevkropp existerar a^{-1}, och så även $a^{-1}b$, i K. Alla element i K är på formen xy^{-1}, så det finns $c, d \in R$ så att $a^{-1}b = cd^{-1}$.

$$a^{-1}b = cd^{-1} \quad \Rightarrow \quad b = acd^{-1} \quad \Rightarrow \quad bd = ac$$

$$aR \cap bR \neq \{0\}$$

Varje kommutativ nolldelarfri ring R är en Oredomän, eftersom $ab = ba \in aR \cap bR$.
Till exempel är ringen

$$\{a + \sqrt{3}b \mid a, b \in \mathbb{Z}\}$$

alltså en Oredomän. Hur ser då fraktionskroppen ut?
För varje element $a + \sqrt{3}b$ vill vi lägga till en invers $\frac{1}{a+\sqrt{3}b}$.

$$\frac{1}{a + \sqrt{3}b} = \frac{a - \sqrt{3}b}{a^2 - 3b^2} = \left(\frac{a}{a^2 - 3b^2}\right) + \sqrt{3}\left(\frac{b}{3b^2 - a^2}\right) = c + \sqrt{3}d \qquad c, d \in \mathbb{Q}$$

så fraktionskroppen är

$$\{a + \sqrt{3}b \mid a, b \in \mathbb{Q}\}.$$

Ett exempel på en nolldelarfri ring som inte är en Oredomän är följande:
Låt K vara någon kropp, och låt $G = \langle x, y \rangle$ vara den fria monoiden på

symbolerna x och y. Det betyder att G består av alla ändliga strängar av x och y. Multiplikation i G ges av sammansättning av strängar, till exempel

$$yxx \cdot yy = yxxyy.$$

$$\text{Sätt} \quad K[G] = \{\sum_i k_i g_i \mid k_i \in K,\ g_i \in G\}.$$

Detta är då en nolldelarfri ring:
Addition ges av

$$\sum_i k_i g_i + \sum_j h_j g_j = \sum_l r_l g_l \quad \text{där } l \text{ går över alla } i \text{ och } j$$

$$\text{och} \quad r_l = \begin{cases} k_l + h_l & \text{om } g_l \text{ förekommer i båda summorna} \\ k_l & \text{om } g_l \text{ bara förekommer i den första summan} \\ h_l & \text{om } g_l \text{ bara förekommer i den andra summan.} \end{cases}$$

Multiplikation ges av

$$\sum_i k_i g_i \cdot \sum_j h_j g_j = \sum_{i,j} k_i h_j g_i g_j$$

där summan alltså går över alla par av i och j.

För att visa att $K[G]$ är nolldelarfri behöver vi först införa en ordning på elementen i G.
Ordna först elementen efter antalet symboler i strängen, så till exempel $x < xy$. För strängar av samma längd, ordna som i ett lexikon, så till exempel $x < y$ och $yx < yy$.
För varje ändlig delmängd av G finns då alltid precis ett största element.
Antag nu att

$$\sum_i k_i g_i \cdot \sum_j h_j g_j = \sum_{i,j} k_i h_j g_i g_j = 0$$

där $\sum_i k_i g_i \neq 0$ och $\sum_j h_j g_j \neq 0$.
Låt g_α vara den största av alla g_i, och g_β den största av alla g_j.
Vi kan anta att $k_\alpha, h_\beta \neq 0$.
Då måste $g_\alpha g_\beta$ vara den största av alla strängar i produkten:
För alla $g_i g_j$ där g_i kortare än g_α eller g_j kortare än g_β är det klart att $g_i g_j < g_\alpha g_\beta$.
Låt säga att g_i är av samma längd som g_α och g_j samma längd som g_β. Då kan $g_i g_j = g_\alpha g_\beta$ endast om $g_i = g_\alpha$ och $g_j = g_\beta$, och annars är $g_i g_j < g_\alpha g_\beta$.

Termen $k_\alpha h_\beta g_\alpha g_\beta$ kan alltså inte tas ut av någon annan term. Då måste $k_\alpha h_\beta = 0$. Men K är en kropp och har inga nolldelare, så k_α eller h_β måste vara 0. Men det är en motsägelse, så vi kan alltså inte ha nolldelare i $K[G]$.

Titta nu på vänsteridealen

$$K[G]x = \{\sum_i k_i g_i x \mid k_i \in K,\ g_i \in G\}$$

$$K[G]y = \{\sum_i k_i g_i y \mid k_i \in K,\ g_i \in G\}$$

Notera att $g_i x \neq g_j y$ oavsett val av g_i och g_j eftersom den sista symbolen alltid kommer att skilja dem åt, så

$$K[G]x \cap K[G]y = \{0\}.$$

Vänster Orevillkor är inte uppfyllt. Höger Orevillkor är inte heller uppfyllt eftersom

$$xK[G] = \{\sum_i k_i x g_i \mid k_i \in K,\ g_i \in G\}$$

$$yK[G] = \{\sum_i k_i y g_i \mid k_i \in K,\ g_i \in G\}$$

och $xg_i \neq yg_j$ för alla i, j.
$K[G]$ är alltså ingen Oredomän och har då heller ingen fraktionskropp.

Slutligen kan det vara på sin plats med ett exempel på en icke kommutativ ring som uppfyller Orevillkoret.

Definition 10. *En **högernoethersk domän** är en nolldelarfri ring där varje högerideal är ändligt genererat, det vill säga genereras av ett ändligt antal element. En **vänsternoethersk domän** definieras analogt.*

Ett ekvivalent villkor för högernoetherskhet är att för varje kedja av högerideal

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

finns ett n så att

$$I_n = I_{n+1} = \dots.$$

Betrakta nu derivering som en linjär operator D på vektorrummet av reella oändligt deriverbara funktioner

$$f \longmapsto f'_x = Df.$$

Multiplikation med variabeln x kan också ses som en sådan operator

$$f \longmapsto xf.$$

Dessa två operatorer uppfyller $Dx - xD = 1$.
Vi ska betrakta ringen

$$W = \mathbb{C}\langle x, D\rangle/(Dx - xD - 1)$$

som generaras av dessa två operatorer, där $\mathbb{C}\langle x, D\rangle$ alltså är $\mathbb{C}[G]$ för den fria monoiden G på x och D.
Denna ring kallas den första Weyl algebran är en icke kommutativ Ore-domän.
Multiplikationen i denna ring är uppenbarligen inte kommutativ, eftersom $Dx = xD + 1 \neq xD$. Denna likhet gör också att varje element i W kan skrivas som

$$\sum_{i=0}^{k} p_i(x) \cdot D^i$$

där $p_i(x)$ är något polynom med koefficienter i $\mathbb{C}$.
Till exempel är

$$Dx^2 - xD = (xD + 1)x - xD = xDx + x - xD =$$

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

Lemma 4. *W är en Noethersk domän.*

Bevis. $R = \mathbb{C}\langle x, D\rangle$ är noethersk (varje ideal är ändligt genererat).
Vi inför en filtrering på R. Låt

$$F_d = \{\text{polynom av grad} \leq d\}.$$

Notera att här är till exempel x^2D såväl som xD^2 av grad 3. Vi får att

$$F_d/F_{d-1} = \{\text{monom av grad } d\}.$$

Låt $\overline{z} \in F_i/F_{i-1}$ och $\overline{y} \in F_j/F_{j-1}$. Det vill säga $\overline{z} = z + F_{i-1}$ och $\overline{y} = y + F_{j-1}$, för monom z och y av grad i respektive j. Definiera multiplikation som

$$\overline{z} \cdot \overline{y} = zy + F_{j+i-1},$$

så $\overline{z} \cdot \overline{y} \in F_{i+j}/F_{i+j-1}$.
Då måste vi ha att

$$\frac{F_i}{F_{i-1}} \cdot \frac{F_j}{F_{j-1}} = \frac{F_{i+j}}{F_{i+j-1}}.$$

Sätt nu

$$grR = F_0 \oplus \frac{F_1}{F_0} \oplus \frac{F_2}{F_1} \oplus \dots .$$

Denna ring är isomorf till $\mathbb{C}\langle x, D\rangle$, så grR är noethersk.
Antag nu att $I_0 \subset I_1 \subset I_2 \subset \dots$ är ideal av W. Vi vill visa att, för tillräckligt stort m är $I_m = I_{m+1}$.
Notera följande

$$(I_m \cap F_d) \subset (I_m \cap F_{d+1}) \subset \dots,$$

$$\frac{I_m \cap F_d}{I_m \cap F_{d-1}} \text{ är en delmängd av } \frac{F_d}{F_{d-1}}$$

$$\text{och } \frac{I_m \cap F_i}{I_m \cap F_{i-1}} \cdot \frac{I_m \cap F_j}{I_m \cap F_{j-1}} = \frac{I_m \cap F_{i+j}}{I_m \cap F_{i+j-1}}.$$

$$\text{Sätt } grI_m = I_m \cap F_0 \oplus \frac{I_m \cap F_1}{I_m \cap F_0} \oplus \frac{I_m \cap F_2}{I_m \cap F_1} \oplus \dots .$$

grI_m är då ett ideal av grR. Eftersom grR är noethersk är $grI_m = grI_{m+1}$ för något tillräckligt stort m.
Påstående: Detta medför att $I_m = I_{m+1}$.
För att visa påståendet antag motsatsen, det vill säga att det finns $p \in I_{m+1}$ sådant att $p \notin I_m$. Antag också att p är det polynom av minsta grad som har denna egenskap, och sätt $grad(p) = d$. Då måste

$$(I_m \cap F_d) \subset (I_{m+1} \cap F_d) \quad \text{och} \quad (I_m \cap F_{d-1}) = (I_{m+1} \cap F_{d-1})$$

och vi får att

$$\underbrace{\frac{I_m \cap F_d}{I_m \cap F_{d-1}}}_{A} \subset \underbrace{\frac{I_{m+1} \cap F_d}{I_{m+1} \cap F_{d-1}}}_{B}.$$

Lägg märke till att A är monomen av grad d i grI_m, och att B är monomen av grad d i grI_{m+1}. Men $grI_m = grI_{m+1}$, så vi måste ha att $A = B$. Det motsäger antagandet om p, så vi måste ha att $I_m = I_{m+1}$ och W är därmed noethersk. □

Följande sats visar att W är en Oredomän.

Sats 7. *Varje högernoethersk domän är en höger Oredomän.*

Bevis. Antag att R är en högernoethersk domän. Välj godtyckligt $a, b \in R$. Vi vill visa att $aR \cap bR \neq \{0\}$.
Betrakta högeridealet

$$I = (b, ab, a^2b, a^3b, \dots)$$

Eftersom R är en högernoethersk domän måste I vara ändligt genererat. Antag därför att

$$I = (c_1, \dots, c_k),$$

där varje c_i, $i = 1, \ldots, k$, är en linjärkombination av ett ändligt antal element $a^j b$. Låt t vara det största heltal sådant att $a^t b$ förekommer i uttrycket för något $c_1, \ldots c_k$. Då är

$$I = (c_1, \ldots c_k) \subseteq (b, ab, a^2 b, \ldots a^t b) \subseteq I$$

så

$$I = (b, ab, a^2 b, \ldots a^t b).$$

Varje $a^s b$, för $s > t$ måste alltså vara en linjärkombination av $b, ab, \ldots a^t b$. Med andra ord är $b, ab, a^2 b, \ldots$ linjärt beroende. Det betyder att

$$\sum_{1=0}^{s} a^i b c_i = 0 \quad \text{där ej alla } c_i \text{ är } 0.$$

Låt c_r vara den första som ej är 0. Då är

$$a^r b c_r + a^{r+1} b c_{r+1} + \cdots + a^n b c_n = 0$$

$$\Longleftrightarrow$$

$$a^r (b c_r + ab c_{r+1} + \cdots + a^{n-r} b c_{n-r}) = 0$$

$$\Longleftrightarrow$$

$$b c_r + ab c_{r+1} + \cdots + a^{n-r} b c_{n-r} = 0$$

$$\Longleftrightarrow$$

$$a(b c_{r+1} + \cdots + a^{n-r-1} b c_{n-r-1}) = -b c_r = b(-c_r).$$

Vi har alltså

$$aR \cap bR \neq \{0\}$$

och R är en höger Oredomän. □

Analogt kan man visa att varje vänsternoethersk domän är en vänster Oredomän.

Referenser

[1] J.A. Beachy, W.D Blair
Abstract algebra
Waveland press

[2] N.L. Biggs
Discrete mathematics
Oxford University Press, 2009, andra upplagan

[3] P.M. Cohn
Skew fields - Theory of general division rings
Cambrige University Press, 1995

[4] J.H. Conway, D.A. Smith
On quaternions and octonions
A K Peters, 2003

[5] J.B. Fraleigh
A first course in abstract algebra
AW, 2002

[6] I.N. Herstein
Topics in algebra
Ginn and company, 1964, första upplagan

[7] J.W. Milnor, J. Stasheff
Characteristic classes
Princeton University Press, 1974

[8] Wikipedia
`sv.wikipedia.org`
`en.wikipedia.org`