Grunnleggende konsepter i algebra

John Aslak Wee Kleven

27. februar 2023

I dette notatet skal vi se på grunnleggende konsepter i algebraen. Notatet er skrevet for den som aldri har sett disse konseptene, og innholdet er valgt for å kunne ha en matematisk(/algebraisk) diskusjon av kvaternionene etterpå. Referanser er [3] og [1].

1 Grupper

1.1 Definisjon

Prototypisk eksempel: $\mathbb{Z}$ med addisjon. Bare husk at grupper ikke trenger å være kommutative.

Definisjon 1.1. En 2-tuppel $(G, *)$ er en gruppe hvis $* : G \times G \to G$ er en funksjon, og

1. $a * (b * c) = (a * b) * c$ for hver $a, b, c \in G$,
2. Det fins en $e \in G$ slik at $e * a = a * e = a$ for hver $a \in G$. (Merk at e er unik),
3. For hver $a \in G$ fins $b \in G$ slik at $a * b = b * a = e$.

Vi skriver vanligvis a^{-1} for b-en i aksiom nr. 3 (så fort vi har vist at den er unik).

Kommentar. Vi kaller en gruppe *additiv* hvis vi kaller gruppeoperasjonen $+$, og *multiplikativ* hvis vi kaller gruppeoperasjonen $*$ eller $\cdot$ eller $\times$. Dette er fordi addisjon og multiplikasjon danner ofte grupper, og hvis man er i en kontekst hvor man har begge samtidig så blir det et behov for å skille mellom dem.

Kommentar. Når man har jobba når med grupper, så er det vanlig å sløyfe gruppeoperasjonen. For eksempel i $(G, *)$ skriver man vanligvis abc for $a * b * c$.

Eksempel 1.2. Mengdene

$$\{A \in \mathbb{R}^{n\times n} \mid \det(A) \neq 0\} \quad \text{og} \quad \{A \in \mathbb{R}^{n\times n} \mid \det(A) = \pm 1\}$$

er alle grupper under matrisemultiplikasjon.

Eksempel 1.3. Heltallene er en additiv gruppe, $(\mathbb{Z}, +)$, hvor minus blir inversen. De reelle tallene har både en additiv gruppe $(\mathbb{R}, +)$, og en multiplikativ gruppe

$$\mathbb{R}^* = \{x \in \mathbb{R} \mid x \neq 0\} = \mathbb{R} \setminus \{0\}$$

under multiplikasjon, hvor divisjon blir inversen.

Eksempel 1.4. Den komplekse enhetssirkelen

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

danner en gruppe under multiplikasjon.

De siste to eksemplene er grupper hvor man kan bytte rekkefølgen på gange-operasjonen:

Definisjon 1.5. En gruppe $(G, *)$ er *abelsk* hvis multiplikasjonen er *kommutativ*, altså hvis $a * b = b * a$ for hver $a, b \in G$.

1.2 Undergrupper

En undergruppe skal være en gruppe inni en annen gruppe.

Definisjon 1.6. En mengde $G' \subseteq G$ av en gruppe $(G, *)$ er en *undergruppe* hvis $(G', *)$ er en gruppe og $*$ er samme gruppeoperasjon som $(G, *)$.

Eksempel 1.7. (Dumt eksempel): For hver gruppe G er både G og $\{e\}$ undergrupper.

Eksempel 1.8. La G være en gruppe, og $g \in G$ et element. Da er

$$\{g^i \mid i \in \mathbb{Z}\} = \{\cdots, g^{-2}, g^{-1}, e, g, g^2, \cdots\}$$

en undergruppe av G. Denne kalles *undergruppen generert av* g, og skrives vanligvis (g) eller $\langle g \rangle$.

Eksempel 1.9. Vi har en kjede av additive undergrupper: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Eksempel 1.10. Mengden

$$G = \left\{ \begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & e & f \end{pmatrix} \mid a, b, c, d, e, f \in \mathbb{R},\ a, c, f \neq 0 \right\}$$

er en gruppe siden diagonalelementene (egenverdiene) er alle ikkenull, så disse matrisene er alle inverterbare. Her er en undergruppe:

$$G' = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R},\ a, b, c \neq 0 \right\} \subset G$$

Eksempel 1.11. Heltallene modulo n er gruppe; for eksempel er $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ en additiv gruppe med

$$\overline{1} + \overline{2} = \overline{3}$$
$$\overline{1} + \overline{3} = \overline{0}$$

og så videre. Dette er moduloregning. Et eksempel på dette er det man kan kalle klokkeregning (f.eks. "to timer etter klokka elleve er klokka ett"), som er $\mathbb{Z}_{12}$.

Eksempel 1.12. Gitt to grupper $(G, *_G)$ og $(H, *_H)$ kan vi definere en "produktgruppe" på

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

hvor vi bruker operasjonene fra G og H, punktvis

$$(a, b) *_{G\times H} (c, d) = (a *_G c, b *_H d)$$

Identiteten i $G \times H$ blir (e_G, e_H). Man kan gjøre dette produktet for så mange grupper man vil (inklusiv uendelig mange).

1.3 Gruppehomomorfier

Intuisjon: En (gruppe)homomorfi er en funksjon som bevarer all struktur (som en gruppe) har. De minner om lineærfunksjoner mellom vektorrom.

Definisjon 1.13. La $(G, *_G)$ og $((G, *_{G'})$ være grupper. En funksjon $f : G \to G'$ er en *(gruppe)homomorfi* hvis

$$f(g *_G h) = f(g) *_{G'} f(h)$$

for hver $g, h \in G$.

Eksempel 1.14. Eksponensialfunksjonen $\exp(x) = e^x$ tilfredsstiller

$$\exp(x) \cdot \exp(y) = \exp(x + y)$$

så $\exp : \mathbb{R} \to \mathbb{R}$ er en gruppehomomori fra $(\mathbb{R}, +)$ til $(\mathbb{R} \setminus \{0\}, \cdot)$ Tilsvarende er logaritmen $\log : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ en gruppehomomorfi som går den andre veien.

Eksempel 1.15. Funksjonen $f : \mathbb{Z} \to \mathbb{Z}_n$ ved "projiseringen" $f(n) = \overline{n}$.

Hvis en gruppehomomorfi også er bijektiv, så vil den bevare all struktur en gruppe har. Derfor får de et spesielt navn:

Definisjon 1.16. En gruppehomomorfi $f : G \to G'$ er en *isomorfi* hvis den i tillegg til å være en gruppehomomorfi, er bijektiv. I så fall sier vi at G og G' er *isomorfe*.

Isomorfier bevarer alle påstander man kan si om en gruppe som kun bruker gruppeoperasjonene, så de er kliss like for alle (algebraiske) formål.

Eksempel 1.17. I forrige eksempel så vi på eksponensialfunksjonen og logaritmer. Hvis vi begrenser kodomenet og ser på

$$\exp : \mathbb{R} \to \mathbb{R}^+, \qquad \log : \mathbb{R}^+ \to \mathbb{R}$$

så blir disse funksjonene surjektive, og siden de er injektive fra før av blir de isomorfier. Så de reelle tallene som en additiv gruppe $(\mathbb{R}, +)$ er isomorf med de positive reelle tallene under multiplikasjon $(\mathbb{R}^+, \cdot)$. Påstander om disse gruppene kan vi altså overføre fra den ene til den andre.

2 Ringer

Intuisjon: En ring er et slags generalisert tallsystem.
Prototypisk eksempel: $\mathbb{Z}$ og $\mathbb{R}^{n\times n}$

Definisjon 2.1. En 3-tuppel $(R, +, \cdot)$ er en *ring* hvis $+$ og $\cdot$ er funksjoner fra $R \times R$ til R og

1. $(R, +)$ er en (additiv) abelsk gruppe,
2. $(R, \cdot)$ er en semigruppe, altså at $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for hver $a, b, c \in R$, og
3. Multiplikasjon distribuerer på begge sider over addisjon, altså

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{og} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

for hver $a, b, c \in R$.

Advarsel: Matematikere er ikke enige om detaljene ved hva ordet "ring" skal bety. Her har brukt vi den mest generelle definisjonen av de som brukes. Noen krever at ringer har 1 (se definisjon 2.9), og noen krever at den er kommutaiv (se definisjon 2.12).

Gruppeidentieten til $(R, +)$ kalles nullelementet til ringen, og skrives 0. Den additive inversen til en $a \in R$ skrives $-a$, så $a + (-a) = 0$ for hver $a \in R$.

Eksempel 2.2. Disse er alle ringer mange kjenner fra før av:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Eksempel 2.3. Mengden av $n \times n$-matriser $\mathbb{R}^{n\times n}$ er en ring. Den additive identiteten er nullmatrisen. I $\mathbb{R}^{n\times n}$ er ikke multiplikasjon kommutaitv, og ikke alle elementer har (multiplikative) inverser, i motsetning til $\mathbb{Q}, \mathbb{R}$ og $\mathbb{C}$.

Eksempel 2.4. Mengden $C[0, 1]$ av kontinuerlige funksjoner f på formen $f : [0, 1] \to \mathbb{R}$, danner en ring med punktvis addisjon og multiplikasjon;

$$(f + g)(x) = f(x) + g(x), \quad \text{og} \quad (f \cdot g)(x) = f(x) \cdot g(x).$$

Eksempel 2.5. La V være et vektorrom. Mengden av alle lineærfunksjoner

$$\mathcal{L}(V) = \{f : V \to V \mid f \text{ lineærfunksjon}\}$$

danner en ring under punktivs addisjon og komposisjon. Altså er $(\mathcal{L}(V), +, \circ)$ en ring, med

$$(f + g)(x) = f(x) + g(x) \quad \text{og} \quad (f \circ g)(x) = f(g(x))$$

som ringoperasjoner.

Eksempel 2.6. $\mathbb{R}[x]$, mengden av alle polynomer med koeffisienter i $\mathbb{R}$ og i én variabel x, danner en ring under vanlig multiplikasjon og addisjon av polynomer. Man kan også lage polynomringer med flere variable, som $\mathbb{R}[x, y]$. Når man har to variable kan man velge velge om xy og yx skal være like, eller ulike. I begge tilfeller får man ringer. Vanligvis betyr $\mathbb{R}[x, y]$ at

Eksempel 2.7. Dualtallene

$$\mathbb{R}[\varepsilon] = \{(a, b) \mid a, b \in \mathbb{R}\}$$

er en ring med operasjonene

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{og} \quad (a, b) \cdot (c, d) = (ac, ad + bc).$$

Elementet (a, b) skrives som $a + b\varepsilon$. Så siden $(0, 1)^2 = (0, 0)$ sier vi at $\varepsilon^2 = 0$. Med denne notasjonen kan vi generere dualtallene fra $\mathbb{R}[x]$ ved å kreve at $x^2 = 0$. Siden vi kan tenke på $\mathbb{R}[x]$ som at vi har tatt $\mathbb{R}$, kunstig lagt til et element x, og kunstig gjort det om til en ring, så kan vi se på $\mathbb{R}[\varepsilon]$ som at vi tar $\mathbb{R}$, kunstig legger til en $\varepsilon \neq 0$ og krever at $\varepsilon^2 = 0$.

Dualtallene har en matriserepresentasjon i $\mathbb{R}^{2\times 2}$ hvor

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad \text{og} \quad \varepsilon \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Sånn sett kan vi se på dualtallene som en underring av $\mathbb{R}^{2\times 2}$.

Eksempel 2.8. La $(G, *)$ være en gruppe. Mengden

$$R = \{f : G \to G \mid f \text{ er en gruppehomomorfi}\}$$

danner en ring, kalt *endomorfi*[1] *ringen* til gruppa, med punktvis addisjon og komposisjon som ringoperasjonene, altså med de samme operasjonene som $\mathcal{L}(V)$: For $f, h \in R$, definer $f + h$ og $f \cdot h = f \circ h$ ved

$$(f + h)(x) = f(x) + h(x); \quad (f \circ h)(x) = f(h(x))$$

for hver $x \in G$. Da er $(R, +, \circ)$ en ring.

Når man snakker om ringer, så er det mange adjektiver man kan slenge på.

Definisjon 2.9. En ring R har *enhet* hvis det fins en $e \in R$ slik at $ex = xe = x$ for hver $x \in R$. (Dette elementet kalles enheten til R, og skrives 1).

Definisjon 2.10. Et elment a i en ring med enhet R er en enhet / er inverterbart hvis det fins en $b \in R$ slik at

$$ab = ba = 1.$$

Definisjon 2.11. En ring med enhet R er en *divisjonsring* hvis for hver $0 \neq x \in R$ fins $y \in R$ slik at

$$xy = yx = 1.$$

Dette er det vi kaller divisjon.

Definisjon 2.12. En ring R er *kommutativ* hvis multiplikasjonen er kommutativ, altså hvis

$$ab = ba$$

for hver $a, b \in R$.

[1] En (gruppe)homomorfi fra G til G kalles en endomorfi. Tilsvarende kan lineærfunksjoner også kalles endomorfier, så $\mathcal{L}(V)$ er sånn sett endomorfiringen til vektorrommet V.

Eksempel 2.13. Med disse adjektivene er dualtallene $\mathbb{R}[\varepsilon]$ en kommutativ ring med enhet som *ikke* er en divisjonsring, siden det fins ingen $x \in \mathbb{R}[\varepsilon]$ slik at $x\varepsilon = 1$. Altså kan man ikke dele på ε.

Eksempel 2.14. Mengden

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^m} \in \mathbb{Q} \mid a \in \mathbb{Z}, m \in \mathbb{N}_0\right\}$$

med addisjon og multiplikasjon som i $\mathbb{Q}$, er en ring. Denne ringen blir dermed ekte skvist mellom $\mathbb{Z}$ og $\mathbb{Q}$, siden den er en underring av $\mathbb{Q}$ som selv har $\mathbb{Z}$ som underring. Vi kan tenke på $\mathbb{Z}[1/2]$ som at vi har tatt $\mathbb{Z}$, gjort 2 inverterbar (ved å kunstig legge til $1/2$), og sett hva slags ring vi ville fått ut av det[2]. Før vi gjorde denne konstruksjonen, har $\mathbb{Z}$ enhetene ± 1. Ved å gjøre 2 inverterbar i $\mathbb{Z}[1/2]$ blir også alle toerpotenser $4, 8, 16, 32, \cdots$ også inverterbare. (Relatert til dette er det at mengden av inverterbare elementer i en ring R med enhet danner en multiplikativ gruppe).

Noen av ringene vi så over er eksempler på ringer som er spesielt fine, nemlig kommutative divisjonsringer. Disse kalles

Definisjon 2.15. En *kropp* er en kommutativ divisjonsring.

Kropper betegnes vanligvis med k, $\mathbb{F}$, og $\mathbb{K}$. I dette notatet vil vi bruke k.

Eksempel 2.16. De vanligste eksemplene på kropper er $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$. $\mathbb{Z}$ er ikke en divisjonsring, så det er ikke en kropp.

Eksempel 2.17. For hver $n \in \mathbb{Z}$ er

$$\mathbb{Q}(\sqrt{n}) = \{p + q\sqrt{n} \in \mathbb{C} \mid p, q \in \mathbb{Q}\}$$

en kropp, hvor vi definerer addisjon og multiplikasjon til å være som i $\mathbb{C}$. (Merk at hvis n er et kvadrattall så blir dette bare $\mathbb{Q}$, så det mest interessante er når n ikke er et kvadrattall.) Kroppen $\mathbb{Q}(\sqrt{n})$ er skvist mellom to kjente kropper:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{n}) \subset \mathbb{C}.$$

Eksempel 2.18. Ringen $\mathbb{Z}_n$ av heltallene modulo n, for en $n \in \mathbb{N}$, er en kropp hvis og bare hvis n er et primtall. For eksempel er

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

en kropp. For eksempel, siden

$$\overline{2} \cdot \overline{3} = \overline{1}$$

i denne ringen (siden $2 \cdot 3 = 6 \equiv 1 \pmod 5$) er $\overline{2}$ og $\overline{3}$ hverandres inverser. Dermed blir $\mathbb{Z}_5$ en divisjonsring, siden $\overline{1}$ er enheten og dermed sin egne invers og $\overline{0}$ er nullelementet.

[2]Det generelle konseptet av å ta en mengde med ting i en ring og å gjøre dem inverterbare kalles lokalisering. Den interesserte leser kan lese om det i [3, s. 224ff] hvor det går under navnet brøkringer / "rings of fractions", og i den mer avanserte boka [2]. I dette tilfellet kan vi også tenke på det som et eksempel på en faktorring, som dette notatet ikke sier noe om, da $\mathbb{Z}[1/2]$ er isomorf med $\mathbb{Z}[x]/(2x-1)$.

2.1 Ringhomomorfier

Mellom alle algebraiske strukturer har man et konsept av *funksjoner som bevarer struktu*. For vektorrom er det lineærfunksjoner. For grupper er det gruppehomomorfier. For algebraer (som kommer senere) er det algebrahomomorfier. For monoider, representasjoner og moduler (ikke nevnt i dette notatet) er det monoidehomomorfier, representasjonshomomorifer og modulhomomorfier. Tilsvarende vil ringhomomorfi en være funksjon mellom ringer som bevarer struktur.

Definisjon 2.19. La R og S være ringer, og $f : R \to S$ en funksjon. Da er f en *ringhomomorfi* hvis

1. $f(a + b) = f(a) + f(b)$ for hver $a, b \in R$, og
2. $f(a \cdot b) = f(a) \cdot f(b)$ for hver $a, b \in R$.

Tilsvarende definisjonen av gruppehomomorfier har vi også ringisomorfier, og de vil bevare all struktur en ring kan ha.

Definisjon 2.20. En ringhomomorfi er en isomorfi hvis den er bijektiv.

Eksempel 2.21. Det sies ofte at de komplekse tallene $\mathbb{C}$ har en representasjon av matriser ved

$$a + bi \leftrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{R}^{2\times 2}$$

(merk at mengden av alle reelle matriser på denne formen danner en ring).

Det dette vil si er at funksjonen $f : \mathbb{C} \to \mathbb{R}^{2\times 2}$ gitt ved

$$f(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

er en isomorfi mellom ringer. Det betyr spesielt at vi kan oversette konsepter mellom matriser og komplekse tall. Kall matriseringen for R. Ved isomorfien over vil komplekskonjugering i $\mathbb{C}$ tilsvare transponering i $\mathbb{R}$, altså

$$f(\overline{z}) = f(z)^T$$

og determinantfunksjonen tilsvarer lengden:

$$f(|z|^2) = \det(f(z)).$$

2.2 Isomorfier

På samme måte som for grupper skal en isomorfi være en biejtkvi ringhomomorfi:

Definisjon 2.22. La $f : R \to S$ være en ringhomomorfi. Da er f en *isomorfi* hvis f i tillegg er bijektiv.

2.3 Underringer

På samme måte som for grupper, skal en underring være en liten ring inni en større ring.

Definisjon 2.23. La $(R, +, \cdot)$ være en ring. Da er en mengde $S \subseteq R$ en *underring* hvis $(S, +, \cdot)$ er selv en ring, og hvor $+$ og $\cdot$ er de fra R, begrensa til S.

På samme måte som for grupper er det en fin karakterisering av når en ring er en underring.

Teorem 2.24. La R være en ring. En ikketom mengde $S \subseteq R$ er en underring hvis og bare hvis for hver $a, b \in S$ vil $a - b \in S$ og $ab \in S$.

Eksempel 2.25. Her er en kjede av underringer du sikkert har sett før:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

3 Algebraer

Prototypisk eksempel: $\mathbb{R}^{n\times n}$ er både en ring og et $\mathbb{R}$-vektorrom.

En algebra kan vi tenke på som en ring som også er et vektorrom.

Definisjon 3.1. La k være en kropp. En (assosiativ) k-algebra er en mengde Λ med funksjoner $+ : \Lambda \times \Lambda \to \Lambda$, $\cdot : \Lambda \times \Lambda \to \Lambda$ og $\cdot : k \times \Lambda \to \Lambda$ slik at

1. $(\Lambda, +, \cdot)$ er en ring,
2. $(\Lambda, +, \cdot)$ (nå med den andre $+$-en) er et vektorrom over k, og
3. Skalarproduktet og ringmultiplikasjonen samsvarer; for hver $a \in k$ og $\lambda, \lambda' \in \Lambda$ vil
$$a \cdot (\lambda \cdot \lambda') = (a \cdot \lambda) \cdot \lambda' = \lambda \cdot (a \cdot \lambda')$$

Én av grunnene til å studere algebraer, slik jeg forstår det, er at ved å ha en vektorromsstruktur kan vi gjøre lineæralgebra. For eksempel siden Λ er et vektorrom over k så har ringen en basis (som vektorrom over k), og med det kan vi snakke om ting som dimensjonen til Λ (over k) og sånt.

Algebraer med enhet har en fin karakterisering:

Lemma 3.2. Anta at Λ er en k-algebra med $1 \in \Lambda$ (altså at Λ, som ring, har enhet). Da har Λ en underring k' isomorf med k slik at skalarmultiplikasjonen $\cdot : k \times \Lambda \to \Lambda$ samsvarer med restriksjonen av ringmultiplikasjonen $\cdot : \Lambda \times \Lambda \to \Lambda$ på $k' \times \Lambda$.

Poenget er at skalarmultiplikasjonen er "det samme" som ringmultiplikasjonen "med" kopien av k inni Λ.

Bevis. (skisse) Definer en injektiv ringhomomorfi $\varphi : k \times \Lambda \to \Lambda$ ved $\varphi(a) = a \cdot 1$, og $\cdot$-en er skalarproduktet. Da vil bildet til φ være en underring/underkropp av Λ som er isomorf med k. Vis deretter at multiplikasjon med denne underkroppen er det samme som skalarproduktet. □

Eksempel 3.3. Vektorrommet $\mathbb{R}^2$ er en $\mathbb{R}$-algebra med er en $\mathbb{R}$-algebra med

$$\begin{aligned}(a, b) \cdot (c, d) &= (ac, bd),\\ (a, b) + (b, d) &= (a + b, c + d),\\ r \cdot (a, b) &= (ra, rb).\end{aligned}$$

Underkroppen som karakteriseringen snakker om er da

$$\{(a, a) \in \mathbb{R}^2 \mid a \in \mathbb{R}\}$$

Tilsvarende er $\mathbb{R}^n$ det for hver n, og også er k^n en k-algebra for hver kropp k.

Eksempel 3.4. La V være et vektorrom over en kropp k. Da er mengden

$$R = \begin{pmatrix} k & 0 \\ V & k \end{pmatrix} = \left\{ \begin{pmatrix} a & 0 \\ v & b \end{pmatrix} \mid a, b \in k, v \in V \right\}$$

en k-algebra med de operasjonene som følger av matrisemultiplikasjonen:

$$\begin{pmatrix} a & 0 \\ v & b \end{pmatrix} \begin{pmatrix} c & 0 \\ u & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ c \cdot v + b \cdot u & bd \end{pmatrix}$$

Skalarproduktet $a \cdot r$ for en $a \in k$ og $r \in R$ blir å gange i hvert element i r med a. Ved karakteriseringen i 3.2 vil skalarproduktet samsvare med å bare gange med elementer fra underringen

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in k \right\}$$

som er isomorf med k.

Eksempel 3.5. Kroppen $\mathbb{Q}(\sqrt{n})$ nevnt over, har $\mathbb{Q}$ som underkropp og kan dermed bli sett på som en $\mathbb{Q}$-algebra som også er en kropp.

4 Referanser

[1] John B. Fraleigh. *A First Course in Abstract Algebra*. 7. utg. Pearson, 2014. ISBN: 9780201407518.

[2] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. CRC Press, 1969. ISBN: 9780201407518.

[3] P. B. Bhattacharya and S. K. Jain and S. R. Nagpaul. *Basic Abstract Algebra*. Cambridge University Press, 1994. ISBN: 0521466296.