SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Algebraiska strukturer – Halvgrupper, Grupper, Ringar, Kroppar

av

Sebastian Alevad

2021 - No K13

Algebraiska strukturer – Halvgrupper, Grupper, Ringar, Kroppar

Sebastian Alevad

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Paul Vaderlind

2021

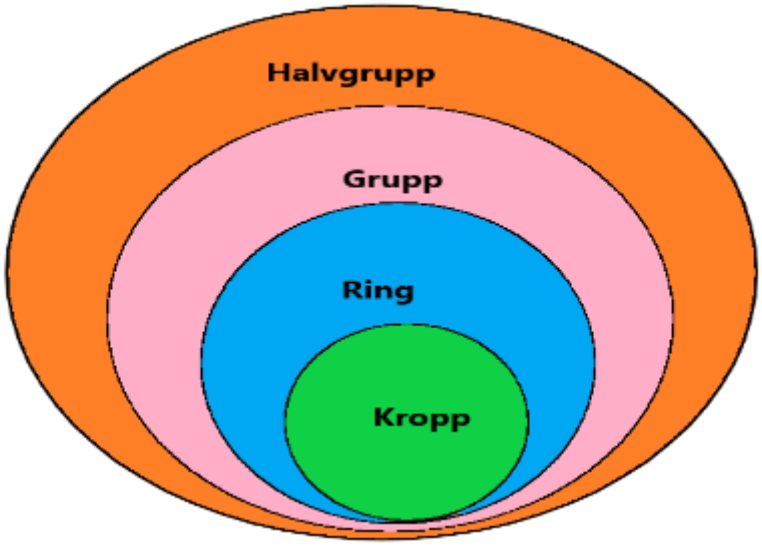
Abstract

This essay will function as an introduction to algebraic structures. In abstract algebra - or as it is also called, modern algebra - one studies the algebraic structures, these structures are defined as a set of elements equipped with a number of operations. In this essay I will only handle structures equipped with one or two operations, these are for example: addition, multiplication, geometric rotations, matrix addition and matrix multiplication. Depending on the algebraic structure, it must abide by a certain set of basic properties. These basic properties are the commutative and associative law for addition and multiplication and the distributive law for multiplication over addition. The set of elements does not have to be finite, if a neutral element and an inverse element exists or not. Even though there are more structures, this essay will contain following algebraic structures: semigroups, groups, rings and fields. But each of these four individual structures can be broken down into different categories, depending on if they abide by one or more of our basic properties.

Innehållsförteckning

Introduktion

Det här arbetet kommer handla om olika algebraiska strukturer. En algebraisk struktur är en icke tom mängd som utrustas med en eller flera operationer eller vad som ibland även kallas kompositioner. Om mängden A utrustas med en operation • så betecknas det med $\langle A,\bullet\rangle$. Strukturen A ska vara sluten med avseende på •, dvs. $a, b \in A \Rightarrow a \bullet b \in A$. A är en struktur under operationen •. Om A istället utrustas med två operationer $\bullet \; och \odot$ så betecknas den på följande vis: $\langle A,\bullet,\odot\rangle$. Operationerna kan vara olika räknesätt, främst addition eller multiplikation, men kan också anta formen av geometriska avbildningar, funktionssammansättning och matrisaddition/multiplikation. Grundmängden A kan till exempel utgöras av olika talmängder, geometriska figurer, matriser eller funktioner. Ju fler operationer som mängden utrustas med, desto mer komplex blir den algebraiska strukturen. I arbetet kommer strukturerna och dess relation till varandra granskas.



Algebraiska strukturer används främst inom abstrakt algebra och är ett verktyg för matematiker att studera olika matematiska system som har gemensamma egenskaper. Arbetet kommer främst stödja sig på Stig Christofferssons ”*Grupper Ringar Kroppar*”[1].

[1] Christoffersson, Stig, *Grupper Ringar Kroppar*, LiberLäromedel, Lund, 1975.

Kort historisk bakgrund

Under mitten av 1700-talet började matematikerna allt mer studera det som vi idag klassificerar som delar av abstrakt algebra. Euler studerade modulo räkning som bland annat skulle lägga grunden för Gauss etablering av cykliska och abelska grupperna. Även bevisen för de associativa lagarna kommer från Gauss forskning.[2] Men både Gauss och Euler var främst intresserade av konkreta resultat och inte generella teorier. Under samma tidsperiod men för en annan del av algebran så studerade Lagrange permutationer. Det var dock inte förens in på 1800-talet som begreppet ”grupper” började användas. Den första var Galois som hade byggt vidare på Gauss forskning om permutationer, Galois grupper är vad vi idag skulle kalla för permutationsgrupper. Galois dog blott 20 år gammal av skador han ådragit sig i en duell.

Under första halvan av 1900-talet skiftade många matematiker sitt fokus från den mer konkreta algebran till den abstrakta algebran, vars syfte var att bevisa mer allmänna teorier. Matematikerna började definiera mer komplexa algebraiska strukturer, såsom ringar och kroppar. Forskningen kring detta område (ibland kallat ”modern algebra”) skedde med stor spridning och ämnet växte sig allt större på kort tid. Många framträdande matematiker deltog i arbetet, deras forskning kom att definiera den abstrakta algebran.[3]

Mellan 1950-1982 hade man genom en väldigt stor satsning klassificerat alla ändliga ”enkla” (icke-triviala grupper med endast normala delgrupper) grupper. Howard Eves som skrivit *Foundations and fundamental concepts of mathematics* menar att de algebraiska strukturerna grupper och halvgrupper är algebrans svar på atomen, då de är grunden för uppbyggandet av många algebraiska system.[4]

Idag används abstrakt algebra inom bl.a. fysik, kemi och kryptologi. Ett annat användningsområde är vid framställning av sudokupussel.

---

[2] Associativa lag: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$, ytterligare förklaring kommer på s.3

[3] Forskare som bl.a. Ernst Kummer, Leopold Kronecker, Richard Dedekind Ernst Steinitz, David Hilbert, Emil Artin, Emmy Noether, George Frobenius och Issai Schur.

[4] Eves, Howard, *Foundations and fundamental concepts of mathematics,* third edition, PWS-Kent publishing company, Boston, 1990, s.128.

Undersökningsdel

1. Halvgrupper

Den första strukturen som behandlas är halvgrupp, den är förhållandevis enkelt uppbyggd och kommer stå som grund i detta arbete.

Definition 1.1 En halvgrupp $\langle H,\bullet\rangle$ är en struktur med en enda operation $\bullet$ som har egenskapen att vara associativ på mängden H, operationen $\bullet$ behöver inte vara kommutativ. Associativiteten betyder att operationen i halvgruppen ej är beroende av hur parenteser placeras:

$$a \bullet (b \bullet c) = (a \bullet b) \bullet c$$

Exempel 1.1 $\langle \mathbb{N}, + \rangle$ är en halvgrupp där $\mathbb{N}$ är de naturliga talen och + är vanlig additionen.

$\langle \mathbb{N},\cdot \rangle$ är också en halvgrupp där $\mathbb{N}$ fortfarande är naturliga talen och $\cdot$ är den naturliga multiplikationen. I båda fallen är strukturen sluten för operationen då addition och multiplikation med positiva heltal alltid ger summan / produkten som ett annat positivt heltal.

Nu kan man stegvis lägga till ytterligare kriterier på strukturen halvgrupp för att öka komplexiteten.

Definition 1.2 Om halvgruppen $\langle H,\bullet\rangle$ har ett neutralt element, kallas det istället för en monoid. De neutrala elementen betecknas ”e”. Det vill säga:

$$a \bullet e = e \bullet a = a \; för \; alla \; a \in H$$

Om monoiden är kommutativ (alltså att $a \bullet b = b \bullet a \; för \; alla \; a, b \in H$) kallas det kommutativ monoid.

Exempel 1.2 De naturliga talen $\langle \mathbb{N} \cup \{0\}, + \rangle$, där + är vanlig addition, bildar en kommutativ monoid där det neutrala elementet är 0, sådant att $n + e = n + 0 = n$.

$\langle \mathbb{N},\cdot \rangle$, där $\cdot$ är vanlig multiplikation, då får vi att: $n \cdot e = n \cdot 1 = n$, då är $\langle \mathbb{N},\cdot \rangle$ också en monoid.

Nu introducerar vi begreppet delstruktur och undersöker vilka egenskaper delstrukturer kan ärva av den tidigare givna strukturen.

Definition 1.3 Låt $\langle H,\bullet\rangle$ vara en halvgrupp och D en icke-tom delmängd till H. Om D är sluten med avseende på $\bullet$, kallas $\langle D,\bullet\rangle$ en delhalvgrupp till $\langle H,\bullet\rangle$. $\langle D,\bullet\rangle$ ärver vissa egenskaper av $\langle H,\bullet\rangle$, såsom associativitet om $\langle H,\bullet\rangle$ är associativ och kommutativ om $\langle H,\bullet\rangle$ är kommutativ. Men delhalvgruppens egenskaper är inte alltid samma som halvgruppens egenskaper. Om det finns ett element i struktur A med en viss egenskap, behöver det inte finnas något sådant element i en delstruktur B. Ett sådant exempel är $\langle \mathbb{N} \cup \{0\}, +\rangle$ (naturliga tal med operationen addition) neutrala element, som inte existerar i delstrukturen $\langle Z_+, +\rangle$ (positiva heltal med operationen addition).

Varje delhalvgrupp är i sig en halvgrupp.

Exempel 1.3 $\langle \mathbb{N}, +\rangle$ är en halvgrupp, från den halvgruppen kan man ta alla jämna tal sådant att: $\langle \mathrm{J}, +\rangle$ är en delhalvgrupp då J är alla jämna positiva heltal och $+$ är vanlig addition.

2. Grupper

En grupp består utav en icke-tom mängd och är utrustad med en operation. Denna grupp kan vi beteckna som $\langle G,\bullet\rangle$ där G är mängden och $\bullet$ är operationen. Till skillnad från halvgrupp krävs även att ett neutralt element existerar och att varje element i G har en invers. Inversen är alltså det motsatta element (kan även vara, funktion, matris, element, rotation, mm.) som ger $a + (-a) = 0$ och $a \cdot a^{(-1)} = 1$

Definition 2.1: En halvgrupp $\langle G,\bullet\rangle$ är en grupp om:

1) Det finns minst ett neutralt element e i G, dvs. ett element e som uppfyller:

$$a \bullet e = e \bullet a = a \; för \; alla \; a \in G$$

2) Till varje $a \in G$ finns minst ett element $a' \in G$ sådant att

$$a \bullet a' = a' \bullet a = e$$

Sats 2.1: Från axiomen följer att det neutrala elementet är unikt och det inversa elementet till $a \in G$ är unikt.

Bevis: Antag att det finns två element e och ê så att $e \bullet g = g = g \bullet e$ och ê $\bullet g = g = g \bullet$ ê för alla element $g \in$ G. Vi tittar nu på produkten $e \bullet$ ê, genom att sätta $g =$ ê i första ekvationen följer att $e \bullet$ ê $=$ ê, om vi istället sätter in $g = e$ i andra ekvationen så får vi att ê $\bullet$ $e = e$. Då blir $e = e \bullet$ ê $=$ ê alltså att $e =$ ê, det neutrala elementet blir unikt. Samma bevis används för att bevisa att det inversa elementet är unikt.

Hittills har vi nämnt kommutativitet i samband med enstaka exempel men vi ska nu definiera det i samband med abelska strukturer.

Definition 2.2 En abelsk grupp är en grupp vars operation $\bullet$ verkar kommutativt, dvs. $\langle G, \bullet \rangle$ är en abelsk grupp om $a \bullet b = b \bullet a$ $för$ $alla$ $a, b \in$ G.

Exempel 2.1: $\langle \mathbb{Z}, + \rangle$ är mängden heltal, operationen $+$ är vanlig addition.

Då två heltal A och B adderas blir summan också ett heltal, vilket också betyder att $\langle \mathbb{Z}, + \rangle$ är sluten.

För heltalen a, b, c gäller:

$$(a + b) + c \ = a + (b + c)$$

Alltså uppfylls associativitet.

$\langle \mathbb{Z}, + \rangle$ är en grupp (alla axiom gäller) med 0 som neutralt element och där för varje heltal a finns ett heltal b sådant att:

$$a + b = 0 \ och \ b + a = 0 \ , b = -a$$

Då vi redan visat att $a + b = b + a$ så är $\langle \mathbb{Z}, + \rangle$ även en abelsk grupp.

Exempel 2.2: $\langle \mathbb{Q} \setminus \{0\}, \bullet \rangle$, $\langle \mathbb{R} \setminus \{0\}, \bullet \rangle$ och $\langle \mathbb{C} \setminus \{0\}, \bullet \rangle$ är grupper där $\bullet$ är vanlig multiplikation. Men $\langle \mathbb{Z}, \bullet \rangle$ är inte en grupp då heltalet 2 saknar en invers i $\mathbb{Z}$. Inversen till 2 under multiplikation är $\frac{1}{2}$, alltså icke ett heltal.

Exempel 2.3: Alla reella $(n\ x\ n)$ matriser med determinanten ≠ 0 bildar en grupp med avseende på matrismultiplikation. Gruppen betecknas $GL_n(\mathbb{R})$, där $\mathbb{R}$ är reella tal. Vi visar att axiomen för en grupp gäller:

1) $A, B\ \in\ GL_n(\mathbb{R})\ \Rightarrow det\ A \neq 0\ och\ det\ B \neq 0 \Rightarrow det(AB) = det\ A \cdot det\ B \neq 0 \Rightarrow AB \in GL_n(\mathbb{R})$

Vilket visar slutenhet.

2) Enligt känd egenskap hos matrismultiplikation så

$$(AB)C = A(BC)\ då\ A, B, C\ \in GL_n(\mathbb{R})$$

Alltså uppfylls associativitet.

3) Det neutrala elementet, enhetsmatrisen, E för $(n\ x\ n)$-matriser ger:

$$EA = AE = A\ då\ A \in\ GL_n(\mathbb{R})$$

4) Inversen till A är A^{-1} och existerar då determinanten är skild från 0 och

$$AA^{-1} = A^{-1}\ \mathrm{A} = \mathrm{E\ om\ A}\ \in\ GL_n(\mathbb{R}).$$

Då axiomen uppfylls, bildar mängden av alla matriser på $(n\ x\ n) - form$ med reella element och determinanter skilda från 0 en grupp under matrismultiplikation. Det är däremot inte en abelsk grupp, då matrismultiplikation inte är kommutativ, ex:

$$A = \begin{pmatrix} 1 & -2 \\ 3 & -1 \end{pmatrix}\ B = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$$

$$AB = \begin{pmatrix} -3 & 4 \\ 1 & 7 \end{pmatrix} medan\ BA = \begin{pmatrix} 7 & -4 \\ -1 & -3 \end{pmatrix}$$

Två strukturer med samma algebraiska egenskaper men som har olika beteckning för elementen och/eller operationen kallas isomorfa. Nedan följer en definition.

Definition 2.3 En isomorfi från gruppen $\langle A, \bullet \rangle$ till gruppen $\langle \mathrm{B}, \Delta \rangle$ är en bijektion $\mathrm{f}: A \rightarrow B$, sådan att:[5]

[5] En bijektiv funktion är en funktion f, från mängden X till Y, som är omvändbar.

$$f(x \bullet y) = f(x) \Delta f(y)$$

för alla $x, y \in A$.

Isomorfiska grupper har samma algebraiska egenskaper. Till exempel om A och B är isomorfa grupper, är A kommutativ om och endast om B är kommutativ. Om man vill poängtera att både A och B är grupper, kallar man f en gruppisomorfi eller en isomorfi mellan grupper. Om A och B är samma grupp är f en (grupp-) automorfi.

Inversen till en gruppisomorfi är en gruppisomorfi och sammansättningen av gruppisomorfier är en gruppisomorfi.

Exempel 2.4 Logaritmen (med fix bas b), är funktionen som avbildar de positiva reella talen på alla reella tal:

$$log_b: \mathbb{R}^+ \to \mathbb{R}$$

Avbildningen är en bijektion ty det finns endast en bild i $\mathbb{R}$ för varje element i $\mathbb{R}^+$ och varje avbildat element i $\mathbb{R}$ har endast ett original i $\mathbb{R}^+$. Avbildningen är en gruppisomorfi och bevarar vissa operationer. Gruppen $\langle \mathbb{R}^+, \cdot \rangle$ där $\cdot$ är vanlig multiplikation granskas. Enligt logaritmlagarna är:

$$log_b(xy) = log_b(x) + log_b(y)$$

Men $\langle \mathbb{R}, + \rangle$ där + är vanlig addition är också en grupp. Vilket gör att logaritmen är en gruppisomorfi från $\langle \mathbb{R}^+, \cdot \rangle$ till $\langle \mathbb{R}, + \rangle$, alltså från positiva reella tal under multiplikation till de positiva reella talen under addition. Grupperna är strukturellt identiska, dvs. isomorfa.

Exempel 2.5 $Q[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in Q\}$ *och* $Q[\sqrt{3}] = \{a + b\sqrt{3} | a, b \in Q\}$

Då är f: $a + b\sqrt{2} \rightsquigarrow a + b\sqrt{3}$ där $a, b \in Q$ en gruppisomorfi från $\langle Q[\sqrt{2}], + \rangle$ till $\langle Q[\sqrt{3}], + \rangle$ (+ är vanlig addition), ty det är en bijektion, alltså:

$$f(a + b\sqrt{2} + a_1 + b_1\sqrt{2}) = f(a + a_1 + b\sqrt{2} + b_1\sqrt{2}) = a + a_1 + (b + b_1)\sqrt{3}$$
$$= a + b\sqrt{3} + a_1 + b_1\sqrt{3} = f(a + b\sqrt{2}) + f(a_1 + b_1\sqrt{2})$$

Däremot finner man att ƒ ej är en gruppisomorfi från $\left\langle Q\left[\sqrt{2}\right] \setminus \{0\},\cdot\right\rangle$ till $\left\langle Q\left[\sqrt{3}\right] \setminus \{0\},\cdot\right\rangle$ då · är vanlig multiplikation. Exempelvis är $f\left(\sqrt{2}\cdot\sqrt{2}\right) = f(2) = 2$ medan $f(\sqrt{2})f(\sqrt{2}) = \sqrt{3}\sqrt{3} = 3$

Isomorfier är specialfall av homomorfier. En homomorfi är en avbildning som bevarar operationen, en isomorfi är en bijektiv homomorfi.

Definition 2.4 En homomorfi (även kallad, homomorf avbildning). Från strukturen $\langle S,*\rangle$ till strukturen $\langle T,\bullet\rangle$ är en avbildning $f: S \to T$, sådan att för alla $x, y \in S$ gäller:

$$f(x * y) = f(x) \bullet f(y)$$

Exempel 2.6 a) $f: x \curvearrowright x^2$ är en homomorfi från $\langle Z,\cdot\rangle$ till $\langle N \cup \{0\},\cdot\rangle$, där operationen är vanlig multiplikation, ty $f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$

b) $f: t \curvearrowright i^t$ är en homomorfi från $\langle N,+\rangle$ till $\langle C,\cdot\rangle$, ty $f: (s+t) = i^{(s+t)} = i^s \cdot i^t = f(s)f(t)$

Det finns även specialfall av grupper, så kallade cykliska grupper.

Definition 2.5: En grupp G är cyklisk om den kan genereras av ett enda element. Det existerar alltså ett element $a \in$ G sådan att

$$G = \{a^k : k \in \text{ Z}\}$$

Exempel 2.7: Antag att en kvadrat roteras medsols. Låt r_1, r_2, r_3, r_4 vara rotationer med respektive 90, 180, 270 och 360 grader. Vi betecknar gruppen som $\langle G, \odot\rangle$ där $\odot$ är sammansättningar och $G = \{r_1, r_2, r_3, r_4\}$.

$$r_1 \odot r_1 = r_2$$

$$r_2 \odot r_3 = r_1$$

$$r_2 \odot r_2 = r_4$$

Gruppen är sluten eftersom vi endast kan generera element i mängden.

För rotationerna a, b, c ges:

$$(a \odot b) \odot c \ = a \odot (b \odot c)$$

Alltså uppfylls associativitet för kvadratrotationer.

$$r_2 = r_1^2 = r_1 \odot r_1$$

$$r_3 = r_1^3 = r_1 \odot r_1 \odot r_1$$

$$r_4 = r_1^4 = r_1 \odot r_1 \odot r_1 \odot r_1$$

Det neutrala elementet för $\langle G, \odot \rangle$ är r_4 då

$$r_1 \odot r_4 = r_4 \odot r_1 = r_1$$

Det existerar en invers för varje element i $\langle G, \odot \rangle$

$$r_1^{-1} = r_3$$

$$r_2^{-1} = r_2$$

$\langle G, \odot \rangle$ är alltså en cyklisk grupp då alla axiomen uppfylls.

3. Ringar

Tillskillnad från grupper, som endast är utrustade med en operation, så är ringar utrustade med två operationer (+,·). Under addition är ringar en abelsk grupp men under multiplikation är ringar en halvgrupp, för ringar måste även den distributiva lagen gälla.

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Definition 3.1 En ring är en algebraisk struktur med en mängd och två operationer som betecknas: ⟨R, +,· ⟩. (+) är addition och (·) är multiplikation. Följande axiom definierar den algebraiska strukturen ringar:

1) R är sluten med avseende på + och ·.

2) ⟨R, + ⟩ är en abelsk grupp.

3) ⟨R,· ⟩ är associativ och därför en halvgrupp

4) För addition ska distributiva lagar gälla för multiplikation, alltså att:

$$a(b+c) = ab + ac \text{ samt } (a+b)c = ac + bc$$

Om dessutom multiplikation är kommutativ så är R en kommutativ ring.

Exempel 3.1 Under addition och multiplikation räknas $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$ som kommutativa ringar. För att $\langle Z, +, \cdot \rangle$ ska vara en ring så måste bara distributivitet visas. Distributivitet kan visas genom:

$$a \cdot (b+c) = a(b+c) = ab + ac = a \cdot b + a \cdot c \; för \; a, b, c \in Z$$

Exempel 3.2 $\langle F, +, \cdot \rangle$ mängden F är alla kontinuerliga funktioner från $\mathbb{R} \rightarrow \mathbb{R}$ utrustade med operationerna addition och multiplikation:

$$(f+g)(x) = f(x) + g(x) \; och \; (f \cdot g)(x) = f(x)g(x)$$

De reella funktionerna är kommutativa under addition, alltså $g(x) + f(x) = f(x) + g(x)$.

Reella funktioner är även kommutativa under multiplikation, alltså $g(x) \cdot f(x) = f(x) \cdot g(x)$.

Kontinuerliga funktioner från $\mathbb{R} \rightarrow \mathbb{R}$ är associativa då $f \cdot (g \cdot h) = (f \cdot g) \cdot h$

Även de distributiva lagarna gäller för kontinuerliga funktioner i $\mathbb{R}$:

$$f \cdot (g+h) = (f \cdot g) + (f \cdot h)$$

Det betyder att $\langle F, +, \cdot \rangle$ är en kommutativ ring.

Ett icke-kommutativt exempel skulle vara sammansatta funktioner. Vid sammansättning av funktioner behöver inte operationen vara kommutativ.

Exempel 3.3 Antag funktionerna $f(x) = x^2$ och $g(x) = x - 3$, vid sammansättning av f och g får vi

$$f \circ g(x) = (x-3)^2$$

Där variabeln x i funktionen f(x) bytts ut mot funktionen g(x).

Vid sammansättning av g och f får vi istället

$$g \circ f(x) = x^2 - 3$$

Där variabeln x i funktionen g(x) bytts ut mot funktionen f. Då $(x-3)^2 \neq x^2 - 3$ är sammansättningen ∘ inte kommutativ.

Exempel 3.4 Ytterligare exempel på icke-kommutativa ringar är alla $(n\ x\ n)$ matriser då $n \geq 2$, eftersom multiplikation av matriser motsvarar sammansättningen av linjära funktioner.

Ringen innehållande matrisaddition/multiplikation är sluten, kommutativa under matrisaddition, associativa under matrismultiplikation, de distributiva lagarna gäller men $(n\ x\ n)$ matriserna är inte kommutativa under matrismultiplikation.

Exempel 3.5 Om vi granskar beviset till varför $(-1)(-1) = 1$ så ser vi att det bevisas genom att applicera samma axiom som för en kommutativ ring.

Det är klart att $1 - 1 = 0$ då operationen är addition med additiva inversen.

$$1 + (-1) = 0 \text{ eller } (-1) + 1 = 0$$

$$0 = 0 \cdot 0 = \big(1 + (-1)\big)\big(1 + (-1)\big) =$$

$$1 \cdot 1 + 1 \cdot (-1) + (-1) \cdot 1 + (-1) \cdot (-1) =$$

$$1 + (-1) + (-1) + (-1)(-1) =$$

$$(-1) + (-1)(-1) =$$

$$0 = (-1) + (-1)(-1)$$

Addera 1 till båda sidorna:

$$1 + 0 = 1 + (-1) + (-1)(-1)$$

$$1 = (-1)(-1)$$

Mängden är sluten. Vi ser att $1 + (-1) = (-1) + 1$ alltså kommutativ för addition. Vi kan kontrollera associativitet under multiplikation genom att testa

$$\big((-1) \cdot (-1)\big) \cdot 1 = (-1) \cdot \big((-1) \cdot 1\big)$$

Och från $(0) \cdot \big(1 + (-1)\big) = 0 \cdot 1 + 0 \cdot (-1)$ ser vi att distributiva lagarna gäller.

Ur beviset får vi också fram att kommutativitet gäller för multiplikation. Alla axiom är då uppfyllda.

Det finns speciella delmängder till ringar som kallas ideal.

Definition 3.2

I är en icke-tom delmängd till ringen R och är ett ideal om det uppfyller:

a) $a, b \in I \Rightarrow a - b \in I$ (operationen är additiv invers i det här fallet)

b) $r \in R \; och \; a \in I \Rightarrow ra, ar \in I$

I är en delring till R ty (a) säger att $(I, +)$ är en delgrupp till (R, +) och ur (b) följer att $a, b \in I$ ger $ab \in I$ dvs I är sluten under multiplikation.

Exempel 3.6 Heltal $mod\ n$:

$\mathbb{Z}/\ n\mathbb{Z} = \{0,1,2, \dots, n-1\}$ där $\mathbb{Z}$ är en ring och $n\mathbb{Z}$ är ett ideal för $\mathbb{Z}$. $\mathbb{Z}/\ n\mathbb{Z}$ är kvotringen[6] för $\mathbb{Z}$ av $n\mathbb{Z}$, där $n\mathbb{Z}$ är en additiv delgrupp och $a(nx) = n(ax) \in n\mathbb{Z}$ för varje $a \in \mathbb{Z}$ och $nx \in \mathbb{Z}$.

$\mathbb{Z}$ är en sluten kommutativ ring dessutom innehåller den ett identitetselement, i fallet mod n = 0.

I definition 2.3 och 2.4 gick vi igenom isomorfi och homomorfi för grupper, nu ska detta utvecklas på och det ska handla om ringhomomorfi/ringisomorfi. En ringhomomorfi *f* från R till S kan alltså tolkas som en grupphomomorfi från ⟨R, +⟩ till ⟨S, +⟩

Definition 3.3 Låt R och S vara ringar. Varje avbildning $f: R \to S$, sådan att för alla $x, y \in R$ gäller:

$$f(x + y) = f(x) + f(y) \text{ och } f(xy) = f(x)f(y)$$

Om detta uppfylls är avbildningen en ringhomomorfi och om avbildningen är bijektiv är den dessutom en ringisomorfi. Inverser och sammansättningar av ringisomorfier är också ringisomorfier.

Exempel 3.7 Tillordningen (en avbildning från en mängd X till en mängd Y är en tillordning av ett element i Y på varje element i X) mellan linjära avbildningar på ett n-dimensionellt

[6] För varje ideal H i en ring kallas R/H en kvotring.

vektorrum V_n och matriser (för en fix bas i V_n) är en ringisomorfi mellan ringen av linjära avbildningar på V_n och $M_n(R)$. Omvänt svarar matriser i $M_n(R)$ entydigt på de linjära avbildningarna från vektorrummet V_n. $M_n(R)$ är en ring då de linjära avbildningarna på vektorrummet V_n bildar en ring under punktvis addition av avbildningar(matrisaddition) och sammansättningar (matrismultiplikation).

Exempel 3.8 Låt polynomringen {P,+,·} där P är mängden av alla reella polynom och operationerna är addition och multiplikation, vara en kommutativ ring med en etta. Formen för en polynomring med reella koefficienter är:

$$a_0 + a_1X + a_2X^2 \ldots$$

där $a_i \in \mathbb{R}$. Antag att vi har tre polynom:

$$p(x) = \sum_{i=0} a_i x^i$$

$$q(x) = \sum_{j=0} b_j x^j$$

$$t(x) = \sum_{k=0} c_k x^k$$

Addition av polynom definieras:

$$p(x) + q(x) = \sum_{i=0} (a_i + b_j) x^i$$

Multiplikation av polynom definieras:

$$q(x) \cdot t(x) = \sum_{k} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

Polynomen måste vara kommutativa under addition, alltså:

$$(a_0 + a_1X + a_2X^2 \ldots) + (b_0 + b_1X + b_2X^2 \ldots) =$$

$$(b_0 + b_1X + b_2X^2 \ldots) + (a_0 + a_1X + a_2X^2 \ldots) =$$

$$(a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 \ldots$$

Detta vet vi då addition av reella tal ($a_i, b_i \in \mathbb{R}$) är kommutativa.

Under multiplikation måste ringen vara associativ:

$$p(x)\cdot\Big(q(x)\cdot t(x)\Big)=\left(\sum_i a_i x^i\right)\cdot\left(\left(\sum_j b_j x^j\right)\cdot\left(\sum_k c_k x^k\right)\right)$$

$$=\left(\sum_i a_i x^i\right)\left(\sum_j\left(\sum_{k+l=j} b_k\cdot c_l\right)x^j\right)=\sum_i\left(\sum_{j+m=i} a_m\cdot\left(\sum_{k+l=j} b_k\cdot c_l\right)\right)x^i$$

$$=\sum_i\left(\sum_{j+k+l=i} a_j\cdot b_k\cdot c_l\right)x^i=\sum_i\left(\sum_{j+m=i}\left(\sum_{k+l=j} a_k\cdot b_l\right)\cdot c_m\right)x^i$$

$$=\left(\sum_j\left(\sum_{k+l=j} a_k\cdot b_l\right)x^j\right)\left(\sum_i c_i x^i\right)$$

$$=\left(\left(\sum_i a_i x^i\right)\cdot\left(\sum_j b_j x^j\right)\right)\cdot\left(\sum_k c_k x^k\right)=\Big(p(x)\cdot q(x)\Big)\cdot t(x)$$

På liknande sätt går det att bevisa distributivitet:

$$p(x)\cdot\Big(q(x)+t(x)\Big)=\left(\sum_i a_i x^i\right)\cdot\left(\left(\sum_j b_j x^j\right)+\left(\sum_k c_k x^k\right)\right)$$

$$=\left(\sum_i a_i x^i\right)\cdot\left(\sum_j (b_j+c_j)x^j\right)=\left(\sum_i\left(\sum_{j+k=i} a_j\cdot(b_k+c_k)\right)x^i\right)$$

$$=\left(\sum_i\left(\sum_{j+k=i} a_j b_k+a_j c_k\right)x^i\right)=\sum_i\Big(\sum_{j+k=i} a_j b_k+\sum_{j+k=i} a_j c_k\Big)\,x^i$$

$$=\Big(\sum_i\Big(\sum_{j+k=i} a_j b_k\Big)\,x^i\Big)+\Big(\sum_i\Big(\sum_{j+k=i} a_j c_k\Big)\,x^i\Big)$$

$$=\left(\sum_i a_i x^i\right)\left(\sum_j b_i x^j\right)+\left(\sum_i a_i x^i\right)\left(\sum_j c_i x^j\right)=p(x)q(x)+p(x)t(x)$$

Med samma metod visar det att:

$$\Big(q(x)+t(x)\Big)\cdot p(x)=\ q(x)p(x)+t(x)p(x)$$

Dessutom visar det sig att {P,+,·} är kommutativ under multiplikation

$$(a_0 + a_1X + a_2X^2 \dots)(b_0 + b_1X + b_2X^2 \dots) =$$

$$(b_0 + b_1X + b_2X^2 \dots)(a_0 + a_1X + a_2X^2 \dots) =$$

$$(a_0b_0) + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 \dots)$$

{P,+,·}är en kommutativ ring.

4. Kroppar

En kropp är en kommutativ ring, vars nollskillda element bildar en abelsk grupp under multiplikation. Utav de strukturer som arbetet berör, så är ringar och kroppar utrustade med flest operationer, men en kropp har utöver de kriterium som ringar uppfyller, ytterligare kriterium som måste uppfyllas.

Definition 4.1 En kropp består utav en mängd element M samt två binära operationer $(+)$ och $(\bullet)$.

a) $(+)$ och $(\bullet)$ är kommutativa och associativa.

b) De distributiva lagarna gäller: $a \bullet (b + c) = a \bullet b + a \bullet c$

c) Det finns additiva och multiplikativa identitetselement e, för addition är $e = 0$, för multiplikation är $e = 1$.

d) Varje element har en additiv invers, varje element $a \neq 0$ har en multiplikativ invers

Additiva inversen för a är $-a$ då $a + (-)a = 0$

Multiplikativa inversen för a är a^{-1} $då$ $a \bullet a^{-1} = 1$

Kroppar utrustas alltså med (addition, additiv invers, multiplikation och multiplikativ invers).

Exempel 4.1 Alla rationella tal utrustade med operationerna addition och multiplikation $\langle \mathbb{Q}, +, \cdot \rangle$ är en kropp. Detta visas genom att granska axiomen i definitionen:

De nollskillda rationella talen är kommutativa och associativa under både addition och multiplikation. De distributiva lagarna gäller. Enhetselementen 0 (additiv) och 1

(multiplikativ) existerar och varje element i $\mathbb{Q}$ har en additiv och multiplikativ invers sådant att:

$$a + (-)a = 0 \; och \; a \cdot a^{-1} = 1$$

Alla axiom för att $\langle \mathbb{Q}, +, \cdot \rangle$ ska klassas som en kropp är därmed uppfyllda.

Exempel 4.2 Heltal mod 5:

$\mathbb{Z}/\,5\mathbb{Z} = \{0,1,2,3,4\}$ är en kropp.

Heltal mod 6:

$\mathbb{Z}/\,6\mathbb{Z} = \{0,1,\ldots,5\}$ är inte en kropp.

Först utreds varför $\mathbb{Z}/\,5\mathbb{Z}$ är en kropp:

$\mathbb{Z}/\,n\mathbb{Z}$ är kommutativ, både under addition och under multiplikation, ty

$$a + b = b + a, \qquad a \bullet b = b \bullet a, \qquad a, b \in \mathbb{Z}$$

För varje element i $\mathbb{Z}/\,5\mathbb{Z}$ finns ett inverst element, dessa kan studeras i ett multiplikationsschema:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Produkterna i tabellen som blir 1 i mod 5 indikerar ett inverst tal. Alltså blir inversen till

$1 = 1$, invers till 2 = 3, invers till 3 = 2 och invers till 4 = 4

Nu till $\mathbb{Z}/\,6\mathbb{Z}$. Likt tidigare exempel är den kommutativ under addition och multiplikation. Men till skillnad från $\mathbb{Z}/\,5\mathbb{Z}$ saknar $\mathbb{Z}/\,6\mathbb{Z}$ inverst element för elementen 2, 3 och 4. Alltså är $\mathbb{Z}/\,6\mathbb{Z}$ inte en kropp, ty de uppfyller inte alla axiom.

Från exempel 3.6 kan man se att vissa värden för n i $n\mathbb{Z}$ gör så att $n\mathbb{Z}$ är en kropp, med andra värden för n blir $n\mathbb{Z}$ en ring.

Exempel 4.3: $n\mathbb{Z}$ är en kropp om och endast om n är ett primtal.

Antag att a är ett heltal så att $0 < a < n$ och att a inte är nollelementet i $n\mathbb{Z}$. Eftersom n är ett primtal så följer det att a och n är relativt prima. Enligt Euklides algoritm måste då alla a mellan 0 och n vara inverterbara (relativt till mod n) vilket leder till att $n\mathbb{Z}$ är en kropp. Om man istället antar att n inte är ett primtal, skulle vi kunna faktorisera $n = m_1 m_2$.

$$1 < m_1 m_2 = n$$

Om m_1, m_2 är nollskilda och $m_1 m_2 = n = [0] = z$, betyder det att alla ringens element inte är inverterbara och är därför ingen kropp.

Beteckningen för denna kropp då n är ett primtal, är $p\mathbb{Z}$ och är en ändlig kropp.

Exempel 4.4 Undersök om $\langle \mathbb{Q}(\sqrt{2}), +, \cdot \rangle$, där operationerna är vanlig addition och multiplikation, är en kropp.

Låt $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$

$$x, y, z \in \mathbb{Q}(\sqrt{2})$$

Om $x = (a + b\sqrt{2}), y = (c + d\sqrt{2}), z = (e + f\sqrt{2}),$ då $a, b, c, d, e, f \in \mathbb{Q}$ så är $\mathbb{Q}(\sqrt{2})$ stängd under + då:

$$x + y = (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

$\langle \mathbb{Q}(\sqrt{2}), +, \cdot \rangle$ är associativ för + då:

$$\begin{aligned} x + (y + z) &= (a + b\sqrt{2}) + \left((c + d\sqrt{2}) + (e + f\sqrt{2})\right) \\ &= (a + b\sqrt{2}) + \left((c + e) + (d + f)\sqrt{2}\right) \\ &= \left((a + c) + (b + d)\sqrt{2}\right) + (e + f\sqrt{2}) \\ &= \left((a + b\sqrt{2}) + (c + d\sqrt{2})\right) + (e + f\sqrt{2}) = (x + y) + z \end{aligned}$$

Identitetselementet för + är $0 = 0 + 0\sqrt{2}$ då:

$$x + 0 = \left(a + b\sqrt{2}\right) + \left(0 + 0\sqrt{2}\right) = (a + 0) + (b + 0)\sqrt{2} = a + b\sqrt{2} = x$$

$$0 + x = \left(0 + 0\sqrt{2}\right) + \left(a + b\sqrt{2}\right) = (o + a) + (o + b)\sqrt{2} = a + b\sqrt{2} = x$$

För varje element x, finns det en additiv invers av x så att $-x = -a + (-b)\sqrt{2}$ då:

$$x + (-x) = \left(a + b\sqrt{2}\right) + \left(-a + (-b)\sqrt{2}\right) = \left(a + (-a)\right) + \left(b + (-b)\right)\sqrt{2} = 0 + 0\sqrt{2} = 0$$

$$(-x) + x = \left(-a + (-b)\sqrt{2}\right) + \left(a + b\sqrt{2}\right) = \left((-a) + a\right) + \left((-b) + b\right)\sqrt{2} = 0 + 0\sqrt{2} = 0$$

För varje element $x \neq 0$, finns det en multiplikativ invers av x så att $x \cdot x^{-1} = 1$, $x^{-1} = \frac{1}{a+b(\sqrt{2})}$. Men vi skriver om det så det blir på rätt form genom att multiplicera bråket med $\frac{a-b\sqrt{2}}{a-b\sqrt{2}}$. Då får vi $\frac{1}{a+b(\sqrt{2})} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$ vilket är på rätt form då $\frac{a}{a^2-2b^2}$ och $\frac{-b}{a^2-2b^2}$ är rationella tal.

$\left(a + b(\sqrt{2})\right) \cdot \left(a + b(\sqrt{2})\right)^{(-1)} = 1$ och $\left(a + b(\sqrt{2})\right)^{(-1)} \cdot \left(a + b(\sqrt{2})\right) = 1$

Operationen + är kommutativ då:

$$x + y = \left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right) = (a + c) + (b + d)\sqrt{2} = (c + a) + (d + b)\sqrt{2}$$
$$= \left(c + d\sqrt{2}\right) + \left(a + b\sqrt{2}\right) = y + x$$

$\mathbb{Q}(\sqrt{2})$ är stängd under · då:

$$x \cdot y = \left(a + b\sqrt{2}\right) \cdot \left(c + d\sqrt{2}\right) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd =$$

$$(ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

Operationen · är associativ då:

$$x \cdot (y \cdot z) = \left(a + b\sqrt{2}\right) \cdot \left(\left(c + d\sqrt{2}\right) \cdot \left(e + f\sqrt{2}\right)\right)$$
$$= \left(a + b\sqrt{2}\right) \cdot \left((ce + 2df) + \left(cf + de\right)\sqrt{2}\right)$$
$$= (ace + 2adf) + (acf + ade)\sqrt{2} + (bce + 2bdf)\sqrt{2} + 2(bcf + bde)$$

$$(x \cdot y) \cdot z = \left((a + b\sqrt{2}) \cdot (c + d\sqrt{2})\right) \cdot (e + f\sqrt{2})$$
$$= ((ac + 2bd) + (ad + bc)\sqrt{2}) \cdot (e + f\sqrt{2})$$
$$= (ace + 2bde) + (acf + 2bdf)\sqrt{2} + (ade + bce)\sqrt{2} + 2(adf + bcf)$$

Vi får att:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

Operationen · är kommutativ då:

$$x \cdot y = (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = a \cdot c + a \cdot d\sqrt{2} + b \cdot c\sqrt{2} + 2b \cdot d$$
$$= (c + d\sqrt{2}) \cdot (a + b\sqrt{2}) = y \cdot x$$

Identitetselementet för · är $1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ då:

$$x \cdot (1 + 0\sqrt{2}) = (a + b\sqrt{2}) \cdot (1) = a + b\sqrt{2} = x$$

$$(1 + 0\sqrt{2}) \cdot x = (1) \cdot (a + b\sqrt{2}) = a + b\sqrt{2} = x$$

Allt som är kvar att visa nu är om de distributiva lagarna för $\mathbb{Q}(\sqrt{2}), +, \cdot\rangle$ gäller.

Vänsterdistributivitet:

$$x \cdot (y + z) = (a + b\sqrt{2}) \cdot \left((c + d\sqrt{2}) + (e + f\sqrt{2})\right)$$
$$= (a + b\sqrt{2}) \cdot \left((c + e) + (d + f)\sqrt{2}\right)$$
$$= (ac + ae) + (ad + af)\sqrt{2} + (bc + be)\sqrt{2} + 2(bd + bf)$$

$$x \cdot y + x \cdot z = (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) + (a + b\sqrt{2}) \cdot (e + f\sqrt{2})$$
$$= \left((ac + 2bd) + (ad + bd)\sqrt{2}\right) + \left((ae + 2bf) + (af + be)\sqrt{2}\right)$$

Vid jämförelse ser vi att $x \cdot (y + z) = x \cdot y + x \cdot z$

Högerdistributivitet:

$$(y+z)\cdot x = \left((c+d\sqrt{2})+(e+f\sqrt{2})\right)\cdot(a+b\sqrt{2})$$
$$= \left((c+e)+(d+f)\sqrt{2}\right)\cdot(a+b\sqrt{2})$$
$$= (ac+ae)+(ad+af)\sqrt{2}+(bc+be)\sqrt{2}+2(bd+bf)$$
$$x\cdot(y+z) = (y+z)\cdot x = x\cdot y + x\cdot z = y\cdot x + z\cdot x$$

$\langle \mathbb{Q}(\sqrt{2}), +, \cdot \rangle$ uppfyller alla axiom och är därför en kropp.

Exempel 4.5 $\langle \mathbb{Q}(\sqrt{2}), +, \cdot \rangle$ är en kropp enl. exempel 4.3 men är avbildningen f: $\langle \mathbb{Q}(\sqrt{2}) \rangle \rightarrow \langle \mathbb{Q}(\sqrt{3}) \rangle$ en kroppsisomorfi? Låt $f(\sqrt{2}) = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})\ och\ a, b\ \in \mathbb{Q}$

Om man antar att f är en kroppisomorfi så skulle $f(\sqrt{2})^2 = f\left(\sqrt{2}^2\right) = f(2) = 2$, då skulle

$$f(\sqrt{2})^2 = (a+b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3} = 2$$

Alltså får man $2 = a^2 + 3b^2$ och $2ab = 0$

Antingen måste då a eller b vara 0. Men detta ger att:

i) $a = 0, 2 = 3b^2, och\ b = \pm\sqrt{2/3}$ vilket inte tillhör de rationella talen.

ii) $b = 0, 2 = a^2$, vilket skulle implicera att $a = \pm\sqrt{2}$ som inte heller är ett rationellt tal.

Avbildningen är inte en kroppisomorfi.

I exempel 4.3 visade vi att $p\mathbb{Z}$ är en kropp då p är ett primtal. Då finns det en sats som säger att för varje kropp K där n är skiljt från 0, finns en minsta delkropp som är skärningen av alla kroppar i K. Denna delkropp är isomorf med $\mathbb{Q}$ eller $p\mathbb{Z}$ om p är ett primtal.

Bevis: En skärning av delkroppar är en ny delkropp, alltså måste skärningen av alla delkroppar i K vara en kropp $k \subseteq K$ som innehåller 1 och därmed $1 + 1 + \cdots + 1$. Om K inte är en ändlig kropp innehåller K alla heltal och därmed också alla rationella tal. Om det finns ändligt många element på formen $1 + 1 + \cdots + 1$, så finns ett m sådant att $m \cdot 1 = 1 + 1 + \ldots + 1 = 0$. Om n är det minsta positiva heltal som uppfyller detta får vi att n måste vara ett primtal eller $n = 1$. Eftersom $p = x \cdot y$ ger att $p = (x \cdot 1)(y \cdot 1)$, då måste antingen x

eller y vara lika med 0, vilket skulle motsäga att n var minst. I och med att vi antagit att $1 \neq 0$ måste n vara ett primtal och elementen på formen $m \cdot 1$ bildar en delkropp med $\mathrm{p}\mathbb{Z}$.

Definition 4.2 Vi sa precis att skärningen eller snittet av en delkropp fortfarande är en delkropp. En primkropp är en delkropp som inte har någon annan delkropp än sig själv, $\mathbb{Q}$ och $\mathrm{p}\mathbb{Z}$ då n är ett primtal är primkroppar.

Exempel 4.6 Visa att en kropps primkropp är isomorf med $\mathbb{Q}$ eller med $\mathrm{p}\mathbb{Z}$ då p är ett primtal.

Primkroppen P till kroppen K måste innehålla e, samt alla multipler till e som vi kan skriva som $ke, k \in \mathbb{Z}$. Vi kan utgå ifrån avbildningen $\varphi: k \curvearrowright ke$ från $\mathbb{Z}$ till K. Då $ke + me = (k+m)e$ och $ke \cdot me = (km)e^2 = (km)e$ så får vi att det är en ringhomomorfi. Då får vi också en delring till K som är bilden $Im\varphi = \{ke | k \in \mathbb{Z}\}$. Kärnan $Ker\varphi$ är ett ideal i $\mathbb{Z}$, på formen $n\mathbb{Z}$ där n är ett naturligt tal. Då är $Im\varphi$ isomorf med $\mathbb{Z}/\mathrm{n}\mathbb{Z}$ (eller som vi också skrivit det, $p\mathbb{Z}$) för $n > 0$ och med $\mathbb{Z}$ då $n = 0$. (obs. då $n > 0$ är $n \neq 1$ ty n måste anta ett primtal)

$Im\varphi$ är alltså isomorf med primkroppen $p\mathbb{Z}$, alltså måste $Im\varphi$ vara primkroppen i K. Om $n = 0$ är $Im\varphi$ kongruent med $\mathbb{Z}$. K innehåller en kvotkropp till $Im\varphi$, denna är isomorf med kvotkroppen till $\mathbb{Z}$, dvs. isomorf med $\mathbb{Q}$. Alltså är primkroppen isomorf med $\mathbb{Q}$ eller med $\mathrm{p}\mathbb{Z}$ då p är ett primtal.

Avslutande exempel för praktisk användning

För att återknyta till inledningen där jag påstod att abstrakt algebra kan nyttjas inom kryptologin vill jag avsluta med ett exempel på hur det kan gå till när man ska överföra krypteringsnycklar mellan två parter på en okrypterad kanal.[7]

1. Vi antar att vi har parterna X och Y som innan överföringen kommit överens om en ändlig cyklisk grupp G^n och en delmängd g som tillhör G.

[7] Buchmann, Johannes A. *Introduction to cryptography* (2nd edition), Springer Science & Business media, 2013, s.190-191.

2. X väljer ett valfritt naturligt tal a så att $1 < a < n$ och skickar sedan g^a till Y.

3. Y väljer sedan ett valfritt naturligt tal b så att $1 < b < n$ och skickar sedan g^b till X.

4. X och Y kan nu beräkna $\left(g^a\right)^b$ och $\left(g^b\right)^a$ var för sig.

Nu har båda parterna den delade krypteringsnyckeln g^{ab} och den cykliska gruppen G uppfyller kriterierna för att vara en hemlig överföring (ju större tal som används, desto säkrare blir metoden). Metoden kallas för Diffie-Hellmans nyckelöverföring och är ett bra exempel på hur abstrakt algebra kan nyttjas i praktiken.

Avslutande ord

Som uppsatsen visar finns det strukturer som sträcker sig från relativt enkla till allt mer komplexa. Det har varit intressant att följa den kategorisering av matematiken som matematikerna arbetat med de senaste 200 åren och att se hur den idag kan nyttjas inom olika områden. Ett exempel är det allt mer ökade behovet av IT-säkerhet som har tvingat fram mer och mer säkra metoder för kommunikation. Till sist vill jag även tacka min handledare Paul Vaderlind som varit till stor hjälp under skrivandets gång.

Källförteckning

Buchmann, Johannes A. *Introduction to cryptography* (2nd edition), Springer Science & Business media, 2013

Christoffersson, Stig, *Grupper Ringar Kroppar*, LiberLäromedel, Lund, 1975

Eves, Howard, *Foundations and fundamental concepts of mathematics,* third edition, PWS-Kent publishing company, Boston, 1990