5B1493, lekt 4, HT06

Konstruktion av de reella talen R. (AEE §4.3)

Informellt:

De rationella talen **Q** kan geometriskt åskådliggöras som punkter på en talllinje. Geometriskt sett finns det dock fler punkter på linjen än dessa rationella. Exvis, om man från 0 avsätter en sträcka lika lång som diagonalen i en kvadrat med sidan 1, så kommer sträckans andra ändpunkt inte att vara en rationell punkt. En idè om hur man kan fånga in dessa ”hål” som tal i ett mera omfattande talsystem går som följer:

Vi föreställer oss att varje punkt på tallinjen (rationell eller ej) delar de *rationella* punkterna i två delar – de som ”är mindre än” (”ligger till vänster om”) hålet och de övriga. Denna ”vänstermängd” – vi kallar den *a* har tydligen följande egenskaper

1. $a \quad \mathbf{Q}$ och $a \neq \mathbf{Q}$, $a \neq$ (Obs *delmängd* av **Q**, inte element i **Q**!)
2. $A \quad a, B \quad \mathbf{Q}$ och $B < A \quad \mathsf{B} \quad a$
3. Det finns inget största element i *a*, dvs:
   Om $A \quad a$ så finns säkert (åtminstone) ett $C \quad a$ så att $A < C$.
   (Informellt: Mängden skall motsvara ett öppet intervall på reella tallinjen – ”högerändpunkten” skall inte räknas med.)

En sådan mängd *a* kallar vi ett *snitt*.

Mot varje punkt på tallinjen svarar alltså ett snitt. Omvänt föreställer vi oss att varje snitt svarar mot en (och endast en) punkt på tallinjen (snittets ”högerändpunkt”). Speciellt svarar maängden av de snitt vars ”högerändpunkt” är ett rationellt tal, mängden **Q**.

Formellt går man nu tillväga på följande vis:

De reella talen förklaras vara identiska med snitten i kropppen **Q**
De rationella talen svarar då mot de snitt vars komplement **Q** – *a* har ett minsta element (nämligen det rationella talet ifråga).

Ordning, addition och multiplikation definieras sedan som beskrivet i AEE (Def 5.1.1, 5.1.3, 5.1.8).

Definition av *ordning*:

$a \leq b \Leftrightarrow$ snittet $a \quad$ snittet b.
$a < b \Leftrightarrow a \leq b$ och $a \neq b$,

Definition av *motsatt* reellt tal: För de snitt *a* som motsvarar rationella tal *P*, $a = \{B \quad \mathbf{Q}, B < A \quad \mathbf{Q}\}$ är det motsatta reella talet $-a$, snittet $\{B \quad \mathbf{Q}, B < -A \quad \mathbf{Q}\}$. För de snitt *a* som inte motsvarar rationella tal är det motsatta reella talet snittet $\{B \quad \mathbf{Q}; -B \quad a\}$.
Om *a* och *b* är två snitt så är mängden $c = \{C \quad \mathbf{Q}; C = A + B$ för några $A \quad a$ och $B \quad b\}$ också ett snitt. Detta snitt tas som definition av $a + b$.

Angående *multiplikation*:
Om *a* och *b* är två snitt ≥ 0 så är mängden $c = \{C \quad \mathbf{Q}; C < A \cdot B$ för några $A \geq 0$ och $a \geq 0$, $B > 0$ och $b\}$ också ett snitt. För sådana *a* och *b* definieras $a \cdot b$ som detta snitt *c*.
För övriga *a* och *b*, definieras $a \cdot b$ av $|a| \cdot |b|$ om både *a* och $b < 0$ och av $-|a| \cdot |b|$ om precis ett av *a* och $b < 0$. ($|a|$ betyder som vanligt, *a* om $a \geq 0$ och $-a$ om $a < 0$.)

Man kan sedan verifiera att alla kropplagarna K1-4,6-9 gäller, men nu tillkommer också den s.k. *supremumegenskapen*:

Om **M** är en mängd reella tal och *B* är ett tal < alla i **M**,

dvs. om $\mathbf{M} \quad \mathbf{R}$ och $A < B$ för alla $A \quad \mathbf{M}$, (dvs om **M** är uppåt begränsad)

så finns det ett minsta reellt tal *C*, som är ≤ alla i **M**,

dvs det finns ett tal *C* sådant att
° $d \leq C$ för alla $d \quad \mathbf{M}$,
° om $e < C$ så finns ett $d \quad \mathbf{M}$ så att $e < d \leq C$..

Supremumegenskapen kan visas vara ekvivalent med den s.k. *intervallinkapslingsegenskapen*:

Om $a_1 \le a_2 \le a_3 \le \ldots\ldots \le a_n \le \ldots\ldots \le b_n \le \ldots\ldots \le b_3 \le b_2 \le b_1$, $n = 1, 2, 3, 4, \ldots\ldots$
så finns det (minst) ett reellt tal x sådant att
$a_1 \le a_2 \le a_3 \le \ldots\ldots \le a_n \le \ldots \le x \le \ldots \le b_n \le \ldots\ldots \le b_3 \le b_2 \le b_1$, $n = 1, 2, 3, 4, \ldots\ldots$

(Dvs om intervallen $[a_n, b_n]$ är inkapslade i varandra: $[a_{n+1}, b_{n+1}] \quad [a_n, b_n]$,
så det finns ett reellt tal x som ligger i alla intervallen.)

Övningar om reella tal:

AEE Övn 5.1 – 5.4

Rosenlicht: Kap 2. 6 – 11, 14 - 15.
(Ersätt ledningen i uppgift 11 med
”First find a positive integer n such that $a > 1 + \frac{1}{n}$ and then prove that
$a^m > 1 + \frac{m}{n}$ for all integers m.”

Funktioner

Definition av begreppet

Definition: Låt **X** och **Y** vara två mängder. En *funktion f* av *typ* **X** → **Y** är detsamma som en delmängd av **X** × **Y**, sådan att

1. Om (x, y) och (x, z) f, så är $y = z$
2. Om x **X** så finns något y **Y** sådant att (x, y) f.

Mängden f kallas vanligtvis funktionens *graf* och man föredrar att skriva

$y = f(x)$ i stället för (x, y) f

Mängden **X** är funktionens *definitionsmängd* $\mathbf{D}_f$ och de y som kan uppträda som andraelement i grafen, dvs. $\{y$ **Y**; $y = f(x)$ för något x **X**$\}$ är funktionens *värdemängd* $\mathbf{V}_f$.

Några synonymer

Svenska	Engelska
Funktion avbildning, tillordning	*Function, mapping*
Definitionsmängd, urbild, domän	*Domain*
Värdemängd, bild	*Range, image*

Mera beteckningkonventioner och terminologi

”f är en funktion av *typ* **X** → **Y**” förkortas till ”f : **X** → **Y**”

Om **M** **X**: $f(\mathbf{M}) = \{y$ **Y**; $y = f(x)$ för något x **M**$\}$

Om **M** **Y**: $f^{-1}(\mathbf{M}) = \{x$ **X**; $y = f(x)$ för något y **M**$\}$

Om f är sådan att $f(x) = f(z)$ endast om $x = z$ så säger man att f är *inverterbar* (eller är en *injektion*)

För inverterbara funktioner gäller att

$\{(y, x)$ **Y** × **X**; $y = f(x)\}$ är en funktion av typ $\mathbf{V}_f$ → **X.** Denna s.k. inversfunktion skrivs f^{-1}.

Om $\mathbf{V}_f$ = **Y** så säger man att funktionen avbildar *på* **Y** (eller är en *surjektion*).

Om f både är inverterbar och på (både är en injektion och en surjektion) så sägs den vara en *bijektion* och avbildningen mellan **X** och **Y** är *en-en-tydig* (den är en *1-1-avbildning*).

Sammansättning

Om f : **X** → **Y** och g: **Y** → **Z**, så finns det ett naturligt sätt att kombinera dessa till en funktion g: **X** → **Z**, nämligen

$h(x) = g(f(x))$.

Denna *sammansättning* (eng. *composition*) betecknas $f \circ g$.

Observera att sammansättning av två funktioner bara kan göras om typerna är passande, nämligen att f:s värdemängd måste ligga i g:s definitionsmängd. Exempelvis är sammansättning alltid möjligt för det fall att **X** = **Y** = **Z**.

Sammansättningsoperationen uppfyller alltid den associativa lagen

$$f \circ (g \circ h) = (f \circ g) \circ h$$

Däremot gäller i allmänhet inte den kommutativa lagen (se övning F5 nedan).

Bland funktionerna av typen **X** → **X** utmärker sig en som är speciellt ”enkel”, den s.k. *identiteten*:

$i_{\mathbf{X}}(x) = x$

Dess graf $\{(x, x); x$ **X**$\}$, är ”diagonalen” i **X** × **X**.

Antal, mäktighet, kardinalitet. (AEE §3.3, 6.1)

Det är inte svårt att övertyga sig om att om två mängder **X** och **Y** har *n* st element så finns det en bijektion mellan mängderna. (Räkna exempelvis upp de båda elementen i de båda mängderna och låt $y = f(x)$ betyda att x och y har fått samma nummer vid uppräkningen). Omvänt om det finns en bijektion mellan mängderna och **X** har n st. element, så har också **Y** *n* st. element.

Denna iaktagelse har lett till följande generella definition av ”antal” eller *mäktighet* hos mängder som inte nödvändigtvis är ändliga:

Två mängder har samma *mäktighet* (eller *kardinalitet*) om det finns en bijektion mellan dem.

Mäktigheten hos mängden **X** betecknas gärna $|\mathbf{X}|$.

För ändliga mängder finns det alltså en mäktighet för varje naturligt tal.
Ex.vis $|\{a, b, c\}| = 3$, $|\ \ | = 0$

Dessa mäktigheter kan på ett naturligt sätt ordnas: Notera först att om **X** och **Y** är ändliga mängder med *m* resp. *n* element, $m < n$, så finns det en injektion $\mathbf{X} \to \mathbf{Y}$ men inte någon $\mathbf{Y} \to \mathbf{X}$.

Detta leder till den allmänna överenskommelsen att **X** har mindre eller samma mäktighet än **Y** om det finns en injektion $\mathbf{X} \to \mathbf{Y}$ och skriver $|\mathbf{X}| \leq |\mathbf{Y}|$.

Ett kanske inte alldeles förvånande men inte särskilt trivialt faktum är man kan bevisa att om $|\mathbf{X}| \leq |\mathbf{Y}|$ och $|\mathbf{Y}| \leq |\mathbf{X}|$, så är $|\mathbf{X}| = |\mathbf{Y}|$ (Bernsteins lemma)

Mera förvånande är kanske att det finns många (i själva verket ∞ många) olika oändliga mäktigheter och att mängder **X** och **Y** där **X** **Y** men **X** ≠ **Y** mycket väl kan ha samma mäktighet.

Exempelvis kan man visa att

$|\mathbf{N}| = |\mathbf{Z}| = |\mathbf{Q}|$ [1] (Notera att **N** **Z** **Q**, men att ingen av dessa mängder är lika.)

$|\mathbf{N}| < |\mathbf{R}| = |\mathbf{C}|$ [2]

Mängd med samma kardinalitet som **N** kallar man *uppräkneliga* och de reella talen sägs ha *kontinuums mäktighet*.

Det var länge en öppen fråga om det fanns någon mäktighet som ligger strikt mellen $|\mathbf{N}|$ och $|\mathbf{R}|$. Den allmänna förmodan var att det inte fanns någon sådan (kontinuumhypotesen). Det hela reddes ut av Cohen (1963) som visade att både hypotesen och dess motsats var förenlig med det gängse axiomsystemet för mängdläran (som vi inte tar upp i den här kursen). Den märkliga slutsatsen är att det finns olika, lika intuitivt rimliga mängdläror; en där hypotesen är sann och där den är falsk!

Övningar:

F1. Vilka är funktionerna av typ $\{1,2,3\} \to \{0,1\}$

F2. Om **Y** består av två element och **X** en mängd (vilken som helst), försök beskriva vilka funktionerna av $\mathbf{X} \to \mathbf{Y}$ är med hjälp av begreppet delmängd.

F3. Finns det några funktioner av typ $\to \mathbf{R}$ resp. $\mathbf{R} \to$?

F4. Verifiera den associativa lagen för sammansättningsoperationen

F5. a. Om $f \circ g$ och $g \circ f$ existerar, vad kan då sägas om funktionernas typer?
b. Om f och g: $\mathbf{R} \to \mathbf{R}$, $f(x) = e^x$ och $g(x) = x^2$. Vilka är då $(f \circ g)(x)$ och $(g \circ f)(x)$.

F6. Verifiera att om $f : \mathbf{X} \to \mathbf{Y}$ så är $f \circ i_{\mathbf{X}} = f$ och $i_{\mathbf{Y}} \circ f = f$.

F7. Verifiera att om $f : \mathbf{X} \to \mathbf{Y}$ är bijektion, så är $f^{-1} \circ f = i_{\mathbf{X}}$ och $f \circ f^{-1} = i_{\mathbf{Y}}$.
Och omvänt: Om $g \circ f = i_{\mathbf{X}}$ och $f \circ h = i_{\mathbf{Y}}$ för några funktioner g och h, så är f en bijektion och $g = h = f^{-1}$.

---

1 Att $|\mathbf{N}| = |\mathbf{Q}|$, se AEE Sats 3.3.3.
2 Att $|\mathbf{N}| < |\mathbf{R}|$, se AEE, Sats 6.1.1.

F8. Verifiera att f: $\mathbf{X} \rightarrow \mathbf{Y}$ är en injektion om och bara om $f \circ g = f \circ h \quad g = h$.
Och att f: $\mathbf{X} \rightarrow \mathbf{Y}$ är en surjektion om och bara om $g \circ f = h \circ f \quad g = h$.
(Underförstått att f, g och h har valts så att de angivna sammansättningarna är meningsfulla:)

Relationer (AEE §1.2, 1.3)

Definition: En *relation* **G** i mängden **M** är detsamma som en delmängd av **M** × **M**.

I stället för (*a*, *b*) **G** skriver man gärna *a* **G** *b*

Exempel på viktiga relationer:

1a. På **R** (även **N**, **Z**, **Q**,):

Olikhet, $a < b$ kan uppfattas som en relation i ovanstående mening.

Mängden **G** består av de par (*a*,*b*) **R** × **R** för vilka $a < b$. **G** kan lämpligen betecknas med < och i och för sig skulle man kunna skriva (*a*,*b*) < i stället för $a < b$ – men det gör man inte så gärna!

1b. På motsvarande sätt kan den oströnga olikheten $a \leq b$ uppfattas som en sådan relation.

För dessa relationer gäller

a **G** *b* och *b* **G** *c* *a* **G** *c* (*Transitivitet*)

För den stränga olikheten < gäller dessutom att

högst en av *a* **G** *b*, $a = b$ och *b* **G** *a* är riktig.

Relationer av detta slag kallas *ordningsrelationer* och mängden **M** sägs vara *partiellt ordnad*.

Om sedan alltid någon av *a* **G** *b*, $a = b$ och *b* **G** *a* är riktig så säger man att **M** är *totalordnad*.

2. På **N** (även **Z**)

”Gå jämt upp i”

Mängden **G** består då av de (*a*,*b*) **N** × **N** för vilka ekvationen $a \cdot x = b$ har en lösning (i **N**). En vanlig beteckning för denna relation är $a|b$.

3. På **M** (vilken mängd som helst):

Identitet $a = b$.

Mängden **G** består då av de par (*a*,*b*) **M** × **M** för vilka $a = b$.

4a. På **N** (även **Z**)

”Ha samma paritet som”.

Mängden **G** består då av de (*a*,*b*) **N** × **N** som antingen båda är jämna eller båda ä udda, (dvs de par (*a*,*b*) som har samma rest när man delar dem med 2).

4b. Mera generellt

”Tillhör samma restklass mudulo *n*” (*n* heltal ≥ 2)

Mängden **G** består då av de (*a*,*b*) **N** × **N** som har samma rest när man delar dem med *n*.

För relationerna i exemplen nr 3 och 4 gäller:

a **G** *a* (*Reflexivitet*)

a **G** *b* ⇔ *b* **G** *a* (*Symmetri*)

och transitivitet:

a **G** *b* och *b* **G** *c* *a* **G** *c*

Relationer som uppfyller dessa tre lagar kallas *ekvivalensrelationer*. Sådana relationer skapas naturligt när man har att göra med ting som visserligen inte är identiska men ändå är lika i något avseende. (Ex i vardagslivet: … ha samma färg som …, … ha samma pappa som …, … ha samma pris som …, m.m., m.m.)

En mycket generell konstruktion inom mängdläran som leder till ekvivalensrelationer är som följer:
Låt **M** vara någon mängd som är uppdelad i ett antal (kan vara oändligt) disjunkta delar $\mathbf{M}_i$, $i \in \mathbf{I}$,

$\mathbf{M} = \bigcup_{i \in \mathbf{I}} \mathbf{M}_i$

$\mathbf{M}_i \cap \mathbf{M}_j = \emptyset$, för alla i och $j \in \mathbf{I}$, $i \neq j$,

i så fall är realtionen a **G** b: ”a och b tillhör samma delmängd $\mathbf{M}_i$ ” en ekvivalensrelation.

Övningar

R1. Verifiera att relationen i exempel nr 2 ovan är en ordningsrelation. Är **N** därigenom totalordnad? Finns det något tal i **N** som är ”mindre än” alla andra (dvs. ett $n \in \mathbf{N}$ för vilket $n|a$ för alla $a \in \mathbf{N}$? Finns det något tal i **N** som är ”större än” alla andra (dvs. ett $m \in \mathbf{N}$ för vilket $a|m$ för alla $a \in \mathbf{N}$?

R2. Är relationen ”vara (hel)syskon till” symmetrisk? reflexiv? transitiv?
Hur blir det för relationerna ”vara barn till min mamma och pappa” resp. ”vara kusin till”?

Grupper

En mängd **M**, försedd med ett räknesätt, här skrivet , (dvs. en funktion $\mathbf{M} \times \mathbf{M} \to \mathbf{M}$), sådant att

I. $(a \quad b) \quad c = a \quad (b \quad c)$ för alla a, b och $c \quad \mathbf{M}$, (Associativitet)

II. det finns ett speciellt element i **M**, vi kallar det här 1, sådant att
$1 \quad a = a \quad 1 = a$ för alla $a \quad \mathbf{M}$, (Existens av enhet)

III. till varje $a \quad \mathbf{M}$ finns ett *inverst* element, vi skriver a^{-1}, sådant att
$a^{-1} \quad a = a \quad a^{-1} = 1$. (Existens av invers)

kallas en *grupp*. Vi skriver här (**M** ,) för gruppen.

Om dessutom

IV. $a \quad b = b \quad a$ för alla a och $b \quad \mathbf{M}$, (Kommutativitet)

så säger man att gruppen är *kommutativ* eller *abelsk*.

Några exempel på abelska grupper är

1. De positiva rationella talen med räknesättet multiplikation, $(\mathbf{Q}_+, \cdot)$
2. De reella talen utom 0, med räknesättet multiplikation, $(\mathbf{R} - \{0\}, \cdot)$
3. Heltalen med räknesättet addition $(\mathbf{Z}, +)$
4. De reella talen, med räknesättet addition, $(\mathbf{R}, +)$
5. Mängden av vektorer i $\mathbf{R}^n$, med räknesättet addition, $(\mathbf{R}^n, +)$
6. Mängden av 2× 2-matriser med räknesättet addition.

Och några exempel på grupper som inte är abelska

7. Mängden av 2× 2-matriser med determinant ≠ 0 och räknesättet matrismultiplikation.
8. Mängden strängt växande funktioner $\mathbf{R} \to \mathbf{R}$ med räknesättet ”sammansättning av funktioner”

och allmännare

9. Om **A** är en godtycklig mängd och **M** är mängden av en-en-tydiga funktioner f: $\mathbf{A} \to \mathbf{A}$, (dvs. funktioner som är inverterbara och avbildar *på* **A**) och räknesättet är ”sammansättning av funktioner”.

Övningar:

G1. Verfiera att mängderna med räknesätten exemplen 1 – 9 ovan verkligen är grupper resp. abelska grupper.

G2. Varför är $(\mathbf{N}, +)$ och $(\mathbf{N}, \cdot)$ inte några grupper?

G3. Varför är $(\mathbf{Q}, \cdot)$ inte någon grupp?

G4 Varför är mängden av vektorer i $\mathbf{R}^n$ $(n \geq 2)$ med räknesättet ”skalärprodukt” inte någon grupp?

G5. Varför är vektorerna i $\mathbf{R}^3$ med räknesättet ”kryssprodukt” inte någon grupp?

G6. Låt **M** vara mängden som består av de båda talen ±1. Om man som räknesätt tar ”multiplikation”, är (**M,**) då en grupp?

G7. Verifiera att är mängden **M** av bijektioner $\mathbf{X} \to \mathbf{X}$ så är $(\mathbf{M}, \circ)$, ∘ är sammansättnings-operationen, en grupp. Är gruppen abelsk?

G8. Låt **X** i föregående uppgift vara mängden {0, 1}. Vilka är bijektionerna? Skriv upp gruppens ”multiplikationstabell”. Är gruppen abelsk?

G9. Låt **X** i stället vara mängden {0, 1, 2}. Vilka är bijektionerna? Skriv upp gruppens ”multiplikationstabell”. Är gruppen abelsk?

Ringar

Mängder **M** som är försedda med två ”räknesätt” – vi kallar dem addition (betecknad +) och multiplikation (betecknad ·), för vilka gäller att

Ri1 $A + 0 = A$, (**Neu+)**

Ri2 $A + B = B + A$, (**Kom+**)

Ri3 $(A + B) + C = A + (B + C)$, $(A \cdot B) \cdot C = A \cdot (B \cdot C)$. (**Ass+, Ass·**)

Ri4 Till varje A **M** finns ett ”motsatt tal” $-A$ med egenskapen

$$A + (-A) = 0 \qquad \textbf{(Inv+)}$$

Ri5
$$(A + B)\cdot C = (A \cdot C) + (B \cdot C),$$
$$C \cdot (A + B) = (C \cdot A) + (C \cdot B), \qquad \textbf{(Dist)}$$

kallas en *ring*, (**M**, + , ·)

Notera att man kan formulera definitionen av begreppet ring så här:

(**M**, + ,·) är en ring om (**M**, +) är en abelsk grupp försedd med ett räknesätt ”·” som uppfyller den associativa lagen och de distributiva lagerna (Dist).

Exempel på ringar är

1. heltalen **Z** med räknesätten addition och multiplikation,
2. **M** = {jämna heltal} med räknesätten addition och multiplikation,
2. **Q**, **R** och **C** (de komlexa talen) med räknesätten addition och multiplikation,
3. $n \times n$-matriserna med räknesätten matrisaddition och -multiplikation,
4. restklasserna modulo n (n något heltal ≥ 2) med addition och multiplikation som räknesätt.

Om multiplikationen är kommutativ, dvs om

$$A \cdot B = B \cdot A$$

för alla A och B i **M**,

så har man en *kommutativ ring*.

Om det i **M** finns ett speciellt element 1 med egenskapen

$$A \cdot 1 = 1 \cdot A = A \text{ för alla } A \quad \textbf{M},$$

så föreligger en *ring med enhet*.

Övningar:

Ri1. Verifiera att påståendena i ex 1 – 4 ovan är riktiga. Vilka av dessa ringar är kommutativa och vilka har en enhet?

Ri2. Är (**N** + ; ·) en ring?

Ri3. Är ($\mathbf{Q}_+$ + ; ·) en ring? $\mathbf{Q}_+$ är mängden av de positiva rationella talen.

Kroppar

Mängder **M** som åtminstone innehåller två element (här betecknade 0 och 1) och är försedda med två ”räknesätt” – vi kallar dem addition (betecknad +) och multiplikation (betecknad ·), för vilka gäller att

K1 $A + 0 = A$, $A \cdot 1 = A$, (**Neu+, Neu·)**

K2 $A + B = B + A$, $A \cdot B = B \cdot A$, (**Kom+, Kom·**)

K3 $(A + B) + C = A + (B + C)$, $(A \cdot B) \cdot C = A \cdot (B \cdot C)$, (**Ass+, Ass·**)

K4 $(A + B) \cdot C = (A \cdot C) + (B \cdot C)$, (**Dist**)

K9+ till varje A **M** finns ett ”motsatt tal” $-A$ med egenskapen

$$A + (-A) = 0, \quad \textbf{(Inv+)}$$

K9· till varje A **M**, $A \neq 0$, finns ett ”inverst tal” A^{-1} med egenskapen

$$A \cdot A^{-1} = 1, \quad \textbf{(Inv·)}$$

kallas en *kropp*.

Om dessutom en relation ”<” (olikhet) är definierad så att

K6 för alla A och B gäller exakt en av relationerna $A < B$, $A = B$, $B < A$, (**O1**)

K7 om $A < B$ och $B < C$ så är $A < C$, (**O2**)

K8 $A < B \quad A + C < B + C$ och, om $C > 0$: $A < B \quad A \cdot C < B \cdot C$, (**O3+, O3·**)

så säger man at**t M** är en *ordnad kropp.*

Inom kropparna kan man bedriva *aritmetik* dvs räkning med de fyra räknesätten. +, –, · och /.

(**Q**, + , ·), (**R**; + , ·) och (**C**, + , ·) är exempel på kroppar samt (**Q**, + , ·, <) och (**R**; + , ·, <) på ordnade sådana.

Notera att definitionen av begreppet kropp kan kan skrivas så här:

(**M**, + , ·) är en kropp om

° (**M**, +) är en abelsk grupp med enhet 0,
° (**M** – {0}, ·) är en abelsk grupp och
° distributiva lagen $(A + B) \cdot C = (A \cdot C) + (B \cdot C)$ gäller.

K1. Verifiera att om **M** = $\{a + b\sqrt{2}$, a och b **Q**$\}$, så är (**M**, + , ·) en kropp.

K2. Verifiera att restklasserna mod 2 med räknesätten addition och multiplikaion är en kropp.

K3. Utgör restklasserna mod 3, resp mod 4 med räknesätten addition och multiplikation kroppar?

K4* För vilka heltal $n \geq 2$ utgör restklasserna mod n med räknesätten addition och multiplikation en kropp?

Uppgifter (Om heltalsaritmetik)

1. Visa utifrån Peanos axiom att
varje tal n **N**, $n \neq 0$, har en ”närmaste föregångare”, dvs $n = m^+$ för något m **N.**

2. Visa utifrån Peanos axiom och definitionen av addition
a. att $0 + n = n$ för alla n **N**
b. att $n + m^+ = n^+ + m$ för alla n och m **N**
c. kommutativa lagen för addition, dvs att $n + m = m + n$ för alla n och m **N**
d. associativa lagen för addition, dvs. att
$(n + m) + p = n + (m + p)$, för alla n, m och p **N**
e. Annuleringslagen för addition, dvs för alla x, y och z **N** gäller att
$x + z = y + z$ $x = y$

3. Visa utifrån Peanos axiom och definitionen av multiplikation
a. att $n \cdot 0^+ = n$, för alla n **N**,
b. och med hjälp av kommutativa och associativa lagarna för addition att
$(n + m) \cdot p = (n \cdot p) + (m \cdot p)$

4. Visa utgående från Peanos axiom, definitionerna och räknelagarna för addition och multiplikation, samt definitionerna av subtraktion och division,
a. $n - 0 = n$, för alla n **N**,
b. $n + (m - p) = (n + m) - p$
c. $n - (m - p) = (n - m) + p$
d. $n - (m + p) = (n - m) - p$
e. $\frac{0}{n} = 0$ för alla n **N**, $n \neq 0$ och $\frac{m}{0^+} = m$ för alla m **N**.
f. $n \cdot \frac{m}{p} = \frac{(n\,m)}{p}$
g. $\frac{n}{m} + \frac{p}{d} = \frac{((n \cdot d) + (m \cdot p))}{(m \cdot d)}$

5. Om α och β Z. Visa utgående från räknelagarna för **Z** (**Z1-9**) att
a. Om $\alpha = [(n, m)]$ n, m **N**, så är $-\alpha = [(m, n)]$.
b. $(-1) \cdot \alpha = -\alpha$
c. Låt subtraktion i **Z** *definieras* av $\alpha \triangleq \beta = \alpha + (-\beta)$. Visa att detta, för de tal i **Z** som svarar mot de naturliga talen **N**, överensstämmer med den subtraktion (**D–**) som användes i **N**.