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 $\mathbf{X} \to \mathbf{Y}$, definerad på **X** och skriver $|\mathbf{X}| \leq |\mathbf{Y}|$. Vidare

X har samma mäktighet än **Y** om det finns en bijektion $\mathbf{X} \to \mathbf{Y}$, definierad på **X** och skriver $|\mathbf{X}| = |\mathbf{Y}|$.

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)

(Dvs. om det finns injektioner $f : \mathbf{X} \to \mathbf{Y}$ och $g: \mathbf{Y} \to \mathbf{X}$ definierade *på* respektive mängder, så finns det också en biljektion $\mathbf{X} \to \mathbf{Y}$, definierad på **X**.)

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 $\mathbf{X} \neq \mathbf{Y}$ 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!

---

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

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

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 b) $c = a$ (b c) för alla a, b och c **M**, (Associativitet)

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

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

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

Om dessutom

IV. a $b = b$ a för alla a och b **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 (**Z**, +)
4. De reella talen, med räknesättet addition, (**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”.
10. Alla kongruensavbillidningar (avbildningar som bevarar avstånd mellan punkter av en plan rektangel (eller allmännare någon figur) på sig själv med sammansättning som gruppoperation.

    Anmärkning: Figurer med större symmetri genererar ”större” grupper än sådana med ”mindre” symmetri. Gruppen kan sägas beskriva figurens symmetriegenskaper. Fundera litet på vilka grupper som man får för ickekvadratiska rektanglar, kvadrater resp. cirklar.

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 lagarna (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 för alla A och B i **M** gäller att

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

så har man en *kommutativ ring*.

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

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

så föreligger en *ring med enhet*.

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

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

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

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

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

så säger man att **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.

Övningar lekt 5

Övningar om grupper:

1. Verfiera att mängderna med räknesätten exemplen 1 – 9 ovan verkligen är grupper resp. abelska grupper.
2. Varför är (**N**, +) och (**N**, ·) inte några grupper?
3. Varför är (**Q**,·) inte någon grupp?
4. Varför är mängden av vektorer i $\mathbf{R}^n$ ($n \geq 2$) med räknesättet ”skalärprodukt” inte någon grupp?
5. Varför är vektorerna i $\mathbf{R}^3$ med räknesättet ”kryssprodukt” inte någon grupp?
6. Låt **M** vara mängden som består av de båda talen ±1. Om man som räknesätt tar ”multiplikation”, är (**M,**) då en grupp?
7. Verifiera att (**M**, o) är en grupp om **M** är mängden av bijektioner $\mathbf{X} \rightarrow \mathbf{X}$ och o är sammansättningsoperationen. Är gruppen abelsk?
8. Låt **X** i föregående uppgift vara mängden {0, 1}. Vilka är bijektionerna? Skriv upp gruppens ”multiplikationstabell”. Är gruppen abelsk?
9. Låt **X** i stället vara mängden {0, 1, 2}. Vilka är bijektionerna? Skriv upp gruppens ”multiplikationstabell”. Är gruppen abelsk?

Övningar om ringar:

10. Verifiera att påståendena i ex 1 – 4 ovan är riktiga. Vilka av dessa ringar är kommutativa och vilka har en enhet?
11. Är (**N** + ; ·) en ring?
12. Är ($\mathbf{Q}_+$ + ; ·) en ring? $\mathbf{Q}_+$ är mängden av de positiva rationella talen.

Övningar om kroppar:

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

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

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

16 För vilka heltal $n \geq 2$ utgör restklasserna mod n med räknesätten addition och multiplikation en kropp? Bevisa påståendet

Dagens uppgift: 13