# Explorativ övning 9

## MÄNGDER MED ALGEBRAISKA OPERATIONER*

De fyra räknesätten: addition, subtraktion, multiplikation och division är, vad man ofta kallar, (aritmetiska) operationer på mängden av alla tal. Addition och multiplikation av vanliga funktioner är också operationer.

Inom algebran är man ofta intresserad av olika egenskaper hos operationer. Två mängder som tillåter operationer med samma egenskaper kan ofta studeras samtidigt – man behöver inte bevisa samma satser flera gånger om man vet att dessa satser gäller för varje mängd med operationer som satisfierar vissa villkor. I detta avsnitt definierar vi begreppet operation och några mycket allmänna egenskaper hos operationer t ex associativitet och kommutativitet.

Begreppet operation är ett specialfall av begreppet funktion. Därför repeterar vi först att med en funktion $f$ från en mängd $X$ till en mängd $Y$ menar man vanligen en regel som till varje $x \in X$ ordnar exakt ett element $y \in Y$. Då skriver man $y = f(x)$ och $f : X \to Y$. Låt oss också repetera att $X \times Y$ betecknar **den kartesiska produkten** av mängderna $X$ och $Y$ dvs

$$X \times Y = \{(x, y) : x \in X \text{ och } y \in Y\}.$$

Nu är vi beredda att definiera begreppet operation:

**(9.1) Definition.** Med en **binär operation** på mängden $M$ menar man en funktion som till varje par $(a, b) \in M \times M$ ordnar ett element $a * b$ i $M$. Mängden $M$ med operationen "$*$" kommer att betecknas med $(M, *)$. Man säger att mängden $M$ är **sluten** med avseende på operationen "$*$". □

Definitionen säger att en operation på $M$ till två godtyckliga element $a, b \in M$ ordnar ett element $a * b \in M$. Här följer några exempel på operationer:

**(9.2) Exempel.** (a) Låt $M$ vara en av mängderna $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ och låt $a * b = a + b$ vara den vanliga summan av $a$ och $b$.

*__MAL200, ht 99__

(b) Med samma $M$ som i (a), låt $a * b = ab$ vara den vanliga produkten av $a$ och $b$.

(c) Låt $M$ vara mängden av alla reella funktioner och $f * g = f + g$ den vanliga summan av två funktioner $f, g \in M$ dvs $(f+g)(x) = f(x) + g(x)$ då $x \in \mathbb{R}$. Om t ex $f(x) = x^2$ och $g(x) = \sin x$ så är $(f+g)(x) = x^2 + \sin x$.

(d) Låt $M = \mathbb{Z}_2 = \{0, 1\}$ vara mängden av alla rester vid division med 2. Man kan definiera en operation $\oplus$ på $M$ enligt följande tabell:

| $\oplus$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

(e) Låt $M = \{S, F\}$ vara mängden av möjliga sanningsvärden av alla utsagor. Betrakta operationen $\vee$ på $M$ (disjunktionen) i enlighet med den välkända tabellen:

| $\vee$ | S | F |
|---|---|---|
| S | S | S |
| F | S | F |

$\square$

Enbart det faktum att man har en operation på en mängd är oftast inte tillräckligt för att studera mängden. Därför vill man veta lite mera om olika egenskaper hos operationer.

**(9.3) Definition.** Man säger att operationen $*$ på $M$ är **associativ** om $(a*b)*c = a*(b*c)$ då $a, b, c \in M$. Operationen är **kommutativ** om $a * b = b * a$ då $a, b \in M$. $\square$

**Exempel.** (a) Alla operationer i Exempel (9.2) är associativa och kommutativa.

(b) Subtraktionen är varken kommutativ eller associativ på $\mathbb{Z}$ dvs om $a * b = a - b$ så gäller inte att $a * b = b * a$ eller $(a * b) * c = a * (b * c)$ ty vanligen $a - b \neq b - a$ och $(a - b) - c \neq a - (b - c)$. Bästa sättet att visa dessa påståenden är att ge motexempel: t ex $2 - 3 \neq 3 - 2$ och $(3 - 2) - 1 \neq 3 - (2 - 1)$. $\square$

**(9.4) Definition.** Man säger att $e \in M$ är ett **neutralt element** för operationen $*$ om $e*a = a*e = a$ då $a \in M$. Man säger att $a' \in M$ är en **invers** till $a \in M$ om $a*a' = a'*a = e$. $\square$

**Exempel.** (a) 0 är ett neutralt element för additionen på $M = \mathbb{Z}$ (eller $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) ty $0 + a = a + 0 = a$ då $a \in M$. Inversen till $a \in M$ är $-a$ ty $a + (-a) = (-a) + a = 0$. Inversen kallas här motsatta talet.

(b) Talet 1 är ett neutralt element för multiplikationen på $M$ ($M$ som i (a)) ty $1 \cdot a = a \cdot 1 = a$ då $a \in M$. Inversen till $a \in M$ finns enbart då $a' = 1/a \in M$. Om $M = \mathbb{R}$ så har alla tal invers utom 0. Om $M = \mathbb{Z}$ så har enbart $a = \pm 1$ inverse (motivera varför!). □

**(9.5) Proposition.** $(M, *)$ *har högst ett neutralt element. Om operationen på* $M$ *är associativ och* $a \in M$ *har invers så är den entydig.*

**Bevis.** Om $e'$ också är ett neutralt element så har vi

$$\begin{aligned} e' &= e * e' \qquad \text{ty } e \text{ är neutralt} \\ &= e \qquad \text{ty } e' \text{ är neutralt.} \end{aligned}$$

Låt $a'_1$ också vara en invers till $a$. Då gäller

$$a'_1 = a'_1 * e = a'_1 * (a * a') = (a'_1 * a) * a' = e * a' = a'.$$

□

**(9.6) Anmärkning.** Om $M = \{a_1, a_2, \ldots, a_n\}$ är en ändlig mängd så definierar man ofta operationer på $M$ med hjälp av **"multiplikationstabeller"**:

$$\begin{array}{c|ccccc} * & a_1 & \ldots & a_j & \ldots & a_n \\ \hline a_1 & & & & & \\ \vdots & & & & & \\ a_i & & & a_i * a_j & & \\ \vdots & & & & & \\ a_n & & & & & \end{array}$$

Varje sådan tabell ger en operation på $M$. Med hjälp av tabellen kan man lätt avgöra om operationen på $M$ är kommutativ (hur?) eller om det finns ett neutralt element (hur?). Men det är mycket besvärligare att avgöra om operationen är associativ (se övningar). □

**(9.7)** Avsnittets syfte var att bekanta sig med begreppet **binär operation** på en mängd $M$. Det viktigaste exemplet på sådana operationer är de fyra räknesätten på olika talmängder. I övningarna kommer vi att undersöka olika egenskaper hos dessa operationer:

- associativitet
- kommutatitivitet
- neutrala element
- inverser (motsatta element)

## Övning A

1. Förklara begreppen associativ och kommutativ operation med hjälp av addition och subtraktion på heltalen $\mathbb{Z}$.

2. Med avseende på vilka av följande operationer är $\mathbb{Z}$ sluten? Vilka av dessa operationer på $\mathbb{Z}$ är associativa, kommutativa, vilka har ett neutralt element? Varje gång då det finns ett neutralt element bestäm alla element som har invers.

   (a) $m * n = mn + 1$
   (b) $m * n = m + n - mn$
   (c) $m * n = m^2 + n^2$
   (d) $m * n = 2^{mn}$
   (e) $m * n = 2$
   (f) $m * n = SGD(m, n)$
   (g) $m * n = \max(m, n)$
   (h) $m * n = MGM(m, n)$

## Övning B

1. Hur många operationer finns det på en mängd med 2 element? Hur många av dessa är kommutativa?

2. Hur många operationer finns det på en mängd med 3 element? Hur många av dessa är kommutativa? Generalisera Dina slutsatser till mängder med $n$ element.

## Övning C

1. Ge exempel på en mängd med en operation som är

   (a) associativ, men ej kommutativ;

   (b) kommutativ, men ej associativ.

2. Ge tre exempel på mängder med operationer som är associativa, har neutralt element och är sådana att varje element har invers.

   **Anmärkning.** En mängd $G$ med en operation $*$ som är associativ, har neutralt element och är sådan att varje element har invers kallas **grupp**. Grupper har en mycket stor betydelse i hela matematiken och flera av dess tillämpningar (kemi, fysik, kryptografi, kodningsteori). Gruppteorin utvecklades från arbeten om algebraiska ekvationer av J.L. Lagrange, N.H. Abel och E. Galois.