# Algebraiska strukturer, 21 januari

## MÄNGDER OCH OPERATIONER

De fyra räknesätten: addition, subtraktion, multiplikation och division är, vad man ofta kallar, (aritmetiska) operationer i mängder av alla tal.

**Definition.** Låt $M$ vara en mängd. En **binär operation** $*$ på $M$ är en regel som till varje ordnat par $(x, y)$ av element i $M$ ordnar ett nytt element i $M$. Detta nya element skriver vi $x * y$.

$$(x, y) \mapsto x * y \in M$$

Definitionen säger att en binär operation är en funktion från kartesianska produkten $M \times M = \{(x, y) \mid x, y \in M\}$ till $M$.

---

**Exempel 1.** (a) Låt $M$ vara en av mängderna $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ och låt $a * b = a + b$, $(a, b) \mapsto a + b$

(b) $M = \mathbb{N}$, $m * n = m^n$, $(m, n) \mapsto m^n \in \mathbb{N}$.

(c) $M = \mathbb{Z}$, $m * n = m - n$. (Obs! $*$ - ej operation på $\mathbb{N}$, ty, t.ex., $2 * 3 = 2 - 3 \notin \mathbb{N}$).

(d) Låt $M$ vara mängden av $(2 \times 2)$-matriser med reella element och $A * B = AB$, den vanliga matrisprodukten för $A$, $B \in Mat_2(\mathbb{R})$.

---

Om $M = \{a_1, a_2, \ldots, a_n\}$ är en ändlig mängd så definierar man ofta operationer på $M$ m h a "multiplikationstabeller" (Cayleytabeller):

| $*$ | $a_1$ | $\ldots$ | $a_i$ | $\ldots$ | $a_j$ | $\ldots$ | $a_n$ |
|---|---|---|---|---|---|---|---|
| $a_1$ | $a_1 * a_1$ | $\ldots$ | $a_1 * a_i$ | $\ldots$ | $a_1 * a_j$ | $\ldots$ | $a_1 * a_n$ |
| $\vdots$ | | $\ddots$ | | | | | |
| $a_i$ | $a_i * a_1$ | $\ldots$ | $a_i * a_i$ | $\ldots$ | $a_i * a_j$ | $\ldots$ | $a_i * a_n$ |
| $\vdots$ | | | | $\ddots$ | | | |
| $a_j$ | $a_j * a_1$ | $\ldots$ | $a_j * a_i$ | $\ldots$ | $a_j * a_j$ | $\ldots$ | $a_j * a_n$ |
| $\vdots$ | | | | | | $\ddots$ | |
| $a_n$ | $a_n * a_1$ | $\ldots$ | $a_n * a_i$ | $\ldots$ | $a_n * a_j$ | $\ldots$ | $a_n * a_n$ |

---

**Exempel 2.** Låt $M = \{-1, 1\}$, $*$ är en vanlig multiplikation. Multiplikationstabellen för $*$ blir då

| $*$ | $1$ | $-1$ |
|---|---|---|
| $1$ | $1$ | $-1$ |
| $-1$ | $-1$ | $1$ |

---

**Definition.** En operation $*$ på $M$ kallas **kommutativ** om $a * b = b * a$ för alla $a, b \in M$. Den kallas **associativ** om $a * (b * c) = (a * b) * c$ då $a$, $b$, $c \in M$. Man säger att $e \in M$ är ett **neutralt element** för $*$ om $a * e = e * a = a$ då $a \in M$.

---

**Exempel 3.** (a) De vanliga additionen och multiplikationen är kommutativa och associativa på $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$.

(b) Betrakta $(\mathbb{N}, *)$, där $m * n = m^n$. $*$ är inte kommutativ, ty t.ex $2 * 3 = 2^3 = 8 \neq 3^2 = 3 * 2$, den är inte associativ heller, ty t.ex. $2 * (2 * 3) = 2 * 2^3 = 2^{2^3} = 2^8$, men $(2 * 2) * 3 = 2^2 * 3 = (2^2)^3 = 2^6$.

Med hjälp av multiplikationstabellen kan man lätt avgöra om operationen är kommutativ (Hur?), har ett neutralt element (Hur?).

Obs! Att kontrollera att operationen är associativ är inte lika lätt!!

GRUPPER

**Definition.** Låt $G$ vara en mängd och låt $*$ vara en operation på $G$ dvs

(0) $a * b \in G$ då $a, b \in G$ (sluthet).

Man säger att $(G, *)$ är en **grupp** om

(1) $*$ är associativ, dvs $(a * b) * c = a * (b * c)$, då $a, b, c \in G$;

(2) det finns $e \in G$ så att $e * a = a * e = a$ då $a \in G$ (neutralt element eller identiteselement),

(3) till varje $a \in G$ ska det finnas ett element $a' \in G$ så att $a' * a = a * a' = e$ (invers)

Vi skriver $(G, *)$. Det följer från Sats 5.1 att i varje grupp finns det endast ett neutralt element (identitetselement) och varje gruppelement $a$ har endast en invers $a'$.

**Exempel 4.** (a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ med operationen $+$ är grupper (ej $\mathbb{N}$)

(b) Om vi utelämnar 0 ur $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ får vi grupper med avseende på den vanliga multiplikationen ($(\mathbb{Z} \setminus \{0\}, \cdot)$ är inte en grupp).

(c) Låt $X$ vara en mängd och låt $G$ bestå av bijektiva funktioner. Operationen $*$ är sammansättningen av två funktioner: $(f * g)(x) = f(g(x))$. $(G, *)$ är en grupp (Visa!)

(d) Låt $G$ bestå av rotationer och speglingar av planet som överför $n$-höringen på sig själv och låt $*$ vara sammansättningen. $(G, *)$ är en grupp.

**Sats 5.1.** I varje grupp finns det endast ett neutralt element $e$ och varje gruppelement $a$ har endast en invers $a'$.

**Bevis.** 1. Låt $e$ och $f$ vara element i $G$ som uppfyller

$$a * e = e * a = a \text{ då } a \in G \tag{1}$$
$$a * f = f * a = a \text{ då } a \in G \tag{2}$$

Då gäller $f =$ (enligt (1) $= e * f =$ (enligt (2)) $= e$, dvs $f = e$.

2. Låt $a \in G$ och låt $b, c \in G$ uppfylla

$$a * b = b * a = e \text{ och } a * c = c * a = e,$$

($e$ är det neutrala elementet). Då gäller

$$b = b * e = b * (a * c) = (\text{assoc}) = (b * a) * c = e * c = c,$$

dvs $b = c$.

Inversen till $a \in G$ betecknar man ofta $a^{-1}$.

**Anmärkning.** (a) När man definierar en grupp så beskriver man mängden $G$ av dess element och gruppoperationen $*$. Formellt borde man säga att $(G, *)$ är en grupp. Icke-desto mindre säger man oftast att $G$ är en grupp.

(b) Vi vet redan att symbolen "$*$" som betecknar en operation kan tolkas på olika sätt. När det gäller beteckningar finns det två vanliga typer som dels beror på traditionen dels på bekvämligheten. Det är säkert bekvämare att skriva $ab$ eller $a \cdot b$ i stället för $a * b$. Då säger man om **multiplikativ notation**. Inversen betecknas då med $a^{-1}$. Ibland är denna notation inte helt naturlig, speciellt när gruppoperationen är addition. Då använder man **additiv notation** dvs man tolkar "$*$" som "$+$". Inversen betecknas då med $-a$ och identitetselementet med 0.

---

**Proposition.** Låt $G$ vara en grupp och $a$, $b$, $c \in G$. Då gäller strykningarna

$$\begin{array}{ll} (a) & a * c = b * c \Rightarrow a = b \\ (b) & c * a = c * b \Rightarrow a = b \end{array}$$

**Bevis.** (a) Multiplicera från höger med inversen $c^{-1}$ till $c$. Enligt associativiteten får vi

$$\begin{aligned} (a * c) * c^{-1} = (b * c) * c^{-1} &\Leftrightarrow a * (c * c^{-1}) = b * (c * c^{-1}) \\ &\Leftrightarrow a * e = b * e \Leftrightarrow a = b. \end{aligned}$$

---

**Cayleytabell.** Låt $G = \{a_1, \ldots, a_n\}$ vara en ändlig mängd. Varje operation på $G$ kan beskrivas m h a Cayleytabell. Cayleytabellen för en grupp har följande egenskap: Varje element förekommer precis en gång i varje rad och precis en gång i varje kolonn, ty en rad i tabellen består av produkterna $a_i * a_1, \ldots, a_i * a_j, \ldots, a_i * a_n$, alla dessa produkter ger olika element i $G$ därför att $a_i * a_j = a_i * a_k$ ger $a_j = a_k$. I almänhet är det inte lätt avgöra om en operation på $G$ definierar en grupp genom att studera Cayleytabellen. Genom inspektion av denna upptäcker man lätt om det finns ett neutralt element (Hur?) och om varje element har en invers (varje rad och varje kolonn måste innehålla det neutrala elementet). Associativiteten är svårt att kontrollera.