Algebraiska strukturer, 28 januari

RELATIONER

En **relation** R på en mängd X är en godtycklig mängd bestående av par (x, y), där $x,\ y \in X$.

Man skriver $x \sim_R y$ ($x \sim y$) om $(x, y) \in R$. Men "$\sim$" ersätts oftast med andra tecken som traditionellt betecknar kända relationer t ex med "$\leq$" eller "$|$".

Exempel. 1. Låt $X = \mathbb{N}$ och låt $R_1 = \{(x, x), x \in \mathbb{N}\}$. R_1 beskriver likheten: $x \sim_{R_1} y$ omm $x = y$.

2. Låt $X = \mathbb{Z}$ och $R_2 = \{(x, x + 5k), x \in \mathbb{Z}, k \in \mathbb{Z}\}$. Då $x \sim_{R_2} y$ omm $5|(x - y)$.

3. Låt $X = \mathbb{R}$ och $R_3 = \{(x, y), x \leq y\}$. R_3 beskriver relationen "mindre eller lika".

EKVIVALENSRELATIONER

En relation $\sim$ på X är en **ekvivalensrelation** om

- $x \sim x$ för alla $x \in X$ (**reflexiv**)
- $x \sim y \Leftrightarrow y \sim x$ (**symmetrisk**)
- $x \sim y$ och $y \sim z \Rightarrow x \sim z$ (**transitiv**)

Relationerna R_1, R_2 är ekvivalensrelationer, R_3 är ej symmetrisk.

PARTITIONER

Låt X vara en mängd, $X_i \subseteq X$, $X_i \neq \emptyset$, $i \in I$. Man säger att X_i, $i \in I$, utgör en **partition** av X om

$$X = \cup_{i \in I} X_i \text{ och } X_i \cap X_j = \emptyset \text{ då } X_i \neq X_j.$$

Låt $\sim$ vara en ekvivalensrelation på X och $x \in X$. Mängden

$$[x] = \{y \in X, \text{ där } y \sim x\}, \quad x \in X.$$

$[x]$ kallas då för ekvivalensklassen till x under $\sim$.

Sats 9.1. Ekvivalensklasserna under varje ekvivalensrelation på X bildar en partition av X. Omvänt, givet en partition så finns det ekvivalensrelation på X, vars ekvivalensklasser utgörs precis av X_i, $i \in I$.

Bevis. 1. Låt $\sim$ vara en ekvivalensrelation på X. Eftersom $x \sim x$ för varje $x \in X$, gäller $x \in [x]$ och $X = \cup_{x \in X}[x]$ (unionen av alla ekvivalensklasserna).

Låt nu $[a]$ och $[b]$ vara två icke-disjunkta ekvivalensklasser. Vi vill visa att $[a] = [b]$. Då får vi att **två ekvivalensklasser antingen är lika eller disjunkta**. Eftersom $[a] \cap [b] \neq \emptyset$ finns det c som tillhör såväl $[a]$ som $[b]$. Ur symmetriet och transitiviteten följer att

$$c \in [a] \text{ och } c \in [b] \Rightarrow a \sim c \text{ och } c \sim b \Rightarrow a \sim b$$

Välj nu $x \in [a]$ godtyckligt. Då gäller $x \sim a$ som tillsammans med $a \sim b$ ger $x \sim b$ och därmed $x \in [b]$ och $[a] \subseteq [b]$. Av symmetriskäl har man också $[b] \subseteq [a]$ och alltså $[a] = [b]$.

2. Definiera $\sim$ enligt

$$x \sim y \Leftrightarrow \text{ } x \text{ och } y \text{ tillhör samma } X_i$$

Reflexivitet och symmetri är uppenbara. $\sim$ är transitiv, ty $x \sim y$ och $y \sim z \Leftrightarrow$ det finns $i \in I$ så att $x, y \in X_i$ och det finns $j \in I$ så att $y, z \in X_j$ varav $y \in X_i \cap X_j$. Eftersom $X_i \cap X_j \neq \emptyset$ omm $X_i = X_j$, får vi att $x, y, z \in X_i = X_j$, dvs $x \sim z$. Altså är $\sim$ en ekvivalensrelation. Det framgår också att ekvivalensklasser under $\sim$ utgörs av mängderna X_i, $i \in I$.

Ur sats 9.1 följer att två ekvivalensklasser antingen är lika eller disjunkta och dessutom $x \in [a]$ omm $[x] = [a]$.

DELBARHET

Definition. Om a och b är två heltal så säger man att b **delar** a om $a = bq$, där q är ett heltal. Detta betecknas $b|a$.

Några egenskaper hos delbarhetsrelation.

Låt a, b, $c \in \mathbb{Z}$. Då gäller

(a) om $d|a$ och $d|b$ så gäller $d|(a \pm b)$;

(b) om $a|b$ och $b|c$ så gäller $a|c$;

(c) om $a|b$ och $b|a$ så är $b = \pm a$.

KONGRUENSER

Låt n vara ett positivt heltal, a, $b \in \mathbb{Z}$. Man säger att a och b är **kongruenta modulo** n om $n|(a-b)$. Man skriver $a \equiv b \mod n$ eller $a \equiv_n b$. Uttrycket $a \equiv b \mod n$ kallas **kongruens**.

Sats 10.1. Kongruens modulo n är en ekvivalensrelation på $\mathbb{Z}$ för varje positivt heltal n.

Bevis. Reflexiv: $a \in \mathbb{Z} \Rightarrow a \equiv a \mod n$, ty $a - a = 0$ och $n|0$.

Symmetrisk: $a, b \in \mathbb{Z}$ och $a \equiv b \mod n \Rightarrow n|(a-b) \Rightarrow n|(b-a) \Rightarrow b \equiv a \mod n$.

Transitiv: $a, b, c \in \mathbb{Z}$, $a \equiv b \mod n$, $b \equiv c \mod n \Rightarrow n|(a-b)$ och $n|(b-c) \Rightarrow n|((a-b)+(b-c))$, dvs $n|(a-c) \Rightarrow a \equiv c \mod n$.

Ekvivalensklasserna under denna ekvivalensrelation kallas kongruensklasserna modulo n.

Exempel. Det finns tre kongruensklasser modulo 3:

$[0] = \{x \in \mathbb{Z}, x \equiv_3 0\} = \{x \in \mathbb{Z}, 3|x\} = \{\ldots, -3, 0, 3, \ldots\}$,

$[1] = \{x \in \mathbb{Z}, x \equiv_3 1\} = \{x \in \mathbb{Z}, 3|(x-1)\} = \{\ldots, -2, 1, 4, \ldots\}$,

$[2] = \{x \in \mathbb{Z}, x \equiv_3 2\} = \{x \in \mathbb{Z}, 3|(x-2)\} = \{\ldots, -1, 2, 5, \ldots\}$.

Divisionsalgoritmen. Om a och b är heltal och $b \neq 0$ så är

$$a = bq + r, \text{ där } 0 \leq r < |b|.$$

Både q och r är definierade entydigt av a och b.

Definition. Talen q och r i Divisionsalgoritmen kallas för **kvoten** och respektive **resten** vid division av a med b.

Sats 10.2. Låt n vara ett positivt heltal. Varje heltal är kongruent modulo n med precis ett av heltalen $0, 1, \ldots, n-1$.

Bevis. Låt $a \in \mathbb{Z}$. Enligt Divisionsalgoritmen är

$$a = nq + r, \text{ där } 0 \leq r < n.$$

Då är $a - r = nq$ vilket medför att $n|(a-r)$ och $a \equiv_n r$. Vi har alltså att a är kongruent med minst ett av heltalen $0, 1, \ldots, n-1$. För att visa unikness antar vi att $a \equiv_n s$, där $0 \leq s < n$. Då gäller $a - s = nt$, för något heltal t, och $a = nt + s$. Detta medför att $s = r$, ty resten är definierad entydigt av a och n.

För kongruensrelationen modulo n har man

$$[x] = [r], \text{ där } r \text{ är resten vid divisionen av } x \text{ med } n \ ,$$

ty $x \equiv_n r$ och därmed $x \in [r]$, och eftersom olika kongruensklasser saknar gemensamma element får vi $[x] = [r]$.

Av sats 10.2 följer att det finns precis n kongruensklasser modulo n: $[0], [1], \ldots, [n-1]$.

Mängden av alla kongruensklasser kommer att betecknas med $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ eller $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ eller enkelt $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Definition. För $[a], [b] \in \mathbb{Z}_n$ definierar vi

$$[a] \oplus [b] = [a+b] \text{ och } [a] \odot [b] = [ab].$$

Är operationerna väl-definierade?

Lemma. I $\mathbb{Z}_n$ gäller följande:

om $[a_1] = [a_2]$ och $[b_1] = [b_2]$ så är $[a_1 + b_1] = [a_2 + b_2]$ och $[a_1 b_1] = [a_2 b_2]$.

Sats 11.1. $\mathbb{Z}_n$ är en abelsk grupp med avseende på operationen $\oplus$.

Bevis. Associativitet:

$$[a] \oplus ([b] \oplus [c]) = [a] \oplus [b+c] = [a + (b+c)]$$
$$([a] \oplus [b]) \oplus [c] = [a+b] \oplus [c] = [(a+b) + c]$$

så att $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$, ty $a + (b+c) = (a+b) + c$.

$[0]$ är det neutrala elementet. Inversen till $[r]$ är $[-r]$, ty $[r] \oplus [-r] = [r-r] = [0] = [-r+r] = [-r] \oplus [r]$.

Alltså är $\mathbb{Z}_n$ en grupp. Den är abelsk, ty $[a] \oplus [b] = [a+b] = [b+a] = [b] \oplus [a]$.

Obs! $(\mathbb{Z}_n, \odot)$ är aldrig en grupp, ty $[0]$ saknar invers. $\mathbb{Z}_n \setminus \{[0]\}, \odot)$ behöver inte heller vara en grupp, ty t ex $[2] \odot [3] = [6] = [0]$ i $\mathbb{Z}_6$.
