Algebra och talteori

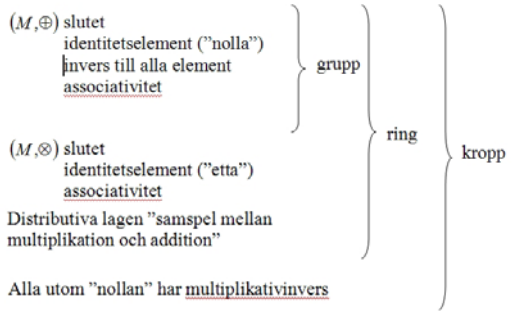
MMGL31

Föreläsning 4

VT 2010

Samuel Bengmark

Rep. strukturer



$(\mathbb{Z}_n,+,\cdot)$ en ring

Exempel $\mathbb{Z}_4$

+	0	1	2	3
0				
1				
2				
3				

·	0	1	2	3
0				
1				
2				
3				

- Slutenhet, identiteter, inverser, (kommutativt) syns
- Associativa lagarna, och distributiva lagen får kollas separat.

Idag

- $\mathbb{Z}_n$ är ring.
- Multiplikativt inverterbara element i $\mathbb{Z}_n$
- $\mathbb{Z}_p$ är kropp omm p primtal

Invers

Definition

Antag att e är identitetselement map operationen $*$.

Ett element b så att

$a*b=b*a=e$

kallas invers till a map $*$.

Inversen till a map operationen $\otimes$ kallas den additiva inversen och betecknas ofta –a, pss kallas inversen till a map operationen $\otimes$ för den multiplikativa inversen och den betecknas a^{-1}

Vilka element i $\mathbb{Z}_n$ har multiplikativ invers?

- För att svara på detta måste vi förstå när ekvationen $ax\equiv_n 1$ har lösning. Tittar först på den mer allmänna ekvationen

$$ax\equiv_n c$$

Att lösa $3x \equiv_7 5$

Exempel

- $3x \equiv_7 5 \Leftrightarrow 3x+7y=5$
- Löser först $3x+7y=SGD(3,7)=1$.
- Finner att $3\cdot(-2)+7\cdot1=1$, tex med E.A.
- Multiplicerar med 5. Får $3\cdot(-10)+7\cdot5=5$
- Slutsats $x=-10 \equiv_7 4$

Testa alltid lösningen: $3\cdot4 = 12 \equiv_7 5$

Att lösa $2x \equiv_{24} 22$

- $2x \equiv_{24} 22 \Leftrightarrow 2x+24y=22$
- Partikulärlösning: $2x+24y=SGD(2,24)=2$
  - E.A. ger $2\cdot(-11)+24\cdot1=2$
  - Multiplicerar med $22/2=11$: $2\cdot(-121)+24\cdot11=22$
  - Finner $x_p=-121 \equiv_{24} 11$
- Homogenlösning: $2x+24y=0 \Leftrightarrow x+12y=0$
  - $x_h=12k$, $y_h=-k$,

Slutsats: $x=x_p+x_h=11+12k$, dvs $x\in\{11,23\}$

Att lösa $ax \equiv_n c$

- $ax \equiv_n c \Leftrightarrow xa+yn=c$
- Hitta partikulärlösning x_p och y_p till $xa+yn=c$
  - Löser först $xa+yn=SGD(a,n)$ tex med E.A.
  - Multiplicerar sedan med $c/SGD(a,n)$
  - Lösning saknas om $SGD(a,n) \not| c$
- Hitta homogenalösningarna x_h och y_h till $xa+yn=0$.
  - Dessa är $x_h=k\cdot n/SGD(a,n)$, $y_h=k\cdot -a/SGD(a,n)$
- Om $SGD(a,n)|c$ finns $SGD(a,n)$ stycken lösningar

$$x = \frac{c}{SGD(a,n)} x_p + k\frac{n}{SGD(a,n)}$$

Multiplikativt inverterbara element i $\mathbb{Z}_n$

a har invers i $\mathbb{Z}_n$

$\Leftrightarrow ax \equiv_n 1$ har lösning

$\Leftrightarrow SGD(a,n)|1$

$\Leftrightarrow SGD(a,n)=1$

Mängden av inverterbara

Definition

I en ring $(M,\oplus,\otimes)$ betecknar M^* mängden av alla element inverterbara map operationen $\otimes$

OBS! M en kropp omm $M^*=M\backslash\{0\}$.

Exempel

- $\mathbb{Z}_n^*=\{a\in\{0,\ldots n-1\}, SGD(a,n)=1\} =$
  $= \{$ a som är relativt prima med n$\}$.
- $\mathbb{Z}^*=\{\pm1\}$
- $\mathbb{R}^*=\mathbb{R}\backslash\{0\}$, alltså kropp

Kansellation

Funkar bara för element med invers (genom multiplikation med dess invers).

Exempel

$3a \equiv_5 3b \Leftrightarrow a \equiv_5 b$ eftersom $3\in\mathbb{Z}_5^*$.

Har multiplicerat med $3^{-1} \equiv_5 2$

Exempel

$3a \equiv_6 3b \not\Leftarrow a \equiv_6 b$ eftersom $3\notin\mathbb{Z}_6^*$

Tex gäller att $3\cdot2 \equiv_6 3\cdot0$ men $2 \not\equiv_6 0$.

$\mathbb{Z}_p$ kropp omm p ett primtal.

Om p är ett primtal gäller att
$\mathbb{Z}_p^* = \{ a \in \{0,\ldots p-1\}, \text{SGD}(a,p)=1 \} = \{1,\ldots,p-1\} = \mathbb{Z} \setminus \{0\}$.

Om n ej primtal finns alltid något tal a i {0,…,n-1} som delar n. Därmed saknas invers för a och slutsatsen blir att $\mathbb{Z}_n$ ej är en kropp.

Exempel $(\mathbb{Z}_5,+,\cdot)$

Exempel $\mathbb{Z}_5$

+	0	1	2	3	4
0					
1					
2					
3					
4					

·	0	1	2	3	4
0					
1					
2					
3					
4					

$742^{1950} \equiv_{1951} ?$

Fermats lilla sats

Om p är ett primtal och $a \not\equiv_p 0$, då gäller att

$$a^{p-1} \equiv_p 1$$

Exempel

$5^6 \equiv_7 1$

$742^{1950} \equiv_{1951} 1$