Algebra och talteori

MMGL31

Föreläsning 3

VT 2010

Samuel Bengmark

Repetition

- Irreducibla tal och primtal (ej i boken)
  - •Irreducibelt (odelbart) $d \mid p \Rightarrow d \in \{\pm 1, \pm p\}$
  - •Primt $p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b$
- $\mathbb{E}$, avsaknad av primtal och unik faktorisering
- Euklides algoritm, SGD och ax+by
- Aritmetikens fundamentalsats = unik faktorisering i $\mathbb{Z}$
- Bygger på att alla irreducibla tal i $\mathbb{Z}$ också är prima, vilket skall bevisas nu.

Idag

- Grupp, ring och kropp
- Kongruensräkning

Åter till: Irreducibla är prima i $\mathbb{Z}$!

Skall alltså visa att om p är ett irreducibelt tal och p|mn så kommer p|m eller p|n.

- Antag att p är irreducielt
- Skall nu visa att p|m·n $\Rightarrow$ p|m eller p|n.
- Om p|m är vi klara.
- Antag därför att p|mn och och att p$\not|$m. Visa att p|n.
- Att p inte delar m och p är irreducibelt finner vi att SGD(p,m)=1, dvs 1=xp+ym.
- Multiplicera med n och får n=xpn+ymn=xpn+ykp=p(xn+yk), dvs p|n.

p|mn $\Leftrightarrow$ mn=kp

Strukturer för mängder

- Grupp $(M,\oplus)$
- Ring $(M,\oplus,\otimes)$
- Kropp $(M,\oplus,\otimes)$

Symbolerna $\oplus$ och $\otimes$ kan kan representera vilka operationer som helst.

Generellt om strukturer

- I kursen kommer vi titta på fler talmängder än $\mathbb{Z}$ och $\mathbb{E}$: Tex
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- $\mathbb{Z}_n$ för olika värden på n
- $\mathbb{Z}$[i]

Det finns gemensamma och särskiljande egenskaper som synliggörs i begreppen grupp, ring och kropp som vi nu inför.

Grupp

Definition

En mängd M med en operation $\oplus$ kallas en grupp om följande gäller

1. Slutet: $a,b \in M \Rightarrow a \oplus b \in M$
2. Identitet finns: $\exists o \in M, \forall a \in M$ gäller att $a \oplus o = o \oplus a = a$
3. Inverser finns: $\forall a \in M, \exists b \in M$ så att $a \oplus b = o$
4. Associativa lagen: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

Exempel på grupper

Ex 1: $(\mathbb{Z},+)$

Ex 2: $(\mathbb{Q},+)$

Icke-exempel: $(\mathbb{N},+)$

Ex 3: $(\mathbb{Z}_n,+)$

Ex 4: $(\mathbb{Q}\setminus\{0\},\cdot)$

Ex 5: (2×2-matriser, +)

Ring och kropp

Definition

En talmängd med två operation $\oplus$ och $\otimes$ kallas en ring om

- $(M,\oplus)$ är en grupp
- för $\otimes$ gäller att:
  1. Slutet: $a,b \in M \Rightarrow a \otimes b \in M$
  2. Identitet finns map. $\exists e \in M, \forall a \in M$ gäller att $a \otimes e = e \otimes a = a$
  3. Associativa lagen $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
- Distributiva lagen: $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$

Om dessutom varje element $a \neq o$ har invers så kallas det kropp.

Exempel på ringar och kroppar

Repetition: kongruens

Definition

- Två heltal x och y sägs vara kongruenta modulo n om n | x-y.
- Man skriver $x \equiv y \bmod n$ eller $x \equiv_n y$
- Mängden av alla kongruensklasser utgör en mängd som vi betecknar $\mathbb{Z}_n$.

Obs: Varje tal är kongruent med något av talen 0,1, … n-1 modulo n, dvs

$\mathbb{Z}_n=\{0,1,2,\ldots,n-1\}$.

Exempel

$1 \equiv_7 8$

$0^2 \equiv_2 0$, $1^2 \equiv_2 1$ (paritet bevaras vid kvadrering)

$0^2 \equiv_4 0$, $1^2 \equiv_4 1$, $2^2 \equiv_4 0$, $3^2 \equiv_4 1$ (inga kvadrater $\equiv_4 2$ eller 3)