Talleori

Fermats lille teorem: Hvis p er et primtall og $\bar{a} \neq \bar{0}$ i $\mathbb{Z}/(p)$, så er $\bar{a}^{p-1} = \bar{1}$ i $\mathbb{Z}/(p)$.

Korollar: Vi har $\bar{a}^p = \bar{a}$ for alle restklasser $\bar{a}$.

Eksempel: Vis at $3n^{14} + 7n^3 + 4n^7$ alltid er delelig med 7 for $n \in \mathbb{Z}$.

I $\mathbb{Z}/(7)$ har vi: $3n^{14} + 7n^3 + 4n^7 = \bar{3}\bar{n}^{14} + \bar{7}\bar{n}^3 + \bar{4}\bar{n}^7$

$= \bar{3}\cdot\bar{n}^7\cdot\bar{n}^7 + \bar{4}\bar{n}^7 = \bar{3}\bar{n}^7 + \bar{4}\bar{n}^7 = \bar{7}\bar{n}^7 = \bar{0}$.

($\bar{n}^{14} = \bar{n}^7$, $\bar{n}^7 = \bar{n}$, $\bar{7} = \bar{0}$)

Altså er $3n^{14} + 7n^3 + 4n^7$ delelig med 7.

Eulers φ-funksjon: $\varphi(n)$ = antall k, $1 \leq k < n$, slik at n og k er innbyrdes primiske.

p et primtall: $\varphi(p) = p - 1$

Eulers teorem: La $t \in \mathbb{N}$. Hvis a er innbyrdes primisk med t, så er $\bar{a}^{\varphi(t)} = \bar{1}$ i $\mathbb{Z}/(t)$.

Wilsons teorem: $\overline{(p-1)!} = -\bar{1}$ i $\mathbb{Z}/(p)$ hvis p er et primtall.

produktet av alle ikke-null restklasser i $\mathbb{Z}/(p)$.

Kvadratsummer: Et tall $n \in \mathbb{N}$ er en kvadratsum dersom det finnes tall $a, b = 0, 1, 2, \ldots$ slik at $n = a^2 + b^2$.

Teorem: Et primtall p er en kvadratsum hvis og bare hvis $p = 2$ eller $p \equiv 1 \pmod 4$.

Teorem: Et naturlig tall n er en kvadratsum hvis og bare hvis hver primfaktor $p \equiv 3 \pmod 4$ forekommer et like antall ganger.

Pytagoreisk trippel: $x, y, z \in \mathbb{N}$ slik at $x^2 + y^2 = z^2$. (primitivt dersom x, y, z ikke har felles faktor)

Teorem: Enhver av x, y, z er et primitivt pytagoreisk trippel med x som oddetall. Da finnes det innbyrdes primiske tall p, q slik at

$$x = p^2 - q^2,\ y = 2pq,\ z = p^2 + q^2$$

Sjekk: $x^2 + y^2 = (p^2 - q^2)^2 + (2pq)^2 = p^4 - 2p^2q^2 + q^4 + 4p^2q^2$

$= p^4 + 2p^2q^2 + q^4 = (p^2 + q^2)^2$

Algebraiska strukturer

Binär operation på A: En funktion $f: A^2 \to A$ som ofta betecknas med $a * b$ istället för $f(a,b)$

(i) **Associativ:** $a*(b*c) = (a*b)*c$

(ii) **Kommutativ:** $a*b = b*a$

(iii) **Neutralt element:** $a*e = e*a = a$

(iv) **Inverst element till a:** $a*\tilde{a}^{-1} = \tilde{a}^{-1}*a = e$.

(v) **Distributiv lag:** $a\cdot(b+c) = a\cdot b + a\cdot c$, $(b+c)\cdot a = b\cdot a + c\cdot a$

Grupper: $(G,*)$ heter den en grupp om

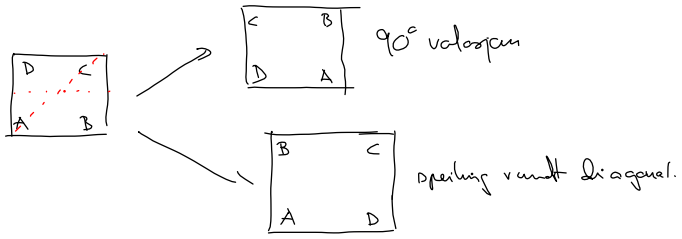
(i) $*$ är associativ

(ii) Det finns ett neutralt element e.

(iii) Alla element $a \in G$ har ett inverst element a^{-1}.

En grupp där $*$ är kommutativ, heter en **abelsk** grupp.

Exempel:



Ring: $(R,+,\cdot)$ är en ring om:

(i) $+$ är associativ

(ii) Det finns ett neutralt element 0 för $+$ $(a+0 = 0+a = a)$

(iii) Varje element a har en additiv invers $(-a)$ $(a+(-a) = (-a)+a = 0)$

} $(R,+)$ är en grupp

(iv) $+$ är kommutativ $(a+b = b+a)$

} som är abelsk.

(v) $\cdot$ är associativ

(vi) Det finns ett neutralt element 1 för $\cdot$ $(a\cdot 1 = 1\cdot a = a)$

(vii) $\cdot$ är distributiv med $+$, dvs $a(b+c) = ab+ac$, $(b+c)a = ba+ca$.

Om $\cdot$ är kommutativ, kallas $(R,+,\cdot)$ en kommutativ ring.

Kroppar: $(K,+,\cdot)$ heter en kropp dessutom den är en kommutativ ring, där varje $a \neq 0$ har en multiplikativ invers a^{-1}.

Exempel: $(\mathbb{Z},+,\cdot)$ är en (kommutativ) ring, men inte en kropp.

$(\mathbb{Q},+,\cdot)$ är en kropp.

$(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ är kroppar.

$\mathbb{Z}/(p)$ är en kropp (p primtal)

$\mathbb{Z}/(t)$ är en ring.

Ordnad kropp: En kropp $(K,+,\cdot)$ heter en ordnad kropp om den finns en total ordning $\leq$ på K så att

(i) $a \leq b \Rightarrow a+c \leq b+c$

(ii) $a, b \geq 0 \Rightarrow ab \geq 0$.

Undergrupper og homomorfier

Grupper: $(G,*)$ er en gruppe. En delmengde $H \subseteq G$ kalles en **undergruppe** dersom $(H,*)$ er en gruppe, dvs hvis

(i) $e \in H$

(ii) $a,b \in H$, da er $a*b \in H$

(iii) $a \in H$, da er $a^{-1} \in H$.

Homomorfier: $\varphi : G \to G'$ (to grupper) er en homomorfi dersom

$\varphi(a*b) = \varphi(a) * \varphi(b)$ for alle $a,b \in G$

$\Longrightarrow \quad \varphi(e) = e' \,,\ \varphi(a^{-1}) = \varphi(a)^{-1}$

En **isomorfi** er en bijektiv homomorfi

Ringer: $(R,+,\cdot)$ En delmengde $I \subseteq R$ kalles et **ideal** dersom:

(i) $0 \in I$

(ii) Hvis $a,b \in I$, da er $a+b \in I$

(iii) Hvis $a \in I$, da er $-a \in I$

(iv) Hvis $a \in I$, $r \in R$, da er $ar \in I$ og $ra \in I$.

Homomorfier: $\varphi : R \to S$ er en **homomorfi** dersom

(i) $\varphi(a+b) = \varphi(a)+\varphi(b)$

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$

(iii) $\varphi(1_R) = 1_S$

En isomorfi er en bijektiv homomorfi.

Kvotientkonstruksjoner: R ring, I et ideal i R, R/I

Ekvivalensrelasjon på R: $x \sim y \iff y - x \in I$.

$R/\sim \;=\; R/I$ = mengden av alle ekvivalensklasser $[x]$ for $x \in R$.

Vil definere operasjoner $+,\cdot$ på $R/\sim$ ved å sette

$$\left.\begin{aligned}[x]+[y] &= [x+y] \\ [x][y] &= [xy]\end{aligned}\right\} \text{Veldefinert?} \quad \text{OK!}$$

Lemma: Hvis $x \sim x'$ og $y \sim y'$, da er $x+y \sim x'+y'$ og $xy \sim x'y'$.

Bevis: Vi har $x \sim x'$, dvs $x'-x \in I$ dvs $x' = x+i$

Vi har $y \sim y'$, dvs $j = y'-y \in I$, dvs $y' = y+j$

Skulle så $x+y \sim x'+y'$: $x'+y'-(x+y) = (x+i)+(y+j)-x-y = i+j \in I$ OK.

— " — $xy \sim x'y'$: $x'y'-xy = (x+i)(y+j)-xy$

$$= xy+xj+iy+ij-xy = \underbrace{xj}_{\in I} + \underbrace{iy}_{\in I} + \underbrace{ij}_{\in I} \in I \quad \text{OK.}$$

Kardinaltal

En mängd A är **uppräknelig** om det finns en numrering i form av en lista

$a_1, a_2, a_3 \ldots$ som innehåller alla element i A.

$\mathbb{N} = \{1, 2, 3, \ldots\}$

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

$\mathbb{Q}$ är uppräknelig.

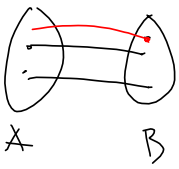
Lemma: $A_1, A_2, \ldots, A_n$ är uppräknelig, då $A_1 \times A_2 \times \ldots \times A_n$ är uppräknelig.

Lemma: Om $A_1, A_2, \ldots$ är uppräknelig, då $\bigcup_{n \in \mathbb{N}} A_n$ är uppräknelig.

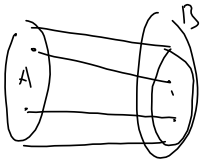
$\mathbb{R}$ är icke uppräknelig (Cantors diagonalargument).

Definition: (i) $|A| = |B|$ om det finns en bijektion $f: A \to B$.

(ii) $|A| \leq |B|$ om det finns en injektion $f: A \to B$

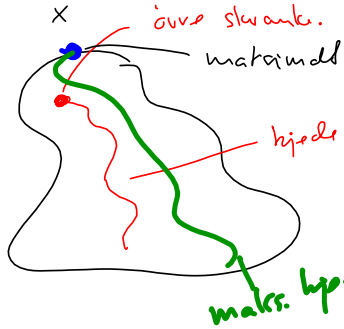


Cantor-Schröder-Bernstein: Om $|A| \leq |B|$ och $|B| \leq |A|$, så är $|A| = |B|$.



Kardinaltalen är totalt ordnade: För alla mängder A, B är antingen $|A| \leq |B|$ eller $|B| \leq |A|$.

Zorns Lemma: Om $(X, \leq)$ är en partiellt ordnad mängd där varje kedja har en övre skranka, så har X ett maximalt element.



: **Hausdorffs maximumsprincip:** En varje partiellt ordnad mängd har en maximal kedja.