Matematikens grunder

det det Ifall ni är sena kan ni ringa 0730694058 så kommer någon och öppnar.

Innehåll

1 Mängdlära

De matematiska objekt vi inte kommer att ge en fullständigt rigorös definition av är **mängder** och dess **objekt** (samt vad det innebär för ett objekt att "tillhöra" en mängd). Däremot kommer vi att postulera 10 axiom som bestämmer hur mängder, vad de än är, måste bete sig.

"Definition" 1.1. En **mängd** är en samling objekt. Ett **element** är ett objekt i en mängd.

Notation 1.2. Om X betecknar en mängd, och x är ett element i X, då skriver vi att $x \in X$ (läses "x ligger i X", "x tillhör X", etc.).

Anmärkning 1.3. Notera att vi ännu inte har gett ett konkret exempel på en mängd. Naiva exempel finns det gott om: "Mängden av alla människor", "Mängden av alla böcker i mitt rum", etc. För att rigoröst konstruera mängder krävs att vi mer rigoröst förklarar vad mängder är. Detta gör vi nu genom att postulera hur det som klassas som mängder måste bete sig; vilka egenskaper de måste ha. Läsaren kan för nu *anta* att en mängd finns. Vi kommer senare att göra detta axiom explicit, varpå vi med hjälp av andra axiom kommer att kunna skapa flera mängder (bland annat alla mängder som läsaren har sett under sin matematikundervisning).

1.1 Likhet - Axiom of extension

Låt A och B beteckna två mängder. Vad vill vi att "likhet" ska betyda? Strikt menat säger vi att två mängder, A och B, är likadana om, för varje påstående, P, så är $P(A)$ är sant om och endast om $P(B)$ är sant. Detta är dock omöjligt att utvärdera i praktiken eftersom det potentiellt finns oändligt många påståendet man kan applicera. Därför postulerar vi följande axiom.

Definition 1.4. AXIOM OF EXTENSION
Två mängder, A och B, är **lika med varandra** om och endast om de innehåller samma element. Vi skriver då

$$A = B. \tag{1.1}$$

Om A *inte* är lika med B, då skriver vi

$$A \neq B. \tag{1.2}$$

Exempel 1.5. För varje mängd A har vi att $A = A$.

Det finns även andra förhållanden än likhet som är av intresse för oss. Vi säger att A är en **delmängd** av B om och endast om varje element i A tillhör B. Ekvivalent uttryckt säger vi att B **innesluter** A. Detta skrivs med följande symboler

$$A \subset B. \tag{1.3}$$

Om A *inte* är en delmängd av B skriver vi

$$A \not\subset B. \tag{1.4}$$

Om $A \subset B$ och $A \neq B$ skriver vi att $A \subsetneq B$.

Följande är några grundläggande egenskaper som notionerna delmängd och likhet innehar.

Proposition 1.6. Låt A, B och C vara godtyckliga mängder. Då gäller följande.

1. **Reflexivitet:** $A = A$.
2. **Symmetri:** Om $A = B$, då är $B = A$.
3. **Transivitet:** Om $A = B$ och $B = C$, då är $A = C$.

Bevis. Vi bevisar transivitet och lämnar de övriga som övningar för läsaren. Anta alltså att $A = B$ och att $B = C$. Låt $a \in A$ vara godtycklig. Eftersom $A = B$ har vi att $a \in B$, och eftersom $B = C$ har vi därpå att $a \in C$. Varje element av A är alltså ett element av C. Låt nu $c \in C$ vara godtycklig. Eftersom $B = C$ har vi att $c \in B$ och eftersom $A = B$ har vi därpå att $c \in A$. Varje element av C är alltså ett element av A. Mängderna A och C innehåller därför samma element, med andra ord har vi att $A = C$. □

Anmärkning 1.7. Notera att vi använde den symmetriska egenskapen hos "=" när vi bevisade transivitet. Övning: när gjorde vi det?

Liknande har vi följande grundläggande regler för delmängder.

Proposition 1.8. Låt A, B och C vara godtyckliga mängder. Då gäller följande.

1. **Reflexivitet:** $A \subset A$.
2. **Anti-symmetri:** Om $A \subset B$ och $B \subset A$, då är $A = B$.
3. **Transivitet:** Om $A \subset B$ och $B \subset C$, då är $A \subset C$.

Bevis. Vi bevisar reflexivitet och lämnar det övriga till läsaren. För varje $a \in A$ har vi att $a \in A$. Per definition har vi därför att $A \subset A$. □

Övning 1.9. Vi har noterat att $A \subset A$ för varje mängd A. Har vi någonsin att $A \in A$? Notera först att frågan är väldefinierad. (Se nästa sektion för mer.)

1.2 Konstruktion av mängder - Axiom of specification

Definition 1.10. AXIOM OF SPECIFICATION
För varje mängd A och för varje egenskap $P(-)$ finns det en (unik) mängd B med egenskapen att, $x \in B$ om och endast om $x \in A$ och $P(x)$ är sant.

Vi använder följande notation för denna mängd:

$$B = \{a \in A : P(a)\}. \tag{1.1}$$

Proposition 1.11. "nothing contains everything"
För varje mängd A finns det en mängd B så att $B \notin A$.

Bevis. För varje mängd x låt $P(x)$ vara påståendet $x \notin x$. Enligt Axiom of Specification finns därför mängden

$$B \coloneqq \{a \in A : a \notin a\}. \tag{1.2}$$

Vi påstår att $B \notin A$. För en motsägelse, anta motsatsen. Anta alltså att $B \in A$. Vi har nu två fall: antingen (i) är $P(B)$ sant, eller (ii) så är $P(B)$ falsk. Om $P(B)$ är sann, då är $B \notin B$, per definition av $P(-)$. Eftersom $B \in A$ har vi per definition av B att $B \in B$, alltså är $P(B)$ falsk. Motsägelse. Om $P(B)$ är falsk, då är $B \in B$, per definition av $P(-)$. Per definition av B måste vi därför ha att $P(B)$ är sann. Motsägelse.

Antagandet att $B \in A$ leder alltså till en motsägelse, varpå dess negation måste vara sann. Vi ser därför att $B \notin A$. □

Låt oss nu för tydlighetens skull postulera ett antagande om existens. Vi kommer senare se ett starkare antagande om existens varpå detta axiom blir överflödigt.

Definition 1.12. AXIOM OF EXISTENCE
Det finns en mängd.

Vi visar nu att det finns en mängd utan några element.

Proposition 1.13. Det finns en mängd, betecknad $\emptyset$, med egenskapen att för varje mängd t har vi att $t \notin \emptyset$.

Bevis. Enligt Axiom of Existence finns det en mängd, X. Enligt Axiom of Specification kan vi därför skapa mängden

$$\emptyset \coloneqq \{x \in X : x \notin X\}. \tag{1.3}$$

Låt t vara en godtycklig mängd. Om $t \in \emptyset$ då är $t \in X$ och $t \notin X$, vilket är en motsägelse. Alltså är $t \notin \emptyset$. □

1.3 Par - Axiom of Unordered Pairs

För alla mängder a, b finns det en (unik) mängd C så att för varje mängd x har vi att x ligger i C om och endast om $x = a$ eller $x = b$

Notation 1.14.

$$C \coloneqq \{a, b\} = \{b, a\} \tag{1.1}$$

Anmärkning 1.15. Axiomet för oordnade par säger att för vilka två mängder som helst, finns det en mängd som har båda mängderna som element (och ingenting annat). Detta betyder inte att mängderna och elementen är olika, mängderna kallas för element när de är i relation till ett objekt.

Anmärkning 1.16. En svagare version av axiomet är att, för alla mängder a, b finns det en mängd C så att a, b ligger i C. Detta kan även skrivas

$$\forall a, b \, \exists C : a, b \ \in C$$

Anmärkning 1.17. Skillnaden mellan den starkare och svagare versionen av axiomet är att den starkare versionen antyder den svagare, alltså ställer den få villkorliga krav och är mer tillämplig än den svagare.

Proposition 1.18. Axiomet för oordnade par går att bilda med hjälp av den svagare versionen av axiomet och axiom of specification.

Bevis. Anta att C' har egenskaperna

$$x \in C \iff x = a \textit{ eller } x = b \tag{1.2}$$

Enligt axiom of specification, finns mängden

$$B \coloneqq \{x \in C | x = a \textit{ eller } x = b\} \tag{1.3}$$

Vi har att $a \in B$ eftersom $a \in C$ och $a = a$
Vi har att $b \in B$ eftersom $b \in C$ och $b = b$
För en motsägelse, om $x \in B$ då gäller att $x \in C$ och $x \in a$ eller $x \in b$ □

Definition 1.19. SINGELTON
En singelton är en x så att, (i) $x \neq \emptyset$, och att (ii) för alla x, y i x behöver $x = y$.

Notation 1.20. Om $a \in x$ och x är en singelton, skriver vi $\{a\} \coloneqq x$. Med detta menas att a är en mängd som kan innehålla flera element, medan x är en singelton med endast a som element.

Notation 1.21. En mängd som definieras som att ha samma element två gånger (eller fler), är identisk med en mängd med den elementen endast en gång. Därför kan vi skriva

$$\{a\} \coloneqq \{a, a\} \tag{1.4}$$

Definition 1.22. ORDNADE PAR
Låt a, b vara mängder. Det ordnade paret av a, b är följande mängd:

$$(a, b) \coloneqq \{\{a\}, \{a, b\}\} \tag{1.5}$$

Detta är även lika med $\{\{a\}, \{b, a\}\}$, som i sin tur är lika med $\{\{b, a\}, \{a\}\}$.

Anmärkning 1.23. Enligt matematiken är mängder egentligen oordnade, $\{a, b\} = \{b, a\}$, dock finns det tillfällen där en bestämmelse av ordning behövs. Detta leder till att $(a, b) \neq (b, a)$, pågrund av att $\{\{a\}, \{a, b\}\}$ inte är detsamma som $\{\{b\}, \{a, b\}\}$.

Lemma 1.24. Låt a, b vara mängder. Vi har att (a, b) är en singelton om och endast om $a = b$.

Sats 1.25. Låt a, b vara mängder. Vi har att $(a, b) = (x, y)$ om och endast om $a = x$ och $b = y$.

Bevis. ($\Longleftarrow$): $(A = B) \Longrightarrow P(A) \equiv P(B))$ □

Bevis. ($\Longrightarrow$): Anta att $(a, b) = (x, y)$. Detta leder till att vi får två fall:
Fall 1) Anta att $a = b$, då är a, b en singelton enligt lemma 1.24. Vidare, om $(a, b) = (x, y)$, är x, y också en singelton, och $x = y$. Eftersom $\{x\}$ ligger i $\{\{x\}, \{x, y\}\} = (x, y)$ och $\{a\}$ ligger i (a, b), måste vi därför ha att $\{x\} = \{x\}$. Vilket visar att $x = a = y = b$.

Fall 2) Anta att $a \neq b$, då är $\{a, b\}$ inte en singelton. Detta innebär att det ordnade paret $(a, b) = \{\{a\}, \{a, b\}\}$ endast innehåller exakt en singelton. Detsamma gäller $(x, y) = (a, b)$. Eftersom $\{x\}$ är en singelton innebär det att $\{x, y\}$ inte är en singelton, vilket visar att $\{x\} = \{a\}$. Då det är en unik singelton i $(x, y) = (a, b)$, följer därav $\{a, b\} = \{x, y\}$. □

1.4 Sammansättning - Axiom of Union

För varje mängd $\mathcal{C}$ finns det en (unik) mängd u, så att för varje mängd x har vi att x ligger i u om och endast om det finns ett X i C så att x ligger i X.

Notation 1.26. Mängden av u betecknas som $\bigcup_{x \in \mathcal{C}} X$ och kallas för "Union av samlingen $\mathcal{C}$"

Exempel 1.27. Det finns ett x i unionen av A och B ($A \bigcup B$), om och endast om x ligger i A eller x ligger i B.

Anmärkning 1.28. Anta en mängd som är en kollektion av mängder, då skapar vi en ny mängd vars element är de element som ligger i någon av de mängderna i kollektionen. Alltså om x är en mängd, så är $\bigcup x$ också en mängd, och om A och B är mängder, då är $A \bigcup B$ också en mängd som innehåller alla de element som A och B innehåller.

Sats 1.29. För varge ike-tom mängd C finns det en (unik) mängd Z, så att för varge mängd x gäller att

$$x \in Z$$

så att, för alla$x \in \mathcal{C}, x \in X$.(1.1)

Notation 1.30. Mängden Z ovan beteknas

$$\bigcap_{x \in \mathcal{X}} X. \tag{1.2}$$

Bevis. Övnig. □

Notation 1.31. För mängder A,B,C skrivs

$$A \bigcap B \coloneqq \bigcap_{x \in \{A,B\}} X. \tag{1.3}$$

1. $\bigcap_{x \in \emptyset} X$ är inte definerad.
2. "Interaction över $\emptyset$"kan defineras om vi fixserar en mängd E och endast kollar på e som består av delmängden till E.

Övning 1.32. hur?

Övning 1.33. A, B, C är tre mängder

1. $A \bigcap (C \bigcup C) = (A \bigcap B) \bigcup (A \bigcap C)$.
2. $A \bigcup (B \bigcap C) = (A \bigcup B) \bigcap (A \bigcup)$.
3. $A \bigcup (A \bigcap B) = A$.
4. $A \bigcap (A \bigcup B) = A$.

Övning 1.34. Def differens

$$x \in E$$

så att, för varge x,

$$x \in A, x \notin B \tag{1.4}$$

Definition 1.35. Difference

A, B är mängder. Genom att använda Axiom of spesificatin, får vi att för alla X (mängd) och för alla P (påstående) är

$$Y \coloneqq \{x \in A | P(x)\} \tag{1.5}$$

$$E = \{x \in A | x \notin B\}. \tag{1.6}$$

Notation 1.36. $E \coloneqq A \backslash B$

Definition 1.37. Om vi fixserar en mängd u och en mängd A är en del mängd av u. Då kallar vi $u \backslash A = \{X \in u | x \notin A\}$ och beteknas A^c.

Övning 1.38. Vi har att $A, B, u.\ A, B \subseteq u$. Bevisa följande:

1. $\emptyset^c = u, u^c = \emptyset$.
2. $(\mathrm{A}^c)^c = A$.
3. $\mathrm{A} \bigcap A^c = \emptyset$.
4. $\mathrm{A} \bigcup A^c = u$.
5. $\mathrm{A} \subseteq B \iff B^c \subseteq A^c$.
6. $(\mathrm{A} \bigcup B)^c = A^c \bigcap B^c$.

1.5 Potens - Axiom of Powerset

För varge mängd A fins det en (unik) mängd p, så för varje mängd x har vi att

$$X \in P \iff X \subseteq A. \tag{1.1}$$

Notation 1.39. Beteknet $p(A)$ kallas potens mängden av A, bevisa följaen påståenden

Exempel 1.40.

1. $p(\emptyset) = \{\emptyset \text{ för alla}, \emptyset \in p(A), A \in p(A)\}$
2. $P(\{a\}) = \{\emptyset, \{a\}\}$
3. $P(\{a, b\}) = \{\emptyset, \{a, b\}, \{a\}, \{b\}\}$

om x $\subset \{a\}$då för varge$x \in X : x \in \{a\}$
$\iff$ x=a

$\iff$ Fall 1.) x=$\emptyset$
Fall 2.)a) x inte likamed $\emptyset, b$)För varge$x, y \in X, x = a$

Övning 1.41. Låt u vara en mängd, vi har att

1. $\bigcup X = x \in p(A)$.
2. $\bigcap X = x \in P(A)$.

Bevis. 1.

$$\bigcap_{x \in \mathcal{P}(A)} X = A \tag{1.2}$$

Låt $x \in A$ Vara godtyklig. **Det finns ett ellement** x i $p(A)$ så att $x \in A$, nämligen x = A. Per defenition AV unionen har vi derför att

$$x \in \bigcap_{x \in \mathcal{P}(A)} X = A. \tag{1.3}$$

Vi gör det omvänt. Låt $x \in \bigcup X$ vara godtyckligt per definition av unionen, det finns en mängd $x \in p(A)$ så att $x \in X$. Sedan per defenition av $p(A)$ har vi att $x \subseteq A$. Slutligen per defenition av delmängden gör att vi har vi att $x \in A$. □

Övning 1.42. Bevisa: $\bigcap_{x \in \mathcal{P}(A)} X = \emptyset$.

Övning 1.43. BBevisa att: För varge A och B, gäller ett $A \subseteq B$ går mot $p(A) \subseteq p(B)$

1.6 Direkt produkter

Sats 1.44. Låt A och B vara mängder. Det finns en unik mängd D så att för varje mängd X har vi att $X \in D$ om och endast om det finns ett $a \in A$ och ett $b \in B$ så att $X = (a, b)$.

Bevis. Genom Axiom of Union har vi att mängden $A \cup B$ finns. Från Axiom of Powerset har vi att $\mathcal{P}(A \cup B)$ och $\mathcal{PP}(A \cup B)$ finns. Vi har att $\{a\} \in \mathcal{P}(A \cup B)$, och liknande att $\{a, b\} \in \mathcal{P}(A \cup B)$. Därav följer det att $(a, b) = \{\{a\}, \{a, b\}\} \subset \mathcal{P}(A \cup B)$. Vilket säger att $(a, b) \in \mathcal{PP}(A \cup B)$, per Axiom of Powerset. Genom Axiom of Specification finns mängden D, definierat som

$$D = \{x \in \mathcal{PP}(A \cup B) \mid \exists a \in A, \exists b \in B : x = (a, b)\} \tag{1.1}$$

Med definitionen av D är satsen bevisad. □

Notation 1.45. Mängden D beteckas $A \times B$ och kallas för direkt produkten av mängderna A och B.

2 Funktioner

Definition 2.1. En **funktion** f är en triplett bestående av en definitionsmängd/ domän, X, en målmängd/ kodomän Y, och en graf Γ_f, dvs. $f \coloneqq (X, Y, \Gamma_f)$. För mängden $\Gamma_f \subset (X \times Y)$ gäller det att

$$\forall x \in X \ \exists! y \in Y : (x, y) \in \Gamma_f$$

Notation 2.2. funktioner

1. $\forall x \in X \ \exists! y \in Y : (x, y) \in \Gamma_f$ betecknas $f(x) = y$, kallas bilden av x under y
2. $f \coloneqq (X, Y, \Gamma_f)$ betecknas ofta som $f : X \to Y$. Man säger att f är en funktion/ map från X till Y
3. Om mängderna X och Y är underförstådda kan vi beteckna funktionen endast genom f
4. $f(x) = y$ kan även skrivas som $f : x \mapsto y$, som säger att f skickar x till y.

2.1 Likhet - Funktioner

Definition 2.3. LIKHET
Två funktioner $f \coloneqq (X, Y, \Gamma_f)$ och $f' \coloneqq (X', Y', \Gamma_{f'})$ är lika med varandra då om och endast om deras domän är lika ($X = X'$), deras kodomän är lika ($Y = Y'$) och deras graf är lika ($\Gamma_f = \Gamma_{f'}$).

Anmärkning 2.4. Notera att $(\Gamma_f = \Gamma_{f'}) \iff \forall x \in X, \ (x, f(x)) = (x, f'(x)) \iff \forall x \in X, \ f(x) = f'(x)$

Exempel 2.5. Exempel på funktioner

För varje mängd X är **identitetsfunktionen** av mängden den funktion som mappar alla element från X till samma element i X, dvs.

$$\begin{aligned} id_X :& X \to X \\ & x \mapsto x \end{aligned}$$

Låt $X = \{\emptyset\}$, mängden $Y = \{\emptyset, \{\emptyset\}\}$ och mängden $\Gamma_f = \{(\emptyset, \{\emptyset\})\} \subset (X \times Y)$. Då gäller det att en av funktionerna $f = (X, Y, \Gamma_f)$ från X till Y är

$$\begin{aligned} f :& X \to Y \\ & \emptyset \mapsto \{\emptyset\} \end{aligned}$$

Övning 2.6. Hur många funktioner finns det från $Y \to X$?

2.2 Komposition av Funktioner

Definition 2.7. KOMPOSITION AV TVÅ FUNKTIONER
Låt $f : X \to Y$ och $g : Y \to Z$ vara funktioner så att kodomän till f är domän till g. Då är kompositionen av f följt med g funktionen:

$$\begin{aligned} g \circ f :& X \to Z \\ & x \mapsto g(f(x)) \end{aligned}$$

Sats 2.8. Låt $f : X \to Y$ vara en funktion. Då har vi att

$$id_Y \circ f = f = f \circ id_X \tag{2.1}$$

Bevis. Övning □

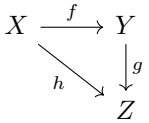
Anmärkning 2.9. Mängden av alla funktioner/ grafer av $f : X \to Y$ betecknas Y^X. Det gäller att $Y^X \subset \mathcal{P}(X \times Y)$.

Övning 2.10. skriv Y^X formellt

Övning 2.11. Låt mängden $X = \{\emptyset, \{\emptyset\}\}$ och $Y = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$

1. beskriv alla funktioner från X till Y
2. om $g : X \to Y$ betecknar funktionen $\emptyset \mapsto \{\emptyset\}$, $\{\emptyset\} \mapsto \emptyset$. Beskriv en funktion $\Psi : Y^X \to Y^X$ med hjälp av g.
3. FÖRLÄNGNING: beskriv två funktioner $X^X \to X^X$ med hjälp av g.

Definition 2.12. KOMMUTATIVA DIAGRAM
Låt $f : X \to Y$, $g : Y \to Z$ och $h : X \to Z$ vara funktioner. Då säger vi att diagrammet



kommuterar om och endast om $g \circ f = h$

Övning 2.13. Beskriv påståendet i Sats 2.8 med hjälp av kommutativa diagram

Sats 2.14. Associativitet hos Komposition
Låt $f : X \to Y$, $g : Y \to Z$ och $h : Z \to W$ vara funktioner. Vi har

$$h \circ (g \circ f) = (h \circ g) \circ f \tag{2.2}$$

som funktion från X till W

Bevis. Övning □

Övning 2.15. Beskriv Sats 2.14 med hjälp av kommutativa diagram

2.3 Bijektioner

Notation 2.17. g kallas för inversen till f och betecknas f^{-1}.

Sats 2.18. Om $f : X \to Y$ är inverterbar, då är inversen unik.

Bevis. Låt $f : X \to Y$ vara en inverterbar funktion. Per definition av finns det en funktion $g : Y \to X$ så att $f \circ g = id_X : X \to Y$ och $g \circ f = id_Y : Y \to Y$ gäller att

$$\text{för alla } y \in \ Y, g(y) = g(y'). \tag{2.1}$$

Från $g \circ f = id_Y : Y \to Y$ för g' har vi att

$$\begin{aligned} g(y) &= g((f \circ g')(y)) \\ &= g \circ (f \circ g')(y) && \text{(per definition av komposition)} \\ &= ((g \circ f) \circ g')(y) && \text{(komposition är associativ)} \\ &= (id_X \circ g')(y) && \text{(g uppfyller...)} \\ &= g'(y). && \text{(per definition av } id_X\text{)} \end{aligned} \tag{2.2}$$

□

Definition 2.19. BIJEKTIONER
1.) Låt $f : X \to Y$ vara en funktion. Vi säger att f är injektiv om

$$\text{för alla } x, x' \in X f(x) = f(x') \text{ vilket implicerar } x = x' \tag{2.3}$$

$$\equiv \text{ för alla } x, x' \in X, x \neq x' \implies f(x) \neq f(x'). \tag{2.4}$$

2.) Vi säger att f är surjektiv om

$$\text{för alla } y \in Y \text{ finns det ett } x \in X \text{ så att } f(x) = y \text{ vilket innebär att } (x, y) \in \Gamma_f. \tag{2.5}$$

3.) Vi säger att f är bijektiv om f är både injektiv och surjektiv, alltså

$$\text{för alla } y \in Y, \text{ finns det ett unikt } x \in X \text{ så att } f(x) = y \tag{2.6}$$

Exempel 2.20. dfg

1.
$$X = \{\emptyset\}, Y = \{\emptyset\}, \{\emptyset\} \tag{2.7}$$
$$f : X \mapsto Y \tag{2.8}$$

2.
$$g : Y \mapsto X, \emptyset \mapsto \emptyset, \emptyset \mapsto \emptyset \tag{2.9}$$

3.
$$X = \emptyset, \emptyset Y = \emptyset, \emptyset f : X \mapsto Y, \emptyset \mapsto \emptyset, \emptyset \mapsto \emptyset \tag{2.10}$$

Anmärkning 2.21. Notera i 3.) $X \nsubseteq Y$ men det finns en bijektion $f : X \to Y$. Bijektivitet är en svagare form av likhet".

Sats 2.22. En funktion $f : X \to Y$ är inverterbar om och endast om den är bijektiv.

Bevis. Övning □

Definition 2.23. BILDER
Låt $f : X \to Y$ vara en funktion, låt $A \subset X$ vara en delmängd av X. **Bilden** av A under f är delmängden $f(A) \subset Y$ given av

$$f(A) = y \in Y | x \in A : f(A) = y \tag{2.11}$$

Bilden av x under f kallas för bilden av f

Övning 2.24. Karaktärisera Surjektivitet genom bilder.
f är surjektiv om och endast om $f(X) = Y$

Bevis. Övning □

Exempel 2.25.
$$X = \{\emptyset\}, Y = \{\emptyset, \{\emptyset\}\}, f : X \to Y \emptyset \mapsto \{\emptyset\} \tag{2.12}$$

$$f(x) = y \in Y | \exists x \in X : f(x) = y = \emptyset \tag{2.13}$$

Definition 2.26. URBILDER
Låt $f : X \to Y$ vara en funktion, låt $c \subset Y$ vara en delmängd av Y. **Urbilden** av c under f är delmängden $f^{-1}(c) \subset X$ av X given av

$$f^{-1}(c) = x \in X | f(x) \in c \tag{2.14}$$

När $c = y$ är en singleton, då skriver vi också $f^{-1}(y)$ istället för $f^{-1}(y)$.

Anmärkning 2.27. Viss konflikt med notation f^{-1} som notation för inversen (när den finns).
1) f^{-1} finns endast när f är inverterbar.
2) $f^{-1}(c)$ är alltid definierad (För alla f, för alla c i Y)
3) f är inverterbar då $f^{-1}(y) = f^{-1}(y)$

Sats 2.28. Låt $f : X \to Y$ vara en funktion. Låt $\mathcal{A} \subset \mathcal{P}(X)$ vara en samling av delmängder av X och låt $\mathcal{C} \subset \mathcal{P}(Y)$ vara en samling av delmängder av Y. Vi har att:

$$1.a) f^{-}1(\bigcup_{v \in \mathcal{C}} v) = \bigcup_{v \in \mathcal{C}} f^{-}1(v) \tag{2.15}$$

Man säger att $f^{-}1$ respektera unionen.

$$1.b) f^{-}1(\bigcap_{v \in \mathcal{C}} v) = \bigcap_{v \in \mathcal{C}} f^{-}1(v) \tag{2.16}$$

$$2.a) f(\bigcup_{A \in \mathcal{A}} A) = \bigcup_{A \in \mathcal{A}} f(A) \tag{2.17}$$

$$2.b) f(\bigcap_{A \in \mathcal{A}} A) \subset \bigcap_{A \in \mathcal{A}} f(A) \tag{2.18}$$

Bevis. 1. a) För alla $x \in X$ har vi att

$$x \in f^{-}1(\bigcup_{v \in \mathcal{C}} v) \iff f(x) \in \bigcup_{v \in \mathcal{C}} v \tag{2.19}$$

enligt definition av urbild.

$$\iff \exists v : f(x) \in v \tag{2.20}$$

Enligt definition av union.

$$\iff \exists v : x \in f^{-}1(v) \tag{2.21}$$

Enligt definition av urbild.

$$\iff x \in \bigcup_{v \in \mathcal{C}} f^{-}1(v) \tag{2.22}$$

Enligt definition av union. □

Bevis. Övning. □

Övning 2.29. Ge exempel på en funktion $f : X \to Y$ och två delmängder $A, B \subset X$ så att

$$f(A \bigcap B) \neq f(A) \bigcap f(B) \tag{2.23}$$

En lösning: $X = \{\emptyset, \{\emptyset\}\}$, $Y = \{\emptyset\}$ $f : X \to Y$, $\emptyset, \{\emptyset\} \mapsto \emptyset$
$A = \{\emptyset\}$, $B = \{\{\emptyset\}\}$
$A \bigcap B = \emptyset$ så $f(A \bigcap b) = f(\emptyset) = \{y \in Y | \exists x \in \emptyset : f(x) = y\} = \emptyset$ men $f(A \bigcap b) = f(\emptyset) = \{y \in Y | \exists x \in \emptyset : f(x) = y\} = \emptyset$ ... $= f(B) \implies f(A) \bigcap f(B) = \{\emptyset\} \bigcap \{\emptyset\} = \{\emptyset\} \neq \emptyset$

Övning 2.30. Låt $f : X \to Y$ vara en funktion och låt $v \subset Y$ vara en delmängd av Y. Vi har att

$$f^{-}1(Y\ v) = x\ f^{-}1(v) \tag{2.24}$$

Övning 2.31. Låt $f : X \to Y$ vara en funktion. I termer av urbilder, singletons och den tomma mängden, beskriv vad det innebär att f är
1) injektiv 2) surjektiv 3) bijektiv

Övning 2.32. Låt Y vara en mängd. Det finns en unik funktion från $\emptyset$ till y. ("universal property of $\emptyset$")

Övning 2.33. Låt S vara en singletom och låt X vara en mängd. Det finns en unik funktion från X till S. ("Universal property of singletons")

Övning 2.34. Låt S och S' vara singletons. Det finns en unik bijektion mellan dem. (Använd universal property of singletons)

3 Naturliga talen

Definition 3.1. AXIOM OF INFINITY
Det finns en mängd X_0 så att
1. $\emptyset \in X_0$
2. $\forall x \in X_0, \{x\} \in X_0$

Definition 3.2. INDUKTION
En mängd A är **induktiv** om
1. $\emptyset \in A$
2. $\forall a \in A, \{a\} \in A$

Lemma 3.3. För varje samling $\mathcal{C} \neq \emptyset$ av induktiva mängder ($\forall C \in \mathcal{C}, C$ är induktiv) har vi att $\bigcap_{C \in \mathcal{C}} C$ är induktiv.

Bevis. Låt $\mathcal{C}$ vara en godtycklig samling av induktiva mängder. Vi har att $\emptyset \in C$ för varje C i $\mathcal{C}$. Per definition av $\bigcap_{C \in \mathcal{C}} C$ har vi därför att $\emptyset \in \bigcap_{C \in \mathcal{C}} C$. Låt $x \in \bigcap_{C \in \mathcal{C}} C$. Vi har då att:

$$\begin{aligned} & \forall C \in \mathcal{C}, x \in C && \text{(per definition av } \textstyle\bigcap\text{)} \\ \implies & \forall C \in \mathcal{C}, \{x\} \in C && (\forall C \in \mathcal{C}, C \text{ induktivt}) \\ \implies & \{x\} \in \bigcap_{C \in \mathcal{C}} C. && \text{(per definition av } \textstyle\bigcap\text{)} \end{aligned}$$

Per definition är därför $\bigcap_{C \in \mathcal{C}} C$ induktiv. □

Definition 3.4. NATURLIGA TALEN
Låt X_0 vara en induktiv mängd (existerar genom Axiom of Infinity). Vi definierar (mängden av) de **naturliga talen** som $\mathbb{N} := \bigcap_{C \in \mathcal{C}_0} C$, där $\mathcal{C}_0 := \{X \subseteq X_0 \mid X \text{ är induktiv}\}$

Anmärkning 3.5. $\mathbb{N}$ är induktiv från lemma 3.3.

Lemma 3.6. De naturliga talen är den unika mängd som är en delmängd av varje induktiv mängd.

Bevis. Anta att A är en induktiv mängd. Från lemma 3.3 har vi då att $A \bigcap X_0$ är induktiv. Eftersom $A \bigcap X_0 \subseteq X_0$ har vi att $A \bigcap X_0 \in \mathcal{C}_0$. Därav följer att $\mathbb{N} = \bigcap_{C \in \mathcal{C}_0} C \subseteq A \bigcap X_0 \subseteq A$ (följt från definitionen av $\bigcap$). Anta att $\mathbb{N}'$ är en induktiv mängd som är en delmängd av varje induktiv mängd. Vi har då att

1. $\mathbb{N} \subseteq \mathbb{N}'$ ($\mathbb{N} \subseteq A$ för alla induktiva mängder A, och $\mathbb{N}'$ är induktiv)
2. $\mathbb{N}' \subseteq \mathbb{N}$ ($\mathbb{N}' \subseteq A$ för alla induktiva mängder A, och $\mathbb{N}$ är induktiv)

Alltså har vi att $\mathbb{N} = \mathbb{N}'$. □

Definition 3.7. 1. Ett **naturligt tal** är ett element i $\mathbb{N}$.
2. Vi skriver $0 \coloneqq \emptyset \in \mathbb{N}$.
3. Låt $S : \mathbb{N} \to \mathbb{N}$ beteckna funktionen $n \mapsto \{n\}$ (senare $S(n) =: n + 1$).

Sats 3.8. Vi har att:
1. $0 \notin S(\mathbb{N})$
2. S är injektiv.
3. För varje delmängd $M \subseteq \mathbb{N}$ så att
   i. $0 \in M$
   ii. $\forall m \in \mathbb{N}, m \in M \implies S(m) \in M$

   har vi att $M = \mathbb{N}$.

Anmärkning 3.9. 1.2.3. kallas för Peanoaxiomen. 3. kallas för Principen om Matematisk Induktion.

Bevis. 1. $\forall n \in S(\mathbb{N}) \exists m \in \mathbb{N} : S(m) = n$ (per definition av $S(\mathbb{N})$) $\implies \{m\} = n$ (per definition av S). Eftersom $0 = \emptyset \neq m$ för varje $m \in \mathbb{N}$ ser vi att $0 \notin S(\mathbb{N})$.

2. Anta att $n, m \in \mathbb{N}$ så att $S(n) = S(m)$. Per definition av S har vi att $\{n\} = S(n) = S(m) = \{m\} \implies n = m$ (per definition av singeltons).

3. $M \subseteq \mathbb{N}$ per definition $\mathbb{N} \subseteq M$ eftersom i), ii) innebär att M är induktiv och $\mathbb{N}$ är en delmängd av varje induktiv mängd.

□

Sats 3.10. För varje triplett, (X, a, f), där X är en mängd, $a \in X$ och $f : X \to X$, finns det en unik funktion $\varphi : \mathbb{N} \to X$ så att:

1. $\varphi(0) = a$
2. $f \circ \varphi = \varphi \circ S : \mathbb{N} \to X$

I diagram: finns det inte φ så att $\varphi(0) = a$ och följande diagram kommenterar:

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{e} & X \\ \downarrow{\scriptstyle S} & & \downarrow{\scriptstyle f} \\ \mathbb{N} & \xrightarrow{\varphi} & X \end{array}$$

Anmärkning 3.11. Rekursionssatsen tillåter oss att definera saker "rekursivt"

Exempel 3.12. Ex. Definera $(a_n)_n$, genom $a_0 = 2$, $a_{n+1} = 3 + 4a_n$ för varje $n \geq 1$

Den finns tack vare rekursionssatsen applicerad på $(\mathbb{R}, 2, x \mapsto 3 + 4x)$

Bevis. Övning □

Sats 3.13. (mat.Ind): För varje $n \in \mathbb{N}$ låt P(n) vara ett påstående. För att bevisa att P(n) är sant för varje $n \in \mathbb{N}$ räcker det med att bevisa att:

1. P(0) sant
2. För varje $n \in \mathbb{N}$, P$(n)_{sant} \Rightarrow P(S(\text{n}))_{sant}$

Bevis. Definiera $M = \{n \in \mathbb{N} : P(n) \text{ är sant}\}$

1. $0 \in M$
2. Har vi att för varje $n \in \mathbb{N}$, $n \in M \Rightarrow S(n) \in M$
3. Enligt Peanoaxiom följer att $M = \mathbb{N}$, alltså är P(n) sant för alla $n \in \mathbb{N}$

□

3.1 Addition

Vi använder Rekursionssatsen för att definiera addition och induktion för att bevisa hur addition fungerar.

Definition 3.14. För varje $a \in \mathbb{N}$ enligt Rekursionssatsen applicerad på (N, a, S) finns det en unik funktion φ_a^+:$\mathbb{N} \to \mathbb{N}$ så att:

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\varphi_a^\times} & \mathbb{N} \\ \downarrow S & & \downarrow S \\ \mathbb{N} & \xrightarrow{\varphi_a^\times} & \mathbb{N} \end{array}$$

Alltså: För varje $n \in \mathbb{N}$, $S(\varphi_a^+(n)) = \varphi_a^+(S(n))$ Vi skriver att för varje $b \in \mathbb{N}$, $a + b :=\varphi_a^+(\text{b})$

Definition 3.15. Addition (sfunktionen) på $\mathbb{N}$ är funktionen

$\mathbb{N} \times \mathbb{N} \to \mathbb{N}$
$(a, b) \mapsto$a,b:= φ_a^+(b)

Sats 3.16. För varje $a, b, c \in \mathbb{N}$ har vi att:

1. $0 + a = a = a + 0$ (0 är identiteten för addition)
2. $(a + b) + c = a + (b + c)$ (addition är associativ)
3. $a + b = b + a$ (addition är kommutativ)

Bevis. : i) Fall $a = 0$: vi har att $0 + 0 = \varphi_0^+(0) = 0$

Anta att $n \in$N och att $0 + n = 0 = n + 0$ (induktionsantagande)

WTS: $0 + S(n) = S(n) = S(n) + 0$

$M = \{n \in \mathbb{N} : P(n)\} \subseteq \mathbb{N}$

i) $0 \in M$

ii) För alla $n \in \mathbb{N}$, $n \in M \Rightarrow S(a) \in M \Rightarrow m = M$ □

Anmärkning 3.17. $a = \varphi_a^+(0) =: a + 0$

För varje $b \in \mathbb{N}$,

$a + S(b) = \varphi_a^+(S(b))$ (def av at) $= S(\varphi_a^+(b)$ (rekursionssatsen) $= S(a + b)$ (def. av at)

Vi har att $0 + S(n) = \varphi_0^+(S(n))$ (Def. av OT)

$= S(\varphi_0^+(n)$ (rek. satsen)

$= S(0 + n)$ (def. av OT)

$= S(n)$ (induktionsantagande)

$= S(n) + 0$ (def. av $S(n)t$)

Övning 3.18.

ii) Övning:

iii) Först: induktion på b att $S(a) + b = S(a + b)$

Fall 1: Om $b = 0$ har vi att $S(a) + 0 = S(a) = S(a + 0)$

Anta: $b \in \mathbb{N}$ och $S(a) + b = S(a + b)$

WTS: $S(a) + S(b) = S(a + S(b))$

Vi har att $S(a) + S(b) = S(S(a) + b)$ (från anmärkning 3.17.)

$=(S(S(a + b)$ (induktionsantagandet)

$= S(a + S(b))$ (från anmärkning 3.17.)

Bevis. Enligt principen om matematisk induktion har vi att

$S(a) + b = S(a + b)$ för varje $a, b \in \mathbb{N}$

Vi bevisar nu att $a + b = b + a$ för varje $a, b \in \mathbb{N}$

Låt $a \in \mathbb{N}$ vara godtycklig. Vi gör induktion på b.

Fall 1: $b = 0$ då följer påståendet från i).

Anta att $b \in \mathbb{N}$, $a + b = b + a$ (induktionsantagande)

WTS: $a + S(b) = S(b) + a$

Vi har att $a+S(b)$ (från anmärkning 3.17.) $= S(a+b)$ (induktionsantagandet)$= S(b+a)$ (föregående resultat med ombytta roller på a och b) $= S(b) + a$

Enligt principen om matematisk induktion har vi att $a + b = b + a$ för varje $a, b \in \mathbb{N}$

□

Sats 3.19. För alla naturliga tal $a, b, c \in \mathbb{N}$ har vi att

$$a + c = b + c \text{ implicerar att } a = b.$$

Bevis. Låt $P(c)$ vara påståendet att satsen ovan är sant för alla $a, b \in \mathbb{N}$ samt ett specifikt $c \in \mathbb{N}$. Vi bevisar att $P(c)$ är sant för alla $c \in \mathbb{N}$ med hjälp av principen om matematisk induktion. Om $c = 0$ är $P(c)$ påståendet att

$$a + 0 = b + 0 \text{ implicerar att } a = b.$$

Detta stämmer eftersom $a + 0 = \varphi_a^+(0) = a$ och $b + 0 = \varphi_b^+(0) = b$ per definition.
Anta nu att $c \in \mathbb{N}$ och att $P(c)$ är sant. Vi visar nu att $P(S(c))$ är sant. Alltså att

$$a + S(c) = b + S(c) \text{ implicerar att } a = b.$$

Anta nu att $a + S(c) = b + S(c)$. Eftersom $a + S(c) = S(a + c)$ och $b + S(c) = S(b + c)$ har vi att

$$S(a + c) = a + S(c) = b + S(c) = S(b + c),$$

alltså att $S(a + c) = S(b + c)$. Eftersom S är injektiv innebär det att $a + b = a + c$. Eftersom $P(c)$ är sant får vi att $a = b$. Enligt principen om matematisk induktion ser vi att påståendet $P(c)$ är sant för alla $c \in \mathbb{N}$, alltså att $a + c = b + c$ implicerar att $a = b$ för alla $a, b, c \in \mathbb{N}$. □

Notation 3.20.

$$1 \coloneqq S(0) \in \mathbb{N}$$

Sats 3.21 (Följdsats)**.** För alla $n \in \mathbb{N}$ har vi att $S(n) \neq n$

Bevis. Kladd, skriv renare sen. Visa att

1. $1 \neq 0$
2. $S(n) = n + 1$ $\qquad (n + 1 = n + S(0) = S(n + 0) = S(n))$
3. Använd tidigare sats för att visa att

   $$S(n) = n \implies n + 1 = n + 0 \implies 1 = 0$$

   Vilket ger en motsägelse. (Följdsats och kommutivitet av addition)

□

3.2 Multiplikation

Definition 3.22 (Övning)**.** Fixera $a \in \mathbb{N}$. Definiera multiplikation med a.
Tips: Använd Rekursionssatsen: (X, x_0, f)

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\varphi_a^\times} & \mathbb{N} \\ \downarrow{\scriptstyle S} & & \downarrow{\scriptstyle \varphi_a^+} \\ \mathbb{N} & \xrightarrow{\varphi_a^\times} & \mathbb{N} \end{array}$$

$$a \cdot b = ab \coloneqq \varphi_a^\times(b)$$

Definition 3.23. Multiplikation(sfunktionen) på $\mathbb{N}$ är given av

$$\begin{aligned} \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

Sats 3.24 (Övning)**.** För alla $a, b, c \in \mathbb{N}$ har vi att

1. $1 \cdot a = a = a \cdot 1$ (1 är identitet med hänvisning till $\cdot$)
2. $(ab)c = a(bc)$ ($\cdot$ är associativt)
3. $ab = ba$ ($\cdot$ är kommutativt)
4. (i) $a(b + c) = ab + ac$
   (ii) $(a + b)c = ac + bc$ ($\cdot$ är distributiv över $+$)

Lemma 3.25. Vi har att $S(\mathbb{N}) = \mathbb{N}\backslash\{0\}$

Bevis. Peanoaxiomen ger att $0 \notin S(\mathbb{N})$, varpå

$$S(\mathbb{N}) \subseteq \mathbb{N}\backslash\{0\}$$

För att visa att $\mathbb{N}\backslash\{0\} \subseteq S(\mathbb{N})$, låt $P(n)$ för alla $n \in \mathbb{N}$ vara påståendet att

$$n = 0 \text{ eller } n \in S(\mathbb{N}).$$

Vi visar att $P(n)$ är sant för alla $n \in \mathbb{N}$ genom principen om matematisk induktion.
Låt $n = 0$ Per definition är $P(0)$ sant.
Anta nu att $n \in \mathbb{N}$ och att $P(n)$ är sant. Vi vill visa att $P(S(\mathbb{N}))$ är sant, alltså att

$$S(n) = 0 \text{ eller } S(n) \in S(\mathbb{N}).$$

Eftersom

$$S(\mathbb{N}) = \{a \in \mathbb{N} \mid \text{ det finns ett } b \in \mathbb{N} \text{ sådan att } S(b) = a\}$$

har vi att $S(n) \in S(\mathbb{N})$. Alltså är $P(S(n))$ sant. Enligt principen om matematisk induktion har vi att $P(n)$ är sant för alla n i $\mathbb{N}$. Alltså, för alla $n \in \mathbb{N}\backslash\{0\}$ är $n \in S(\mathbb{N})$. Det visar att $\mathbb{N}\backslash\{0\} \subseteq S(\mathbb{N})$ varpå $S(\mathbb{N}) = \mathbb{N}\backslash\{0\}$ □

Sats 3.26. För alla $a, b \in \mathbb{N}$, $ab = 0 \implies a = 0$ eller att $b = 0$

Bevis. (Kom ihåg: $P \implies Q \equiv \neg Q \implies \neg P$) Vi visar att om $a \neq 0$ och $b \neq 0$ har vi att $ab \neq 0$
Anta alltså att $a \neq b$ och $b \neq 0$. Det innebär från Lemma 3.25 att det finns $a', b' \in \mathbb{N}$ så att

$$\begin{aligned} ab &= S(a') \cdot S(b') \\ &= (a' + 1) \cdot (b' + 1) && \text{(definition av } n + 1) \\ &= (a'b' + a' + b') + 1 && \text{(distributivitet av } \cdot \text{ över } + \text{ samt associativitet)} \\ &= S(a'b' + a' + b') && \text{(definition av } n + 1) \\ &\in S(\mathbb{N}) \end{aligned}$$

Eftersom $S(\mathbb{N}) \not\ni 0$ ser vi att $ab \neq 0$ □

4 Relationer

Definition 4.1. Låt X vara en mängd. En binär relation på X är en delmängd, R, av $X \times X$

Notation 4.2. Om x, y ligger i X då skriver vi xRy om och endast om $R = R$ som mängder

Exempel 4.3. Låt R vara lika med den tomma mängden som en delmängd av X kryssprodukt X. Det ger null-relationen på X: För alla x och y så är x relation y alltid falskt

Exempel 4.4. R lika med X kryssprodukt X som är en delmängd av X kryssprodukt X. Det ger den triviala relationen på X: För varje x och y som ingår i X, är x relation y alltid sant.

Exempel 4.5. Låt R vara mängden $\{(x, y)$ som ingår i X kryssprodukt X då x är lika med y $\}$. Det ger likhetsrelationen på X: För alla x och y som ingår i X så gäller $xrelationy$ om och endast om x är lika med y

Exempel 4.6. Låt R vara lika med mängden $\{A, B\}$ som ingår i potensmängden av X, kryssprodukt, potensmängden av X när A är en delmängd av B. Det ger delmängdsrelationen på potensmängden av X: För alla A och B i potensmängden av X, så gäller A relation B om och endast om A är en delmängd av B.

Exempel 4.7. Låt R vara mängden (det ordnade paret A, B som ingår i potensmängden av X krosprodukt protensmängden av X för A bijektiv med B). Det ger kardinalitetsrelationen på potensmängden av X: För alla A och B som ingår i potensmängden av X så gäller A relation B om och endast om A är bijektiv med B

Exempel 4.8. Låt X vara lika med de naturliga talen. Vi säger att a är en delmängd av b om det finns ett c i de naturliga talen för $a + c = b$. Låt R vara mängden det ordnade paret a, b som ingår i de naturliga kryssprodukt de naturliga talen för a är en delmängd av b. Det ger ordningsrelationen på de naturliga talen: För alla a, b som ingår i de naturliga talet gäller a relation b om och endast om a är en delmängd av b.

Exempel 4.9. Låt R vara en relation på X. Negationen av R är relationen: R är mängden det ordnade paret x, y som ingår i kryssprodukten av X och X för det ordnade paret x, y som inte ingår i mängden R

Definition 4.10. Låt X vara en mängd och R en relation på X. Vi säger att:

1. R är reflexiv om och endast om för alla x i X och x R x.
2. R är symmetrisk om och endast om för alla x och y i X och x R y medför det y R x
3. R är transitiv om och endast om för alla x, y och z i X då x R y och y R z så medför det att x R z gäller.
4. R är antisymmmetrisk om och endast om för alla x och y i X, då x R y och y R x gäller, medför det att $x = y$.
5. R är jämförbar om och endast om för alla x och y i X och x R y eller y R x gäller.

Övning 4.11. Gå igenom föregående exempel och säg för varje relation vilka av egenskaperna ovan den har. I olika sammanhang så är olika typer av relationer av intresse. Vi kommer främst behöva en typ av relation kallad ekvivalensrelation.

5 Ekvivalenstalen

Definition 5.1. En relation R på X är en ekvivalensrelation om R är reflexiv, symmetrisk och transitiv.

Exempel 5.2. Kardinalitetsrelationen på $\mathcal{P}$ är en ekvivalensrelation.

Anmärkning 5.3. Vi skriver ofta $\sim$ efter $\sim_R$ istället för R och $x \sim y$ eller $x \sim_R y$ istället för x R y

Definition 5.4. Låt X och S vara mängder och låt $f : X \to S$ vara en funktion från $X \longrightarrow S$. Ekvivalensrelationen på X definierad av f är relationen:

$$\sim = \{(x, y) \in X \times X \mid f(x) = f(y)\} \subseteq X \times X$$

Exempel 5.5. För alla x, $y \in X$ skriver vi $x \sim_f y$ om och endast om $f(x) = f(y)$

Övning: Beskriv likhetsrelationen på X som $\sim$ av g för någon funktion $g : X \to T$
Lemma: $\sim_f$ av f är en ekvivalensrelation. Övning

Definition 5.6. Låt X vara en mängd och låt $\sim$ vara en ekvivalensrelation.

1. För alla $x \in X$, då $\sim$ ekvivalensklassen av x är delmängden:

$$\overline{x} = \{y \in X \mid y \sim x\} \subseteq X$$
$$\overline{x} \in \mathcal{P}X$$

2. Kvotmängden av X modulo $\sim$ är mängden bestående av alla ekvivalensklasser av X, alltså:

$$\begin{aligned} X\sim &= \{A \text{ i potensmängden av } x \mid \text{ det finns ett } x \text{ i } X : A \text{ är lika med } \overline{x}\} \\ &= \{\overline{x} \mid x \text{ i } X\} \end{aligned}$$

3. Kvotfunktionen av X modulo $\sim$ är funktionen:

$$\begin{aligned} \pi : X &\longrightarrow X/\sim \\ x &\longmapsto \overline{x} \end{aligned}$$

Anmärkning 5.7. π är surjektiv per definition

Exempel 5.8. Låt $\sim$ *vararelatioinenpådenaturligatalengivenav* :
Det definiterar en ekvivalensrelation och $\sim$ *ekvivalensernagesav* :
$\overline{0} = \overline{2} = \overline{4} = \overline{6} = ... = \{0, 2, 4, 6, 8, ...\}$
$\overline{1} = \overline{3} = \overline{5} = \overline{7} = ... = \{1, 3, 5, 7, 9, ...\}$

6 Heltalen

För att skapa heltalen ($\mathbb{Z}$) behöver vi ett sätt att skapa de negativa talen. Detta gör vi med hjälp av följande konstruktion: På mängden $\mathbb{N} \times \mathbb{N}$, låt $\sim$ vara relationen där följande gäller för varje $(k, l), (m, n)$ i $\mathbb{N} \times \mathbb{N}$:

$$(k, l) \sim (m, n) \Longleftrightarrow k + n = m + l.$$

Sats 6.1. Relationen $\sim$ ovan är en ekvivalensrelation.

Bevis. Övning. (Tips: Börja exempelvis med att visa att för varje (k,l) i $\mathbb{N}\times\mathbb{N}$, $k+l=k+l \Rightarrow (k,l)\sim(k,l)$). □

Anmärkning 6.2.

1. Ekvivalensklassen $\overline{(k,l)}$ kommer att vara k-l i $\mathbb{Z}$. Så $\sim$ "säger att"

$$k-l=m-n \iff k+n=m+l.$$

2. Vi kommer att skriva att:

$-2 \coloneqq \overline{(0,2)} = \overline{(1,3)} = \overline{(2,4)} = ... = \{(0,2),(1,3)...\}$

$-1 \coloneqq \overline{(0,1)} = \overline{(1,2)} = \overline{(2,3)} = ... = \overline{(a,a+1)} = \{(0,1),(1,2)...\}$

$0 \coloneqq \overline{(0,0)} = \overline{(1,1)} = ...$

$1 \coloneqq \overline{(1,0)} = \overline{(2,1)} = ...$

Definition 6.3. Mängden av heltal betecknad $\mathbb{Z}$, är kvotmängden $\mathbb{Z} \coloneqq \mathbb{N}\times\mathbb{N}/\sim$ där relationen tilde ($\sim$) är definierad enligt ovan.

Låt $\pi : \mathbb{N}\times\mathbb{N} \to \mathbb{Z}$ beteckna kvotfunktionen. Låt 0 vara definierad som $\pi(0,0) \in \mathbb{Z}$ och 1 som $\pi(1,0) \in \mathbb{Z}$.

Anmärkning 6.4. Vi skulle kunna skriva till exempel $\underline{0}$ eller $\overline{0}$ och så vidare, för att urskilja 0 i $\mathbb{Z}$ och 0 i $\mathbb{N}$, men vi gör inte det.

i) Vi kommer att se att det finns en kanonisk inklusion $\mathbb{N} \to \mathbb{Z}$ (som uppfyller en massa kriterier) där $0 \mapsto 0$ och $1 \mapsto 1$. Via den funktionen identifierar vi 0 i $\mathbb{N}$ med 0 i $\mathbb{Z}$.

ii) Notation 0 (respektive 1) används oftast för additions- (respektive multiplikations-) identiteten (i en ring, grupp etc).

Generellt sett: var pedantisk; använd alltid olika notationer till två olika saker i ett visst bevis.

Rigoröst är minus (-) följande: $a+(-a)=0$ Så hur skapar vi minus med denna egenskap?

Sats 6.5. För varje $(k,l),(k',l'),(m,n),(m'n')$ i $\mathbb{N}\times\mathbb{N}$ har vi att: om $\pi(k,l)=\pi(k'l')$ och $\pi(m,n)=\pi(m',n')$ då är

$$\pi(k+m,l+n)=\pi(k'+m',l'+n').$$

Bevis.

$$\pi(k,l)=\pi(k',l') \iff (k,l)\sim(k',l') \iff k+l'=k'+l.$$

$$\pi(m,n)=\pi(m',n') \iff (m,n)\sim(m',n') \iff m+n'=m'+n.$$

Om vi adderar de högra leden i ovantående ekvationer (samt använder att addition av de naturliga talen är kommutativt och associativt) får vi att

$$k+m+l'+n'=k'+m'+l+n.$$

Vilket implicerar att

$$\pi(k+m,l+n)=\pi(k'+m',l'+n').$$

□

Definition 6.6.

1.) För varje (a,b) i $\mathbb{Z} \times \mathbb{Z}$, eftersom $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ är surjektiv finns det (k,l), (m,n) i $\mathbb{N} \times \mathbb{N}$ så att $\pi(k, l) = a$ och $\pi(m, n) = b$.

2.) Vi definierar additionsfunktionen på $\mathbb{Z}$ genom

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a, b) &\mapsto a + b \coloneqq \pi(k + m, l + n). \end{aligned}$$

Anmärkning 6.7. Från satsen ovan ser vi att + är en väldefinierad funktion; den beror inte på valet av (k,l) och (m,n).

Definition 6.8. Ett heltal är ett element i $\mathbb{Z}$.

Sats 6.9. För varje a i $\mathbb{Z}$ så finns det ett unikt b i $\mathbb{Z}$ så att $a + b = 0$.

Bevis. Låt $k, l \in \mathbb{N}$ så att $a = \pi(k, l)$. Låt $b \coloneqq \pi(l, k)$. Vi har då att

$$\begin{aligned} a + b &= \pi(k + l, l + k) && \text{(Definition av addition för } \mathbb{Z}.) \\ &= \pi(k + l, k + l) && \text{(Addition är kommutativt i } \mathbb{N}.) \\ &= \pi(0, 0) && \text{(Övning.)} \\ &= 0. && \text{(Definition av 0 i } \mathbb{Z}.) \end{aligned}$$

Notera att valet av b är oberoende av (k,l). Alltså: Om a istället var $a = \pi(k', l')$ för några (k', l') i $\mathbb{N}$, då har vi att

$$\begin{aligned} \pi(k, l) &= a \\ &= \pi(k', l') \\ &\Rightarrow (k, l) \sim (k', l') \\ &\iff k + l' = k' + l && \text{(I } \mathbb{N}.) \\ &\iff l' + k = l + k' && \text{(Addition är kommutativ i } \mathbb{N}.) \\ &\iff (l', k') \sim (l, k) \\ &\iff \pi(l', k') = \pi(l, k). \end{aligned}$$

Om $m, n \in \mathbb{N}$ också är så att $C \coloneqq \pi(m, n)$ ger att $a + c = 0$, då har vi

$$\begin{aligned} \pi(k + l', l + k') &= a + b && \text{(Definition av a+b)} \\ &= 0 = \pi(0, 0) && \text{(Definition av 0)} \\ &= a + c && \text{(Utifrån vår definition av } c) \\ &= \pi(k + m, l + n) && \text{(Definition av } a + c) \\ &\Rightarrow (k + l') + (l + n) \\ &= (k + m) + (l + k') \\ &\Rightarrow l' + n = m + k' && \text{(Detta led kan utvecklas.)} \\ &\Rightarrow (k', l') \sim (m, n) \\ &\Rightarrow b = \pi(k', l') = \pi(m, n) = c. \end{aligned}$$

□

Definition 6.10. Definition/Notation: För varje $a \in \mathbb{Z}$, den unika $b \in \mathbb{Z}$ så att $a+b=0$ betecknas $-a$ och kallas den additiva inversen till a.

Notation 6.11. $-a$ läses "minus a".

Definition 6.12. Multiplikationsfunktionen på $\mathbb{Z}$ är funktionen

$$\begin{aligned} \cdot : &\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ &(a,b) \mapsto a \cdot b \coloneqq \pi(km+ln, kn+lm). \end{aligned}$$

Där $(k,l),(m,n) \in \mathbb{N} \times \mathbb{N}$ är så att $a = \pi(k,l)$ och $b = \pi(m,n)$.

Sats 6.13. För varje $(k,l),(m,n),(k',l'),(m',n') \in \mathbb{N} \times \mathbb{N}$ har vi att om $\pi(k,l) = \pi(k',l')$ och $\pi(m,n) = \pi(m',n')$ då är

$$\pi(km+ln, kn+lm) = \pi(k'm'+l'n', k'n'+l'm').$$

Bevis. Övning. □

Anmärkning 6.14. Från satsen ovan ser vi att multiplikationsfunktionen $(\cdot)$ är väldefinierad oberoende av vilka $(k,l)(m,n) \in \mathbb{N} \times \mathbb{N}$ så att $a = \pi(k,l)$ och $b = \pi(m,n)$.

Sats 6.15. För alla $a,b,c \in \mathbb{Z}$ har vi att:

1. $a+b = b+a$. (Addition är kommutativt.)
2. $(a+b)+c = a+(b+c)$. (Addition är associativt.)
3. $0+a = a = a+0$. (0 är identitet till $+$.)
4. $(-a)+a = 0 = a+(-a)$. ($-$ är invers till $+$.)
5. $ab = ba$. (Multiplikation är kommutativt.)
6. $(ab)c = a(bc)$. (Multiplikation är associativt.)
7. $1 \cdot a = a = a \cdot 1$. (1 är identitet till $\cdot$.)
8. $a(b+c) = ab+ac$ och $(a+b)c = ac+bc$. ($\cdot$ är distributiv över $+$.)

Bevis. Övning. □

Definition 6.16. $a|b \iff \exists k \in Z : ak = b$

Sats 6.17. $\forall a,b > 0\ \exists! q,r$
$0 \leq r < a$ så att
$b = qa + r$

Definition 6.18. Ett primtal är ett positivt heltal $p \in \mathbb{Z}$ så att $p \neq 1$ och för varje $a \in \mathbb{Z}$ så att $a|p$ har vi att a = ± 1 eller a = ± p
Ett sammansatt tal är ett positivt heltal $a \in \mathbb{Z}$ så att $a \neq 1$ och a inte är ett primtal

Anmärkning 6.19. Om a $a \in \mathbb{Z}$ är ett sammansatt tal då finns r,s $\in \mathbb{Z}$ så att a=rs

Sats 6.20. $\forall a \in \mathbb{Z}$, $a > 1$, $\exists$ pimtal p så att $p|a$

Bevis. Låt

$$S := \{d \in \mathbb{Z} | d > 1 \text{ och } d|a \subseteq \mathbb{N}\}$$

Eftersom $a|a$ har vi att S $\neq \emptyset$. Enligt WOP har S ett minimalt element p. Om p inte är ett primtal finns det r,s $\in \{2, -, p-1\}$ så att p = rs. Det innebär att $r|a$ och $s|a$, varpå r,s $\in S$. Det motsäger minimaliteten hos p. □

Sats 6.21. Det finns oändligt många primtal

Bevis. Övning □

6.1 Unik primtalsfaktorisering

Sats 6.22. För varje heltal a$\in \mathbb{Z}, a > 1$, finns det primtal p_1, - , p_r så att

$$a = p_1 p_2 \cdots p_r$$

Dessa primtal är unika till permutation (alltså om q_a, $\cdots$, q_s primtal så att a = $p_1 p_2 \cdots p_r$ då är r = s och $\exists \sigma \in S_n = \text{Aut}(\{1, -, r\})$ så att $q_1 = p_{\sigma(1)}$, $q_2 = p_{\sigma(2)}$, $\cdots$, $q_r = p_{\sigma(r)}$)

Bevis. Existens: För varje $a \geq 2$ låt P(a) vara påståendet att det finns en sekvens av primtal vars produkt är a
Eftersom 2 är ett primtal ser vi att P(2) stämmer. Låt a vara ett godtyckligt heltal, a ¿ 1, och P(2), P(3) till P(a-1) stämmer. Om P(a) inte stämmer då finns det r,s $\in \mathbb{Z}$, så att

$$a = rs$$

Eftersom P(r) och P(s) stämmer, ger det att P(a) stämmer. Motsägelse. Därför stämmer P(a). Enligt principen om stark matematisk induktion, stämmer P(a) för alla a $\in \mathbb{Z} > 1$

Unikhet: Övning □

Definition 6.23. Låt A vara en ring. Ett ideal av A är en delmägd I $\subseteq$ A så att

1. 0 $\in$ I
2. $\forall$ x,y $\in$ I, x+y $\in$ I ("I är stängd under addition")
3. $\forall a \in A$, $\forall x \in$ I, ax $\in$ I ("I är stängd under multiplikation med A")

Definition 6.24. Låt A vara en ring. Ett primideal av A är ett ideal P $\subseteq$ A så att

1. P $\neq$ A
2. $\forall x, y \in A$ $\qquad xy \in P \Rightarrow x \in P$ eller $y \in P$

Sats 6.25. $\mathbb{Z}$ är en Primial ideal domain : För varje ideal I $\subseteq \mathbb{Z}$ $\exists!$n$\in \mathbb{Z} \leq 0$ så att I = n$\mathbb{Z}$

Bevis. Om I = {0} ser vi att $I = 0\mathbb{Z} = \{a0 \mid a \in \mathbb{Z}\}$. Anta därför att I $\neq$ {0}. Det innebär att $I \cap \mathbb{Z} > 0 \neq \emptyset$. Enligt WOP $\exists$!n$\in$ $\mathbb{Z}$ som är minimalt i $I \cap \mathbb{Z}$¿0. Eftersom n $\in$ I har vi, per defination av ideal att an $\in$I, för alla a$\in$ $\mathbb{Z}$. Alltså, n$\mathbb{Z}$ $\subseteq$I. Låt nu m$\in$I vara godtycklig. WLOG anta att m > 0. Eftersom $\mathbb{Z}$ är en Euklidean domain finns ett heltal q $\in$ $\mathbb{Z}$, r $\in \{0, -, n-1\}$ så att m = qn + r

Det innebär att r = m+(-qn) $\in$ I (per defination 2 och 3 av ideal). Om r $\neq$ då har vi att n $\in$ I$\cap\mathbb{Z} > 0$ och r< n, vilket motsäger minimaliteten hos n. Alltså är r = 0 och m=qn$\in$n$\mathbb{Z}$
Unikhet: Övning

□

Sats 6.26. Låt $a, b, c \in \mathbb{Z}$. Vi har att a delar bc och $sgd(a, b) = 1$ vilket implicerar att a delar c.

Bevis. Eftersom $sgd(a, b) = 1$ finns det $r, s \in \mathbb{Z}$ så att $r\dot{a} + s\dot{b} = 1$. Det innebär att $rac + sbc = c$. Eftersom $a|bc$ har vi att $a|sbc$ varpå $a|(rac + sbc)$. □

Sats 6.27. Följdsats: För varje $a, b \in \mathbb{Z}$ har vi att $sgd(a, b) = sgd(a, c) = 1$ vilket implicerar att $sgd(a, bc) = 1$.

Bevis. Övning. □

Sats 6.28. (Euclids Lemma): Låt $a_1, ..., a_r \in \mathbb{Z}$. Låt p vara ett primtal. Vi har att $p|a_1...a_r$ vilket implicerar att det finns ett $i = l, -, r$ så att $p|a$.

Bevis. Anta motsatsen, alltså att för varje $i = l, -, r$ så delar p inte a_i. Eftersom $sgd(p, a_i)|p$ har vi att $sgd(p, a_i) = 1$ eller $sgd(p, a_i) = p$. Då p inte delar a har vi att $sgd(p, a_i) = 1$ för alla i. Det innebär att $sgd(p, a_1...a_r) = 1$ (Övning: Från följdsats (induktion).) varpå p inte delar $a_1...a_r$. Motsägelse. □

Övning 6.29. Låt $a, b \in \mathbb{Z}_{>0}$, säg $q \in \mathbb{Z}$, $r \in \{0, -, a - 1\}$ så att $b = qa + r$. Visa att $sgd(a, b) = sgd(a, r)$.

6.2 Modulär aritmetik

Definition 6.30. Låt A, B vara två ringar. En (ring) (homo)morfi från A till B är en funktion $f : A \to B$ så att för varje $a, b \in A$,

$$\begin{aligned} f(a + b) &= f(a) + f(b) && (f \text{ ''respekterar addition''}) \\ f(ab) &= f(a)f(b) && (f \text{ ''respekterar multiplikation''}) \\ f(1) &= 1. \end{aligned}$$

Övning: Ge exempel och icke exempel.

Definition 6.31. Fixera ett n i $\mathbb{Z}$ som är större än 0. På mängden $\mathbb{Z}$, låt $\equiv$ (mod n) beteckna relationen $a \equiv b$ (mod n) som implicerar att $n|(a - b)$. Om $a \equiv b$ (mod n) säger vi att a är lika med/kongruent/ekvivalent med b mod/modulo n.

Sats 6.32. Relationen $\equiv (modn)$ är en ekvivalensrelation.

Bevis. För varje a, b, c

i) $n|0$ vilket implicerar att $n|(a-a)$ samt att $a \equiv a \pmod{n}$.

ii) $a \equiv b \pmod{n}$ implicerar att $n|(a-b)$ per definition av $\equiv \pmod{n}$. Detta implicerar i sin tur att det finns ett $k \in \mathbb{Z}$ så att $nk = (a-b)$ per definition av delbarhet. Detta medför att $n\dot{(}-k) = -nk = -(a-b) = b-a$, vilket per definition av delbarhet implicerar att $n|(b-a)$. Slutligen implicerar detta att $b \equiv a \pmod{n}$ per definition av $\equiv \pmod{n}$.

iii) $a \equiv b \pmod{n}$ och $b = c \pmod{n}$. Per definition av $\equiv \bmod n$ får vi att $n|(a-b)$ och att $n|(b-c)$. Per definition av delbarhet följer det att det finns ett $k \in \mathbb{Z}$ så att $nk = a-b$ och att det finns ett $l \in \mathbb{Z}$ så att $nl = b-c$. Detta implicerar att $a-c = (a-b)+(b-c) = nk+nl = n(k+l)$ samt att $n|(a-c)$ och slutligen att $a \equiv c \pmod{n}$. □

Notation 6.33. Låt $\frac{\mathbb{Z}}{n\mathbb{Z}}$ (läses ''$\mathbb{Z}$ mod n'') beteckna kvotmängden av $\mathbb{Z}$ med hänvisning till $\equiv \pmod{n}$, och för varje $a \in \mathbb{Z}$, låt $\overline{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ beteckna ekvivalensklassen av a.

Övning 6.34. Generalisera konstruktionen av $\frac{\mathbb{Z}}{n\mathbb{Z}}$ för godtycklig ring A och ideal $I \subset A$, för att skapa $\frac{A}{I}$. (Pröva med $A = R[x], I = (x^2+1)$.)

Lemma 6.35. För alla $a \in \mathbb{Z}$ finns det ett unikt $r \in \{0, \ldots, n-1\}$ så att $\overline{a} = \overline{r}$ i $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Bevis. (Existens) Euklid's algoritm ger att det finns $q \in \mathbb{Z}, r \in \{0, \ldots, n-1\}$ så att $a = qn + r$. Det innebär att $a - r = qn$ vilket implicerar att $n|(a-r)$. Per definition av relationen på modulo n ser vi att $\overline{a} = \overline{r}$.
(Unikhet) Om $r' \in \{0, \ldots, n-1\}$ så att $\overline{a} = \overline{r'}$, då har vi att $n|(a-r')$ vilket per definition implicerar att det finns ett heltal q' så att $nq' = a - r'$. Från unikhet av (kvoter och) rester ser vi att $r = r'$. □

Exempel 6.36.

1. $\frac{\mathbb{Z}}{1\mathbb{Z}} = \{\overline{0}\}$
2. $\frac{\mathbb{Z}}{2\mathbb{Z}} = \{\overline{0}, \overline{1}\}$
3. $\frac{\mathbb{Z}}{3\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}\}$
4. $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$
   "Ekvivalensklassen av a representeras av resteb då vi delar a med n".

Definition 6.37 (Addition)**.** Addition på $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ges av funktionen

$$\begin{aligned} + : \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} &\to \frac{\mathbb{Z}}{n\mathbb{Z}} \\ (\overline{a}, \overline{b}) &\longmapsto \overline{a+b} \end{aligned}$$

Med andra ord: För alla $\overline{a}, \overline{b} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$, välj $x \in \overline{a}, y \in \overline{b}$ där vi definierar att $\overline{a} + \overline{b} = \overline{x+y}$.

Sats 6.38. $+$ är väldefinierad. (Overoende av representant av $a \in \overline{a}$)

Bevis. Låt $a, a' \in \overline{a}$ och $b, b' \in \overline{b}$ vara godtyckliga. Det innebär att $a' \equiv a \pmod{n}$, vilket per definition ger att $n|(a-a')$ och vidare att det finns ett heltal k så att $nk = a - a'$. Med samma

process får man även att det finns ett heltal l sådan att $nl = b - b'$. Det innebär att

$$\begin{aligned}(a+b)-(a'+b') =& (a-a')+(b-b')\\ =& nk+nl = n(k+l),\end{aligned}$$

vilket implicerar att $n|((a+b)-(a'+b'))$

samt att $a+b \equiv a'+b' \pmod{n}$

och slutligen att $\overline{a+b} = \overline{a'+b'}$.

□

Definition 6.39 (Additiv invers)**.** För alla $\overline{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$, låt $-\overline{a} \coloneqq \overline{-a}$

Övning 6.40. Visa att $-\overline{a}$ är väldefinierad

Sats 6.41. För alla $\overline{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ har vi att $\overline{a} + (-\overline{a}) = \overline{0}$ i $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Övning. □

Övning 6.42.
1. Definiera multiplikation i $\frac{\mathbb{Z}}{n\mathbb{Z}}$
2. Verifiera att $\frac{\mathbb{Z}}{n\mathbb{Z}}$ med $+, \cdot, \overline{0}, \overline{1}$ är en ring.

Notation 6.43. Kvotmängden $\pi : \mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ kallas ofta för den kanoniska funktionen från $\mathbb{Z}$ till $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Sats 6.44.
1. (i) $\pi(0) = \overline{0}$
   (ii) För alla $a, b \in \mathbb{N}$ har vi att $\pi(a+b) = \pi(a) + \pi(b)$
2. (i) $\pi(1) = \overline{1}$ (π är en ringhomomorfi)
   (ii) För alla $a, b \in \mathbb{Z}$ har vi att $\pi(ab) = \pi(a)\pi(b)$

Exempel 6.45. $\frac{\mathbb{Z}}{2\mathbb{Z}} = \{\overline{0}, \overline{1}\}$
$\overline{0} + \overline{0} = \overline{0+0} = \overline{0}$
$\overline{0} + \overline{1} = \overline{0+1} = \overline{1}$
$\overline{1} + \overline{0} = \overline{1+0} = \overline{1}$
$\overline{1} + \overline{1} = \overline{1+1} = \overline{2} = \overline{0}$

Exempel 6.46 (Application)**.** Vi visar att $x^2 - 5y^2 = 2$ har inga heltalslösningar.
Anta att a, b löser ekvationen, alltså att

$$\begin{aligned} & a^2 - 5b^2 = 2 \\ \implies & \overline{a}^2 - \overline{5}\overline{b}^2 = \overline{2} && \text{i } \frac{\mathbb{Z}}{n\mathbb{Z}} \text{ för alla } n \in \mathbb{Z} \\ \text{välj } n=5 \implies & \overline{a}^2 - \overline{0}\overline{b}^2 = \overline{2} \\ \implies & \overline{a}^2 = \overline{2}\end{aligned}$$

Vi undersöker alla kvadrater i $\frac{\mathbb{Z}}{5\mathbb{Z}}$:

$$\overline{0}^2 = \overline{0^2} = \overline{0}$$
$$\overline{1}^2 = \overline{1^2} = \overline{1}$$
$$\overline{2}^2 = \overline{2^2} = \overline{4}$$
$$\overline{3}^2 = \overline{3^2} = \overline{4}$$
$$\overline{4}^2 = \overline{4^2} = \overline{1}$$

Därmed ser vi att $\overline{a}^2 = \overline{2}$ inte har någon lösning, vilket ger en motsägelse. Därmed har ekvationen $x^2 - 5y^2 = 2$ inga heltalslösningar.