KUNGL
TEKNISKA
HÖGSKOLAN

Algebra och kryptografi

Tomas Ekholm
Niklas Eriksen
Magnus Rosenlund

Institutionen för matematik, 2002

Grekiska alfabetet

alfa	A	α	iota	I	ι	rho	P	ρ
beta	B	β	kappa	K	κ	sigma	Σ	σ
gamma	Γ	γ	lambda	Λ	λ	tau	T	τ
delta	Δ	δ	my	M	μ	ypsilon	Υ	υ
epsilon	E	ε	ny	N	ν	fi	Φ	φ
zeta	Z	ζ	xi	Ξ	ξ	chi	X	χ
eta	H	η	omikron	O	o	psi	Ψ	ψ
theta	Θ	θ	pi	Π	π	omega	Ω	ω

Innehåll

Några ord på vägen

Detta kompendium är skapat för att användas som litteratur till KTHs Matematiska Cirkel under läsåret 2002–2003. Kompendiet består av sju avsnitt, som svarar mot de sju träffar vi planerat, samt ett inledande avsnitt. Kompendiet är inte tänkt att läsas på egen hand, utan ska ses som ett skriftligt komplement till undervisningen på de sju träffarna.

Som den mesta matematik på högre nivå är kompendiet kompakt skrivet. Detta innebär att man i allmänhet inte kan läsa det som en vanlig bok. Istället bör man pröva nya satser och definitioner genom att på egen hand exemplifiera. Därmed uppnår man oftast en mycket bättre förståelse av vad dessa satser och deras bevis går ut på.

Övningsuppgifterna är fördelade i två kategorier. De med udda nummer har facit, och syftet med dessa är att eleverna ska kunna räkna dem och på egen hand kontrollera att de förstått materialet. De med jämna nummer saknar facit och kan användas som examination. Det rekommenderas dock att man försöker lösa även dessa uppgifter även om man inte examineras på dem. Om man kör fast kan man alltid fråga en kompis, en lärare på sin skola eller någon av oss.

Vi bör också nämna att få av uppgifterna är helt enkla. Kika därför inte i facit efter några få minuter (om du inte löst uppgiften), utan prata först med kompisar eller försök litet till. Alla uppgifter ska gå att lösa med hjälp av informationen i detta kompendium.

Vi tackar professorerna Dan Laksov och Carel Faber för deras givande kommentarer om denna skrift.

Författarna, september 2002

0 Bra att veta

0.1 Mängder

En **mängd** innehåller ting, utan repetition och ordning. Tingen kallar vi för **element**. Den **tomma mängden** $\emptyset$ är den mängd som inte innehåller någonting.

Mängder kan presenteras genom att elementen skrivs mellan ett par krullparenteser $\{\}$. Om ett element a tillhör en mängd G använder vi notationen $a \in G$.

Exempel 0.1 *Den tomma mängden* $\emptyset = \{\}$.

Exempel 0.2 *Att en mängd inte tar hänsyn till repetition eller ordning innebär att* $\{1,2,3\} = \{1,2,2,1,3,3,2,1\}$.

Exempel 0.3 *Vanliga mängder är de* $\mathbf{naturliga\ talen}$ $\mathbb{N} = \{0,1,2,3,\dots\}$ *och* $\mathbf{heltalen}$ $\mathbb{Z} = \{\dots,-3,-2,-1,0,1,2,3,\dots\}$.

Ett alternativt sätt att presentera mängder är att innanför krullparanteser skriva ett uttryck följt av ett kolon, därefter restriktioner för uttrycket.

Exempel 0.4 *En mängd kan ofta skrivas på flera sätt. Vi kan även skriva* $\mathbb{Z}$ *som* $\{\pm n : n \in \mathbb{N}\}$.

Exempel 0.5 *De* $\mathbf{rationella\ talen}$ *eller* $\mathbf{bråken}$ *betecknas från engelskans quotient som* $\mathbb{Q} = \left\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}, b \neq 0\right\}$.

Det är vanligt att låta ett litet plus markera att man avser endast de positiva elementen i en mängd av tal.

Exempel 0.6 $\mathbb{Z}_+ = \{n \in \mathbb{Z} : n > 0\}$ *och* $\mathbb{Q}_+ = \{q \in \mathbb{Q} : q > 0\}$

Låt A och B vara två mängder. $\mathbf{Unionen}$ $A \cup B = \{a : a \in A$ eller $a \in B\}$ är den mängd som består av alla a sådana att a tillhör minst en av mängderna A och B. $\mathbf{Snittet}$ $A \cap B = \{a : a \in A, a \in B\}$ är mängden av alla gemensamma element i A och B. **Differensen** mellan A och B skrivs som $A \setminus B = \{a : a \in A, a \notin B\}$ (eller som $A - B$).

Vi använder notationen $|A|$ för att ange antalet element i A.

Exempel 0.7 *Vi kan skriva heltalen som* $\mathbb{Z} = \{a : a \in \mathbb{N}\} \cup \{-a : a \in \mathbb{N}\}$. *Vi inser att* $\mathbb{Z}$ *innehåller ett oändligt antal element, d.v.s.* $|\mathbb{Z}| = \infty$.

Exempel 0.8 *Låt* $G = \{1,3,4,7,9\}$ *och* $H = \{1,2,3,7,8,11\}$. *Vi har* $G \cup H = \{1,2,3,4,7,8,9,11\}$, $G \cap H = \{1,3,7\}$, $G \setminus H = \{4,9\}$, $H \setminus G = \{2,8,11\}$, $|G| = 5$, $|H| = 6$, $|G \cup H| = 8$ *och* $|G \cap H| = 3$. *Observera att* $|G| + |H| = |G \cup H| + |G \cap H|$. *Kan du visa detta i det allmänna fallet? Se övning 1.1.*

Mängden B sägs vara en **delmängd av** A om varje element i B även är ett element i A. Vi brukar notationen $B \subseteq A$.

Exempel 0.9 *Följande mängdinklusioner gäller:* $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$.

Vi kan bilda den **kartesiska produkten** $A \times B = \{(a, b) : a \in A, b \in B\}$. Paret (a, b) är ordnat, d.v.s. (a, b) behöver inte vara samma element som (b, a). Ett vanligt exempel på en kartesisk produkt är talplanet $\mathbb{Z} \times \mathbb{Z}$ där punkter kan vara t.ex. $(2, 5)$ eller $(-2, 3)$.

0.2 Avbildningar

Det mesta inom matematiken handlar om avbildningar av olika slag. Den formella definitionen är följande:

Definition 0.10 *Låt A och B vara två mängder. En* **avbildning** $\phi : A \longrightarrow B$, *är något som till varje element $a \in A$ tilldelar exakt ett element $b \in B$. Vi skriver då $\phi(a) = b$ eller $\phi : a \longmapsto b$.*

Exempel 0.11 *Låt $A = \{1, 2, 3\}$ och $B = \{4, 5\}$ vara två mängder. En funktion $f : A \longrightarrow B$ definierad genom $f(1) = 4, f(2) = f(3) = 5$ är en avbildning.*

Exempel 0.12 *En funktion $f : \mathbb{Q} \longrightarrow \mathbb{Q}$, t.ex. $f(x) = x^2$, är en avbildning.*

Exempel 0.13 *En funktion $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, t.ex. $f(x) = x + 1$, är en avbildning.*

0.3 Induktion

Induktion handlar om att visa påståenden som sägs gälla för vissa mängder, t.ex. mängden av alla heltal. Vi vill kanske visa att den aritmetiska summan $1 + 2 + 3 + \ldots + n$ blir $\frac{(n+1)n}{2}$ för alla positiva heltal n. Vi kan naturligtvis visa detta för **några** n genom att sätta in värden och räkna, men detta räcker inte för att visa det för **alla** n. Vi ska nu titta på hur man kan använda induktion för att visa sådana påståenden.

Idén är att vi ska kunna visa att om påståendet gäller för $n = p$, så gäller det även för $n = p + 1$. Om vi dessutom lyckas visa att det gäller för $n = 1$, så gäller det därmed även för $n = 2$, $n = 3$, $n = 4$, och så vidare. Det räcker alltså att visa basfallet $(n = 1)$ och induktionssteget (att påståendet är sant för $n = p$ alltid medför att påståendet är sant för $n = p+1$). Vi ger problemet ovan som exempel.

Exempel 0.14 *Vi börjar med basfallet. Om vi sätter $n = 1$ innehåller summan bara en term, 1. Det andra uttrycket blir $\frac{(n+1)n}{2} = \frac{2 \cdot 1}{2} = 1$. Eftersom uttrycken är lika för $n = 1$ har vi klarat av basfallet.*

Nu till induktionssteget. Vi måste visa att **om** *påståendet gäller för $n = p$, så gäller det även för $n = p + 1$. Vi låtsas därför (vi gör antagandet) att*

$$1 + 2 + 3 + \ldots + p = \frac{(p+1)p}{2}$$

och kollar om vi med hjälp av detta kan visa att

$$1 + 2 + 3 + \ldots + p + (p+1) = \frac{(p+2)(p+1)}{2}.$$

Det visar sig inte vara särskilt svårt. Med hjälp av vårt antagande får vi

$$\begin{aligned} 1 + 2 + 3 + \ldots + p + (p+1) &= (1 + 2 + 3 + \ldots + p) + (p+1) \\ = \frac{(p+1)p}{2} + (p+1) &= \frac{p(p+1) + 2(p+1)}{2} = \frac{(p+1)(p+2)}{2}. \end{aligned}$$

Därmed har vi visat induktionssteget.

Sätter vi samman basfall och induktionssteg ser vi nu att

$$1 + 2 + 3 + \ldots + n = \frac{(n+1)n}{2}$$

för samtliga positiva heltal n.

Induktion påminner om att välta oändligt långa rader med dominobrickor. För att göra detta krävs två saker. Det ena är att brickorna står tillräckligt tätt, det vill säga att om bricka p välter, så välter även bricka $p + 1$. Detta svarar mot induktionssteget. Det andra som krävs är att någon välter den första brickan. Detta svarar naturligtvis mot basfallet.

0.4 Delbarhet och aritmetikens fundamentalsats

Denna sats är, som namnet antyder, väldigt viktig inom aritmetiken (räknandet med heltal). För de flesta är den dock så välbekant, att den ibland glöms bort. Vi börjar med två definitioner.

Definition 0.15 *Heltalet k är en delare till heltalet m om det finns ett heltal n så att $m = k \cdot n$. Vi skriver då att $n = \frac{m}{k}$ och $k|m$ ("k delar m").*

Definition 0.16 *Ett* **primtal** *p är ett heltal större än 1, vars enda positiva delare är 1 och p.*

Vi är nu redo att formulera aritmetikens fundamentalsats.

Sats 0.17 *Varje heltal kan faktoriseras i primtal på ett unikt sätt, bortsett från ordningen på primtalen.*

Exempel 0.18 *Betrakta talet 48. Om vi vill skriva det som en produkt av primtal så blir dessa primtal alltid fyra tvåor och en trea, d.v.s.* $48 = 2^3 \cdot 3$. *Något annat sätt att bilda* 48 *finns inte.*

Definition 0.19 *Om ett tal* c *delar båda* a *och* b *säger vi att* c *är en* **gemensam delare** *till* a *och* b. *Den* **största gemensamma delaren** *till* a *och* b *betecknas* $\mathrm{sgd}(a, b)$. *Exempelvis är* $\mathrm{sgd}(6, 9) = 3$ *och* $\mathrm{sgd}(48, 64) = 16$. *Om* $\mathrm{sgd}(a, b) = 1$ *säger vi att* a *och* b *är* **relativt prima**.

0.5 Binära tal

När vi skriver vanliga tal, t.ex. 135, så menar vi egentligen att vi adderar ett antal tiopotenser. Vi har $135 = 1 \cdot 100 + 3 \cdot 10 + 5 \cdot 1 = 1 \cdot 10^2 + 3 \cdot 10^1 + 5 \cdot 10^0$. Talet 10 fungerar då som **bas**. Naturligtvis behöver man inte använda 10 som bas. Det går lika bra med exempelvis 2. Eftersom vi vanligtvis som koefficienter innan potenserna använder alla tal som är mindre än 10 ska vi i detta fall använda alla tal som är mindre än 2, d.v.s. 1 och 0. Om vi använder notationen $(n)_a$ för att ange att talet n står i basen a, så får vi exempelvis att $(19)_{10} = (10011)_2$, eftersom $19 = 16 + 2 + 1 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$.

1 Grupper

1.1 Operationer

En **binär operation $*$ på en mängd** G är en avbildning som till varje ordnat par $(a, b) \in G \times G$ associerar ett element $*(a, b)$ eller mer vanligt $a * b$ i G. Eftersom det är ett ordnat par behöver $a * b$ inte vara samma element som $b * a$.

Låt H vara en delmängd av G. Mängden H kallas **sluten under** $*$ om $a * b \in H$ för alla $a, b \in H$. Vi använder notationen $* : G \times G \to G$ som säger att $*$ är en avbildning som tar ett par (a, b) där $a, b \in G$ och ger ett nytt element i G.

Vi ger några exempel på avbildningar.

Exempel 1.1 *Låt $f : \mathbb{Z} \to \mathbb{N}$ sådan att $f(a) = a^2$.*

Exempel 1.2 *Låt $g : \mathbb{Z} \times \mathbb{Q} \to \mathbb{Q}$ sådan att $g(a, b) = ab + a$. Observera att (a, b) är ett ordnat par där $a \in \mathbb{Z}$ och $b \in \mathbb{Q}$.*

Föregående exempel på avbildningar är ej binära operationer. Här följer några exempel på binära operationer.

Exempel 1.3 *Låt $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ sådan att $+(a, b) = a + b$. Det fungerar även med $\mathbb{Z}$ istället för $\mathbb{Q}$.*

Exempel 1.4 *Låt $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ sådan att $\cdot(a, b) = a \cdot b$. Även här kan $\mathbb{Q}$ ersättas med $\mathbb{Z}$.*

1.2 Grupper

Definition 1.5 *En mängd G tillsammans med en binär operation $* : G \times G \to G$ kallas en* **grupp** *och betecknas $(G, *)$ om*

(a) för alla $a, b, c \in G$ gäller att $(a * b) * c = a * (b * c)$ (associativa lagen),

(b) det existerar ett element $e \in G$ sådant att för alla $a \in G$ gäller att $e * a = a * e = a$,

(c) det för alla $a \in G$ existerar ett element $a^{-1} \in G$ sådant att $a * a^{-1} = a^{-1} * a = e$.

Kommentar 1.6 *Elementet e i definitionen är entydigt, d.v.s. det finns endast ett element som uppfyller (b). Antag att det finns två element e_1, e_2 som uppfyller (b). Då följer att $e_1 = e_1 * e_2 = e_2$, vilket visar att e_1 och e_2 är samma element.*

Kommentar 1.7 *För varje $a \in G$ är a^{-1} entydigt bestämd. Vi använder ett motsägelsebevis. Antag att a^{-1} ej är entydigt bestämd. Då finns det minst två element till a som vi kallar a_1^{-1} och a_2^{-1} som uppfyller (c) och är sådana att $a_1^{-1} \neq a_2^{-1}$. Vi har att $a_1^{-1} = a_1^{-1} * e = a_1^{-1} * \left(a * a_2^{-1}\right) = \left(a_1^{-1} * a\right) * a_2^{-1} = e * a_2^{-1} = a_2^{-1}$. Detta visar att a^{-1} är entydigt bestämd.*

Elementet e kallas $\mathbf{identitet}$ och a^{-1} kallas $\mathbf{inversen}$ till a.

Vi ger några triviala exempel på grupper och några exempel på kandidater till grupper som fallerar på en eller flera punkter.

Exempel 1.8 *Paret $(\mathbb{Z}, +)$ är en grupp ty $\mathbb{Z}$ är sluten under operationen $+$ och*

(a) för alla $a, b, c \in \mathbb{Z}$ gäller att $(a + b) + c = a + (b + c)$,

(b) identiteten $e = 0$ eftersom för alla $a \in \mathbb{Z}$ gäller att $a + 0 = 0 + a = a$,

(c) för alla $a \in \mathbb{Z}$ gäller att inversen är $-a$ eftersom $a + (-a) = (-a) + a = 0$.

Exempel 1.9 *Samma argument som i exempel 1.8 visar att $(\mathbb{Q}, +)$ är en grupp.*

Exempel 1.10 *Paret $(\mathbb{Q}, \cdot)$ är ej en grupp då talet 0 saknar invers. Om vi utesluter 0 från $\mathbb{Q}$ och bildar mängden $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ blir $(\mathbb{Q}^*, \cdot)$ en grupp. Identiteten är $e = 1$ och inversen till $\frac{a}{b} \in \mathbb{Q}^*$ är $\frac{b}{a}$.*

Exempel 1.11 *Vi ser att $(\mathbb{Z}, \cdot)$ ej är en grupp ty alla tal utom 1 och -1 saknar invers. Vi har t.ex. att det ej finns någon invers till $2 \in \mathbb{Z}$, ty $2n = 1$ saknar heltalslösningar.*

Definition 1.12 *Antalet element i en grupp G brukar kallas $\mathbf{ordningen}$ av G och betecknas $o(G) = |G|$.*

En grupp $(G, *)$ kallas ändlig om $o(G) = |G| < \infty$ och $\mathbf{abelsk}$ om kommutativa lagen gäller, d.v.s. om $a * b = b * a$ för alla $a, b \in G$. Grupperna $(\mathbb{Z}, +)$ och $(\mathbb{Q}, +)$ är abelska, eftersom $a + b = b + a$ för alla $a, b \in \mathbb{Q}$.

1.3 Delgrupper

Definition 1.13 *Låt $(G, *)$ vara en grupp. Paret $(H, *)$ kallas en $\mathbf{delgrupp\ av}$ $(G, *)$ om $H \subseteq G$ och $(H, *)$ är en grupp.*

Då det inte råder någon tvekan om vad gruppoperationen är uttrycker vi oss lite slarvigt och säger att H är en delgrupp av G om $(H, *)$ är en delgrupp av $(G, *)$.

Exempel 1.14 *$(\mathbb{Z}, +)$ är en delgrupp av $(\mathbb{Q}, +)$ ty $\mathbb{Z} \subseteq \mathbb{Q}$.*

Sats 1.15 *Låt $(G, *)$ vara en grupp. Vi har att H är en delgrupp av G om och endast om*

(a) $H \subseteq G$,

(b) H *är sluten under operationen* $*$,

(c) identiteten $e \in H$,

(d) $a \in H$ *medför att* $a^{-1} \in H$.

BEVIS: Låt H vara en delgrupp av G. Då H är en grupp följer påståendena direkt. Omvänt, antag att $H \subseteq G$ är sluten under operationen $*$, identiteten $e \in H$ och att varje element $a \in H$ har en invers $a^{-1} \in H$. Vi måste visa att associativa lagen gäller. Låt $a, b, c \in H$. Då följer att $a, b, c \in G$ och därmed att $(a * b) * c = a * (b * c)$ eftersom G är en grupp. □

1.4 Ekvationslösning

Låt oss studera hur vi löser ut x ur en ekvation av typen $a + x = b$, där $a, b \in \mathbb{Z}$. Vi vet att $(\mathbb{Z}, +)$ är en grupp, därför finns det en invers $(-a)$ till a. Vi adderar den till höger- och vänsterled och får $(-a) + (a + x) = (-a) + b$. Vi använder associativa lagen och egenskaper för inverser och får $(a + (-a)) + x = (-a) + b$ eller $x = (-a) + b$. Vi löser ekvationer av typen $a \cdot x = b$, där $a, b \in \mathbb{Q}^*$ på precis samma sätt. Vi kan lösa denna ekvation i varje grupp. Låt $(G, *)$ vara en grupp och $a, b \in G$. Vi löser ekvationen $a * x = b$ enligt följande

$$\begin{aligned} a * x &= b, \\ a^{-1} * (a * x) &= a^{-1} * b, \\ \left(a^{-1} * a\right) * x &= a^{-1} * b, \\ e * x &= a^{-1} * b, \\ x &= a^{-1} * b. \end{aligned}$$

Härligt! Vad kul det är med grupper.

1.5 Övningar

Övning 1.1 *Låt G och H vara två ändliga mängder. Visa att relationen $|G| + |H| = |G \cup H| + |G \cap H|$ gäller.*

Övning 1.2 *Låt $G = \mathbb{Q} \setminus \{-1\}$. Definiera $*$ på G genom $*(a, b) = a + b + ab$. Visa att $(G, *)$ definierar en grupp.*

Övning 1.3 *Låt G vara som i övning 1.2. Bestäm lösningen till ekvationen $2 * (x * 3) = 7$ i G.*

Övning 1.4 *Låt $(H, *)$ vara en grupp. Visa att $H_a = \{b \in H : b * a = a * b\}$ är en delgrupp av H.*

Övning 1.5 *Låt $(G, *)$ vara en grupp och låt H och K vara delgrupper till G. Visa att $H \cap K$ är en delgrupp av G.*

Övning 1.6 *Låt G vara en grupp sådan att $g^2 = e$ för alla element g i G. Visa att G är abelsk.*

2 Kvotgrupper

2.1 Ekvivalensrelationer

Definition 2.1 *Låt G vara en mängd. En* **relation $\sim$ på G**, *är en delmängd X av $G \times G$. Vi säger att a* **är i relation med** *b om $(a, b) \in X$, och skriver detta som $a \sim b$. Relationen $\sim$ kallas en* **ekvivalensrelation** *om för alla $a, b, c \in G$ gäller att*

(a) $a \sim a$ (reflexivitet),

(b) om $a \sim b$ följer att $b \sim a$ (symmetri),

(c) om $a \sim b$ och $b \sim c$ följer att $a \sim c$ (transitivitet).

Exempel 2.2 *Låt $\sim$ vara en relation på mängden av alla människor, sådan att $a \sim b$ om a är far till b. Relationen är varken reflexiv, symmetrisk eller transitiv.*

Exempel 2.3 *Låt $n \in \mathbb{N}$ och $\sim$ vara den relation på $\mathbb{Z}$ sådan att $a \sim b$ om n delar $a-b$, d.v.s. om det finns ett heltal k sådant att $a-b = nk$. Relationen $\sim$ är reflexiv ty n delar $a-a = 0$. Vi visar att $\sim$ är symmetrisk. Antag att n delar $a-b$, då finns det ett heltal k sådant att $a-b = nk$. Vi vill finna ett heltal h sådant att $b-a = nh$. Vi ser att $h = -k$ fungerar. Slutligen visar vi transitiviteten. Antag att $a \sim b$ och $b \sim c$, d.v.s. det finns heltal k och h sådana att $a-b = nk$ och $b-c = nh$. Vi vill visa att det finns ett heltal g sådant att $a-c = ng$. Detta följer eftersom $a-c = a-b+b-c = nk+nh = n(k+h)$, så vi kan välja $g = k+h$.*

Denna relation är en viktig ekvivalensrelation som har beteckningen $\equiv$. Vi skriver att $a \equiv b \pmod{n}$ som uttalas "a är kongruent med b modulo n". Mer om denna relation kommer i kapitel 6 och 7.

Definition 2.4 *Låt $\sim$ vara en ekvivalensrelation på en mängd G och $a \in G$. Mängden av de element i G som är i relation med a kallas* **ekvivalensklassen till** *a och betecknas $[a]$, d.v.s. $[a] = \{b \in G : b \sim a\}$.*

Exempel 2.5 *Vi ska i detta exempel undersöka ekvivalensklasserna till relationen $\equiv$ modulo 5. Vi börjar med $[0]$. Heltalet a är ekvivalent med 0 om det finns ett heltal k sådant att $a-0 = 5k$. Alltså $[0] = \{5k : k \in \mathbb{Z}\}$. På liknande sätt följer att $[1] = \{5k+1 : k \in \mathbb{Z}\}$. Man inser vid lite eftertanke att $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$ och att om $b \notin [a]$ följer att $[a] \cap [b] = \emptyset$.*

Definition 2.6 *En* **partition** *av en mängd G är en mängd delmängder $A_1, A_2, \ldots$ av G sådana att $G = A_1 \cup A_2 \cup A_3 \cup \ldots$ och $A_i \cap A_j = \emptyset$ för alla i och $j \neq i$.*

Låt $A_1, A_2, A_3, \ldots$ vara ekvivalensklasserna till en ekvivalensrelation $\sim$. Dessa mängder bildar en **partition** av G. Omvänt gäller att varje partition av en mängd G definierar en ekvivalensrelation.

2.2 Kvotgrupper

För att åstadkomma det vi vill i detta delkapitel behöver vi införa lite notationer samt definitioner.

Definition 2.7 *Låt $(G, *)$ vara en grupp och låt H vara en delgrupp av G. Antag att $a \in G$. Vi inför notationen $a * H = \{a * b : b \in H\}$ och $H * a = \{b * a : b \in H\}$. Vi säger att $a * H$ och $H * a$ är* **vänstersidoklassen** *respektive* **högersidoklassen** *till H som innehåller elementet a. Gruppen H säges vara en* **normal delgrupp** *av G om $a * H = H * a$ för alla $a \in G$.*

Exempel 2.8 *Låt H vara en delgrupp av en grupp G. Antag att $c \in H$. Då följer att $c * H = H$. Beviset följer: Antag att $x \in c * H$. Då finns det ett $h \in H$ sådant att $x = c * h$. Eftersom H är en grupp följer att $x = c * h \in H$. Vi har visat att $c * H \subseteq H$. Antag att $x \in H$. Vi har att $x = (c * c^{-1}) * x = c * (c^{-1} * x) \in c * H$. Detta visar att $H \subseteq c * H$. Alltså är $H = c * H$ och beviset är klart.*

Antag att H är en delgrupp av G. Vi inför relationen, $a \sim b$ om $a^{-1} * b \in H$. Man kan visa att detta definierar en ekvivalensrelation, vilket vi lämnar som en övning och som vi rekommenderar att ni gör innan ni läser vidare.

Låt oss studera $[a]$, d.v.s. vilka element som är i relation med $a \in G$. Antag att $a \sim b$, d.v.s. $a^{-1} * b = c$ för något $c \in H$. Vi får att $b = a * c \in a * H$. Detta visar att $[a] \subseteq a * H$. Vi visar den omvända relationen, d.v.s. $a * H \subseteq [a]$. Antag att $x \in a * H$, då följer att $x = a * h$ för något $h \in H$. Vi har att $a^{-1} * x = h \in H$ och därmed att $a \sim x$. Detta visar att $a * H \subseteq [a]$. Alltså är $[a] = a * H$. Mängden av ekvivalensklasserna till relationen $\sim$ betecknar vi G/H och uttalas "G kvotat med H".

Vi vill göra G/H till en grupp. Vi måste då definiera en gruppoperation på ekvivalensklasserna (som är elementen i G/H). Låt oss försöka med nedanstående definition.

Låt H vara en normal delgrupp av G, $a, b \in G$ samt låt $[a]$ och $[b]$ beteckna deras respektive ekvivalensklass. Vi har att $[a], [b] \in G/H$. Vi inför operationen

$$*_{G/H} : G/H \times G/H \to G/H$$

genom

$$[a] *_{G/H} [b] = [a * b].$$

Här har vi försökt att skilja på gruppoperationerna: Vi har att $*$ är gruppoperationen på G och $*_{G/H}$ gruppoperationen på G/H. I detta läge ska varje matematiker reagera och kräva en förklaring på varför definitionen inte är nonsens. Vi har definierat $*_{G/H}$ på $G/H \times G/H$ genom att välja representanter (a och b) för ekvivalensklasserna och låta $*$ verka på representanterna och därefter ta dess ekvivalensklass. Vi måste övertyga oss om att $[a * b]$ inte beror av vilka representanter vi väljer.

Låt $a \sim c$ och $b \sim d$, d.v.s. $a^{-1} * c = h \in H$ och $b^{-1} * d = g \in H$. Eftersom $[a] *_{G/H} [c] = [b] *_{G/H} [d]$ måste vi visa att $[a * b] = [c * d]$, d.v.s att $(a * b)^{-1} * (c * d) \in H$. Inversen till $a * b$ är $b^{-1} * a^{-1}$, ty $a * b * b^{-1} * a^{-1} = e$. Då H är en normal delgrupp av G följer att för varje $u \in G$ och $v \in H$ finns ett element $v' \in H$ sådant att $v * u = u * v'$. Vi har

$$\begin{aligned}(a*b)^{-1}*(c*d) &= \left(b^{-1}*a^{-1}\right)*(c*d) = b^{-1}*\left(a^{-1}*(c*d)\right)\\ &= b^{-1}*\left(\left(a^{-1}*c\right)*d\right) = b^{-1}*(h*d)\\ &= b^{-1}*\left(d*h'\right) = \left(b^{-1}*d\right)*h' = g*h'.\end{aligned}$$

Eftersom g och h' är element i H följer att även $g * h' \in H$. Vi har nu visat att gruppoperationen är väldefinierad.

Man kan visa att kravet att H ska vara en normal delgrupp av G är nödvändigt, d.v.s. utan kravet är uppgiften omöjlig.

För att visa att $\left(G/H, *_{G/H}\right)$ är en grupp måste vi verifiera gruppaxiomen.

(a) Låt $[a], [b], [c] \in G/H$. Då följer att $\left([a] *_{G/H} [b]\right) *_{G/H} [c] = [a * b] *_{G/H} [c] = [(a * b) * c] = [a * (b * c)] = [a] *_{G/H} [b * c] = [a] *_{G/H} \left([b] *_{G/H} [c]\right)$.

(b) Identiteten är $[e]$ ty, om $[a] \in G/H$ har vi att $[a] *_{G/H} [e] = [a * e] = [a] = [e * a] = [e] *_{G/H} [a]$.

(c) Inversen till $[a] \in G/H$ är $\left[a^{-1}\right]$ ty $[a] *_{G/H} \left[a^{-1}\right] = \left[a * a^{-1}\right] = [e]$ och $\left[a^{-1}\right] *_{G/H} [a] = \left[a^{-1} * a\right] = [e]$.

Gruppen $\left(G/H, *_{G/H}\right)$ kallas kvotgruppen av G och H.

2.3 Grupperna $(\mathbb{Z}_a, +_a)$ och $\left(\mathbb{Z}/a\mathbb{Z}, +_{\mathbb{Z}/a\mathbb{Z}}\right)$

Vi vet att $(\mathbb{Z}, +)$ är en grupp. Låt $a \in \mathbb{Z}$ och bilda mängden

$$a\mathbb{Z} = \{\dots, -2a, -a, 0, a, 2a, 3a, \dots\}.$$

Vi ser att $a\mathbb{Z} \subseteq \mathbb{Z}$ och att $(a\mathbb{Z}, +)$ är en grupp ty $a\mathbb{Z}$ är sluten under $+$, identiteten är $0 \in a\mathbb{Z}$ och inversen till $b \in a\mathbb{Z}$ är $-b$. Delgruppen $(a\mathbb{Z}, +)$ är en normal delgrupp av $(\mathbb{Z}, +)$ ty för varje $b, c \in \mathbb{Z}$ har vi $b + c = c + b$. Vi kan nu bilda mängden av ekvivalensklasser $\mathbb{Z}/a\mathbb{Z}$ som vi får från ekvivalensrelationen $\sim$ på $\mathbb{Z}$ sådan att $b \sim c$ om $-b + c \in a\mathbb{Z}$, d.v.s. om a delar $c - b$. Ekvivalensklasserna blir följande

$$\begin{aligned}[0] &= \{an : n \in \mathbb{Z}\},\\ [1] &= \{an + 1 : n \in \mathbb{Z}\},\\ &\vdots\\ [a-1] &= \{an + a - 1 : n \in \mathbb{Z}\}.\end{aligned}$$

Observera att detta är samma ekvivalensklasser som i exempel 2.3. Vi kan alltså skriva $b \equiv c \pmod{a}$ om $[b] = [c]$ i $\mathbb{Z}/a\mathbb{Z}$.

Eftersom $[0] \cup [1] \cup \ldots \cup [a-1] = \mathbb{Z}$ är detta alla ekvivalensklasser. Mängden

$$\mathbb{Z}/a\mathbb{Z} = \{[0], [1], \ldots, [a-1]\}$$

tillsammans med den binära operationen $+_{\mathbb{Z}/a\mathbb{Z}} : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}$ sådan att $+_{\mathbb{Z}/a\mathbb{Z}}([b], [c]) = [b+c]$ för $b, c \in \mathbb{Z}$ bildar nu gruppen $\left(\mathbb{Z}/a\mathbb{Z}, +_{\mathbb{Z}/a\mathbb{Z}}\right)$ som är kvotgruppen av $\mathbb{Z}$ och $a\mathbb{Z}$.

Låt $\mathbb{Z}_a = \{0, 1, 2, \ldots, a-1\}$ och definiera operationen $+_a : \mathbb{Z}_a \times \mathbb{Z}_a \to \mathbb{Z}_a$ sådan att för $b, c \in \mathbb{Z}_a$ gäller att

$$+_a(b, c) = \begin{cases} b + c & \text{, om } b + c \leqslant a - 1, \\ b + c - a & \text{, om } b + c > a - 1. \end{cases}$$

Vi har lämnat till en övning att visa att $(\mathbb{Z}_a, +_a)$ är en grupp. Denna grupp är lik kvotgruppen $\left(\mathbb{Z}/a\mathbb{Z}, +_{\mathbb{Z}/a\mathbb{Z}}\right)$. Det visar sig att det enda som skiljer dessa grupper från varandra är sättet att beteckna mängderna, elementen och gruppoperationen. Strukturen i grupperna är exakt densamma. Vi kommer i senare kapitel säga att dessa grupper är isomorfa.

2.4 Övningar

Övning 2.1 *Låt $(H, *)$ vara en delgrupp av $(G, *)$ och definiera relationen $\sim$ på G genom att $a \sim b$ om $a^{-1} * b \in H$. Visa att $\sim$ är en ekvivalensrelation.*

Övning 2.2 *En relation $\sim$ på $\mathbb{Q}$ definieras av att $a \sim b$ om och endast om det finns ett heltal m och ett naturligt tal n sådana att*

$$a = b + m2^{-n}.$$

Visa att $\sim$ är en ekvivalensrelation.

Övning 2.3 *Visa att $(\mathbb{Z}_a, +_a)$ är en grupp.*

Övning 2.4 *En grupp $(G, *)$ kallas* **cyklisk** *om det finns ett element $a \in G$ sådant att för alla $b \in G$ finns ett $n \in \mathbb{N}$ sådant att*

$$b = a^n = \underbrace{a * a * a * \ldots * a}_{n \text{ gånger}}.$$

Visa att gruppen $(\mathbb{Z}_7, +_7)$ är cyklisk.

Övning 2.5 *Låt a, b, c och d vara naturliga tal sådana att $c < a$ och $d < b$. Visa att om a och b är relativt prima så finns exakt ett tal x så att $0 \leqslant x \leqslant ab - 1$, $x \equiv c \pmod{a}$ och $x \equiv d \pmod{b}$.*

Övning 2.6 *Beskriv ekvivalensklasserna i kvotgruppen $\mathbb{Z}/\{0\}$.*

3 Homomorfier och isomorfier av grupper

I det här kapitlet ska vi titta närmare på olika avbildningar mellan grupper. Vi kommer också att bevisa ett mycket känt och användbart resultat kallat Lagranges sats.

Det är brukligt att låta ab beteckna $a*b$, där $*$ är gruppoperationen. Det kommer vi att göra i detta kapitel. Vi kommer också framöver använda konventionen att $(\mathbb{Z}_a, +) = (\mathbb{Z}_a, +_a)$, d.v.s. vi avser alltid den naturliga gruppoperationen.

3.1 Avbildningar

Definition 3.1 *Låt A och B vara två mängder, och låt $\phi : A \longrightarrow B$ vara en avbildning mellan dem.* **Bilden** *av ϕ betecknas $\mathrm{Im}(\phi)$ och är mängden av alla $b \in B$ sådana att $b = \phi(a)$ för något $a \in A$. Lite mer formellt: $\mathrm{Im}(\phi) = \{\phi(a) : a \in A\}$.*

Exempel 3.2 *Låt $\phi : (\mathbb{Q}, +) \longrightarrow (\mathbb{Q}, +)$ vara definierad genom $\phi(x) = x + 1$. Då har vi att $\mathrm{Im}(\phi) = \mathbb{Q}$, eftersom varje rationellt tal kan skrivas som summan av 1 och ett annat rationellt tal.*

Definition 3.3 *Låt A och B vara två mängder. En avbildning $\phi : A \longrightarrow B$ kallas*

- **injektiv** *(eller 1 - 1) om det för varje $b \in \mathrm{Im}(\phi)$ finns precis ett $a \in A$ sådant att $\phi(a) = b$.*
- **surjektiv** *(eller på) om $\mathrm{Im}(\phi) = B$.*
- **bijektiv** *om ϕ är både injektiv och surjektiv.*

Exempel 3.4

(a) Funktionen $f : \mathbb{Q}_+ \longrightarrow \mathbb{Q}$ definierad av $f(x) = x$ är injektiv men inte surjektiv, ty det finns inget $x \in \mathbb{Q}_+$ så att $f(x) = -2$.

(b) Funktionen $g : \mathbb{Q} \longrightarrow \mathbb{Q}_+ \cup \{0\}$ definierad av $g(x) = x^2$ är surjektiv men inte injektiv, ty vi har för varje $x \in \mathbb{Q}$ att $g(x) = g(-x)$.

(c) Funktionen $h : \mathbb{Q} \longrightarrow \mathbb{Q}$ definierad av $h(x) = x + 1$ är både injektiv och surjektiv, d.v.s. bijektiv.

Låt A, B och C vara mängder och låt $f : A \longrightarrow B$ och $g : B \longrightarrow C$ vara två avbildningar. Vi noterar att sammansättningen $g \circ f : A \longrightarrow C$ är:

- injektiv om f och g är injektiva
- surjektiv om f och g är surjektiva

- bijektiv om f och g är bijektiva

Definition 3.5 *Låt $\phi : A \longrightarrow B$ vara en avbildning mellan två mängder A och B och låt $C \subseteq \mathrm{Im}(\phi) \subseteq B$. Mängden $\{a \in A : \phi(a) \in C\}$ betecknas $\phi^{-1}(C)$. Vi har alltså en väldefinierad avbildning*

$$\phi^{-1} : \{\textit{delmängder av } \mathrm{Im}(\phi)\} \longrightarrow \{\textit{delmängder av } A\}$$

Om vi identifierar ett element $b \in B$ med delmängden $\{b\} \subseteq B$ och ett element $a \in A$ med delmängden $\{a\} \subseteq A$ samt kräver att ϕ är injektiv, så får vi att

$$\phi^{-1} : \mathrm{Im}(\phi) \longrightarrow A$$

är en avbildning mellan elementen i $\mathrm{Im}(\phi) \subseteq B$ och elementen i A. Vi kallar denna avbildning för **inversen** *till ϕ. Vi måste kräva att ϕ är injektiv för att $\phi^{-1} : \mathrm{Im}(\phi) \longrightarrow A$ ska vara en avbildning, d.v.s. för att vi ska ha att det för varje $b \in \mathrm{Im}(\phi)$ finns exakt ett $a \in A$ så att $\phi^{-1}(b) = a$. Tänk igenom detta.*

Exempel 3.6 *Låt $\phi : (\mathbb{Q}, +) \longrightarrow (\mathbb{Q}, +)$ vara definierad genom $\phi(x) = x + 1$. Eftersom ϕ är bijektiv existerar $\phi^{-1} : \mathrm{Im}(\phi) \longrightarrow (\mathbb{Q}, +)$. I detta fall är det enkelt att se att inversen blir $\phi^{-1}(x) = x - 1$.*

Exempel 3.7 *Låt $\phi : (\mathbb{Q}_+, +) \longrightarrow (\mathbb{Q}, +)$ vara definierad genom $\phi(x) = \frac{x}{2}$. Läsaren får själv övertyga sig om att ϕ är injektiv. Därför existerar $\phi^{-1} : \mathrm{Im}(\phi) = (\mathbb{Q}_+, +) \longrightarrow (\mathbb{Q}_+, +)$ och är definierad genom $\phi^{-1}(x) = 2x$.*

3.2 Lagranges sats

Sats 3.8 *Låt H vara en delgrupp av en grupp G. Då finns en bijektion, d.v.s. en bijektiv avbildning mellan vänstersidoklasserna och högersidoklasserna till H i G.*

BEVIS:

Låt ϕ : {högersidoklasser} $\longrightarrow$ {vänstersidoklasser} definierad genom $\phi(Hg) = g^{-1}H$. Vi ser att ϕ är väldefinierad eftersom om $Hg' = Hg$ så gäller att $g' = hg$ för något $h \in H$ och därför att $\phi(Hg') = (g')^{-1}H = (hg)^{-1}H = g^{-1}h^{-1}H = g^{-1}H = \phi(Hg)$.

Vi har även att ϕ är injektiv eftersom, om vi låter $Hf \neq Hg$ och antar att $f^{-1}H = g^{-1}H$ så innebär det att $f^{-1} = g^{-1}h$ för något $h \in H$. Men genom att invertera båda leden d.v.s. $(f^{-1})^{-1} = (g^{-1}h)^{-1}$ ser vi att $f = h^{-1}g$ vilket innebär att $Hf = Hh^{-1}g = Hg$ vilket ger oss en motsägelse mot att $Hf \neq Hg$. Alltså är antagandet falskt d.v.s. $f^{-1}H \neq g^{-1}H$ och ϕ injektiv.

Slutligen ser vi att ϕ är surjektiv eftersom vi genererar mängden $\{g^{-1}H : g \in G\}$ av vänstersidoklasser, som naturligtvis är samtliga eftersom G är en grupp och alla element har en invers. Detta visar att ϕ är en bijektion mellan höger- och vänstersidoklasserna till H i G. □

Detta innebär naturligtvis att det finns lika många vänstersidoklasser som högersidoklasser till en delgrupp H av en grupp G.

Definition 3.9 *Låt H vara en delgrupp av en grupp G. Antalet vänstersidoklasser (eller högersidoklasser) till H i G kallas* **index** *för H i G och betecknas $(G : H)$.*

Sats 3.10 *(Lagranges sats) Låt H vara en delgrupp av en ändlig grupp G. Då gäller att*

$$(G : H) = \frac{|G|}{|H|}$$

Speciellt gäller att ordningen för H delar ordningen för G.

BEVIS: Vi vet från föregående kapitel att vänstersidoklasserna till H i G utgör en partition av G och vi vet att antalet vänstersidoklasser är lika med $(G : H)$. Låt $\phi : H \longrightarrow gH$ vara en avbildning definierad av $\phi(h) = gh$. Varje element i gH är på formen gh, där $h \in H$, så ϕ är surjektiv. Antag att $\phi(h_1) = \phi(h_2)$. Då är $gh_1 = gh_2$, och därför $h_1 = h_2$, vilket visar att ϕ är injektiv, och därför också bijektiv. Alltså gäller att $|gH| = |H|$ vilket innebär att alla vänstersidoklasser innehåller lika många element som H. Detta medför att $|G| = |H| \cdot (G : H)$, d.v.s. att $(G : H) = \frac{|G|}{|H|}$. □

Notera att vi lika gärna kunde använt högersidoklasser istället i beviset ovan.

Exempel 3.11 *Låt $G = (\mathbb{Z}/4\mathbb{Z}, +) = \{[0], [1], [2], [3]\}$. Vilka delgrupper av G finns det? Då $|G| = 4$ säger Lagranges sats (Sats 3.10) att delgrupperna kan ha 1,2 eller 4 element. Eftersom varje delgrupp innehåller $e = [0]$ finns endast en delgrupp med 1 element, nämligen den triviala delgruppen $[0]$. Den enda delgruppen med 4 element är G själv (en icke-proper delgrupp av G) eftersom G innehåller 4 element. Slutligen, om en delgrupp H har 2 element är den enda möjligheten att $H = \{[0], [2]\}$ (och detta är en delgrupp), för om H innehåller $[1]$ eller $[3]$ så har vi $H = G$ (läsaren kan själv enkelt övertyga sig om detta).*

Kommentar 3.12 *Av Lagranges sats (Sats 3.10) följer också att antalet element i en kvotgrupp G/H är $|G/H| = (G : H) = |G|/|H|$, eftersom elementen i kvotgruppen är sidoklasser till H i G.*

Exempel 3.13 *Låt $G = (\mathbb{Z}/4\mathbb{Z}, +) = \{[0], [1], [2], [3]\}$, och låt $H = \{[0], [2]\}$ vara en delgrupp av G. Eftersom G är abelsk så är H en normal delgrupp av G och kvotgruppen G/H är därför väldefinierad. Hur många element har den? Eftersom $|G/H| = |G|/|H| = 4/2 = 2$, ser vi att den har 2 element.*

3.3 Homomorfier

Vi ska nu diskutera avbildningar mellan grupper som bevarar den algebraiska strukturen.

Definition 3.14 *En avbildning $\phi : G \longrightarrow F$ mellan två grupper G och F sådan att det för alla $g_1, g_2 \in G$ gäller att*

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$$

kallas en **homomorfi**.

Vi noterar här att i vänstra ledet multiplicerar vi g_1 och g_2 med gruppoperationen i G (för att sedan applicera ϕ), och i högra ledet applicerar vi först ϕ för att sedan multiplicera $\phi(g_1)$ och $\phi(g_2)$ med gruppoperationen i F.

Exempel 3.15 *Låt $\phi : G \longrightarrow F$ vara en avbildning mellan två grupper G och F definierad genom $\phi(g) = e_{_F}$ (identiteten i F) för varje $g \in G$. Då är ϕ en homomorfi, för om $g_1, g_2 \in G$, får vi att $\phi(g_1 g_2) = e_{_F} = e_{_F} e_{_F} = \phi(g_1)\phi(g_2)$.*

Exempel 3.16 *Låt $G = (\mathbb{Z}, +)$ och låt $\phi : G \longrightarrow G$ vara definierad genom $\phi(n) = 2n$ för varje $n \in G$. Då har vi för $n, m \in G$ att $\phi(n + m) = 2(n + m) = 2n + 2m = \phi(n) + \phi(m)$. Detta visar att ϕ är en homomorfi.*

Exempel 3.17 *Låt $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ vara definierad genom $\phi(n) = n + 1$ för varje $n \in \mathbb{Z}$. Låt $n, m \in \mathbb{Z}$. Då har vi $\phi(n + m) = 1 + n + m \neq 2 + n + m = 1 + n + 1 + m = \phi(n) + \phi(m)$. Detta visar att ϕ inte är en homomorfi.*

Sats 3.18 *Låt $\phi : G \longrightarrow F$ vara en surjektiv homomorfi mellan två grupper G och F. Då gäller att*

Om G är abelsk så är F abelsk.

BEVIS: Låt $f_1, f_2 \in F$. Eftersom ϕ är surjektiv finns $g_1, g_2 \in G$ sådana att $\phi(g_1) = f_1$ och $\phi(g_2) = f_2$. Eftersom G är abelsk gäller att $g_1 g_2 = g_2 g_1$ och vi får $f_1 f_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2)\phi(g_1) = f_2 f_1$, vilket visar att F också är abelsk. □

Sats 3.19 *Låt $\phi : G \longrightarrow F$ vara en homomorfi mellan två grupper G och F. Då gäller att*

(a) $\phi(e_{_G}) = e_{_F}$

(b) Om $g \in G$ så har vi $\phi(g^{-1}) = (\phi(g))^{-1}$

(c) Om H är en delgrupp av G så är $\phi(H)$ en delgrupp av F.

(d) Om K är en delgrupp av F gäller att $\phi^{-1}(K)$ är en delgrupp av G.

BEVIS:

(a) Låt $g \in G$. Då har vi $\phi(g) = \phi(ge_{_G}) = \phi(g)\phi(e_{_G})$. Nu multiplicerar vi med $(\phi(g))^{-1}$ och får $(\phi(g))^{-1}\phi(g) = (\phi(g))^{-1}\phi(g)\phi(e_{_G})$ d.v.s. $e_{_F} = e_{_F}\phi(e_{_G}) = \phi(e_{_G})$.

(b) $e_{_F} = \phi(e_{_G}) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$. Detta visar att $\phi(g^{-1}) = (\phi(g))^{-1}$

(c) Låt $\phi(h_1), \phi(h_2) \in \phi(H)$. Eftersom $\phi(h_1)\phi(h_2) = \phi(h_1h_2)$ och $h_1, h_2 \in H$ så följer att $\phi(h_1)\phi(h_2) \in \phi(H)$. Detta visar att $\phi(H)$ är sluten under multiplikationen i F. Eftersom $e_{_F} = \phi(e_{_G})$ och $(\phi(h))^{-1} = \phi(h^{-1})$ för varje $h \in H$ så är $\phi(H)$ en delgrupp av F.

(d) Antag att $g_1, g_2 \in \phi^{-1}(K)$. Då har vi $\phi(g_1)\phi(g_2) \in K$ eftersom K är en delgrupp. Likheten $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ visar att $g_1g_2 \in \phi^{-1}(K)$. Alltså är $\phi^{-1}(K)$ sluten under multiplikationen i G. K måste också innehålla $e_{_F} = \phi(e_{_G})$, så $e_{_G} \in \phi^{-1}(K)$. Om $g \in \phi^{-1}(K)$ så har vi $\phi(g) \in K$, så $(\phi(g))^{-1} \in K$. Men $(\phi(g))^{-1} = \phi(g^{-1})$, så vi måste ha $g^{-1} \in \phi^{-1}(K)$. Alltså är $\phi^{-1}(K)$ en delgrupp av G.

□

Definition 3.20 *Låt G och F vara två grupper, och låt $\phi : G \longrightarrow F$ vara en avbildning mellan dem.* **Kärnan** *till ϕ betecknas $\mathrm{Ker}(\phi)$ och är mängden av $g \in G$ sådana att $\phi(g) = e_{_F}$. Lite mer formellt:*
$Ker(\phi) = \{g \in G : \phi(g) = e_{_F}\} = \phi^{-1}(e_{_F})$.

Exempel 3.21 *Låt $\phi : (\mathbb{Q}, +) \longrightarrow (\mathbb{Q}, +)$ vara definierad genom $\phi(x) = x^2 - 1$. Då har vi att $\mathrm{Ker}(\phi) = \phi^{-1}(0) = \{-1, 1\}$.*

Sats 3.22 *Låt $\phi : G \longrightarrow F$ vara en homomorfi mellan två grupper G och F. Då är $\mathrm{Ker}(\phi)$ en normal delgrupp av G.*

BEVIS: Från punkt d) i Sats 3.19 ovan ser vi att eftersom $e_{_F}$ är en (trivial) delgrupp av F så är $\mathrm{Ker}(\phi) = \phi^{-1}(e_{_F})$ en delgrupp av G. Låt $K = \mathrm{Ker}(\phi), k \in K, g \in G$. Då har vi $\phi(g^{-1}kg) = \phi(g^{-1})\phi(k)\phi(g) = (\phi(g))^{-1}e_{_F}\phi(g) = (\phi(g))^{-1}\phi(g) = e_{_F}$, så $g^{-1}kg \in K$. Alltså har vi för alla $k \in K$ att $kg \in gK$. Eftersom $Kg = \{kg : k \in K\}$ har vi att $Kg \subseteq gK$. Betraktar vi istället $gkg^{-1} \in K$ så följer att $gK \subseteq Kg$. Alltså är $Kg = gK$, d.v.s. $\mathrm{Ker}(\phi)$ är en normal delgrupp av G. □

Kommentar 3.23 *Vi noterar att om vi har en homomorfi $\phi : G \longrightarrow F$ mellan två grupper G och F, så blir kvotgruppen $G/\mathrm{Ker}(\phi)$ väldefinierad (eftersom $\mathrm{Ker}(\phi)$ är en normal delgrupp av G).*

Exempel 3.24 *Låt $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/n\mathbb{Z}, +)$ vara definierad genom att $\phi(m) =$ [rest vid heltalsdivision av m med n]. Då är ϕ en homomorfi, och $\mathrm{Ker}(\phi) = n\mathbb{Z}$.*

Sats 3.25 *Låt $\phi : G \longrightarrow F$ vara en homomorfi mellan två grupper G och F. Då gäller*

$$\mathrm{Ker}(\phi) = e_{_G} \Longleftrightarrow \phi \text{ är injektiv}$$

BEVIS:

- ($\Rightarrow$) Antag att $\mathrm{Ker}(\phi) = e_{_G}$ och att $g_1 \neq g_2$, för $g_1, g_2 \in G$. Vi ska visa att $\phi(g_1) \neq \phi(g_2)$. Men eftersom $g_1 g_2^{-1} \neq e_{_G}$ följer att $\phi(g_1)\phi(g_2)^{-1} = \phi(g_1)\phi(g_2^{-1}) = \phi(g_1 g_2^{-1}) \neq e_{_F}$. Därmed är $\phi(g_1) \neq \phi(g_2)$ så ϕ är injektiv.
- ($\Leftarrow$) Antag att ϕ är injektiv. Genom punkt a) i Sats 3.19 har vi att $\phi(e_{_G}) = e_{_F}$. Eftersom ϕ enligt vårt antagande är injektiv, är $e_{_G}$ det enda element som avbildas på $e_{_F}$. Alltså är $\mathrm{Ker}(\phi) = e_{_G}$.

□

Vi har sett att en homomorfi är en avbildning som bevarar den algebraiska strukturen, men den behöver varken vara injektiv eller surjektiv. En homomorfi som har båda dessa egenskaper har ett speciellt namn.

Definition 3.26 *En bijektiv homomorfi kallas en* **isomorfi**.

Vi säger att två grupper är isomorfa om det finns en isomorfi mellan dem, och detta innebär att grupperna i algebraisk mening är samma objekt. De kan ha olika namn på sina element men eftersom de har samma algebraiska struktur representerar de en och samma grupp.

Exempel 3.27 *Grupperna $(\mathbb{Z}_n, +)$ och $(\mathbb{Z}/n\mathbb{Z}, +)$ är isomorfa genom avbildningen som skickar ett element $x \in \mathbb{Z}_n$ på $[x] \in \mathbb{Z}/n\mathbb{Z}$.*

3.4 Övningar

Övning 3.1 *Låt $\phi : \mathbb{Q} \longrightarrow \mathbb{Q}$ vara definierad genom $\phi(x) = \frac{x}{17}$ för varje $x \in \mathbb{Q}$. Visa att ϕ är bijektiv.*

Övning 3.2 *Låt $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$ vara definierad genom $\phi(n) = n^4 + 2$ för varje $n \in \mathbb{Z}$. Visa att ϕ inte är injektiv.*

Övning 3.3 *Låt $(G, +) = \{g_0 = e_{_G}, g_1, g_2, g_3, g_4, g_5, g_6\}$ vara en grupp med 7 element. Vilka delgrupper har G?*

Övning 3.4 *Låt $G = (\mathbb{Z}_4, +)$, och låt H vara en delgrupp av $G, |H| = 2$. Vilka element kan H innehålla?*

Övning 3.5 *Låt $\phi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Q}, +)$ vara definierad genom $\phi(n) = n$ för varje $n \in \mathbb{Z}$. Visa att ϕ är en homomorfi.*

Övning 3.6 *Låt $\phi : G \longrightarrow F$ vara en bijektiv homomorfi mellan två grupper G och F. Visa att kärnan till ϕ är lika med identiteten i G.*

Övning 3.7 *Låt G vara en icke-abelsk grupp och låt $\phi : G \longrightarrow G$ vara definierad genom $\phi(g) = g^{-1}$ för varje $g \in G$. Utred om ϕ är en homomorfi.*

Övning 3.8 *Låt G vara en grupp och H en normal delgrupp till G. Utred om mängden av högersidoklasser till H i G utgör samma partition av G som mängden av vänstersidoklasser till H i G.*

4 Symmetriska gruppen

4.1 Den symmetriska gruppen

Vi har i föregående avsnitt tittat närmare på injektiva, surjektiva och bijektiva funktioner. Vi ska i detta avsnitt koncentrera oss på bijektiva funktioner (bijektioner) över ändliga mängder.

Definition 4.1 *En* **permutation** $\pi : A \longrightarrow A$ *är en bijektion från en ändlig mängd* A *till samma mängd. I allmänhet väljer man* $A = \mathbb{N}_n = \{1, 2, \ldots, n\}$. *Mängden av alla permutationer* $\pi : \mathbb{N}_n \to \mathbb{N}_n$ *med* n *element betecknas* S_n.

En permutation är kort och gott ett sätt att kasta om ordningen hos ett antal element. Antalet permutationer av 52 kort ger exempelvis antalet sätt att blanda en vanlig kortlek.

Vi kan notera permutationer på flera olika sätt. En variant kallas **tvåradsnotation** och är på formen

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}$$

Eftersom första raden alltid är densamma förkortas detta ofta till **enradsnotation**: $\pi(1)\ \pi(2)\ \pi(3)\ \ldots\ \pi(n)$.

Exempel 4.2 *Låt* $\pi : \mathbb{N}_5 \longrightarrow \mathbb{N}_5$ *ges av* $\pi(1) = 4, \pi(2) = 2, \pi(3) = 5, \pi(4) = 3$ *och* $\pi(5) = 1$. *Då skrivs permutationen som*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

och som $4\ 2\ 5\ 3\ 1$.

Vi kommer så småningom att presentera ett tredje sätt att skriva permutationer.

Hur många permutationer finns det i mängden S_n? Vi kan enkelt räkna ut detta med ett kombinatoriskt resonemang. Metoden vi använder är att vi tittar på hur många sätt vi kan skapa en permutation. Det första elementet, 1, kan avbildas på vilket som helst av elementen i $\mathbb{N}_n$. Det finns alltså n möjligheter. Det andra elementet, 2, kan avbildas på alla element utom det som 1 avbildas på. Här har vi alltså $n-1$ alternativ för varje alternativ för 1. Därmed har vi hittills $n(n-1)$ alternativ. På samma sätt ser vi att 3 kan avbildas på $n-2$ sätt. Fortsätter vi ser vi till slut att vi fått $n \cdot (n-1) \cdot (n-2) \cdot \ldots 2 \cdot 1 = n!$ permutationer. Inga av dessa är lika, och vi kan konstruera samtliga permutationer på detta sätt. Alltså har vi $|S_n| = n!$.

Exempel 4.3 *Betrakta* S_3. *Den innehåller permutationerna* $1\ 2\ 3$, $1\ 3\ 2$, $2\ 1\ 3$, $2\ 3\ 1$, $3\ 1\ 2$ *och* $3\ 2\ 1$. *Detta stämmer med formeln för storleken av* S_3 *eftersom* $3! = 3 \cdot 2 \cdot 1 = 6$.

Av titeln att döma ska detta kapitel handla om en grupp, nämligen symmetriska gruppen. Denna består av elementen i S_n och operationen utgörs av funktionssammansättning. Vi såg i förra avsnittet att om man sätter samman två bijektioner så får man en bijektion. Det innebär att om vi sätter samman permutationerna $\pi, \sigma \in S_n$ så fås en ny permutation $\tau = \pi\sigma \in S_n$. Sammansättning sker som vanligt för funktioner från höger till vänster, det vill säga att vi först applicerar den högra av permutationerna och sedan den vänstra.

Exempel 4.4 *Låt $\pi = 2\ 3\ 4\ 1$ och $\sigma = 4\ 2\ 3\ 1$. Vi vill beräkna $\tau = \pi\sigma$. Denna permutation fås genom att först applicera σ och sedan π (från höger till vänster). Vi undersäker först vad 1 avbildas på. I σ avbildas 1 på 4 och i π avbildas denna 4 på 1. Ett annat sätt att skriva detta är*

$$\tau(1) = \pi(\sigma(1)) = \pi(4) = 1.$$

På samma sätt ser vi att σ avbildar 2 på 2 och att π avbildar denna tvåa på 3, det vill säga att

$$\tau(2) = \pi(\sigma(2)) = \pi(2) = 3.$$

Vi får även att $\tau(3) = \pi(\sigma(3)) = \pi(3) = 4$ samt att $\tau(4) = \pi(\sigma(4)) = \pi(1) = 2$. Sätter vi samma allt detta ser vi att $\tau = 1\ 3\ 4\ 2$.

Sats 4.5 *Elementen i S_n, d.v.s. permutationerna av n element, bildar med sammansättning som operation en grupp.*

Bevis: Vi har redan sett att mängden $\mathbb{N}_n$ är sluten under sammansättning av permutationer. Återstår att visa associativitet, existens av identitetselement samt existens av invers.

Vi kan tänka oss funktioner $f : A \longrightarrow B$ som snören som går från ett element $a \in A$ till det motsvarande elementet $f(a) \in B$. Det går ett snöre för varje $a \in A$. Om vi ska sätta samman två funktioner $f : A \longrightarrow B$ och $g : B \longrightarrow C$ så svarar detta mot att man för varje $b \in B$ tar de snören som går dit (från A) och knyter fast i det snöre som går därifrån (till C). Vi inser nu att om vi ska sätta samman tre funktioner $f : A \longrightarrow B$, $g : B \longrightarrow C$ och $h : C \longrightarrow D$, så spelar det ingen roll om vi knyter ihop snörena vid B innan vi knyter ihop dem vid C eller tvärtom. Detta visar att funktionssammansättning av associativ. Eftersom permutationer är funktioner innebär detta att gruppoperationen i symmetriska gruppen är associativ.

Man inser lätt att identitetsfunktionen $f(x) = x$ är en bijektion, det vill säga en permutation, som fungerar som identitet i symmetriska gruppen. Återstår att visa existens av invers. För bijektiva funktioner $f : A \longrightarrow B$ gäller att det går exakt ett snöre till varje $b \in B$. Om vi låter $g : B \longrightarrow A$ definieras av att vi följer samma snören från B till A ser vi att vi får inversfunktionen till f, samt att denna nya funktion har exakt ett snöre till varje $a \in A$. Därmed är inversen till en bijektiv funktion också en bijektiv funktion, så varje permutation i S_n har en invers i S_n. Beviset är klart. □

Den symmetriska gruppen är inte abelsk, det vill säga att $\sigma\tau = \tau\sigma$ gäller **inte** för alla τ och σ.

Exempel 4.6 *Låt* $\pi = 2\ 3\ 4\ 1$ *och* $\sigma = 4\ 2\ 3\ 1$*. Vi såg i ett tidigare exempel att* $\pi\sigma = 1\ 3\ 4\ 2$*. Om vi beräknar* $\sigma\pi$ *får vi* $2\ 3\ 1\ 4$*. Vi ser alltså att för dessa permutationer har vi* $\pi\sigma \neq \sigma\pi$*.*

4.2 15-spelet

Den symmetriska gruppen är en av de mest studerade grupperna som finns. Det har skrivits en hel del böcker om den, och många forskningsartiklar. Vi ska nu titta närmare på ett enpersonsspel, som kan analyseras med hjälp av permutationer.

Definition 4.7 **15-spelet** *är ett spel på ett rutnät av storlek* 4×4*. På detta finns femton brickor, märkta med talen* $1, 2, \ldots, 15$ *samt en tom position. En möjlig ställning är exempelvis*

11	2	5	14
7	15	3	13
1	□	12	8
4	9	10	6

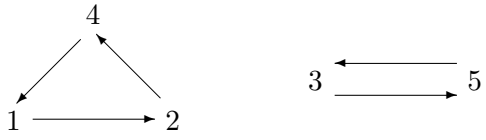
En bricka som ligger intill den tomma positionen kan skjutas till denna position. Spelet startar i denna position

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	□

och målet är att uppnå en position där 14 *och* 15 *har bytt plats, medan övriga brickor ligger kvar.*

15-spelet uppfanns på 1870-talet av Sam Loyd och blev snabbt mycket populärt. Han erbjöd dessutom en prissumma på 1000 dollar till den som först presenterade en korrekt lösning. Trots spelets popularitet var det ingen som lyckades kvittera ut dessa pengar, så det ligger nära till hands att tro att spelet inte går att lösa. Vi ska nu besvara den frågan. Till vår hjälp tar vi ett tredje sätt att skriva permutationer.

Exempel 4.8 *Betrakta permutationen* π *som på enradsnotation skrivs* $2\ 4\ 5\ 1\ 3$*. Vi ser att* 1 *avbildas på* 2*, att* 2 *avbildas på* 4 *samt att* 4 *avbildas på* 1*. Vi ser även att* 3 *avbildas på* 5 *och vice versa. Permutationen kan alltså ritas som nedan.*



Det är inte svårt att inse att varje permutation kan avbildas med en liknande bild. Man brukar kalla varje delfigur en **cykel**. Oftast skrivs den genom att man i en parentes skriver elementen i cykeln i den ordning de förekommer. Det spelar ingen roll vilket element man låter vara först. Cykeln till vänster i exemplet ovan kan alltså skrivas både som $(1\ 2\ 4)$, som $(2\ 4\ 1)$ och som $(4\ 1\ 2)$. Om vi skriver hela permutationen som en följd av cykler har vi skrivit permutationen med **cykelnotation**. I exemplet ovan blir detta $\pi = (1\ 2\ 4)(3\ 5)$. Det spelar ingen roll i vilken ordning man skriver cyklerna. Det framgår av bilden ovan att bortsett från cyklernas ordningsföljd och deras första element så finns det bara ett sätt att skriva en permutation på cykelform.

Ofta låter man bli att skriva ut cykler av längd 1, d.v.s. element som avbildas på sig själva. Permutationen $(1)(2\ 4\ 5)(3)$ kan alltså även skrivas $(2\ 4\ 5)$. Man måste då ange hur många element permutationen innehåller, eftersom det inte är säkert att alla skrivs ut.

Vi kan se varje position i 15-spelet som en permutation av de 16 element som utgörs av de 15 brickorna samt den tomma rutan. Om vi läser rad för rad uppifrån blir då den permutation vi startar med $e = 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ \square$ på enradsnotation. Ett drag består av att den tomma platsen byter plats med en sifferbricka. På cykelform är ett drag en permutation som ser ut som $(k\ \square)$, där k kan vara ett godtyckligt tal mellan 1 och 15. Eftersom man bara kan byta plats på den tomma positionen och en bricka som ligger intill denna är inte alla drag tillåtna jämt, men det går att flytta brickorna så att alla dessa drag blir tillåtna någon gång.

Permutationer som bara består av en cykel av längd 2 kallas **transpositioner**. Varje permutation kan skrivas som en produkt (med produkt menas operationen i gruppen, d.v.s. sammansättning) av transpositioner (se övningarna). Om man fick använda samtliga transpositioner i spelet, så skulle det alltså vara lösbart. Men nu är bara vissa tillåtna. Vad innebär det för lösbarheten?

Lemma 4.9 *Låt $\pi \in S_n$ och låt $\tau = (a\ b)$ vara en transposition. De cykler i π som inte innehåller a eller b kommer också att vara cykler i $\pi\tau$. Om a och b ligger i samma cykel i π så kommer elementen i denna cykel ingå i två cykler i $\pi\tau$. Om a och b ligger i olika cykler i π kommer elementen i dessa cykler ligga i samma cykel i $\pi\tau$.*

Beviset för lemmat finns bland övningarna. Ta då gärna hjälp av följande exempel.

Exempel 4.10 *Låt $\pi = (1\ 4\ 2)(3\ 5)$, $\tau_1 = (1\ 2)$ och $\tau_2 = (2\ 3)$. Då får vi $\pi\tau_1 = (1)(2\ 4)(3\ 5)$ och $\pi\tau_2 = (1\ 4\ 2\ 5\ 3)$ (minns att detta är funktionssammansättningar, så de går från höger till vänster).*

Vi kommer i fortsättningen ha mycket glädje av två funktioner. Funktionen $c : S_n \to \mathbf{N}$ anger hur många cykler en permutation har, inklusive de av längd 1). Exempelvis är $c((1\ 2\ 4)(3\ 5)(6)) = 3$, eftersom permutationen $(1\ 2\ 4)(3\ 5)(6)$

har 3 cykler. Funktionen $d : S_n \to \mathbf{N}$ ges av $d(\pi) = n - c(\pi)$. Denna funktion kallar vi **avståndsfunktionen** i symmetriska gruppen och några av övningarna kommer att visa varför.

Lemma 4.11 *Antag att permutationen π kan skrivas både som en produkt av p transpositioner och som en produkt av q transpositioner. Då är p och q antingen båda jämna eller båda udda.*

BEVIS: Låt $\pi \in S_n$, d.v.s. π är en permutation av n element. Om τ är en transposition, så har produkten $\pi\tau$ antingen en cykel mer eller en cykel mindre än π, enligt föregående lemma. Om $c(\pi)$ är jämnt kommer $c(\pi\tau)$ vara udda och vice versa. Detsamma gäller naturligtvis också för $d(\pi)$ och $d(\pi\tau)$.

Vi betraktar nu $\pi = \tau_1\tau_2 \dots \tau_p$ som en produkt av p transpositioner. Genom att räkna antalet cykler vet vi om $d(\pi)$ är jämnt eller udda. Eftersom p måste vara jämnt om $d(\pi)$ är jämnt och udda om $d(\pi)$ är udda så vet vi om p är jämnt eller udda. □

Vi startar nu 15-spelet med permutationen $1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ \square$ och vill nå permutationen $\pi = 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 15\ 14\ \square$. För att åstadkomma detta ska vi utföra ett antal transpositioner. På cykelform kan π skrivas

$$\pi = (1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)(13)(14\ 15)(\square).$$

Antalet cykler är 15 och därmed är $d(\pi) = 16 - 15 = 1$, ett udda tal. Vi måste alltså utföra ett udda antal transpositioner (drag) för att överföra e till π.

Men titta nu på den tomma positionen. I varje drag går den antingen upp, ner, till höger eller till vänster. Eftersom den till slut återvänt till sin startposition så måste den ha gått lika många gånger åt höger som åt vänster och lika många gånger uppåt som nedåt. Detta innebär att vi använt ett jämnt antal drag, eftersom antalet drag ges av två gånger antalet drag uppåt plus två gånger antalet drag åt vänster.

Men vi kan ju omöjligen ha gjort både ett udda och ett jämnt antal drag. Slutsatsen är att denna position inte kan uppnås. I själva verket kan vi inte uppnå några positioner som svarar mot udda permutationer, om vi vill ha den tomma rutan kvar i nedre högra hörnet.

De permutationer som kan skrivas som en produkt av ett jämnt antal transpositioner bildar delgruppen A_n till S_n (att visa detta lämnas som en övning). Det är inte så svårt att ta reda på hur stor denna delgrupp är.

Lemma 4.12 *I S_n, $n \geqslant 2$, är hälften av permutationerna jämna och hälften udda.*

BEVIS: Betrakta din favorittransposition τ, t.ex. $\tau = (1\ 2)$. Med hjälp av den kan vi para ihop varje jämn permutation med en udda och tvärtom. På detta sätt ska vi visa att de udda är lika många som de jämna.

Tag en jämn permutation π och multiplicera den med τ. Vi får då en udda permutation eftersom produkten kan skrivas som en produkt av ett jämnt antal transposition samt en extra. Om vi å andra sidan tar denna udda permutation och multiplicerar med τ en gång till får vi tillbaka π eftersom τ är sin egen invers. Därmed ser vi att den jämna permutationen π och den udda $\pi\tau$ hör ihop.

På samma sätt kan varje permutation paras ihop med en permutation av den andra sorten. De udda är därför lika många som de jämna. □

De udda permutationerna bildar ingen delgrupp till S_n. Det inses lätt, eftersom e inte är en udda permutation och e måste ingå i varje delgrupp. Däremot är de udda permutationerna sidoklassen till de jämna permutationerna. Om vi tar kvoten S_n/A_n får vi en grupp med två element. Det finns bara en sådan grupp, nämligen $\mathbb{Z}_2$.

Man bör observera att vi inte har visat att man kan uppnå alla ställningar i 15-spelet som svarar mot jämna permutationer. Detta är dock sant. Enklast ser man det genom att visa följande påståenden (se övningarna):

- De permutationer som kan skrivas som en cykel med tre element genererar A_n (de jämna permutationerna i S_n) om $n \geqslant 3$. Exempel: $(1\ 2\ 3), (1\ 2\ 4)$, $(1\ 3\ 4)$ och $(2\ 3\ 4)$ genererar A_4, d.v.s. varje permutation i A_4 kan skrivas som en produkt av dessa cykler.

- Den tomma rutan kan flyttas vart som helst på spelplanen.

- En bricka kan flyttas vart som helst på spelplanen.

- Vi kan flytta 3 godtyckliga brickor A, B och C till ett hörn i den ordningen, så att förflyttningen av B inte påverkar A's position och förflyttningen av C inte påverkar positionen hos A eller B.

□	B
C	A

- Vi får en cykel $(A\ B\ C)$ med tre element om vi flyttar dessa tre element till ett hörn, byter plats på dem till situationen nedan och slutligen gör de ursprungliga dragen baklänges i omvänd ordning. Då kommer B att flyttas tillbaka till C's plats, A till B's plats och C till A's plats. Alla övriga brickor kommer att hamna där de ursprungligen var.

□	A
B	C

- Eftersom vi har tillgång till samtliga permutationer på form $(A\ B\ C)$ så kan vi nu skapa varje jämn permutation.

4.3 Övningar

Övning 4.1 *Skriv permutationen $\pi = 4\ 2\ 7\ 3\ 5\ 8\ 1\ 6 \in S_8$ på cykelnotation och permutationen $\sigma = (3\ 5\ 7)(4\ 2\ 1) \in S_8$ på enradsnotation. Beräkna sedan $\sigma\pi$, $\pi\sigma$, σ^2 samt σ^3.*

Övning 4.2 *Bestäm alla delgrupper av S_3. Vilken av dessa är A_3?*

Övning 4.3 *Undersök om ställningen i definition 4.7 verkligen är möjlig.*

Övning 4.4 *Visa att S_k är en delgrupp av S_n om $k \leqslant n$. Visa även att A_n är en delgrupp av S_n.*

Övning 4.5 *Visa att varje permutation som består av en cykel av längd k kan skrivas som en produkt av $k-1$ transpositioner. Ett användbart exempel är $(1\ 4\ 3\ 5\ 2) = (1\ 4)(4\ 3)(3\ 5)(5\ 2)$.*

Övning 4.6 *Visa att varje jämn permutation i S_n för $n \geqslant 3$, det vill säga varje permutation i A_n för $n \geqslant 3$, kan skrivas som en produkt av cykler av längd tre.*

Övning 4.7 *Visa att den tomma rutan och en godtycklig bricka kan flyttas fritt på spelplanen i 15-spelet. Hur stort område av planen påverkas då vi flyttar en bricka från ett ställe till ett annat?*

Övning 4.8 *Visa att avståndsfunktionen $d(\pi)$ uppfyller följande saker:*

(a) $d(\pi) = 0 \iff \pi = e$.

(b) $d(\pi) = d(\pi^{-1})$.

(c) Om π kan skrivas som en produkt av k transpositioner, så är $k \geqslant d(\pi)$.

Från övning 4.5 följer nu att det minsta antal transpositioner som behövs för att skriva π är $d(\pi)$.

5 Ringar och kroppar

I det här kapitlet ska vi definiera två nya algebraiska strukturer, nämligen ringar och kroppar.

5.1 Ringar

Definition 5.1 *En* **ring** $(R, +, \cdot)$ *är en mängd* R *sluten under två binära operationer* $+$ *och* $\cdot$ *som vi kallar addition och multiplikation, definierade på* R *så att följande är uppfyllt:*

(a) $(R, +)$ *är en abelsk grupp under* $+$*.*

(b) Multiplikationen är associativ, d.v.s. om $a, b, c \in R$ *så gäller* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*.*

(c) Den vänstra och högra distributiva lagen gäller, d.v.s. om $a, b, c \in R$ *så har vi* $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *respektive* $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

(d) R *innehåller en multiplikativ identitet 1, d.v.s. för alla* $a \in R$ *gäller att* $1 \cdot a = a \cdot 1 = a$*.*

(e) Multiplikationen är kommutativ, d.v.s. för alla $a, b \in R$ *gäller* $a \cdot b = b \cdot a$*.*

Ibland definieras ringar utan de två sista egenskaperna (1 och kommutativitet). Vi kommer dock bara betrakta ringar som är kommutativa och har etta.

Exempel 5.2 *Vi vet att* $(\mathbb{Z}, +)$ *och* $(\mathbb{Q}, +)$ *är abelska grupper. Den associativa lagen samt de distributiva lagarna gäller för tal. Vi vet också att multiplikationen är kommutativ och att det finns en multiplikativ identitet 1. Därför följer att* $(\mathbb{Z}, +, \cdot)$ *och* $(\mathbb{Q}, +, \cdot)$ *båda är ringar.*

Exempel 5.3 *Betrakta den cykliska gruppen* $(\mathbb{Z}_a, +), a \in \mathbb{Z}$*. Om vi för varje* $n, m \in \mathbb{Z}_a$ *låter produkten* nm *vara definierad som resten av* $nm \in \mathbb{Z}$ *vid heltalsdivision med* a*, så blir* $(\mathbb{Z}_a, +, \cdot)$ *en ring. Vi har t.ex. att i* $\mathbb{Z}_5$ *är* $2 \cdot 3 = 1$*.*

Liksom i fallet med grupper finns det ett speciellt namn på en avbildning mellan två ringar som bevarar den algebraiska strukturen.

Definition 5.4 *En* **ringhomomorfi** *mellan två ringar* R *och* S *är en avbildning* $\phi : R \longrightarrow S$ *sådan att om* $a, b \in R$ *så gäller att*

(a) $\phi(a + b) = \phi(a) + \phi(b)$

(b) $\phi(ab) = \phi(a)\phi(b)$

Exempel 5.5 *Låt $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_a$ vara definierad genom $\phi(n) =$ (rest vid heltalsdivision av n med a). Då blir ϕ en ringhomomorfi.*

Definition 5.6 *En* **ringisomorfi** *är en bijektiv ringhomomorfi.*

Exempel 5.7 *De abelska grupperna $(\mathbb{Z}, +)$ och $(2\mathbb{Z}, +)$ är isomorfa under avbildningen $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$ definierad av $\phi(x) = 2x$. Men ϕ är ingen ringisomorfi mellan $(\mathbb{Z}, +, \cdot)$ och $(2\mathbb{Z}, +, \cdot)$ ty $\phi(xy) = 2xy \neq 4xy = 2x2y = \phi(x)\phi(y)$.*

5.2 Kroppar

Eftersom alla ringar är grupper under additionen $+$, finns alltid en additiv invers $-a$ till varje element a i ringen. En multiplikativ invers till ett element a i ringen är ett element a^{-1} så att $a \cdot a^{-1} = 1 = a^{-1} \cdot a$. Frågan är nu om alla element a i ringen har en multiplikativ invers. Svaret är att i allmänhet finns inte någon multiplikativ invers a^{-1} till varje element a i ringen. Vi inför därför en beteckning $U(R)$ för mängden av inverterbara element i en ring R. Lite mer formellt: $U(R) = \{a \in R : a^{-1} \in R\}$.

Sats 5.8 *Låt R vara en ring. Mängden $U(R)$ av inverterbara element i R är en grupp med multiplikationen i R som operation.*

BEVIS: Som vanligt måste vi verifiera axiomen. Det står klart att U(R) är sluten under multiplikation. Multiplikationen är associativ, eftersom detta gäller för alla element i R. Enheten 1 tillhör $U(R)$ eftersom den är sin egen invers (eftersom $1 \cdot 1 = 1$). Det återstår bara det sista axiomet; vi måste visa att alla element i $U(R)$ har en invers i $U(R)$.

Eftersom elementen i $U(R)$ är inverterbara har de en invers i R. För att visa att denna invers ligger i $U(R)$ måste vi visa att inversen är inverterbar. Men om $a \in U(R)$ har inversen b, d.v.s. att $a \cdot b = 1$, då har b inversen a. Alltså ligger b i $U(R)$, vilket var vad vi skulle visa. □

Definition 5.9 *Ett element som har en multiplikativ invers i en ring kallas en* **enhet** *i ringen.*

Om alla element $a \neq 0$ i en ring R $(\neq \{0\})$ är enheter, d.v.s. $U(R) = R - \{0\}$ så har vi en speciell sorts ring med ett eget namn.

Definition 5.10 *En ring K $(\neq \{0\})$ i vilken alla nollskilda element är enheter kallas en* **kropp**.

Exempel 5.11 $(\mathbb{Q}, +, \cdot)$ *är ett exempel på en kropp.*

Exempel 5.12 $(\mathbb{Z}, +, \cdot)$ *är ingen kropp. Det finns t.ex. ingen multiplikativ invers till 3 i $\mathbb{Z}$, d.v.s. 3 är ingen enhet i $\mathbb{Z}$.*

Exempel 5.13 *$\mathbb{Z}_p$ är en kropp då $p \in \mathbb{Z}$ är ett primtal. Detta kommer att visas i nästa kapitel.*

Sats 5.14 *I en kropp bildar alla element utom 0 en grupp med multiplikation som operation.*

BEVIS: I en kropp K har alla element utom 0 en invers så de bildar mängden $U(K)$. Enligt sats 5.8 ovan är detta en grupp med multiplikationen som operation. □

5.3 Övningar

Övning 5.1 *Vad är $3 \cdot 4$ i $(\mathbb{Z}_7, +, \cdot)$?*

Övning 5.2 *Vad är $5 \cdot (-3)$ i $(\mathbb{Z}_6, +, \cdot)$?*

Övning 5.3 *Ge ett exempel på en ring R i vilken det finns $a, b \in R$ och $a, b \neq 0, a \neq b$ så att $a \cdot b = 0$.*

Övning 5.4 *Ett element a i en ring R kallas nilpotent om $a^n = 0$ för något $n \in \mathbb{Z}_+$. Visa att om a och b är nilpotenta element så är också $a + b$ nilpotent. Tips: Använd binomialsatsen, kapitel 6.*

Övning 5.5 *Visa att den multiplikativa inversen till en enhet i en ring är unik.*

Övning 5.6 *Ge exempel på en kropp K i vilken det finns $x \in K$ så att vi för något $n \in \mathbb{Z}_+$ får $nx = 0$.*

6 Fermats lilla sats

De flesta av läsarna känner säkert till Fermats (stora) sats, som säger att ekvationen $x^n + y^n = z^n$ saknar positiva heltalslösningar för $n \geqslant 3$. Denna har nyligen bevisats av Andrew Wiles. Det finns även en Fermats lilla sats, som vi ska titta närmare på i detta kapitel. Den utgör hörnstenen i RSA-kryptering (se nästa kapitel) och är dessutom tämligen lätt att visa.

Sats 6.1 *(Fermats lilla sats)*

Om a är ett heltal och p ett primtal, så gäller att

$$a^p \equiv a \pmod{p}.$$

Vi ska i detta avsnitt presentera flera bevis för denna sats. Vi börjar med det som är mest algebraiskt och går sedan vidare mot mer kombinatoriska bevis.

6.1 Första beviset

Det första beviset är nästan trivialt, eftersom vi gjort mycket förarbete i föregående kapitel. Vi behöver dock följande definition och lemma.

Definition 6.2 *Låt G vara en grupp och a ett element i G. Då är elementets* **ordning** *given av $o(a) = \min\{n > 0 : a^n = e\}$.*

Vi ser att e är det enda element i gruppen som har ordning 1.

Lemma 6.3 *Låt G vara en grupp och a ett element i gruppen av ordning k. Då utgör mängden $A = \{e, a, a^2, \ldots, a^{k-1}\}$ en delgrupp av G.*

Beviset lämnas som en övning. Den viktiga egenskapen att utnyttja är att $a^k = e$, så vi får exempelvis att $a^{k+3} = ea^3 = a^3$. Vi ser också att delgruppens ordning är samma som elementets ordning.

Vi är nu redo att bevisa Fermats lilla sats.

BEVIS: Vi betraktar kroppen $\mathbb{Z}_p$. De inverterbara elementen $U(\mathbb{Z}_p)$ bildar en grupp med multiplikation som operation. Eftersom $\mathbb{Z}_p$ har p element och $U(\mathbb{Z}_p)$ innehåller alla element i $\mathbb{Z}_p$ utom 0, så följer att $U(\mathbb{Z}_p)$ har $p-1$ element. Detta är gruppens ordning. Enligt Lagranges sats har varje delgrupp en ordning som delar gruppens ordning. Men eftersom varje element har samma ordning som en delgrupp, så kommer varje element ha en ordning som delar gruppens ordning. Speciellt gäller att

$$a^{p-1} \equiv (a^{o(a)})^{\frac{p-1}{o(a)}} \equiv 1^{\frac{p-1}{o(a)}} \equiv 1 \pmod{p}$$

(kom ihåg att 1 är identiteten i $U(\mathbb{Z}_p)$). Om vi multiplicerar med a får vi Fermats lilla sats för alla element i $\mathbb{Z}_p$ utom 0. Sätter vi $a = 0$ är dock satsen trivialt uppfylld. □

6.2 Andra beviset

Vi ska nu titta på två alternativa bevis av Fermats lilla sats. Det kan tyckas överflödigt att visa samma sats flera gånger, och om målet med bevisen bara var att visa satsen så stämmer detta. Det finns dock andra anledningar till att man presenterar ett bevis. En är att man ger insikt till varför satsen är sann, en annan att de tekniker som används i beviset är intressanta i sig. Båda dessa anledningar gör att fler än ett bevis är önskvärt.

Det andra beviset utnyttjar att om två olika element b och c i en grupp G multipliceras med samma element $a \in G$, så fås två olika element.

BEVIS: Låt u vara produkten av samtliga noll-skilda tal i $\mathbb{Z}_p$, d.v.s. $u = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}$. Vi vet att $U(\mathbb{Z}_p)$ är en grupp med multiplikation som operation. I en grupp vet vi att om $b \neq c$ så följer att $ab \neq ac$, eftersom $ab = ac$ leder till $b = c$ genom att vi multiplicerar med a^{-1}. Därmed får vi $p-1$ olika element om vi multiplicerar $1, 2, \ldots, p-1$ med a. Eftersom $U(\mathbb{Z}_p)$ innehåller exakt $p-1$ element får vi varje element i $U(\mathbb{Z}_p)$ exakt en gång. Detta ger att

$$u \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv a^{p-1}u \pmod{p}.$$

Eftersom u har invers i $\mathbb{Z}_p$ följer att $1 \equiv a^{p-1} \pmod{p}$, och om vi förlänger med a får vi $a \equiv a^p \pmod{p}$. □

För att bättre förstå beviset ovan tittar vi på ett exempel.

Exempel 6.4 *I $\mathbb{Z}_7$ finns de inverterbara elementen $\{1, 2, 3, 4, 5, 6\}$. Beräkningen i beviset ovan, om vi väljer $a = 3$, blir*

$$\begin{aligned} u \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 &\equiv (3 \cdot 5) \cdot (3 \cdot 3) \cdot (3 \cdot 1) \cdot (3 \cdot 6) \cdot (3 \cdot 4) \cdot (3 \cdot 2) \\ &\equiv 3^6 \cdot 5 \cdot 3 \cdot 1 \cdot 6 \cdot 4 \cdot 2 \equiv 3^6 \cdot u \pmod{p}. \end{aligned}$$

6.3 Tredje beviset

Det tredje beviset visar vi med hjälp av tre hjälpsatser. Det är litet mer kombinatoriskt och använder sig inte av ringstrukturen hos $\mathbb{Z}_p$. Däremot kräver det kännedom om binomialsatsen och induktion. Induktion beskrev vi som hastigast i kapitel 0 och binomialsatsen följer här (utan bevis).

Sats 6.5 *Låt $n! = n \cdot n-1 \cdot n-2 \cdot \ldots \cdot 2 \cdot 1$, $0! = 1$ och låt $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Då gäller att*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Som exempel på denna sats kan vi ta $n = 2$. Då gäller, som vi alla vet, att

$$(a+b)^2 = \binom{2}{0} a^2 b^0 + \binom{2}{1} a^1 b^1 + \binom{2}{2} a^0 b^2 = a^2 + 2ab + b^2.$$

Talen $\binom{n}{k}$ kallas binomialkoefficienter och man kan visa att de är heltal. Vi ska nu titta på hur dessa beter sig när vi räknar modulo p när p är ett primtal.

Lemma 6.6 *För ett primtal p och för $0 < i < p$ gäller att*

$$\binom{p}{i} \equiv 0 \pmod{p}.$$

BEVIS: Påståendet ovan är samma sak som att säga att p delar $\binom{p}{i}$. Vi sätter $k = \binom{p}{i} = \frac{p!}{i!(p-i)!}$, vilket ger $p! = k\ i!\ (p-i)!$. Men vi vet, genom aritmetikens fundamentalsats (se kapitel 0), att varje tal kan primtalsfaktoriseras på endast ett sätt. Eftersom p är ett primtal, som ingår i faktoriseringen av vänsterledet, så måste det även ingå i primtalsfaktoriseringen av högerledet. Men p delar varken $i!$ eller $(p-i)!$, eftersom deras primtalsutvecklingar bara innehåller tal som är mindre än i respektive $p-i$, så p delar $k = \binom{p}{i}$. Därav följer att $\binom{p}{i} \equiv 0 \pmod{p}$. □

Det är vanligt, t.o.m. på högskolan, att man ser studenter använda sig av "likheten" $(a+b)^n = a^n + b^n$, vilket inte är korrekt. Fast om n är ett primtal gäller detta, om vi räknar modulo n.

Lemma 6.7 *Om p är ett primtal gäller $(a+b)^p \equiv a^p + b^p \pmod{p}$.*

BEVIS: Enligt binomialsatsen har vi

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i.$$

Eftersom binomialkoefficienterna $\binom{n}{i}$ för $0 < i < p$ är noll modulo p blir det enda som återstår

$$(a+b)^p \equiv \binom{p}{0} a^p b^0 + \binom{p}{p} a^0 b^p \equiv a^p + b^p \pmod{p}.$$

□

Detta kan nu generaliseras till längre summor.

Lemma 6.8 *Om p är ett primtal gäller $(a_1 + a_2 + \ldots + a_k)^p \equiv a_1^p + a_2^p + \ldots + a_k^p \pmod{p}$.*

BEVIS: Vi använder induktion. Basfallet $k = 1$ är trivialt uppfyllt och fallet $k = 2$ såg vi i förra lemmat. Återstår att visa lemmat för godtyckligt k.

Vi antar att påståendet gäller för k, det vill säga att $(a_1+a_2+\ldots+a_k)^p \equiv a_1^p+a_2^p+\ldots+a_k^p \pmod{p}$. Vi vill visa att det då gäller för $k+1$, det vill säga att $(a_1+a_2+\ldots+a_{k+1})^p \equiv a_1^p + a_2^p + \ldots + a_{k+1}^p \pmod{p}$. Men detta är inte svårt. Med hjälp av föregående lemma kan vi skriva

$$\begin{aligned}(a_1 + a_2 + \ldots + a_k + a_{k+1})^p &\equiv ((a_1 + a_2 + \ldots + a_k) + a_{k+1})^p \\ &\equiv (a_1 + a_2 + \ldots + a_k)^p + a_{k+1}^p \\ &\equiv a_1^p + a_2^p + \ldots + a_k^p + a_{k+1}^p \pmod{p}.\end{aligned}$$

Därmed ser vi att om formeln gäller för summor med k termer så gäller den även för summor med $k+1$ termer. Vi kan konstatera att formeln gäller för summor med godtyckligt många termer. □

Det är nu enkelt att visa Fermats sats:

$$a^p \equiv (\underbrace{1+1+\ldots+1}_{a \text{ st}})^p \equiv \underbrace{1^p+1^p+\ldots+1^p}_{a \text{ st}} \equiv \underbrace{1+1+\ldots+1}_{a \text{ st}} \equiv a \pmod{p}.$$

6.4 Övningar

Övning 6.1 *Undersök om 28 är ett primtal genom att beräkna 4^{28} och 5^{28} modulo 28.*

Övning 6.2 *Låt G vara en grupp och a ett element i gruppen av ordning k. Visa att mängden $A = \{e, a, a^2, \ldots, a^{k-1}\}$ utgör en delgrupp av G.*

Övning 6.3 *Beräkna $(a+b)^4$ och $(2a+3b)^3$.*

Övning 6.4 *Visa att $a^p \equiv a \pmod{2p}$ om p är ett udda primtal och a inte delar p.*

Övning 6.5 *Beräkna*

$$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \ldots \binom{n}{n}$$

genom att välja lämpliga värden på a och b i binomialsatsen.

Övning 6.6 *Använd föregående övning och Lemma 6.6 för att visa att*

$$2^p \equiv 2 \pmod{p}$$

för primtal p. Detta följer naturligtvis också av Fermats sats.

Övning 6.7 *Vi kan använda det andra beviset av Fermats lilla sats för att generalisera den. Tag ett positivt heltal m och betrakta ringen $\mathbb{Z}_m$ och kroppen $U(\mathbb{Z}_m)$. Om a ligger i $U(\mathbb{Z}_m)$ gäller att*

$$a^{|U(\mathbb{Z}_m)|+1} = a \pmod{m}.$$

Visa detta!

Övning 6.8 *Fermats sats formuleras ofta, för p primtal och a som inte delar p, som*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Utnyttja denna formulering för att visa att

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq},$$

där p och q är två olika primtal.

7 RSA-kryptering

Kryptering handlar om att skriva om meddelanden så att bara mottagaren kan läsa meddelandet. Ett klassiskt trick är exempelvis att flytta fram varje bokstav $m = 3$ tre steg i alfabetet. Ordet `alfabetet` blir då `doidehwhw`, vilket är svårare att känna igen. Endast den som vet att varje bokstav blivit framflyttad tre steg kan läsa meddelandet, genom att flytta bak varje bokstav tre steg. Detta kallas **Caesarchiffer**.

Detta krypto är dock ganska lätt att knäcka. Man kan prova att flytta varje bokstav ett, två, tre, fyra eller fler steg framåt och när man får en vettig text så är det den rätta. En mer avancerad variant som är svårare att knäcka är att utgå från en längre talsträng $a_1a_2a_3 \dots a_k$ och flytta fram första bokstaven a_1 steg, andra bokstaven a_2 steg och så vidare. När man kommer till bokstav $k+1$ börjar man om från början med a_1. Även detta krypto, som kallas **Vigenèrechiffer**, går att knäcka, men är betydligt svårare.

Vigenèrechiffret har emellertid ett annat problem, som det delar med Caesarchiffret. För att kunna använda det måste avsändaren någon gång ha meddelat nyckeln $a_1a_2 \dots a_k$. Nyckeln kan inte skickas krypterad, eftersom mottagaren ännu inte känner till nyckeln. Mottagaren och avsändaren måste alltså ha träffats och måste dessutom träffas fler gånger, eftersom nyckeln behöver bytas ibland.

Innan vi går vidare kan det vara lämpligt att precisera några av de ord vi använt.

Definition 7.1 *Med ett* **krypto** *menas ett system att omvandla ett meddelande i* **klartext** *till ett* **krypterat** *meddelande och tillbaka. Den avbildning som går från klartext till krypterad text kallas* **krypteringsfunktion** *och dess invers kallas* **dekrypteringsfunktion**. *Varje krypto använder sig av någon sorts parameter,* **nyckel**, *till krypterings- och dekrypteringsfunktionerna.*

7.1 RSA

I kryptona ovan utgörs nycklarna av antalet steg m respektive strängen $a_1a_2 \dots a_k$. I båda kryptona är krypteringsfunktionen samma som dekrypteringsfunktionen, men negationen av nyckeln används vid dekryptering: att flytta bak varje bokstav 3 steg är samma sak som att flytta fram varje bokstav -3 steg.

Poängen med RSA är att göra mötet mellan avsändare och mottagare överflödigt. Tanken är att varje person väljer en nyckel att kryptera med och en nyckel att dekryptera med. Dekrypteringsnyckeln hålls hemlig, men krypteringsnyckeln publiceras offentligt. Detta skulle inte fungera med koderna ovan, eftersom alla som känner till krypteringsnyckeln också automatiskt känner till dekrypteringsnyckeln. I RSA gäller dock att kryptot är konstruerat så att *kunskap om krypteringsnyckeln inte leder till kunskap om dekrypteringsnyckeln*.

Fördelarna med detta är stora. Det blir lätt för en avsändare att skicka krypterade meddelanden till vem som helst i världen, utan att mottagaren och avsändaren

behöver träffas eller förmedla några okrypterade hemligheter. Med detta system kan hemligheter skickas världen över lika lätt som vi skickar ett vanligt epostmeddelande.

Hur ska vi då konstruera detta krypto? Det sker med hjälp av primtal! Med hjälp av Fermats lilla sats kan vi kolla om ett tal är ett primtal. Vi känner å andra sidan inte till någon snabb metod för att finna delarna till ett stort sammansatt tal. Dessa egenskaper gör kryptot möjligt.

Det krypto vi ska studera här kallas RSA, efter upphovsmännen Rivest, Shamir och Adleman. Det upptäcktes under 70-talet och är nu den vanligaste krypteringsmetoden, exempelvis vid kommunikation över internet.

Vi ska nu definiera krypterings- och dekrypteringsfunktionerna till RSA.

Definition 7.2 *Låt p och q vara två primtal och låt $n = pq$ och $m = (p-1)(q-1)$. Välj även två tal e och d sådana att $1 < d, e < m$ och $ed \equiv 1 \pmod{m}$. Då ges krypterings- och dekrypteringsfunktionerna i RSA av*

$$E(x) = x^e \pmod{n}$$

och

$$D(y) = y^d \pmod{n}.$$

Vi ser av definitionen att talen e och n tillhör den offentliga nyckeln som alla känner till, men d måste hållas hemlig. Vi kommer mot slutet av kapitlet gå igenom hur man beräknar d om man känner e och m.

För att dekrypteringsfunktionen ska upphäva verkan av krypteringsfunktionen, så att vi får tillbaka det ursprungliga meddelandet, måste dekrypteringsfunktionen vara invers till krypteringsfunktionen. Vi ska nu bevisa att funktionerna $E(x)$ och $D(y)$ verkligen är varandras inverser.

Sats 7.3 *$D(E(x)) = x$ och $E(D(y)) = y$ för alla positiva heltal x och y mindre än n.*

BEVIS: $D(E(x)) = x$ innebär att $x^{ed} \equiv x \pmod{n}$, det vill säga att $n = pq$ delar $x^{ed} - x$. Det räcker att visa att p och q delar $x^{ed} - x$, eftersom p och q är primtal.

Men här kan vi använda Fermats lilla sats. Eftersom $ed \equiv 1 \pmod{m}$ så är $ed - 1$ en multipel av $m = (p-1)(q-1)$. Vi kan skriva detta som $ed - 1 = k(p-1)(q-1)$ för något heltal k. Fermats lilla sats ger att $x^{p-1} \equiv 1 \pmod{p}$ och vi får

$$x^{ed} \equiv x^{1+k(p-1)(q-1)} \equiv x\ (x^{(p-1)})^{k(q-1)} \equiv x\ 1^{k(q-1)} \equiv x \pmod{p},$$

vilket visar att p delar $x^{ed} - x$. På samma sätt visas att q delar $x^{ed} - x$, och därmed följer att $n = pq$ delar $x^{ed} - x$.

Att visa att $E(D(y)) = y$ ger precis samma räkningar. □

Här följer ett exempel på hur RSA fungerar. För enkelhets skull väljer vi att använda små värden på p och q, så i detta fall är inte kryptot svårt att knäcka.

Exempel 7.4 *Vi väljer två primtal, t.ex.* $p = 7$ *och* $q = 13$*. Vi får då* $n = 7 \cdot 13 = 91$ *och* $m = 6 \cdot 12 = 72$*. Om vi låter* $e = 23$ *kan vi välja* $d = 47$*, eftersom* $e \cdot d \equiv 23 \cdot 47 \equiv 1081 \equiv 15 \cdot 72 + 1 \equiv 1 \pmod{72}$*. Vill vi kryptera* 24 *blir då detta* $24^{23} \equiv 19 \pmod{91}$ *och dekrypterar vi* 19 *får* $19^{47} \equiv 24 \pmod{91}$*.*

Hur gör man egentligen för att utföra dessa beräkningar? Det fungerar inte att på en vanlig miniräknare först beräkna 24^{23} och sedan beräkna dess rest modulo 91. Anledningen är att 24^{23} är ett mycket stort tal, som många miniräknare inte kan hantera. Ett bättre sätt, som också är väldigt effektivt, är följande. Skriv exponenten 23 på binär form (se kapitel 0). Vi får då $23 = (10111)_2$. Genom upprepad kvadrering beräknar vi sedan talen 24^2, 24^4, 24^8 och 24^{16}, hela tiden modulo 91. Eftersom $23 = (10111)_2 = 1 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 1 \cdot 2 + 1 \cdot 1$ följer att $24^{23} = 24^{16+4+2+1} = 24^{16} \cdot 24^4 \cdot 24^2 \cdot 24$. Eftersom vi hela tiden räknar modulo 91 får vi aldrig större tal än miniräknaren klarar av. Vill man räkna på riktigt stora tal bör man dock använda ett lämpligt datorprogram, t.ex. Maple, som hanterar mycket stora tal utan problem.

Exempel 7.5 *I exemplet ovan får vi* $24^2 \equiv 576 \equiv 30 \pmod{91}$*,* $24^4 \equiv 30^2 \equiv 900 \equiv 81 \pmod{91}$*,* $24^8 \equiv 81^2 \equiv 9 \pmod{91}$ *och* $24^{16} \equiv 9^2 \equiv 81 \pmod{91}$*. Därmed får vi* $24^{23} \equiv 81 \cdot 81 \cdot 30 \cdot 24 \equiv 19 \pmod{91}$*.*

7.2 Varför är RSA säkert?

Vi hävdade ovan att RSA är svårt att knäcka. Vi ska nu titta närmare på varför. Om man vill knäcka RSA måste man utgående från de kända nycklarna n och e beräkna någon av de hemliga nycklarna d, m, p eller q (se övningarna). Men för att kunna beräkna d måste vi känna till m, och för att finna m måste vi känna till p och q. Dessa är dock svåra att beräkna, eftersom det i nuläget inte finns någon riktigt snabb metod att faktorisera ett stort heltal. Den enklaste metoden för att faktorisera ett heltal N är att pröva att dela talet med alla primtal mindre än $\sqrt{N}$. Detta tar alldeles för lång tid om N är stort. Det finns metoder som är betydligt snabbare, men även dessa får problem då talen blir omkring 100 siffror långa.

Det är å andra sidan inte svårt att konstruera primtal p och q som är lagom stora. För att skapa ett stort primtal p väljer vi slumpmässigt ett stort tal p'. För att kolla om p' är ett primtal låter vi det genomgå *Fermattestet*.

Fermattestet: Vi ska testa talet p'. Välj slumpmässigt ett tal $a < p'$. Talet a kallas **bas**. Om $a^{p'} \equiv a \pmod{p'}$ så har p' klarat Fermattestet.

Om p' inte klarar Fermattestet vet vi att p' inte är ett primtal, eftersom Fermats lilla sats inte är uppfylld. Annars vet vi att p' kanske är ett primtal. Genom att prova med många olika a får vi ett tillförlitligt test.

Hur stor är sannolikheten att alla baser vi väljer är sådana att ett tal p klarar Fermattestet trots att p är sammansatt. Vi antar det finns någon bas b som gör

att p inte klarar Fermattestet. Då kan man visa att om p klarar Fermattestet med en bas a så kommer p inte att klara Fermattestet med basen $c = ab$. Därav följer att om det finns en bas b sådan att p inte klarar Fermattestet med denna bas, så kommer p att misslyckas i Fermattestet med minst hälften av baserna. Sannolikheten att vi väljer ett tal p' som klarar Fermattestet hundra gånger utan att vara ett primtal blir därför enormt liten (se övningarna).

Det finns emellertid en mängd tal som alltid klarar Fermattestet, trots att de inte är primtal. Dessa kallas *Carmichael-tal*. Dessbättre är de ganska glest utspridda (det minsta är 561). Man kan modifiera testet något så att Carmichael-talen inte klarar detta test.

Om p' inte klarar Fermattestet väljer vi ett annat tal och försöker på nytt tills vi finner ett primtal. Det räcker i allmänhet med 100-200 försök även för mycket stora tal, vilket inte behöver ta mer än några minuter. Sedan finner vi q med samma metod, beräknar n, m, väljer ett e och beräknar d.

I augusti 2002 offentliggjordes en artikel med en ganska snabb och helt säker algoritm för att kolla om ett tal är ett primtal. Algoritmen är dock inte så snabb att den kan konkurrera med Fermattestet. Grundbulten för algoritmen är följande sats, som presenteras utan bevis.

Sats 7.6 *Låt a och p vara relativt prima. Då är p ett primtal om och endast om*

$$(x-a)^p \equiv (x^p - a) \pmod{p}.$$

7.3 Beräkning av d med Euklides algoritm

I vårt exempel ovan hade vi $m = 72$ och $e = 23$, varvid vi konstaterade att $d = 47$ gav $ed \equiv 1 \pmod{m}$. Men hur kunde vi veta att vi skulle prova med 47? Vi ska nu presentera en metod att givet e och m beräkna d så att vi garanterat får $ed \equiv 1 \pmod{m}$. Metoden kallas Euklides algoritm.

Att $ed \equiv 1 \pmod{m}$ innebär att $de = 1 + km$ för något heltal k. Det räcker alltså att finna heltal d och k så att $de - km = 1$. En sådan ekvation kallas *diofantisk*, och den har alltid en lösning om e och m är relativt prima (se avsnitt 0). Vi ska därför välja e så att e och m är relativt prima. Ovan valde vi $e = 23$, vilket är ett primtal. Dess enda delare är 23 (och 1), och eftersom 23 inte delar 72 är de relativt prima. Vi ska nu beräkna lösningen med hjälp av Euklides algoritm.

Eftersom 23 inte delar 72 får vi en rest när vi delar 72 med 23. Vi ser att $72 = 3 \cdot 23 + 3$. Man kan nu visa (se övningarna) att om $a = pb + q$ och a och b är relativt prima, så är också b och q relativt prima (se kapitel 0 för definition av relativt prima). I vårt fall innebär det att 23 och 3 är relativt prima. Vi kan nu fortsätta beräkningarna på samma sätt, men istället för 72 och 23 använder vi 23 och 3. Vi får då tabellen nedan.

$$\begin{aligned} 72 &= 3 \cdot 23 + 3 \\ 23 &= 7 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

När vi som ovan når 1 slutar vi.

Med hjälp av denna tabell kan vi lösa vår diofantiska ekvation. Titta på nedersta raden. Om vi löser ut 1 får vi $1 = 3 - 1 \cdot 2$. På raden ovanför står en tvåa längst till höger, så om vi löser ut tvåan där kan vi ersätta tvåan i vår nuvarande likhet med högre tal. Vi får

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (23 - 7 \cdot 3) = 8 \cdot 3 - 1 \cdot 23.$$

Vi använder nu den översta raden ovan för att bli av med vår trea. Detta ger

$$1 = 8 \cdot 3 - 1 \cdot 23 = 8 \cdot (72 - 3 \cdot 23) - 1 \cdot 23 = -25 \cdot 23 + 8 \cdot 72.$$

Ur denna ekvation ser vi att vi kan välja $d = -25 \equiv 47 \pmod{72}$ och $k = -8$. Det är egentligen bara d vi är intresserade av, men det går inte att beräkna d utan att beräkna k.

7.4 Elektroniska signaturer

Avslutningsvis kan det vara intressant att säga några ord om elektroniska signaturer. Om en person B får ett meddelande från en annan person A, så kan ju B i allmänhet inte vara säker på att det är A som har skickat meddelandet. När exempelvis en bank får meddelandet att alla pengar på ett konto ska sättas in på ett konto i Schweiz, så måste de veta att det är kontohavaren som skickat meddelandet. Detta problem kan vi lösa med RSA.

I RSA krypterar vi oftast med krypteringsnyckeln $E_A(x)$ och dekrypterar med dekrypteringsnyckeln $D_A(x)$. Av sats 7.3 att döma finns det dock inget som hindrar att vi gör tvärtom. Det vi får då är ett meddelande som bara A kan ha krypterat, eftersom A är den enda som känner till $D_A(x)$, men alla kan läsa meddelandet, eftersom alla känner till $E_A(x)$. Det är inte lämpligt att skicka ett meddelande krypterat med $D_A(x)$, eftersom alla kan läsa det, men om A krypterar med $D_A(x)$ och sedan med $E_B(x)$ så kan bara B läsa det. B dekrypterar först med sin egen nyckel $D_B(x)$ och sedan med den allmänt kända nyckeln $E_A(x)$. Om det inte hade varit A som skickat meddelandet hade B inte fått något vettigt meddelande.

7.5 Övningar

Övning 7.1 *Kryptera meddelandena 6 och 17 med nycklar $n = 35$ och $e = 7$. Dekryptera 3 utan att beräkna d.*

Övning 7.2 *Låt $n_A = 91, e_A = 5, d_A = 29, N_B = 35$ och $e_B = 7$. Antag att A vill skicka 3 till B med elektronisk signatur. Vilket meddelande skickar A?*

Övning 7.3 *En person med offentliga nycklar $n = 187$ och $e = 23$ har skickat meddelandet 2, vilket du har uppsnappat genom att tjuvlyssna. Dekryptera meddelandet genom att knäcka koden, det vill säga genom att beräkna de privata nycklarna.*

Övning 7.4 *Om ett tal p inte är ett primtal kommer mer än hälften av alla $a < p$ ge $a^p \not\equiv a \pmod{p}$. Sannolikheten att p klarar Fermattestet är därför mindre än $\frac{1}{2}$. Antag att vi, när vi skapar primtal för RSA, använder Fermattestet hundra gånger innan vi godkänner ett tal. Antag också att det skapas en miljon par (p, q) om dagen. Är det troligt att någon under de närmsta hundra åren kommer att få ett par (p, q) där något av p och q inte är ett primtal?*

Övning 7.5 *Visa att om $a = pb + q$ och a och b är relativt prima, så är också b och q relativt prima.* Tips*: Antag motsatsen, d.v.s. att $\mathrm{sgd}(b, q) = d > 1$ och visa att detta medför att $\mathrm{sgd}(a, b) > 1$. I så fall kan inte a och b vara relativt prima samtidigt som b och q inte är det.*

Övning 7.6 *Visa att om e och m inte är relativt prima, så saknar den diofantiska ekvationen $ed - km = 1$ lösningar.* Tips*: Enligt aritmetikens fundamentalsats har vänsterled och högerled samma delare. Vilka tal delar vänsterledet och vilka delar högerledet?*

Övning 7.7 *Visa att om man, förutom n och e, känner till någon av de andra nycklarna d, m, p och q, så kan man lätt beräkna övriga nycklar. Ett tips är att, om man känner m, utnyttja likheten $(x - p)(x - q) = x^2 - (n - m + 1)x + n$ och finna nollställena till denna ekvation (om du utnyttjar den måste du också visa att den är sann).*

Övning 7.8 *Visa att om p klarar Fermattestet med bas a, men inte klarar Fermattestet med bas b, så klarar det inte heller Fermattestet med bas ab. Du bör använda omformuleringen av Fermats sats att om p inte delar a och p är ett primtal så gäller $a^{p-1} \equiv 1 \pmod{p}$.*