Linjär algebra

Tio förrätter och två efterrätter

Roy Skjelnes

Matematiska Institutionen, KTH.

Typsatt med LaTeX 2$_\varepsilon$ och Ti*k*Z.
Kompilerad 8 september 2014.

Inledande ord

Detta häfte är baserat på en föreläsningsserie jag gav 2010–2011. Varje kapitel motsvarar en föreläsning, och riktar sig till gymnasieelever som läser kursen Linjär algebra för gymnasister. I år består kursen av 12 föreläsningar, och inte 16 som var antalet 2010–2011. De fyra föreläsningarna jag har skurit bort från den ursprungliga kursen finns med som Appendix.

Föreläsningarna är inspirerade och modellerade efter kurshäftet "Matriser og Vektorrom" av Dan Laksov.

Under läsåret 2010–2011 hittade eleverna flera fel i föreläsningsnotaten, och speciellt vill jag nämna Andrian Kimiaei (Norra Real), André Sahlsten (Farsta Gymnasium) och Omar Wazir (Huddinge Gymnasium). Läsåret 2011–2012 hittade Jacob Lindberg (Kärrtorp), Sebastian Strandh (Östra Real) och Ludvig Pucek (Östra Real) ytterligare fel. Sedan har Robin Saaristo (Bromma) kölhalat min svorska med att rätta hundratals fel i de första 6 kapitlen. I 2013–2014 satt Hampus Söderström i Strängnäs och gav min svorska ytterligare en kölhalning, och även andra grammatiska fel fick på foten. Jag mistänker nu att de sex första kapitlen är när intil fria från fel — och om inte så innehållt dessa kapitel mer felaktigheter enn korrektheter.

Leta upp flera fel, det är "gøy" och lärorikt.

Lycka till!

Roy Skjelnes
Stockholm, 25:e juni, 2014.

Förord till reviderad upplaga

Inför läsåret 2014–2015 så har jag gjort en översyn av häftet, korrigerat språket något, rättat några smärre matematiska fel samt lagt till några figurer.

David Rydh
Stockholm, 5:e september, 2014.

Innehåll

Föreläsning 1

Matrisaritmetik

1.1 Matriser

Vi skall definiera något som kallas (2×2)-matriser och sedan utveckla aritmetik på dessa. Matriserna är inte tal, men kan nästan behandlas som tal.

Definition 1.1.1. En (2×2)-matris $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ är fyra reella tal a, b, c, d ordnade i en rektangel.

1.1.2. När vi i detta kapitel skriver matris menar vi alltid en (2×2)-matris.

Exempel 1.1.3. Exempel på matriser är

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \quad \begin{bmatrix} 1 & \pi \\ 1 & 0 \end{bmatrix}.$$

Definition 1.1.4. Två matriser $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ och $B = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ adderas och ger en ny matris

$$A + B = \begin{bmatrix} a + \alpha & b + \beta \\ c + \gamma & d + \delta \end{bmatrix}.$$

Exempel 1.1.5. Vi ser att $A + B = B + A$.

1.2 Skalärmultiplikation

Vi har att

$$A + A = \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix},$$

och detta skriver vi som $2A$. Vi gör följande definition.

Definition 1.2.1 (Skalärmultiplikation)**.** För varje tal k och varje matris A, definierar vi matrisen

$$k \cdot A = \begin{bmatrix} ka & kb \\ kc & kd \end{bmatrix}.$$

1.2.2. Av definitionen av skalärmultiplikationen får vi att

$$\underbrace{A + A + \cdots + A}_{n \text{ kopior}} = n \cdot A.$$

Vi har också att

$$0 \cdot A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Matrisen som bara består av nollor kallas noll-matrisen av uppenbara skäl. Vi skriver $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ för denna matris. Och vi har

$$0 \cdot A = 0.$$

Notera att 0 i vänsterledet ovan är talet 0, medan 0 i högerledet ovan är noll-matrisen. Vi har också den trevliga identiteten av matriser

$$A + 0 = A.$$

Mera notation: vi har

$$-1 \cdot A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}.$$

I fortsättningen skriver vi $-A$ för matrisen $-1 \cdot A$. Detta betyder att vi istället för $B + -1 \cdot A$ skriver $B - A$. Notera också att vi nu har

$$\underbrace{-A - A \cdots - A}_{n \text{ kopior}} = -n \cdot A.$$

Vidare är skalärmultiplikation *distributiv*, dvs

$$(k + \ell) \cdot A = k \cdot A + \ell \cdot A$$
$$k \cdot (A + B) = k \cdot A + k \cdot B$$

där k och ℓ är tal och A och B är matriser.

Exempel 1.2.3. Vi kan nu lösa matrisekvationer på formen

$$4X + 2A = B,$$

där A och B är givna matriser. Vi adderar matrisen $-2A$ på båda sidor och får att vänsterledet blir

$$4X + 2A - 2A = 4X + 0 = 4X,$$

medan högerledet blir $B-2A$. Sedan multiplicerar vi ekvationen med skalären $\frac{1}{4}$, vilket ger

$$X = \frac{1}{4}B - \frac{1}{2}A.$$

1.3 Matrismultiplikation

Vi har definierat addition (och subtraktion) av matriser samt skalärmultiplikation. Vi vill också ha multiplikation: två matriser skall multipliceras ihop och ge en matris. Innan vi definierar detta ska vi skriva matriserna lite annorlunda. En matris

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix}$$

består av två rader och två kolumner. Talen i matrisen kallas element och är indexerade efter vilken rad och kolumn dessa står placerade i. Exempelvis har vi att elementet $a_{1,2}$ är i rad 1 och kolumn 2.

Definition 1.3.1. Låt $A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix}$ och $B = \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix}$ vara två matriser. Vi definierar produkten AB som matrisen

$$AB = \begin{bmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{bmatrix}$$

där elementen ges av följande formler

$$\begin{aligned} c_{1,1} &= a_{1,1}b_{1,1} + a_{1,2}b_{2,1} \\ c_{1,2} &= a_{1,1}b_{1,2} + a_{1,2}b_{2,2} \\ c_{2,1} &= a_{2,1}b_{1,1} + a_{2,2}b_{2,1} \\ c_{2,2} &= a_{2,1}b_{1,2} + a_{2,2}b_{2,2}. \end{aligned}$$

1.3.2. Ser ni mönstret i galenskapen och speciellt hur man kommer ihåg formlerna utan att lära dessa utantill? Om du inte ser mönstret be någon, gärna mig, att förklara hur man utför matrismultiplikationen.

Exempel 1.3.3. Vi har att

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 2 & -1 \end{bmatrix} = \begin{bmatrix} 4 & -1 \\ 8 & -1 \end{bmatrix}.$$

Notera att AB inte alltid är detsamma som BA. Vi har nämligen att

$$\begin{bmatrix} 0 & 1 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ -1 & 0 \end{bmatrix}$$

vilket inte är lika med produkten ovan. Vidare har vi att nollmatrisen multiplicerad med en godtycklig matris ger nollmatrisen $A \cdot 0 = 0 \cdot A = 0$. Notera att när vi nu skrev $0 \cdot A$ så var det en produkt av två matriser, matrisen A och nollmatrisen 0. Men när vi i Avsnitt 1.2.2 använde precis samma notation och skrev $0 \cdot A$ så menade vi talet 0 och skalärmultiplikation.

Definition 1.3.4. Vi definierar identitetsmatrisen $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

1.3.5. Identitetsmatrisen fungerar som talet 1 med avseende på matrismultiplikation. Vi har nämligen att

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,1} \end{bmatrix} = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,1} \end{bmatrix}.$$

Det vill säga att $1 \cdot A = A$ för varje matris A. Vi har också att $A \cdot 1 = A$ vilket läsaren uppmuntras kontrollera. Återigen så noterar vi att vi använder en och samma symbol, nämligen 1, för två olika saker; identitetsmatrisen och talet 1. Speciellt kan vi med $1 \cdot A$ avse antingen skalärmultiplikation av talet 1 med matrisen A eller identitetsmatrisen multiplicerad med matrisen A.

Sats 1.3.6. *Låt A, B och C vara godtyckliga matriser.*

1) Matrismultiplikation är associativ, det vill säga

$$(AB)C = A(BC).$$

2) Matrismultiplikation är distributiv, det vill säga

$$(A + B)C = AC + BC, \quad A(B + C) = AB + AC.$$

Bevis. Se Uppgift 1.5. □

Definition 1.3.7. En matris A är *inverterbar* om det finns någon matris B sådan att

$$AB = 1 \quad \text{och} \quad BA = 1.$$

En matris som inte är inverterbar kallas singulär.

Exempel 1.3.8. Matrisen

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

är inverterbar. Detta eftersom matrisen

$$B = \begin{bmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{bmatrix}$$

har egenskapen att $AB = BA = 1$ (Kolla!).

Exempel 1.3.9. Nollmatrisen är uppenbarligen singulär. Ett annat exempel är matrisen

$$A = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}.$$

Att matrisen A är singulär kan man visa på följande sätt. Antag att A är inverterbar. Då finns en matris $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ sådan att $AB = BA = 1$. Produkten AB är

$$\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ 2a & 2b \end{bmatrix}.$$

Om denna produkt skulle vara lika med identitetsmatrisen måste $a = 1$ och $2a = 0$ samt $b = 0$ och $2b = 1$. Detta är omöjligt vilket betyder att matrisen A inte kan vara inverterbar. Alltså är matrisen singulär.

Sats 1.3.10. *Om matrisen A är inverterbar finns enbart en matris B sådan att $AB = BA = 1$.*

Bevis. Låt B och C vara två matriser sådana att $AB = BA = 1$ och $AC = CA = 1$. Vi skall visa att $B = C$. Vi har

$$B = B \cdot 1 = B \cdot (AC) = (BA) \cdot C = 1 \cdot C = C.$$

vilket var vad vi skulle visa. □

1.3.11. Om en matris A är inverterbar kallas matrisen B som är sådan att $AB = BA = 1$ för inversen till A. Inversen till A betecknar vi med A^{-1}.

Exempel 1.3.12. Betrakta nu en matrisekvation $AX = B$ där A och B är givna matriser och X är den sökta matrisen. Om matrisen A är inverterbar kan vi lösa denna uppgift på vanligt sätt, det vill säga som om det handlade om vanliga tal. Ekvationen $AX = B$ multiplicerar vi med A^{-1}, från *vänster*, och vi får att

$$1 \cdot X = A^{-1}AX = A^{-1}B.$$

Det vill säga $X = A^{-1}B$.

1.4 Uppgifter

Uppgift 1.1. Beräkna matriserna AB, BA och A^2 när

$$A = \begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix} \quad \text{och} \quad B = \begin{bmatrix} 2 & \frac{1}{3} \\ 4 & 5 \end{bmatrix}.$$

Uppgift 1.2. Låt $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ vara en matris där $ad - bc \neq 0$. Definiera matrisen

$$B = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Använd matrisen B för att visa att matrisen A är inverterbar.

Uppgift 1.3. Använd Uppgift 1.2 för att konstruera inversen till matriserna

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 3 & 2 \\ 1 & 2 \end{bmatrix}.$$

Uppgift 1.4. Använd matriserna i Uppgift 1.3 för att bestämma matrisen X i följande tre uttryck

$$a)\ AX = B \quad b)\ XA = B \quad \text{och} \quad c)\ AXB = 1.$$

Uppgift 1.5. Betrakta tre godtyckliga matriser A, B och C. Beräkna först AB och BC, och sedan $(AB)C$ och $A(BC)$. Om du nu har räknat rätt är de två matriserna lika, det vill säga $(AB)C = A(BC)$, och du har visat första delen av Sats 1.3.6. Du kan göra likadant för att visa distributivitet.

Föreläsning 2

Matrisaritmetik II

Vi definierade förra gången (2×2)-matriser och multiplikation av sådana. Idag skall vi definiera dessa begrepp mer allmänt.

2.1 Matriser

Låt m och n vara två fixerade positiva heltal. En $(m \times n)$-matris A är en ordnad rektangel med $m \cdot n$ tal,

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix}.$$

Lägg märke till att en $(m \times n)$-matris består av m rader och n kolumner. Talen i matrisen A kallas *element* och indexeringen av dessa ges av rad och kolumn. Elementet $a_{i,j}$ är placerad på rad i och på kolumn j. En kompakt notation för matrisen är $A = (a_{i,j})$, där vi inte ens indikerar antalet rader och kolumner i matrisen. Med *storleken* av en matris avses antalet rader och kolumner.

Exempel 2.1.1. Exempel på matriser är

$$\begin{bmatrix} 1 & 2 & 3 \end{bmatrix}, \quad \begin{bmatrix} 1 & \pi \\ 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

Den första matrisen är en (1×3)-matris och den andra är en (3×2)-matris.

Definition 2.1.2. Två matriser A och B av samma storlek adderas elementvis och ger en ny matris av samma storlek. Om k är ett tal, så definieras skalärmultiplikationen $k \cdot A$ som matrisen av samma storlek som A, men där varje element är multiplicerad med k.

Exempel 2.1.3. Vi ser att $A + B = B + A$.

2.1.4. Innan vi definierar matrisprodukten inför vi lite summationsnotation. Vi använder symbolen $\sum$ för summa och speciellt använder vi symbolen för att på ett kompakt sätt beskriva summering. Om vi har talen $a_1, \ldots, a_n$ och vill summera dessa skriver vi

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n.$$

Lägg märke till att nedre index indikerar var summationen börjar och övre index indikerar var summationen slutar.

Exempel 2.1.5. Till exempel skriver vi

$$\sum_{i=3}^{7} a_i = a_3 + a_4 + a_5 + a_6 + a_7,$$

och

$$\sum_{i=3}^{5} (13 - i)^{2i} = 10^6 + 9^8 + 8^{10}.$$

2.2 Matrismultiplikation

Vi har hittills definierat addition (och subtraktion) av matriser samt skalärmultiplikation. I detta avsnitt definierar vi multiplikation av två matriser.

Definition 2.2.1. Låt A vara en $(m \times p)$-matris och B en $(p \times n)$-matris. Vi definierar produkten AB som $(m \times n)$-matrisen med elementen

$$c_{i,j} = \sum_{k=1}^{p} a_{i,k} b_{k,j},$$

där $1 \leq i \leq m$ och $1 \leq j \leq n$.

Exempel 2.2.2. Betrakta matriserna

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & -1 & 0 \end{bmatrix} \quad \text{och} \quad B = \begin{bmatrix} 1 & -1 \\ 0 & 1 \\ 1 & 1 \\ 2 & 1 \end{bmatrix}.$$

Matrisen A är (2×4) och B är (4×2). Detta betyder att vi kan utföra produkten

$$AB = \begin{bmatrix} 1+0+3+8 & -1+2+3+4 \\ 0+0-1+0 & 0+1-1+0 \end{bmatrix} = \begin{bmatrix} 12 & 8 \\ -1 & 0 \end{bmatrix},$$

men också produkten

$$BA = \begin{bmatrix} 1+0 & 2-1 & 3+1 & 4+0 \\ 0+0 & 0+1 & 0-1 & 0+0 \\ 1+0 & 2+1 & 3-1 & 4+0 \\ 2+0 & 4+1 & 6-1 & 8+0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 4 & 4 \\ 0 & 1 & -1 & 0 \\ 1 & 3 & 2 & 4 \\ 2 & 5 & 5 & 8 \end{bmatrix}.$$

2.2.3. Nollmatrisen, som är matrisen där alla element är noll, skriver vi fortfarande 0. Läsaren måste själv ha koll på vilken storlek nollmatrisen har. För varje positivt heltal n definierar vi identitetsmatrisen 1 som $(n \times n)$-matrisen

$$1 = (\delta_{i,j}) \quad \text{där} \quad \delta_{i,j} = \begin{cases} 1 & \text{om} \quad i = j \\ 0 & \text{om} \quad i \neq j. \end{cases}$$

Symbolen $\delta_{i,j}$ kallas Kroneckers delta. Inversen till en $(n \times n)$-matris A definieras som $(n \times n)$-matrisen B som har egenskapen att $AB = BA = 1$, där 1 betyder identitetsmatrisen av storlek $(n \times n)$. Inte alla matriser har invers, men om en matris A har en invers så är denna unik och vi skriver A^{-1} för denna matris.

Exempel 2.2.4. Betrakta matriserna

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{bmatrix} \quad \text{och} \quad B = \begin{bmatrix} -40 & 16 & 9 \\ 13 & -5 & -3 \\ 5 & -2 & -1 \end{bmatrix}.$$

Om vi utför matrismultiplikationen AB korrekt får vi

$$AB = \begin{bmatrix} -40+26+15 & 16-10-6 & 9-6-3 \\ -80+65+15 & 32-25-6 & 18-15-3 \\ -40+40 & 16-16 & 9-8 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Läsaren kan själv kontrollera att $BA = 1$. Detta betyder att $B = A^{-1}$ men också att $A = B^{-1}$.

Exempel 2.2.5. Betrakta ekvationssystemet

$$\begin{aligned} x + 2y + 3z &= 4 \\ 2x + 5y + 3z &= 2 \\ x + 8z &= 1. \end{aligned}$$

Detta system kan skrivas som matrisekvationen

$$A \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \\ 1 \end{bmatrix},$$

där A är matrisen

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{bmatrix}.$$

Vi såg i Exempel 2.2.4 att matrisen

$$B = \begin{bmatrix} -40 & 16 & 9 \\ 13 & -5 & -3 \\ 5 & -2 & -1 \end{bmatrix}$$

är inversen till A, det vill säga $B = A^{-1}$. Multiplicerar vi matrisekvationen med A^{-1} från vänster får vi

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = A^{-1}A \begin{bmatrix} x \\ y \\ z \end{bmatrix} = A^{-1} \begin{bmatrix} 4 \\ 2 \\ 1 \end{bmatrix}.$$

Vi har vidare att

$$A^{-1} \begin{bmatrix} 4 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} -119 \\ 39 \\ 15 \end{bmatrix}.$$

Detta betyder att ekvationssystemet har den unika lösningen $x = -119$, $y = 39$ och $z = 15$.

2.3 Uppgifter

Uppgift 2.1. Beräkna matrisprodukten

$$\begin{bmatrix} 1 & 3 & -1 \\ 0 & 1 & 2 \\ 1 & 1 & 1 \\ 0 & 0 & -2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ -1 & -1 \end{bmatrix}.$$

Uppgift 2.2. Använd informationen i Exempel 2.2.4 för att lösa matrisekvationen

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}.$$

Uppgift 2.3. Två personer är och dricker två sorters läsk. Den ena personen konsumerar 15 glas av sort A och 10 glas av sort B. Detta kostar 63 SEK. Den andra personen konsumerar 25 glas av sort A och 17 glas av sort B, till en summa av 106 SEK. Hur mycket kostade sort A per glas? Lös denna uppgift på följande sätt: Först skriver du ekvationerna som kommer från texten på matrisform. Sedan inverterar du den givna (2×2)-matrisen (använd formeln som gavs i förra föreläsningen) och multiplicerar med inversen från vänster.

Uppgift 2.4. Låt A vara en godtycklig $(m \times n)$-matris och låt 1 vara identitetsmatrisen av rätt storlek. Visa att $A \cdot 1 = A$.

Föreläsning 3

Avbildningar av planet

3.1 Euklidiska planet

Vi kommer att behandla linjära avbildningar av planet i detalj. Det mer allmänna fallet behandlas i Appendix B.

Definition 3.1.1. Det euklidiska planet är mängden av alla ordnade par av reella tal. Denna mängd skriver vi som $\mathbf{R}^2$. Med andra ord

$$\mathbf{R}^2 = \{(x, y) \mid x \text{ och } y \text{ är reella tal}\}.$$

Elementen i $\mathbf{R}^2$ kallar vi ofta för *punkter* och vi identifierar punkten (x, y) med (2×1)-matrisen $\begin{bmatrix} x \\ y \end{bmatrix}$, en så kallad *kolumnvektor*.

Planet känner vi oss förtroliga med. Vi skall nu börja titta på en klass av avbildningar från planet till sig självt.

3.2 Matrisavbildningar

Låt $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ vara en fixerad (2×2)-matris. Vi använder denna för att definiera en avbildning

$$T_A \colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$$

på följande sätt. Låt (x, y) vara ett godtyckligt element i $\mathbf{R}^2$. Vi definierar

$$T_A(x, y) = (ax + by, cx + dy).$$

Detta anger vad elementet (x, y) skall skickas till, nämligen elementet $(ax + by, cx + dy)$. Sättet vi använder matrisen A på är som följer. Vi tar det

godtyckliga elementet (x, y) och skriver detta som en (2×1)-matris, vilket sedan multipliceras med matrisen A från vänster:

$$(x, y) = \begin{bmatrix} x \\ y \end{bmatrix} \mapsto A \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix} = (ax + by, cx + dy).$$

Efter matrismultiplikation med A har vi en (2×1)-matris, dvs en kolumnvektor, vilket vi betraktar som en punkt $(ax + by, cx + dy)$ i planet.

Exempel 3.2.1. Låt $A = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$. Denna matris ger avbildningen

$$T_A \colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$$

som skickar elementet (x, y) till $(2x + y, 4x + 3y)$. Speciellt ser vi att $(1, 0)$ skickas till $(2, 4)$ och att $(0, 1)$ skickas till $(1, 3)$. Vidare skickas $(1, 1)$ till $(3, 7)$ och $(0, 0)$ till $(0, 0)$. Det kan nu vara instruktivt att rita upp kvadraten med hörn i punkterna $(0, 0)$, $(1, 0)$, $(0, 1)$ och $(1, 1)$ och sedan se vad denna kvadrat skickas till under avbildningen T_A.

3.3 Linjäritet

I Exempel 3.2.1 ovan kan vi notera att första kolumnen i matrisen A är koordinaterna för $T(1, 0)$ och att andra kolumnen är koordinaterna till $T(0, 1)$. Dessa två element kommer att spela en viktig roll i fortsättningen så vi ger dessa egna namn.

Definition 3.3.1. Elementet $(1, 0)$ skriver vi som e_1 och elementet $(0, 1)$ skriver vi som e_2. Dessa två element kallas *standardbasen* för $\mathbf{R}^2$.

3.3.2. Låt oss återgå till Exempel 3.2.1. Elementet $(1, 1) = e_1 + e_2$ och vi har att $T_A(1, 1)$ ges som matrismultiplikation med matrisen A från vänster. Notera dock att vi har

$$A \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} = A \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + A \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Med andra ord har vi att $T_A(1, 1) = T_A(e_1) + T_A(e_2)$.

Lemma 3.3.3. *Låt A vara en (2×2)-matris och betrakta den inducerade avbildningen $T_A \colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$. För varje element (x, y) i $\mathbf{R}^2$ har vi att*

$$T_A(x, y) = xT_A(e_1) + yT_A(e_2).$$

Bevis. Vi har att $(x, y) = (x, 0) + (0, y) = x \cdot (1, 0) + y \cdot (0, 1)$. Matrismultiplikation, som är distributiv, ger nu

$$A \cdot \begin{bmatrix} x \\ y \end{bmatrix} = A \cdot \left(x \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = x \cdot A \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y \cdot A \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Med andra ord $T_A(x, y) = xT_A(e_1) + yT_A(e_2)$. □

Definition 3.3.4. En avbildning $f\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ kallas *linjär* om

$$f(x, y) = x \cdot f(e_1) + y \cdot f(e_2)$$

för alla element (x, y) i $\mathbf{R}^2$.

3.3.5. Avbildningar i allmänhet kan vara obeskrivligt komplicerade, men dessa skall vi inte fokusera på. Vi skall enbart betrakta linjära avbildningar. En linjär avbildning är bestämd av sitt värde på två element, nämligen e_1 och e_2. Vi har sett att en matrisavbildning T_A, det vill säga en avbildning som kommer från multiplikation med en matris A är linjär. Detta är nämligen kontentan av Lemma 3.3.3. Det omvända gäller också.

Sats 3.3.6. *Låt $f\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ vara en linjär avbildning. Då finns en (2×2)-matris A sådan att matrisavbildningen T_A är den linjära avbildningen f. Mera precist har vi att om $f(e_1) = (a, b)$ och $f(e_2) = (c, d)$ då ges avbildningen f av matrisen*

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}.$$

Bevis. Se uppgifterna. □

3.3.7. Notera att koordinaterna till $f(e_1)$ kommer som första *kolumn*, ej rad, i matrisen A. På samma sätt är koordinaterna till $f(e_2)$ andra kolumn i matrisen.

Exempel 3.3.8. Låt $f\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ vara givet som spegling i y-axeln. Då har vi att

$$f(x, y) = (-x, y). \tag{3.3.8.1}$$

Vi ska verifiera att detta är en linjär avbildning. Vi har att $f(e_1) = (-1, 0)$, vilket också kan skrivas $f(e_1) = -e_1$. Vi har att $f(e_2) = (0, 1) = e_2$. Låt nu (x, y) vara en given punkt i planet. Vi har att

$$f(x, y) = (-x, y) = x(-1, 0) + y(0, 1) = x \cdot f(e_1) + y \cdot f(e_2).$$

Alltså är avbildningen linjär. Detta ger matrisen $A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$. Det betyder att

$$A \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -x \\ y \end{bmatrix},$$

vilket sammanfaller med uttrycket (3.3.8.1).

Exempel 3.3.9. Låt $f\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ vara rotation med $\frac{\pi}{3}$ radianer (eller om du vill 60 grader) moturs omkring origo, dvs punkten $(0,0)$. Detta är en linjär avbildning, vilket betyder att det finns en matris A sådan att $T_A = f$. Om man ritar en tydlig figur ser man att

$$f(e_1) = \left(\cos\frac{\pi}{3}, \sin\frac{\pi}{3}\right) = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right).$$

Den triangel som förekommer i denna tänkta figur förekommer också i din figur när du beskriver $f(e_2)$. Du får att

$$f(e_2) = \left(-\sin\frac{\pi}{3}, \cos\frac{\pi}{3}\right) = \left(-\frac{\sqrt{3}}{2}, \frac{1}{2}\right).$$

Detta ger matrisen

$$A = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{3} & \frac{1}{2} \end{bmatrix}.$$

Speciellt betyder detta att $f(2,5)$ har koordinaterna

$$A \cdot \begin{bmatrix} 2 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 - \frac{5}{2}\sqrt{3} \\ \sqrt{3} + \frac{5}{2} \end{bmatrix}.$$

Definition 3.3.10. Bildrummet till en avbildning $f\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ är alla punkter (y_1, y_2) som är på formen $(y_1, y_2) = f(x_1, x_2)$ för någon punkt (x_1, x_2).

3.4 Uppgifter

Uppgift 3.1. Låt $f\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ vara rotation med $\frac{\pi}{4}$ radianer omkring origo $(0,0)$ men *medurs*. Avbildningen är linjär. Beskriv matrisen A som är sådan att $f = T_A$.

Uppgift 3.2. Avbildningen $T_A\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ ges av matrisen

$$A = \begin{bmatrix} 1 & -2 \\ -3 & 6 \end{bmatrix}.$$

Visa att punkten $P = (-1, 3)$ är med i bildrummet till avbildningen T_A. Bestäm också en punkt Q som inte är med i bildrummet till T_A.

Uppgift 3.3. Visa Sats 3.3.6. Låt f vara en avbildning från planet till planet och konstruera matrisen A som Sats 3.3.6 anger. Använd nu linjäriteten för f till att visa att $f(x, y) = T_A(x, y)$ för alla (x, y) i $\mathbf{R}^2$, vilket betyder att $f = T_A$.

Uppgift 3.4. Låt $T_A \colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ vara den linjära avbildning vi får vid rotation med θ grader, moturs, omkring origo. Använd en bra figur och visa att matrisen A som beskriver avbildningen T_A är

$$A = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}.$$

Föreläsning 4

Geometri i planet

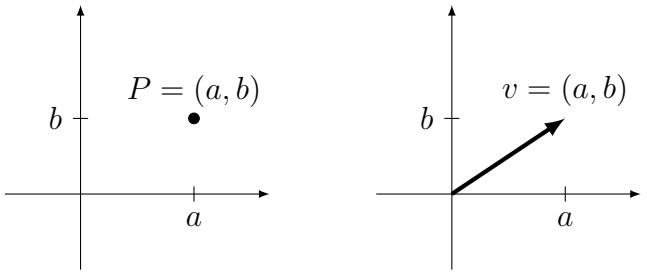
När du läser denna text är det bra om du ritar bilder för att exemplifiera innehållet.

4.1 Vektorer och ortogonalitet

Det euklidiska planet betecknas med $\mathbf{R}^2$ och är mängden av alla ordnade par av reella tal,

$$\mathbf{R}^2 = \{(a, b) \mid \text{reella tal } a \text{ och } b\}.$$

Ett element (a, b) i $\mathbf{R}^2$ kallas ibland för en punkt $P = (a, b)$ och ibland för en vektor $v = (a, b)$. Även om det används olika namn för element i planet är det viktigt att komma ihåg att det alltid handlar om samma begrepp. Anledningarna till de olika namnen är mera av psykologisk art. Bland annat ritar vi en punkt $P = (a, b)$ som en prick i planet, medan en vektor $v = (a, b)$ ofta ritas som en pil som börjar i origo och slutar i (a, b). Både punkter och vektorer kan betraktas som (2×1)-matriser, så kallade kolumnvektorer. Bara undantagsvis betraktas punkter och vektorer som (1×2)-matriser, så kallade radvektorer.



Definition 4.1.1. Längden av en vektor $v = (a, b)$ är definierad som talet $\sqrt{a^2 + b^2}$ och vi skriver $\|v\|$ för detta tal.

4.1.2. Det är klart att det är Pythagoras sats som ligger till grund för definitionen ovan. Ritar man upp vektorn $v = (a, b)$ som en pil ser vi att pilens längd blir hypotenusan i en triangel där kateterna har längd $|a|$ och $|b|$.

4.1.3. Vi noterar att längden till en vektor $v = (a, b)$ alltid är ett icke-negativt tal, och att den enda vektorn med längd $\|v\| = 0$ är noll-vektorn $v = (0, 0)$.

Definition 4.1.4. Betrakta två vektorer $u = (a, b)$ och $v = (c, d)$. Deras *skalärprodukt* är talet definierat som

$$\langle u, v \rangle = ac + bd.$$

Exempel 4.1.5. Om $n = (a, b)$ är en vektor har vi att

$$\langle n, n \rangle = a^2 + b^2 = \|n\|^2.$$

Lemma 4.1.6. *För alla vektorer u, v och w och alla reella tal t har vi att följande identiteter gäller*

1) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$

2) $\langle tu, w \rangle = t\langle u, w \rangle$.

Bevis. Se uppgifterna. □

Definition 4.1.7. Två vektorer u och v är *vinkelräta* (och ibland säger vi ortogonala) om deras skalärprodukt $\langle u, v \rangle = 0$.

Exempel 4.1.8. Betrakta vektorn $u = (2, 5)$ och vektorn $v = (-10, 4)$. Dessa två vektorer är vinkelräta ty

$$\langle u, v \rangle = 2 \cdot (-10) + 5 \cdot 4 = 0.$$

4.2 Linjer

Låt $P = (p_1, p_2)$ vara en punkt och $v = (c, d)$ en vektor skild från nollvektorn $(0, 0)$. Ritar du in punkterna

$$P + v, \quad P + 2v, \quad P + 3v, \quad P - v, \quad P + \frac{3}{2}v$$

så inser du att alla dessa ligger på linjen som går genom punkten P och har riktning v. Vi definierar linjen L, genom punkten P och med *riktningsvektor* v, som mängden

$$L = \{P + tv \mid t \text{ är ett reellt tal}\}.$$

4.2.1. Notera att mängden som en linje L utgör kan skrivas med en massa olika riktningsvektorer och olika punkter. Om P' är någon punkt på linjen L och vektorn v' är nollskild, och sådan att $v' = s \cdot v$ för något tal s, då har vi att

$$L = \{P + tv \mid \text{reella tal } t\} = \{P' + tv' \mid \text{reella tal } t\}.$$

4.2.2. Med riktningsvektorn v till linjen L fixerad får vi parallella linjer $L' = \{Q + tv \mid \text{reella tal } t\}$ till $L = \{P + tv \mid \text{reella tal } t\}$, när vi varierar punkten som riktningsvektorn utgår ifrån.

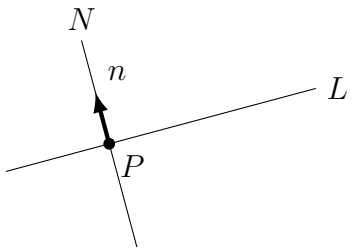
Exempel 4.2.3. Linjen genom origo och med riktningsvektor $v = (3, 4)$ är mängden $\{(3t, 4t) \mid \text{reella tal } t\}$.

4.3 Normallinjer

Låt L vara en given linje i planet. Om v och v' är två riktningsvektorer för linjen L finns det ett tal s sådant att $v' = sv$. Speciellt har vi att om en vektor $n = (a, b)$ är vinkelrät med v så följer det av Lemma 4.1.6 att n också är vinkelrät med v'. En nollskild vektor $n = (a, b)$ som är vinkelrät med riktningsvektorerna till linjen L kallas en *normalvektor* till linjen L. En *normallinje* N till linjen L, genom en punkt P, är linjen

$$N = \{P + tn \mid \text{reella tal } t\}$$

där $n = (a, b) \neq (0, 0)$ är någon normalvektor till linjen L.



4.4 Ekvation för linjer

En linje i planet kan skrivas som lösningarna till en ekvation på formen

$$ax + by + c = 0,$$

för några tal a, b och c, där a och b inte båda kan vara noll. Detta betyder att för en given linje L så finns tal a, b och c sådana att

$$L = \{(x, y) \mid ax + by + c = 0\}.$$

4.4.1. Inte heller ekvationerna är unika. En linje L som ges av ekvationen $ax + by + c = 0$, ges också av ekvationen $atx + bty + ct = 0$, där talet $t \neq 0$.

Lemma 4.4.2. *Låt en linje L vara given som $L = \{P + tv \mid \text{reella tal } t\}$, där $P = (p_1, p_2)$ och $v = (v_1, v_2) \neq (0, 0)$. Låt $n = (a, b)$ vara en nollskild normalvektor för linjen L. En ekvation för linjen L är*

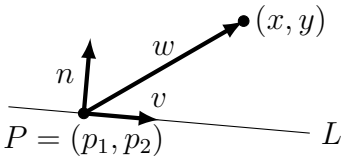
$$ax + by + c = 0,$$

där $c = -ap_1 - bp_2$.

Bevis. Betrakta linjen $L = \{P + tv \mid \text{reella tal } t\}$, där $P = (p_1, p_2)$ och med riktningsvektor $v = (v_1, v_2)$. Låt $n = (a, b)$ vara någon normalvektor till linjen L och betrakta en godtycklig punkt (x, y) i planet. Differensen

$$w = (x - p_1, y - p_2)$$

är en vektor. Flyttar vi pilen som representerar vektorn $(x-p_1, y-p_2)$ till att börja i punkten P så slutar pilen i (x, y). Denna differensvektor $(x-p_1, y-p_2)$ ligger på linjen L om och endast om vektorn är vinkelrät med normalvektorn $n = (a, b)$.



Vi har att $(x-p_1, y-p_2)$ är vinkelrät med normalvektorn n om och endast om deras skalärprodukt är noll. Enligt Definition 4.1.4 är skalärprodukten

$$\langle w, n \rangle = \Big\langle (x - p_1, y - p_2), (a, b) \Big\rangle = ax - ap_1 + by - bp_2 = 0.$$

Det vill säga att en ekvation för linjen L ges som $ax + by + c = 0$ med $c = -ap_1 - bp_2$. □

Lemma 4.4.3. *Låt L vara en linje som ges som nollställemängden till ekvationen $ax + by + c = 0$. Låt $P = (p_1, p_2)$ vara någon punkt sådan att $ap_1 + bp_2 = -c$. Då ges linjen av*

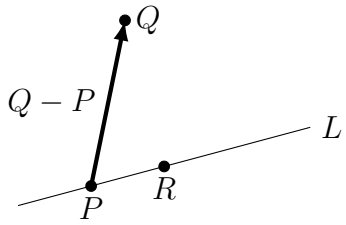
$$L = \{P + t(-b, a) \mid \text{reella tal } t\}.$$

Bevis. Se uppgifterna. □

Exempel 4.4.4. Linjen $L = \{(3t, 4t) \mid \text{reella tal } t\}$ kan också beskrivas som lösningarna till ekvationen $-4x + 3y = 0$.

4.5 Avstånd från en punkt till en linje

Låt Q vara en given punkt i planet och L en given linje. För varje punkt P på linjen kan vi mäta avståndet från Q till punkten P. Avståndet ges som längden av vektorn $Q - P$. Det finns en punkt R på linjen där avståndet till Q är det minsta, och detta avstånd kallar vi avståndet från Q till linjen L. Vi vill beräkna detta avstånd.



Steg 1 Låt linjen L vara given av ekvationen

$$ax + by + c = 0.$$

Vi ska beräkna avståndet från linjen L till punkten $Q = (q_1, q_2)$. Vi låter $P = (p_1, p_2)$ vara någon punkt på linjen, det vill säga att

$$ap_1 + bp_2 + c = 0. \tag{4.5.0.1}$$

Låt v vara en riktningsvektor till linjen. Då är

$$L = \{P + tv \mid \text{reella tal } t\}.$$

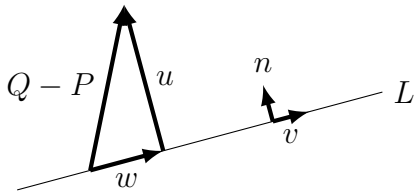
Låt vidare $n = (a, b)$ vara en normalvektor till linjen L, det vill säga en vektor sådan att $\langle n, v \rangle = 0$.

Vi betraktar differensen $Q - P$. Detta är en vektor som vi kan tänka på som en pil som börjar i origo och slutar i koordinaterna $Q - P$. Denna vektor kan vi skriva som

$$Q - P = w + u,$$

där $w = tv$ och $u = sn$. Vi har att

$$Q - P = tv + sn.$$



Steg 2 Avståndet vi försöker bestämma är längden av vektorn $s \cdot n$. Om vi nu betraktar skalärprodukten $\langle Q - P, n\rangle$ så har vi från Lemma 4.1.6 att

$$\langle Q - P, n\rangle = t\langle v, n\rangle + s\langle n, n\rangle = 0 + s\|n\|^2.$$

Detta är en ekvation bestående av tal. Vektorn $n = (a, b)$ antar vi är nollskild, och speciellt har vi att $\|n\|^2 \neq 0$. Därmed har vi ett uttryck för talet

$$s = \frac{1}{\|n\|^2}\langle Q - P, n\rangle. \tag{4.5.0.2}$$

Sats 4.5.1. *Låt L vara linjen som ges av ekvationen $ax + by + c = 0$ och låt $Q = (q_1, q_2)$ vara en godtycklig punkt i planet. Avståndet från punkten Q till linjen L är*

$$\frac{|aq_1 + bq_2 + c|}{\sqrt{a^2 + b^2}}.$$

Bevis. Vi har ovan (4.5.0.2) sett att avståndet ges som längden av vektorn sn, där $n = (a, b)$ och $s = \frac{1}{\|n\|^2}\langle Q - P, n\rangle$. Vi har att längden $\|sn\|$ är

$$\sqrt{(as)^2 + (bs)^2} = \sqrt{s^2(a^2 + b^2)} = |s|\sqrt{a^2 + b^2} = |s| \cdot \|n\|. \tag{4.5.1.1}$$

Vi bestämmer nu ett uttryck för beloppet $|s|$ av talet s. Vi använder Lemma 4.1.6 och får att

$$\langle Q - P, n\rangle = \langle Q, n\rangle - \langle P, n\rangle.$$

Vi har vidare att $\langle Q, n\rangle = \Big\langle (q_1, q_2), (a, b)\Big\rangle = aq_1 + bq_2$, och då också att $\langle P, n\rangle = ap_1 + bp_2$. Punkten P är på linjen och vi har från (4.5.0.1) att $\langle P, n\rangle = -c$. Detta ger att

$$|s| = \frac{1}{\|n\|^2}\Big|\langle Q - P, n\rangle\Big| = \frac{1}{\|n\|^2}\Big|aq_1 + bq_2 - (-c)\Big|.$$

Använder vi nu slutligen (4.5.1.1) ser vi att avståndet från punkten Q till linjen L ges av

$$\|sn\| = \Big|aq_1 + bq_2 + c\Big|\frac{\|n\|}{\|n\|^2} = \frac{|aq_1 + bq_2 + c|}{\sqrt{a^2 + b^2}}.$$

□

4.6 Uppgifter

Uppgift 4.1. Beräkna avståndet från punkten $Q = (1, 2)$ till linjen L som ges av ekvationen $3x + 4y = 5$.

Uppgift 4.2. Använd definitionen av skalärprodukt för att visa båda påståendena i Lemma 4.1.6.

Uppgift 4.3. Visa Lemma 4.4.3, till exempel på följande sätt. Låt L vara linjen som ges av ekvationen $ax + by + c = 0$ och låt L' vara linjen

$$L' = \{P + tv \mid t \text{ reellt tal}\},$$

där P och v är som i Lemmat. För att visa att $L = L'$ måste vi visa att varje punkt i L' är med i L och omvänt. Låt Q vara en punkt i L'. Skriv ut vad detta betyder och kolla att koordinaterna till Q satisfierar ekvationen som bestämmer L. Då har du visat att $L' \subseteq L$. För att visa det omvända kan du använda Lemma 4.4.2.

Föreläsning 5

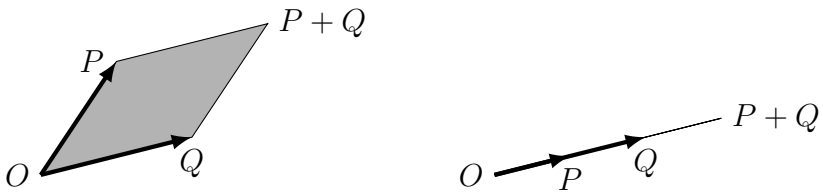
Area och determinant

Förra gången visade vi en formel för avståndet mellan en punkt $P = (p, q)$ och en linje L. Om linjen L var given som nollställemängden till ekvationen $ax + by + c = 0$ var avståndet givet av formeln

$$\frac{|ap + bq + c|}{\sqrt{a^2 + b^2}}.$$

5.1 Area av parallellogram

Två punkter P och Q i planet bildar tillsammans med origo och punkten $P + Q$ ett parallellogram. Varje parallellogram bestäms av två hörnpunkter P och Q. Om P och Q ligger på samma linje genom origo ger de fyra hörnen inte ett parallellogram i ordets vanliga mening, utan enbart ett linjesegment. Vi tillåter dock sådana så kallade degenererade fall.



Proposition 5.1.1. *Låt $P = (p_1, p_2)$ och $Q = (q_1, q_2)$ vara två punkter i planet. Arean av det parallellogram som punkterna P, Q, $P + Q$ och origo spänner upp är*

$$|p_1 q_2 - p_2 q_1|.$$

Bevis. Arean ges som bekant av höjden multiplicerad med bredden. Bredden kan vi bestämma via Pythagoras Sats som $\|Q\| = \sqrt{q_1^2 + q_2^2}$. Höjden är precis

avståndet från P till linjen L som går genom origo och Q. En ekvation för linjen L genom Q och origo är

$$q_2x - q_1y = 0.$$

Av Sats 4.5.1 får vi nu att höjden i parallellogrammet är

$$\frac{|q_2p_1 - q_1p_2|}{\sqrt{q_1^2 + q_2^2}}.$$

Multiplicerar vi nu uttrycket för höjd med uttrycket för bredd erhålls det önskade svaret. □

5.2 Area och avbildningar

Vi har sett att en linjär avbildning $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ ges som matrismultiplikation med en given (2×2)-matris A. Vi kommer ihåg att matrisens två kolumner ges av koordinaterna till $T(1,0)$ och $T(0,1)$. Om vi låter $(a,b) = T(1,0)$ och $(c,d) = T(0,1)$ så bestämmer matrisen

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

avbildningen T. Determinanten av matrisen A är talet

$$\det(A) = ad - bc, \tag{5.2.0.1}$$

som vi bekantade oss med i Uppgift 1.2.

Proposition 5.2.1. *Låt $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ vara en linjär avbildning, given som matrismultiplikation med matrisen A. Låt Ω vara enhetskvadraten i $\mathbf{R}^2$ med hörn $(0,0)$, $(1,0)$, $(0,1)$ och $(1,1)$. Bilden av Ω under avbildningen T är ett parallellogram och arean till parallellogrammet $T(\Omega)$ är $|\det(A)|$.*

Bevis. Kvadraten Ω avbildas på parallellogrammet med hörn $T(1,0) = (a,b)$ och $T(0,1) = (c,d)$. Arean av parallellogrammet ges av Proposition 5.1.1 som beloppet av $ad - bc$, vilket också är uttrycket för determinanten. □

5.3 Sammansättning

Om $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ och $U\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ är två funktioner från planet till planet, kan vi definiera deras sammansättning

$$U \circ T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$$

som är funktionen vi får genom att först använda T och sedan använda U. Med andra ord skickas en godtycklig punkt (x, y) i planet till punkten

$$(x, y) \mapsto T(x, y) \mapsto U(T(x, y)).$$

Läsaren bör lägga notationen på minnet. Funktionssammansättning läses från höger till vänster. Sammansättningen $U \circ T$ betyder att T används först och sedan U. Sammansättningen $T \circ U$ betyder att U används först och sedan T.

Om funktionerna U och T båda är linjära är dessa givna av matriser och matrismultiplikation.

Lemma 5.3.1. *Om matrisen A ger avbildningen T och matrisen B ger avbildningen U ges sammansättningen $U \circ T$ av matrisprodukten BA.*

Bevis. Se uppgifterna. □

Exempel 5.3.2. Låt den linjära avbildningen $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ vara given av matrisen $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$. Proposition 5.2.1 ger att arean av parallellogrammet som enhetskvadraten skickas till under T är $|ad - bc|$. Antag nu att arean är nollskild. Då har vi från tidigare att matrisen A är inverterbar och inversen ges av matrisen

$$B = \frac{1}{ad - bc} \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}.$$

Betrakta nu den linjära avbildningen $U\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ som ges av matrisen B och matrismultiplikation med denna. Av Proposition 5.2.1 följer att enhetskvadraten skickas med U till ett parallellogram med area $|\det(B)|$. Beräknar man determinanten av B får man att

$$\det(B) = \frac{1}{ad - bc} = \frac{1}{\det(A)}.$$

Vad händer med enhetskvadraten under sammansättningen $U \circ T$? Först har vi en avbildning T som skickar enhetskvadraten till ett parallellogram med hörnpunkterna $P = (a, b)$ och $Q = (c, d)$. Sedan har vi en avbildning U som skickar enhetskvadraten till ett parallellogram med hörnpunkterna $P = \frac{1}{ad-cd}(d, -b)$ och $Q = \frac{1}{ad-bc}(-c, a)$. Men sammansättningen ges enligt Lemma 5.3.1 av matrisprodukten BA. Då B är inversen till A har vi att BA är identitetsmatrisen och det följer att sammansättningen $U \circ T$ är identitetsavbildningen. Med andra ord skickas enhetskvadraten till enhetskvadraten.

5.4 Singulära matriser

En matris A vars determinant är noll kallas singulär. Hur ser en sådan ut? Låt A vara given och betrakta den tillhörande linjära avbildningen $T_A\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$. Första kolumnen i A ges av koordinaterna till $T_A(1,0) = (a,b)$. Om $(a,b) = (0,0)$ är det klart att determinanten av A är noll. Antag därför att $(a,b) \neq (0,0)$. Då finns det en unik linje L genom origo och punkten (a,b). Om punkten $T(0,1)$ inte hamnar på linjen L hamnar enhetskvadraten på ett äkta parallellogram med nollskild area. Därför om A skall bli singulär så måste punkten $T(0,1)$ hamna på linjen L. Alla punkter på linjen L är på formen $t(a,b)$, för någon skalär t. Med andra ord så är andra kolumnen i matrisen A lika med (ta,tb). Det betyder att de singulära matriserna är på formen

$$A = \begin{bmatrix} a & ta \\ b & tb \end{bmatrix} \quad \text{eller} \quad A = \begin{bmatrix} 0 & c \\ 0 & d \end{bmatrix}.$$

5.5 Uppgifter

Uppgift 5.1. Betrakta den linjära avbildningen $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ som är bestämd av $T(2,0) = (2,4)$ och $T(0,5) = (3,-7)$. Hitta matrisen A som beskriver avbildningen T.

Uppgift 5.2. Betrakta den linjära avbildningen $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ som är bestämd av $T(2,1) = (2,4)$ och $T(2,3) = (3,-7)$. Hitta matrisen A som beskriver avbildningen T (Skriv upp ett ekvationssystem som du löser genom invertering av en matris).

Uppgift 5.3. Visa Lemma 5.3.1. Visa först att sammansättningen $U \circ T$ är linjär. Visa sedan att sammansättningen ges av matrisen BA.

Uppgift 5.4. Visa att matrisen $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ är inverterbar om och endast om $\det(A) \neq 0$.

Uppgift 5.5. Visa att matrisen $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ är singulär om och endast om ena *raden* i matrisen är en multipel av den andra raden.

Föreläsning 6

Lösningar till ekvationssystem

6.1 Ekvationer

En linjär ekvation i n variabler $x_1, \ldots, x_n$ är en ekvation på formen

$$a_1x_1 + a_2x_2 + \cdots a_nx_n = b,$$

med givna tal $a_1, \ldots, a_n$ och b. Ett *linjärt ekvationssystem* i n variabler $x_1, \ldots, x_n$ är ett ändligt antal linjära ekvationer i variablerna $x_1, \ldots, x_n$.

Exempel 6.1.1. Följande två linjära ekvationer

$$\begin{cases} 2x - y + z &= 3 \\ x + 2y &= 0 \end{cases}$$

är ett ekvationssystem med tre variabler x, y och z. Systemet består av två ekvationer.

6.1.2. Ett allmänt linjärt ekvationssystem skriver vi vanligtvis som

$$(\star) = \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + d_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ \vdots & \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m. \end{cases}$$

Med detta menas att vi har givna tal $a_{i,j}$ för varje $1 \leq i \leq m$ och varje $1 \leq j \leq n$, samt talen $b_1, \ldots, b_m$. Variablerna är $x_1, \ldots, x_n$ och det är n stycken av dessa. Antalet linjära ekvationer i systemet är m.

6.1.3. Lösningsmängden till ett givet ekvationssystem är alla ordnade n-tupler av reella tal $(t_1, \ldots, t_n)$ som satisfierar alla m ekvationerna som förekommer i ekvationssystemet. Detta betyder att för varje $i = 1, \ldots, m$ har vi att $(t_1, \ldots, t_n)$ är sådan att

$$a_{i,1}t_1 + a_{i,2}t_2 + \cdots + a_{i,n}t_n = b_i.$$

6.1.4. Kom ihåg att mängden av *alla* ordnade n-tupler av reella tal bildar det euklidiska n-rummet $\mathbf{R}^n$. Lösningsmängden till ett ekvationssystem i n variabler blir alltid en delmängd av $\mathbf{R}^n$.

Exempel 6.1.5. Betrakta åter igen ekvationssystemet i Exempel 6.1.1. Den sista ekvationen ger att $x = -2y$, vilket insatt i den första ekvationen ger att $2 \cdot (-2y) - y + z = 3$. Det vill säga att $z = 3 + 5y$. Lösningsmängden till ekvationssystemet är alla punkter i $\mathbf{R}^3$ på formen

$$(-2t, t, 3 + 5t)$$

för godtyckliga tal t.

6.2 Systematisk lösning av ekvationssystem

När man skall lösa mera komplexa system än sådana enkla som i Exempel 6.1.1 lönar det sig att vara mera systematisk. Vi börjar med att observera tre enkla operationer som inte ändrar lösningsmängden till ett system.

Radbyte Givet ett ekvationssystem $(\star)$. Detta system består av m ekvationer som vi kallar rader. Det är klart att om vi byter plats på raderna i ett ekvationssystem så ändras inte lösningsmängden.

Multiplikation med ett nollskilt tal Givet ett ekvationssystem $(\star)$. Om vi multiplicerar en rad i ekvationssystemet med ett nollskilt tal $c \neq 0$ får vi ett nytt ekvationssystem. Men det är klart att lösningsmängden inte ändrar sig. Eller?

Addition av en rad till en annan Givet ett ekvationssystem $(\star)$. Multiplicera en given rad i med ett tal c och addera denna nya rad till raden j. I det nya ekvationssystemet $(\star')$ har vi ändrat enbart rad j, men lösningsmängden är den samma som för ekvationssystemet (*). Denna operation på ekvationssystemet är inte lika uppenbar som de två föregående. Notera nu att raden j i det nya ekvationssystemet är

$$(a_{j,1} + ca_{i,1})x_1 + (a_{j,2} + ca_{i,2})x_2 + \cdots + (a_{j,n} + ca_{i,n})x_n = b_j + cb_i.$$

Kolla nu (se uppgifterna) att en lösning $(t_1, \ldots, t_n)$ till ekvationssystemet $(\star)$ också är en lösning till det nya ekvationssystemet $(\star')$ och vice versa.

Elementära radoperationer Vi kan manipulera ett ekvationssystem med de tre operationerna ovan utan att ändra lösningsmängden. Dessa operationer kallas elementära radoperationer.

Exempel 6.2.1. Betrakta ekvationssystemet

$$\begin{cases} x + 3y + z & = 2 \\ 2x + 7y & = 2 \\ -x - 4y + 3z & = 1. \end{cases} \tag{6.2.1.1}$$

Vi tar och adderar -2 gånger rad ett till rad två. Den enda rad som ändrar sig är rad två. Ekvationssystemet blir nu

$$\begin{cases} x + 3y + z & = & 2 \\ y - 2z & = & -2 \\ -x - 4y + 3z & = & 1. \end{cases}$$

Sedan tar vi och adderar 1 gånger rad ett till rad tre. Ekvationssystemet blir nu

$$\begin{cases} x + 3y + z & = & 2 \\ y - 2z & = & -2 \\ -y + 4z & = & 3. \end{cases}$$

Ekvationssystemet har nu variabeln x enbart i den första raden. Låt oss nu ta -3 gånger rad två och addera till rad ett, och sedan tar vi och adderar 1 gånger rad två till rad tre. Ekvationssystemet blir

$$\begin{cases} x + 7z & = & 8 \\ y - 2z & = & -2 \\ 2z & = & 1. \end{cases}$$

Variabeln y förekommer nu enbart i rad två. Vi multiplicerar rad tre med $\frac{1}{2}$, sedan tar vi 2 gånger rad tre och adderar till rad två och slutligen -7 gånger rad tre och adderar till rad 1. Detta ger ekvationssystemet

$$\begin{cases} x & = & \frac{9}{2} \\ y & = & -1 \\ z & = & \frac{1}{2}. \end{cases} \tag{6.2.1.2}$$

Notera att vi enbart har använt elementära radoperationer på ekvationssystemet (6.2.1.1). Detta betyder att lösningsmängden till (6.2.1.1) är precis den samma som lösningsmängden till (6.2.1.2). Men lösningsmängden till (6.2.1.2) är lätt att läsa ut: det är nämligen punkten

$$\left(\frac{9}{2}, -1, \frac{1}{2}\right).$$

6.3 Gauss–Jordanelimination

Tillvägagångssättet som användes i Exempel 6.2.1 kan appliceras på alla ekvationssystem och kallas Gauss–Jordanelimination. Den allmänna algoritmen är som följer: Betrakta ett givet ekvationssystem ($\star$). Börja med första kolumnen. Om alla $a_{1,1}, \ldots, a_{m,1}$ är lika med noll, fortsätt till kolumn två. Om inte, plocka ut en rad i där $a_{i,1} \neq 0$. Byt plats på rad ett och rad i. Multiplicera nu den nya första raden med $a_{1,1}^{-1}$. Detta betyder nu att den första raden är

$$x_1 + a'_{1,2}x_2 + \cdots + a'_{1,n}x_n = b'_1,$$

där $a'_{1,j} = \frac{a_{i,j}}{a_{i,1}}$ och $b'_1 = \frac{b_i}{a_{i,1}}$. Sedan använder vi rad ett för att eliminera all förekomst av x_1 i de andra raderna. Det vill säga, multiplicera rad ett med $-a_{2,1}$ och addera till rad två, multiplicera rad ett med $-a_{3,1}$ och addera till rad tre, och så vidare. Ekvationssystemet blir då på formen

$$\begin{cases} x_1 + a'_{1,2}x_2 + \cdots + a'_{1,n}x_n &= b'_1 \\ \quad a'_{2,2}x_2 + \cdots + a'_{2,n}x_n &= b'_2 \\ \qquad\qquad \vdots & \\ \quad a'_{m,2}x_2 + \cdots + a'_{m,n}x_n &= b'_m. \end{cases}$$

Nu är vi klara med variabeln x_1. Vi tittar nu på kolumn två, men inte på rad ett. Vi stryker bort rad ett för ett tag. Om alla siffror $a'_{2,2}, \ldots, a'_{m,2}$ är noll fortsätter vi till kolumn tre. Om det finns en siffra $a_{j,2}$ som är nollskild, byt plats på rad två och rad j, multiplicera rad två med $a_{j,2}^{-1}$. Rad två blir nu på formen

$$x_2 + a''_{2,3}x_3 + \cdots + a''_{2,n}x_n = b''_2,$$

där vi hela tiden byter namn på koefficienterna. Vad koefficienterna är spelar inte någon roll. Nu använder vi rad två för att eliminera alla förekomster av variabeln x_2 i raderna tre, fyra, $\ldots, m$ och i rad ett. Detta beskriver Gauss–Jordaneliminationen, som vi avslutar efter ett ändligt antal steg.

Exempel 6.3.1. Betrakta ekvationssystemet

$$\begin{cases} x_1 + 2x_2 + x_3 - 3x_4 + 5x_5 + x_6 &= 1 \\ 3x_1 + 6x_2 + 6x_3 - 15x_4 + 21x_5 + x_6 &= 2 \\ 2x_1 + 4x_2 + 3x_3 - 8x_4 + 12x_5 + x_6 &= 3 \\ 5x_1 + 10x_2 + 7x_3 - 19x_4 + 29x_5 + 2x_6 &= 11. \end{cases}$$

Det är lite trist och jobbigt att ta med alla variabler när vi utför Gauss–Jordaneliminationen. Därför skippar vi just detta. Systemet ovan skriver vi

istället som matrisen[1]

$$\left[\begin{array}{cccccc|c} 1 & 2 & 1 & -3 & 5 & 1 & 1 \\ 3 & 6 & 6 & -15 & 21 & 1 & 2 \\ 2 & 4 & 3 & -8 & 12 & 1 & 3 \\ 5 & 10 & 7 & -19 & 29 & 2 & 11 \end{array}\right].$$

Vi utför de elementära radoperationerna som följer. Vi har en ledande etta i första raden, första kolumnen. Denna använder vi för att eliminera talen i första kolumnen, i raderna två, tre och fyra. Detta ger

$$\left[\begin{array}{cccccc|c} 1 & 2 & 1 & -3 & 5 & 1 & 1 \\ 0 & 0 & 3 & -6 & 6 & -2 & -1 \\ 0 & 0 & 1 & -2 & 2 & -1 & 1 \\ 0 & 0 & 2 & -4 & 4 & -3 & 6 \end{array}\right].$$

Vi är nu klara med kolumn ett. I kolumn två finns det enbart noll på raderna två, tre och fyra. Vi fortsätter därför till kolumn tre. Vi byter plats på rad två och rad tre. Och sedan fixar vi till att det blir noll över och under den ledande ettan. Nu borde ni få fram matrisen

$$\left[\begin{array}{cccccc|c} 1 & 2 & 0 & -1 & 3 & 2 & 0 \\ 0 & 0 & 1 & -2 & 2 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -4 \\ 0 & 0 & 0 & 0 & 0 & -1 & 4 \end{array}\right].$$

Vi fortsätter till kolumn fyra, men i raderna tre och fyra finns bara nollor. Vi fortsätter till kolumn fem, och här finns det också enbart nollor i raderna tre och fyra. Vi fortsätter till kolumn sex, och här har vi en ledande etta. Vi fixar nollor över och under den ledande ettan i rad tre, och erhåller

$$\left[\begin{array}{cccccc|c} 1 & 2 & 0 & -1 & 3 & 0 & 8 \\ 0 & 0 & 1 & -2 & 2 & 0 & -3 \\ 0 & 0 & 0 & 0 & 0 & 1 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Här terminerar Gauss–Jordanalgoritmen och vi skall nu läsa av lösningsmängden. Vi börjar med den sista ledande ettan, den i rad tre. Rad tre betyder att $x_6 = -4$. Det finns ingen ledande etta i kolumn fem, vilket betyder att $x_5 = s$ kan väljas godtyckligt. Likadant kan $x_4 = t$ väljas godtyckligt. I rad två har vi en ledande etta för kolumn tre; detta betyder

$$x_3 - 2x_4 + 2x_5 = -3.$$

[1]Denna matris brukar kallas för den *utökade koefficientmatrisen* eller *totalmatrisen* till ekvationssystemet.

Med andra ord gäller att $x_3 = -3 + 2t - 2s$. Det finns inga ledande ettor för kolumn två och detta betyder att $x_2 = u$ också kan väljas godtyckligt. Slutligen har vi att

$$x_1 + 2x_2 - x_4 + 3x_5 = 8.$$

Detta betyder att lösningsmängden till ekvationssystemet är alla punkter i $\mathbf{R}^6$ på formen

$$(8 - 2u + t - 3s, u, -3 + 2t - 2s, t, s, -4),$$

med godtyckliga tal s, t och u.

6.4 Uppgifter

Gauss–Jordanelimination är varken svårt att lära sig eller att förstå även om räkningarna kan bli jobbiga. Om algoritmen är oklar, prata med någon för att genast få klarhet kring denna.

Uppgift 6.1. Lös ekvationssystemet

$$\begin{cases} 2x + 3y + 4z &= 2 \\ 2x + 5y + z &= 5 \\ 4x + 10y - z &= 1. \end{cases}$$

Uppgift 6.2. Visa att radoperationen som beskrivs som addition av rad till en annan i Avsnitt 6.2 inte ändrar lösningsmängden.

Uppgift 6.3. Visa att de tre radoperationerna i Avsnitt 6.2 faktiskt enbart består av två operationer.

Föreläsning 7

Elementära matriser

7.1 Elementära radoperationer och matriser

Vi påminner om att ett ekvationssystem är ett ändligt antal linjära ekvationer i ett ändligt antal okända. Vi skriver ett ekvationssystem som

$$(\star)\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + d_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ \vdots & \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m. \end{cases}$$

Lösningsmängden till ekvationssystemet $(\star)$ är en delmängd av $\mathbf{R}^n$. Det euklidiska n-rummet $\mathbf{R}^n$ är mängden av alla ordnade n-tupler av reella tal. Lösningsmängden till $(\star)$ är alla ordnade n-tupler $(t_1, \ldots, t_n)$ som satisfierar ekvationerna i ekvationssystemet.

7.1.1. Ekvationssystemen kan lösas på ett systematisk sätt. Den algoritm vi använder kallas Gauss–Jordan elimination och använder sig av tre *elementära* radoperationer. De elementära radoperationerna är att a) multiplicera en rad med ett nollskilt tal b) byta plats på två rader och c) addera till en given rad en multipel av en annan rad.

De elementära radoperationerna ändrar inte lösningsmängden till ekvationssystemet men ändrar själva ekvationssystemet. Vi använder elementära radoperationer för att få fram ett ekvationssystem varifrån vi lätt kan läsa av lösningsmängden.

Exempel 7.1.2. Betrakta ekvationssystemet nedan i tre okända x, y och z.

$$\begin{cases} x + y &= 3 \\ y + 2z &= 1 \\ 2x + y + z &= 2 \end{cases} \tag{7.1.2.1}$$

Som brukligt skriver vi upp totalmatrisen till systemet för att inte behöva skriva upp de okända varje gång. Totalmatrisen är

$$\left[\begin{array}{ccc|c} 1 & 1 & 0 & 3 \\ 0 & 1 & 2 & 1 \\ 2 & 1 & 1 & 2 \end{array}\right]. \tag{7.1.2.2}$$

I första kolumnen har vi en ledande etta och vi vill åstadkomma 0 under denna ledande etta. Detta ordnar vi om vi adderar -2 gånger den första raden till den tredje raden. Denna operation ger matrisen

$$\left[\begin{array}{ccc|c} 1 & 1 & 0 & 3 \\ 0 & 1 & 2 & 1 \\ 0 & -1 & 1 & -4 \end{array}\right]. \tag{7.1.2.3}$$

Nu är vi klara med första kolumnen och fortsätter med andra kolumnen. Vi använder 1 på plats $(2,2)$ som ledande etta. Vi skaffar oss noll ovan och under denna ledande etta i två steg. Till den tredje raden adderar vi 1 gånger av rad två och sedan tar vi och adderar till den första raden -1 gånger rad två. Detta ger matrisen

$$\left[\begin{array}{ccc|c} 1 & 0 & -2 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 3 & -3 \end{array}\right]. \tag{7.1.2.4}$$

Slutligen arbetar vi med den tredje kolumnen. Vi multiplicerar rad tre med $\frac{1}{3}$ och skaffar oss en ledande etta. Till den andra raden adderar vi -2 gånger tredje raden och till den första raden adderar vi 2 gånger tredje raden. Detta ger matrisen

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & -1 \end{array}\right]. \tag{7.1.2.5}$$

Nu kan vi läsa av lösningsmängden till ekvationssystemet (7.1.2.1) som

$$(0, 3, -1).$$

Lösningsmängden är en punkt i $\mathbf{R}^3$.

7.1.3. En viktig ingrediens i linjär algebra är matrismultiplikation. Låt

$$A = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \\ d_1 & d_2 & \cdots & d_n \end{bmatrix}$$

vara en given $(4 \times n)$ matris och betrakta följande tre matriser

$$E_1(k) = \begin{bmatrix} k & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad E_{2,3} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad E_{1,3}(k) = \begin{bmatrix} 1 & 0 & k & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Lägg märke till att dessa tre matriser är små modifikationer av identitetsmatrisen. Vidare kan alla tre matriserna multipliceras med matrisen A — från vänster. Vi erhåller att

$$E_1(k)A = \begin{bmatrix} ka_1 & ka_2 & \cdots & ka_n \\ b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \\ d_1 & d_2 & \cdots & d_n \end{bmatrix},$$

det vill säga att multiplikation med matrisen $E_1(k)$ blir detsamma som att multiplicera den första raden i matrisen A med talet k. Vi har att

$$E_{2,3}A = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ c_1 & c_2 & \cdots & c_n \\ b_1 & b_2 & \cdots & b_n \\ d_1 & d_2 & \cdots & d_n \end{bmatrix},$$

det vill säga att multiplikation med matrisen $E_{2,3}$ byter plats på den andra och tredje raden i matrisen A. Slutligen har vi att

$$E_{1,3}(k)A = \begin{bmatrix} a_1 + kc_1 & a_2 + kc_2 & \cdots & a_n + kc_n \\ b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \\ d_1 & d_2 & \cdots & d_n \end{bmatrix},$$

det vill säga att multiplikation med matrisen $E_{1,3}(k)$ tar och adderar k gånger den tredje raden till den första raden.

Definition 7.1.4. De *elementära matriserna* är de följande $(n \times n)$-matriserna.

a) Givet $1 \leq i \leq n$ och ett nollskilt tal k. Låt $E_i(k)$ vara matrisen vi får genom att byta ut elementet (i, i) i identitetsmatrisen med k.

b) Givet $1 \leq i < j \leq n$. Låt $E_{i,j}$ vara matrisen vi får genom att byta plats på raderna i och j i identitetsmatrisen.

c) Givet $1 \leq i, j \leq n$, $i \neq j$ och ett tal k. Låt $E_{i,j}(k)$ vara matrisen vi får genom att byta ut elementet (i, j) i identitetsmatrisen med k.

Sats 7.1.5. *Låt A vara en $(n \times m)$-matris. Att utföra en elementär radoperation på matrisen A är detsamma som att multiplicera A från vänster med en $(n \times n)$ elementär matris. Mera precist har vi*

a) Att utföra multiplikationen $E_i(k)A$ är att multiplicera rad i av matrisen A med talet k.

b) Att utföra multiplikationen $E_{i,j}A$ är att byta plats på raderna i och j i matrisen A.

c) Att utföra multiplikationen $E_{i,j}(k)A$ är att till raden i av A addera k gånger raden j av A.

Bevis. Detta är en lämplig uppgift (se Uppgift 7.2). □

Exempel 7.1.6. Låt oss återgå till exemplet ovan och ekvationssystemet (7.1.2.1). Totalmatrisen till systemet är

$$A = \left[\begin{array}{ccc|c} 1 & 1 & 0 & 3 \\ 0 & 1 & 2 & 1 \\ 2 & 1 & 1 & 2 \end{array}\right]$$

Den första elementära radoperationen vi gjorde var att till rad 3 addera -2 gånger rad 1. I termer av elementära matriser betyder det att multiplicera totalmatrisen A med

$$E_{3,1}(-2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix}.$$

Vi har att

$$E_{3,1}(-2)A = \left[\begin{array}{ccc|c} 1 & 1 & 0 & 3 \\ 0 & 1 & 2 & 1 \\ 0 & -1 & 1 & -4 \end{array}\right]$$

vilket precis är matrisen (7.1.2.3). För att komma till matrisen (7.1.2.4) gjorde vi två elementära radoperationer. Det första vi gjorde var att till den tredje raden addera 1 gånger rad två och detta motsvarar matrisen $E_{3,2}(1)$. Sedan tog vi till den första raden -1 gånger rad 2, det vill säga matrisen $E_{1,2}(-1)$. Matrisen (7.1.2.4) får vi som produkten

$$E_{1,2}(-1)E_{3,2}(1)E_{3,1}(-2)A = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \left[\begin{array}{ccc|c} 1 & 1 & 0 & 3 \\ 0 & 1 & 2 & 1 \\ 0 & -1 & 1 & -4 \end{array}\right].$$

Det vi gjorde sedan var att multiplicera med $E_3(\frac{1}{3})$, sedan multiplicera med $E_{2,3}(-2)$ och slutligen multiplicerade vi med $E_{1,3}(2)$. Hela exemplet ges av matrisprodukten

$$E_{1,3}(2)E_{2,3}(-2)E_3(\tfrac{1}{3})E_{1,2}(-1)E_{3,2}(1)E_{3,1}(-2)A. \tag{7.1.6.1}$$

Notera att det är viktigt att hålla reda på ordningen i matrisprodukten. Utför man produkten (7.1.6.1) så får man matrisen (7.1.2.5).

7.1.7. En $(n \times n)$ matris B är inversen till matrisen A om AB och BA båda blir identitetsmatrisen.

Sats 7.1.8. *Varje elementär matris är inverterbar och inversen till en elementär matris är själv en elementär matris. Mera precist har vi att*

1) Elementärmatrisen $E_i(k)$ har invers $E_i(\frac{1}{k})$.

2) Elementärmatrisen $E_{i,j}$ har invers $E_{i,j}$.

3) Elementärmatrisen $E_{i,j}(k)$ har invers $E_{i,j}(-k)$.

Bevis. Vi visar först påståendet i 1). Låt B vara en elementär matris på formen $E_i(k)$. Då är $k \neq 0$ och vi kan bilda elementärmatrisen $E_i(\frac{1}{k})$. Av Sats 7.1.5 följer det att $E_i(\frac{1}{k})B$ är att multiplicera rad i av matrisen B med $\frac{1}{k}$. Rad i i matrisen $B = E_i(k)$ har talet k på plats i och noll annars. Det är nu klart att $E_i(\frac{1}{k})B = 1$. Vi har visat att $E_i(\frac{1}{k})E_i(k) = 1$ för alla nollskilda k och speciellt också att $E_i(k)E_i(\frac{1}{k}) = 1$. Då har vi visat påstående 1). Se uppgifterna för 2) och 3). □

Exempel 7.1.9. Betrakta matrisen

$$B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 2 & 1 & 1 \end{bmatrix}.$$

Denna matris är den vänstra delen av totalmatrisen i första exemplet. Det följer av beräkningarna vi gjorde att produkten (7.1.6.1) blir

$$E_{1,3}(2)E_{2,3}(-2)E_3(\tfrac{1}{3})E_{1,2}(-1)E_{3,2}(1)E_{3,2}(-2)B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Låt $X = E_{1,3}(2)E_{2,3}(-2)E_3(\frac{1}{3})E_{1,2}(-1)E_{3,2}(1)E_{3,2}(-2)$. Vi ser att $XB = 1$, det vill säga att när vi multiplicerar matrisen B med matrisen X från vänster erhåller vi identitetsmatrisen. Vi vill visa att X är inversen till B och det

kvarstår att visa att $BX = 1$. Vi använder oss av Sats 7.1.8 och multiplicerar uttrycket ovan med $E_{1,3}(-2)$ från vänster. Detta ger

$$E_{2,3}(-2)E_3(\tfrac{1}{3})E_{1,2}(-1)E_{3,2}(1)E_{3,2}(-2)B = E_{1,3}(-2).$$

Upprepar vi detta får vi slutligen att

$$B = E_{3,2}(2)E_{3,2}(-1)E_{1,2}(1)E_3(3)E_{2,3}(2)E_{1,3}(-2).$$

Använder vi nu Sats 7.1.8 och uttrycket för B ovan, ser vi omedelbart att $BX = 1$.

7.2 Uppgifter

Uppgift 7.1. Använd enbart matrismultiplikation och elementära matriser för att göra Gauss–Jordanelimination på ekvationssystemet

$$\begin{cases} x + 2y + z &= 3 \\ -3x + z &= 2 \\ 2y - 2z &= 1. \end{cases}$$

Uppgift 7.2. Visa Sats 7.1.5.

Uppgift 7.3. Visa påståendena 2) och 3) i Sats 7.1.8.

Uppgift 7.4. Använd Gauss–Jordanelimination på matrisen

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 3 & 3 \\ 3 & 5 & 9 \end{bmatrix}$$

för att konstruera A^{-1}.

Föreläsning 8

Konstruktion av inversmatris

8.1 Reducerad trappstegsform

Vi påminner om Gauss–Jordaneliminationen igen. Om A är en matris så kan vi utföra Gauss–Jordanelimination på matrisen. När vi är klara med Gauss–Jordanelimination har vi en matris R som vi kallar den *reducerade trappstegsformen* till matrisen A.

Lemma 8.1.1. *Låt A vara en $(n \times n)$-matris. Då kommer den reducerade trappstegsformen R att innehålla en $(r \times r)$-identitetsmatris som ett block i sitt vänstra övre hörn $(0 \leq r \leq n)$. Om $r = n$, då är den reducerade trappstegsformen R lika med identitetsmatrisen. Annars, om $0 \leq r \leq n-1$, så är den reducerade trappstegsformen till A på formen*

$$R = \begin{bmatrix} 1 & 0 & \cdots & 0 & b_{1,r+1} & * & \cdots & * \\ 0 & 1 & \cdots & 0 & b_{2,r+1} & * & \cdots & * \\ \vdots & & \ddots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & b_{r,r+1} & * & \cdots & * \\ 0 & 0 & \cdots & 0 & 0 & * & \cdots & * \\ \vdots & & \ddots & 0 & 0 & * & \cdots & * \\ 0 & 0 & \cdots & 0 & 0 & * & \cdots & * \end{bmatrix}$$

för några tal $b_{1,r+1}, \ldots, b_{r,r+1}$.

Bevis. Lemmat är en observation som följer direkt av Gauss–Jordan elimination. □

Sats 8.1.2. *Låt A vara en $(n \times n)$-matris. Följande påståenden är ekvivalenta.*

1) Det existerar en $(n \times n)$-matris B sådan att BA är identitetsmatrisen.

2) Den enda $(n \times 1)$-matris som löser ekvationen $AX = 0$ är nollmatrisen $X = 0$.

3) Matrisen A kan skrivas som en produkt av elementära matriser $A = E_1 \cdots E_s$.

Bevis. Vi visar att påstående 1) implicerar påstående 2), sedan att 2) implicerar 3) och slutligen att 3) implicerar påstående 1).

Antag att påstående 1) gäller. Vi vill visa att ekvationen $AX = 0$ enbart har den triviala lösningen. Låt därför X vara en godtycklig lösning, det vill säga en $(n \times 1)$-matris sådan att $AX = 0$. Av påstående 1) har vi att det existerar en matris B sådan att $BA = \mathbf{1}$. Multiplicera matrisekvation $AX = 0$ med matrisen B från vänster och vi erhåller att $BAX = B0$. Vi har att en matris multiplicerad med 0 ger noll, så $B0 = 0$. Eftersom $BA = \mathbf{1}$ så ger detta

$$X = \mathbf{1}X = BA \cdot X = B \cdot 0 = 0,$$

vilket visar påståendet 2).

Antag nu att påståendet 2) gäller. Låt R vara den reducerade trappstegsformen till A. Detta betyder att det existerar elementära matriser $F_1, \ldots, F_s$ sådana att

$$F_s F_{s-1} \cdots F_2 F_1 A = R.$$

Varje elementär matris F har en invers E som också är en elementär matris. Detta betyder att det finns elementära matriser $E_1, \ldots, E_s$ sådan att

$$A = E_1 E_2 \cdots E_s R. \tag{8.1.2.1}$$

Av Lemma 8.1.1 har vi att det finns ett tal $0 \leq r \leq n$ sådan att R är på formen angivet i lemmat. Om $r < n$ är strikt mindre än n då kan vi konstruera matrisen

$$X = \begin{bmatrix} -b_{1,r+1} \\ -b_{2,r+1} \\ \vdots \\ -b_{r,r+1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Denna matris X är nollskild och vi ser att $RX = 0$. Av uttrycket (8.1.2.1) har vi att också $AX = 0$. Detta är dock omöjligt av 2) och följaktligen

måste $r = n$. Detta betyder att den reducerade trappstegsformen $R = \mathbf{1}$ är identitetsmatrisen och att $A = E_1 \cdots E_s$ är en produkt av elementära matriser. Detta visar att 2) medför 3).

Antag nu att påståendet 3) gäller. Det vill säga att $A = E_1 \cdots E_s$, med elementära matriser $E_1, \ldots, E_s$. Låt $B = E_s^{-1} \cdots E_1^{-1}$. Vi har att

$$BA = E_s^{-1} \cdots E_2^{-1} E_1^{-1} E_1 E_2 \cdots E_s.$$

Eftersom $E_1^{-1} E_1 = \mathbf{1}$ kan vi byta ut dessa två matriser med identitetsmatrisen. Då ser vi att $E_2^{-1} \mathbf{1} E_2 = \mathbf{1}$, och slutligen att produkten $BA = \mathbf{1}$. Vi har nu visat satsen. □

Definition 8.1.3. En $(n \times n)$-matris A kallas inverterbar om det finns en $(n \times n)$-matris B sådan att $BA = \mathbf{1}$ och $AB = \mathbf{1}$, där $\mathbf{1}$ är identitetsmatrisen.

Följdsats 8.1.4. *Låt A vara en $(n \times n)$-matris. Om det existerar en $(n \times n)$-matris B sådan att $BA = \mathbf{1}$, då har vi också att $AB = \mathbf{1}$.*

Bevis. Om det finns en matris B sådan att $BA = \mathbf{1}$, då har vi från satsen att matrisen $A = E_1 \ldots E_s$ är en produkt av elementära matriser. Låt $C = E_s^{-1} \cdots E_1^{-1}$. Vi har att $AC = CA = \mathbf{1}$. Om vi visar att $C = B$, då är vi klara. Vi har att

$$B = B\mathbf{1} = B(AC) = (BA)C = \mathbf{1}C = C.$$

□

8.1.5. Detta betyder att för att hitta inversen A^{-1} till en matris A så behöver vi enbart hitta en vänsterinvers: en matris B sådan att $BA = \mathbf{1}$. Då är $B = A^{-1}$.

8.2 Konstruktion av invers

Vi skall nu se hur vi kan använda vad vi vet för att konstruera inversen. Om A är en matris, och R dess reducerade trappstegsform, då har vi ekvationen

$$F_s F_{s-1} \cdots F_1 A = R,$$

för några elementära matriser $F_1, \ldots, F_s$. Vi har att matrisen A är inverterbar om och endast om $R = \mathbf{1}$. Vilket också betyder att $A^{-1} = F_s \cdots F_1$. Om vi vid varje elementär radoperation gör precis samma radoperation på identitetsmatrisen så händer följande. Vi börjar med matriserna $A \mid \mathbf{1}$ och

utför en radoperation, vilket ger $F_1A \mid F_1$. Sedan gör vi nästa radoperation på dessa två matriser. Slutligen har vi

$$F_sF_{s-1}\cdots F_1A \mid F_sF_{s-1}\cdots F_1.$$

Om den reducerade trappstegsformen $R = F_s\cdots F_1A$ är identitetsmatrisen, då har vi att $A^{-1} = F_s\cdots F_1$, vilket är matrisen till höger.

Exempel 8.2.1. Vi skall konstruera inversen till matrisen

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 3 & 3 \\ 3 & 5 & 9 \end{bmatrix}.$$

Vi utför Gauss–Jordanelimination på matrisen

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 2 & 3 & 3 & 0 & 1 & 0 \\ 3 & 5 & 9 & 0 & 0 & 1 \end{array}\right]$$

Vi börjar med den ledande ettan i vänster hörn. Vi adderar -2 av första raden till andra raden och sedan -3 gånger första raden till tredje raden. Detta ger

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 3 & -2 & 1 & 0 \\ 0 & 2 & 9 & -3 & 0 & 1 \end{array}\right]$$

I andra raden har vi vår ledande etta. Vi tar -1 gånger andra raden och lägger till första raden och adderar -2 gånger andra raden till tredje raden. Detta ger

$$\left[\begin{array}{ccc|ccc} 1 & 0 & -3 & 3 & -1 & 0 \\ 0 & 1 & 3 & -2 & 1 & 0 \\ 0 & 0 & 3 & 1 & -2 & 1 \end{array}\right]$$

Sedan tar vi och adderar 1 gånger tredje raden till första raden och adderar -1 gånger tredje raden till andra raden. Slutligen multiplicerar vi tredje raden med $\frac{1}{3}$. Detta ger

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 4 & -3 & 1 \\ 0 & 1 & 0 & -3 & 3 & -1 \\ 0 & 0 & 1 & \frac{1}{3} & -\frac{2}{3} & \frac{1}{3} \end{array}\right]$$

Matrisen

$$B = \begin{bmatrix} 4 & -3 & 1 \\ -3 & 3 & -1 \\ \frac{1}{3} & -\frac{2}{3} & \frac{1}{3} \end{bmatrix}$$

har egenskapen att (kolla) $BA = \mathbf{1}$.

8.3 Uppgifter

Uppgift 8.1. Bestäm inversen till matrisen

$$A = \begin{bmatrix} 2 & 3 & 5 \\ 7 & -1 & 0 \\ 3 & -2 & 1 \end{bmatrix}.$$

Uppgift 8.2. Lös matrisekvationen

$$A \begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \\ z_1 & z_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & 37 \\ -16 & -2 \end{bmatrix},$$

där matrisen A är den i Uppgift 8.1. Detta kan även ses som ett ekvationssystem med 6 ekvationer och 6 obekanta.

Föreläsning 9

Determinanten

9.1 Permutationer

Definition 9.1.1. En avbildning $f\colon T \longrightarrow U$ mellan två mängder T och U är *injektiv* om olika element i T skickas till olika element i U. Med andra ord så är f injektiv om $f(x) = f(y)$ implicerar att $x = y$.

Exempel 9.1.2. Den naturliga avbildningen från de naturliga talen $\mathbf{N} = \{0, 1, 2, \dots, \}$ till heltalen $\mathbf{Z} = \{0, \pm 1, \pm 2, \dots, \}$ är injektiv. Mer allmänt så ger varje delmängd $T \subseteq U$ upphov till en inklusionsavbildning $i\colon T \longrightarrow U$ som är injektiv.

Exempel 9.1.3. Betrakta avbildningen $f\colon \mathbf{N} \longrightarrow \mathbf{N}$ som skickar $x \in \mathbf{N}$ till $f(x) = 2x$. Denna avbildning är injektiv då $f(x) = 2x = 2y = f(y)$ implicerar att $x = y$.

Exempel 9.1.4. Avbildningen $f_1\colon \mathbf{N} \longrightarrow \mathbf{N}$ som skickar x till $f(x) = x + 1$ är injektiv och avbildningen $f_2\colon \mathbf{Z} \longrightarrow \mathbf{Z}$ som skickar x till $f(x) = x + 1$ är injektiv.

Exempel 9.1.5. Avbildningen $g_1\colon \mathbf{N} \longrightarrow \mathbf{N}$ som skickar x till $g(x) = x^2$ är injektiv. Men $g_2\colon \mathbf{Z} \longrightarrow \mathbf{Z}$ som skickar x till x^2 är *inte* injektiv. Till exempel så är $f(1) = f(-1)$, det vill säga $x = 1$ och $x = -1$ skickas på samma tal, nämligen $1^2 = (-1)^2 = 1$.

Definition 9.1.6. En avbildning $f\colon T \longrightarrow U$ mellan mängder är *surjektiv* om det för varje element u i U åtminstone finns ett element x i T sådant att $f(x) = u$.

Exempel 9.1.7. Inklusionsavbildningen $i\colon \mathbf{N} \longrightarrow \mathbf{Z}$ är inte surjektiv. Till exempel finns inte talet -1 med i bilden av inklusionsavbildningen. Faktiskt

så är inklusionsavbildningen av en delmängd $T \subseteq U$ surjektiv endast om $T = U$.

Exempel 9.1.8. Bildrummet till en avbildning $f\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ har vi tidigare definierat, se Definition 3.3.10. Att avbildningen är surjektiv är ekvivalent med att bildrummet är hela planet.

Exempel 9.1.9. Avbildningen "multiplikation med 2" i Exempel 9.1.3 är inte surjektiv. Om vi tar ett udda tal $u = 2n + 1$ så finns det inget heltal x sådant att $u = f(x)$. Additionsavbildningen $f_1\colon \mathbf{N} \longrightarrow \mathbf{N}$ i Exempel 9.1.4 är *inte* surjektiv. Talet 0 är inte i bilden av f_1. Men additionsavbildningen $f_2\colon \mathbf{Z} \longrightarrow \mathbf{Z}$ är surjektiv.

Exempel 9.1.10. Avbildningarna i Exemplet 9.1.5 är inte surjektiva. Medan avbildningen $g_3\colon \mathbf{R} \longrightarrow \mathbf{R}_+ = \{x \in \mathbf{R} \mid x \geq 0\}$ som skickar x till x^2 är surjektiv.

Definition 9.1.11. En avbildning $f\colon T \longrightarrow U$ som är både injektiv och surjektiv kallar vi en bijektiv avbildning. En bijektiv avbildning identifierar definitionsmängden T med värdemängden U.

Lemma 9.1.12. *Låt $f\colon T \longrightarrow T$ vara en avbildning där T är en ändlig mängd. Då gäller följande.*

1) Om f är injektiv, då är f också surjektiv.

2) Om f är surjektiv, då är f också injektiv.

Bevis. Se uppgifterna. □

Definition 9.1.13. Låt $n \geq 1$ vara ett fixerat heltal. En *permutation* av talen $T_n = \{1, 2, \ldots, n\}$ är en bijektiv avbildning $\sigma\colon T_n \longrightarrow T_n$. Mängden av alla permutationer av talen $\{1, \ldots, n\}$ skrivs som $\mathfrak{S}_n$ och kallas den *symmetriska gruppen* på n element.

Exempel 9.1.14. Med $n = 1$ så består $T_1 = \{1\}$ av ett enda element. Det finns då enbart en avbildning $\sigma\colon \{1\} \longrightarrow \{1\}$, nämligen identitetsavbildningen. Denna avbildning är en permutation. Det betyder att $\mathfrak{S}_1 = \{\mathrm{id}\}$.

Exempel 9.1.15. Med $n = 2$ har vi $T_2 = \{1, 2\}$. Vi har identitetsavbildningen id som är en permutation och vi har permutationen σ_1 som skickar 1 till 2 och 2 till 1. Det vill säga avbildningen $\sigma_1\colon T_2 \longrightarrow T_2$ ges av $\sigma_1(1) = 2$ och $\sigma_1(2) = 1$. Det finns inga andra permutationer. Alltså är $\mathfrak{S}_2 = \{\mathrm{id}, \sigma_1\}$.

9.1.16. En avbildning $f\colon T_n \longrightarrow T_n$ skriver vi som matrisen

$$\begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{bmatrix}. \tag{9.1.16.1}$$

Detta betyder helt enkelt att avbildningens värde i elementet i, som är $f(i)$, finns att läsa ut under talet i.

9.1.17. Notera att denna matris inte har något att göra med våra matrisrepresentationer av linjära avbildningar.

9.1.18. Notera också att avbildningen $f\colon T_n \longrightarrow T_n$ är bijektiv om och endast om alla talen $\{1, \ldots, n\}$ förekommer i rad två i matrisen (9.1.16.1).

Exempel 9.1.19. Med $n = 3$ har vi följande permutationer

$$\mathrm{id} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \qquad \sigma_{1,2} = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

$$\sigma_{2,3} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \qquad \sigma_{1,3} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \qquad \sigma_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}.$$

Detta är alla permutationer av talen $\{1, 2, 3\}$ vilket betyder att

$$\mathfrak{S}_3 = \{\mathrm{id}, \sigma_{1,2}, \sigma_{2,3}, \sigma_{1,3}, \sigma_1, \sigma_2\}.$$

Proposition 9.1.20. *Antalet element i $\mathfrak{S}_n$ är $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.*

Bevis. Låt σ vara en permutation av talen $\{1, \ldots, n\}$. Detta är en bijektiv avbildning. Hur kan denna se ut? Det finns n möjliga element som σ kan skicka talet 1 till, nämligen alla tal $1, \ldots, n$. Avbildningen σ kan inte skicka 2 till $\sigma(1)$ eftersom avbildningen skall vara injektiv. Detta betyder att det finns $n-1$ möjliga tal att skicka 2 till, nämligen alla tal $1, \ldots, n$ förutom $\sigma(1)$. På samma sätt finns det $(n-2)$ möjligheter för σ att skicka 3 till, nämligen alla tal $1, \ldots, n$ förutom $\sigma(1)$ och $\sigma(2)$. Detta ger totalt $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = n!$ möjliga permutationer. □

Definition 9.1.21. Låt σ vara en permutation av talen $\{1, \ldots, n\}$. En *inversion* är ett talpar (i, j) med $1 \leq i < j \leq n$ sådant att $\sigma(i) > \sigma(j)$.

Definition 9.1.22. Låt σ vara en permutation av talen $\{1, \ldots, n\}$. Tecknet (signum) till permutationen definierar vi som följer

$$\mathrm{sign}(\sigma) = \begin{cases} 1 & \text{om antalet inversioner är jämnt} \\ -1 & \text{om antalet inversioner är udda.} \end{cases}$$

Vi säger även att permutation är jämn eller udda.

Exempel 9.1.23. Identitetsavbildningen id på talen $\{1, \ldots, n\}$ är en permutation utan inversioner. Detta betyder att $\text{sign}(\text{id}) = 1$.

Exempel 9.1.24. Den symmetriska gruppen $\mathfrak{S}_2$ består av identitetspermutationen och permutationen σ_1 som byter om elementen 1 och 2. Permutationen σ_1 har en inversion och tecknet -1.

Exempel 9.1.25. Elementen i $\mathfrak{S}_3$ är listade i Exempel 9.1.19. I fallet med talen $\{1, 2, 3\}$ finns det tre talpar som kan ge upphov till inversioner. Dessa är $(1, 2)$ och $(1, 3)$ och $(2, 3)$. Vi läser av från listan att identitetspermutationen saknar inversioner, att $\sigma_{1,3}$ har en inversion, att $\sigma_{2,3}$ har en inversion, att $\sigma_{1,3}$ har tre inversioner och att σ_1 och σ_2 har två inversioner. Detta betyder att

$$\text{sign}(\text{id}) = \text{sign}(\sigma_1) = \text{sign}(\sigma_2) = 1$$

$$\text{sign}(\sigma_{1,2}) = \text{sign}(\sigma_{2,3}) = \text{sign}(\sigma_{1,3}) = -1.$$

9.1.26. Vi har nu kommit till ett riktigt monster. Determinanten av en matris är en viktig invariant både inom den linjära algebran såväl som inom andra områden.

Definition 9.1.27. Låt $A = (a_{i,j})$ vara en $(n \times n)$-matris. Determinanten av A är talet

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \text{sign}(\sigma) a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Exempel 9.1.28. Låt $A = (a)$ vara en (1×1)-matris. Vi har att $\det(A) = a$.

Exempel 9.1.29. Låt $A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix}$. Vi har då att

$$\det(A) = \text{sign}(\text{id}) a_{1,1} a_{2,2} + \text{sign}(\sigma_1) a_{1,2} a_{2,1} = a_{1,1} a_{2,2} - a_{1,2} a_{2,1}.$$

Lägg märke till att definitionen av determinanten vi ger ovan sammanfaller med definitionen av determinanten för (2×2)-matriser, som vi gav i (5.2.0.1). Determinanten av en (2×2)-matris är produkten av diagonalelementen minus produkten av antidiagonalelementen.

Exempel 9.1.30. Låt nu $A = (a_{i,j})$ vara en (3×3)-matris. Determinanten är

$$\begin{aligned}
\det(A) &= \sum_{\sigma \in \mathfrak{S}_3} \text{sign}(\sigma) a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdot a_{3,\sigma(3)} \\
&= \text{sign}(\text{id}) a_{1,1} a_{2,2} a_{3,3} + \text{sign}(\sigma_{1,2}) a_{1,2} a_{2,1} a_{3,3} + \text{sign}(\sigma_{2,3}) a_{1,1} a_{2,3} a_{3,2} \\
&\quad + \text{sign}(\sigma_{1,3}) a_{1,3} a_{2,2} a_{3,1} + \text{sign}(\sigma_1) a_{1,2} a_{2,3} a_{3,1} + \text{sign}(\sigma_2) a_{1,3} a_{2,1} a_{3,2} \\
&= a_{1,1} a_{2,2} a_{3,3} - a_{1,2} a_{2,1} a_{3,3} - a_{1,1} a_{2,3} a_{3,2} \\
&\quad - a_{1,3} a_{2,2} a_{3,1} + a_{1,2} a_{2,3} a_{3,1} + a_{1,3} a_{2,1} a_{3,2}.
\end{aligned}$$

I definitionen av determinanten summerar vi över permutationerna $\sigma \in \mathfrak{S}_n$. För varje permutation så kommer motsvarande term innehålla ett element från varje rad och varje kolumn. Vi har, med σ fixerad, att termen ser ut som

$$\operatorname{sign}(\sigma) a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Detta betyder att $a_{1,\sigma(1)}$ är elementet från rad 1 och kolumn $\sigma(1)$. Eftersom σ är en permutation, kommer rad 1 och kolumn $\sigma(1)$ att vara förbrukade. Elementet $a_{2,\sigma(2)}$ återfinns på rad 2 i matrisen och kolumn $\sigma(2)$ där kolumn $\sigma(2) \neq \sigma(1)$.

Proposition 9.1.31. *Låt A vara en övertriangulär $(n \times n)$-matris, det vill säga att $a_{i,j} = 0$ om $i > j$. Då har vi att*

$$\det(A) = a_{1,1} a_{2,2} \cdots a_{n,n}.$$

Bevis. En övertriangulär matris A är på formen

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & \cdots & \cdots & a_{1,n} \\ 0 & a_{2,2} & \cdots & \cdots & \cdots & a_{2,n} \\ \vdots & \ddots & \ddots & & & \vdots \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & a_{n-1,n-1} & a_{n-1,n} \\ 0 & 0 & \cdots & 0 & 0 & a_{n,n} \end{bmatrix}.$$

Betrakta sedan determinantens definition

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sign}(\sigma) a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Den nedersta raden i matrisen A består nästan enbart av nollor; faktiskt så är $a_{n,i} = 0$ såvida inte $i = n$. Detta betyder att vi inte behöver ta med dessa termer i determinantuttrycket. Med andra ord har vi att

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n^n} \operatorname{sign}(\sigma) a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,n},$$

där $\mathfrak{S}_n^n$ är alla permutationer σ av talen $\{1, \ldots, n\}$, sådana att $\sigma(n) = n$. Vi kollar nu på den näst sista raden i matrisen A. Vi har att $a_{n-1,i} = 0$ om inte $i = n-1$ eller $i = n$. Eftersom $\sigma \in \mathfrak{S}_n^n$ fixerar talet n betyder detta att $\sigma(n-1) \neq n$. Detta innebär att vi kan förenkla ytterligare

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n^{n,n-1}} \operatorname{sign}(\sigma) a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n-1,n-1} \cdot a_{n,n},$$

där $\mathfrak{S}_n^{n,n-1}$ är alla permutationer σ sådana att $\sigma(n) = n$, och $\sigma(n-1) = n-1$. Nu är det klart att om vi fortsätter med rad $n-2$ och sedan med rad $n-3$ och hela vägen upp till första raden, så erhåller vi att

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n^{n,\dots,1}} \operatorname{sign}(\sigma) a_{1,1} \cdot a_{2,2} \cdots a_{n,n},$$

där $\mathfrak{S}_n^{n,n-1,\dots,1}$ är alla permutationer σ sådana att $\sigma(i) = i$, för alla $i = n, n-1, \dots, 1$. Det finns bara en sådan permutation och det är identitetspermutationen. Denna permutation har tecknet 1 och resultatet är visat. □

9.2 Uppgifter

Uppgift 9.1. Bestäm determinanten av matrisen

$$A = \begin{bmatrix} 2 & 3 & 5 \\ 7 & -1 & 0 \\ 3 & -2 & 1 \end{bmatrix},$$

och determinanten av dess invers (inversen har du konstruerat tidigare).

Uppgift 9.2. Visa Lemma 9.1.12.

Uppgift 9.3. Beräkna determinanten av *alla* elementära (3×3)-matriser.

Uppgift 9.4. Konstruera en bijektiv avbildning $f \colon \mathbf{N} \longrightarrow \mathbf{Z}$.

Föreläsning 10

Egenskaper hos determinanten

10.1 Inversioner

Vi behöver etablera en liten sats om tecknet till en viss typ av permutationer, så kallade transpositioner. Betrakta mängden av permutationer av talen $\{1, \ldots, n\}$. För varje talpar $1 \leq i, j \leq n$ med $i \neq j$ har vi permutationen $\tau_{i,j}$ som är definierad som

$$\tau_{i,j}(p) = \begin{cases} p & \text{om} \quad p \neq i, p \neq j \\ i & \text{om} \quad p = j \\ j & \text{om} \quad p = i. \end{cases}$$

Denna permutation kallas en transposition. Permutationen $\tau_{i,j}$ byter helt enkelt plats på positionerna i och j och gör i övrigt ingenting. Vi har helt klart att $\tau_{i,j} = \tau_{j,i}$ och att $\tau_{i,j}\tau_{i,j} = \mathrm{id}$.

Lemma 10.1.1. *För varje permutation $\sigma \in \mathfrak{S}_n$ och varje transposition $\tau_{i,j}$ har vi att*

$$\mathrm{sign}(\sigma\tau_{i,j}) = -\mathrm{sign}(\sigma).$$

Bevis. Se uppgifterna. □

Sats 10.1.2. *Låt A vara en $(n \times n)$-matris. Determinantfunktionen har följande egenskaper.*

1) *Om vi multiplicerar en rad i A med ett tal c, så är determinanten av denna nya matris $c \cdot \det(A)$.*

2) *Om två rader i matrisen A är lika, så är $\det(A) = 0$.*

3) Om varje element i raden p av matrisen A är på formen $a_{p,k} = b_{p,k} + c_{p,k}$, för $k = 1, \dots n$, så har vi

$$\det \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \vdots & \\ b_{p,1} + c_{p,1} & \cdots & b_{p,n} + c_{p,n} \\ & \vdots & \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} = \det \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \vdots & \\ b_{p,1} & \cdots & b_{p,n} \\ & \vdots & \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} + \det \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \vdots & \\ c_{p,1} & \cdots & c_{p,n} \\ & \vdots & \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix}.$$

Bevis. Låt oss börja med att visa påstående 1). Låt $B = (b_{i,j})$ vara matrisen vi får när vi multiplicerar rad p av matrisen A med ett tal c. Vi har då att $b_{p,j} = ca_{p,j}$ för alla $j = 1, \dots n$ och $b_{i,j} = a_{i,j}$ om $i \neq p$, för alla $j = 1, \dots, n$. Detta ger

$$\begin{aligned} \det(B) &= \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sign}(\sigma) b_{1,\sigma(1)} \cdot b_{2,\sigma(2)} \cdots b_{n,\sigma(n)} \\ &= \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sign}(\sigma) a_{1,\sigma(1)} \cdots a_{p-1,\sigma(p-1)} c a_{p,\sigma(p)} a_{p+1,\sigma(p+1)} \cdots a_{n,\sigma(n)} \\ &= c \det(A). \end{aligned}$$

Påståendet 3) visas på samma sätt och överlåtes till läsaren. Det som kvarstår är att visa påståendet 2). Låt rad i och rad j i matrisen A vara lika. Detta betyder att $a_{i,k} = a_{j,k}$ för alla $k = 1, \dots, n$. Betrakta determinanten

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sign}(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}.$$

Vi kommer att visa att denna summa är lika med noll och, mera specifikt, att varje term förekommer två gånger men med olika tecken. Fixera en permutation σ och betrakta permutationen

$$\tau(p) = \begin{cases} \sigma(p) & \text{om} \quad p \neq i, p \neq j \\ \sigma(i) & \text{om} \quad p = j \\ \sigma(j) & \text{om} \quad p = i. \end{cases}$$

Då är $a_{i,\sigma(i)} = a_{j,\tau(j)}$ och $a_{j,\sigma(j)} = a_{i,\tau(i)}$, vilket ger att

$$a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} = a_{1,\tau(1)} \cdots a_{n,\tau(n)}.$$

Vi har vidare att $\tau = \sigma\tau_{i,j}$ och av Lemma 10.1.1 ser vi att $\operatorname{sign}(\tau) = -\operatorname{sign}(\sigma)$. Det är nu klart att determinanten $\det(A) = 0$. □

Följdsats 10.1.3. *Om vi byter plats på två olika rader i en matris A, så är determinanten av denna nya matris $-\det(A)$.*

Bevis. Fixera två tal $1 \leq i, j \leq n$ med $i \neq j$. Betrakta matrisen B vars rad i *och* rad j är

$$a_{i,1} + a_{j,1} \quad a_{i,2} + a_{j,2} \quad \cdots \quad a_{i,n} + a_{j,n}$$

De andra raderna i B låter vi vara som i A. Av påstående 2) i satsen ovan har vi att $\det(B) = 0$. Vi använder påstående 3) i satsen ovan på raden i och därefter på raden j och erhåller att

$$\begin{aligned}\det(B) = \det\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \vdots & \\ a_{i,1} & \cdots & a_{i,n} \\ & \vdots & \\ a_{i,1} & \cdots & a_{i,n} \\ & \vdots & \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} + \det\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \vdots & \\ a_{i,1} & \cdots & a_{i,n} \\ & \vdots & \\ a_{j,1} & \cdots & a_{j,n} \\ & \vdots & \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} \\ + \det\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \vdots & \\ a_{j,1} & \cdots & a_{j,n} \\ & \vdots & \\ a_{i,1} & \cdots & a_{i,n} \\ & \vdots & \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} + \det\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \vdots & \\ a_{j,1} & \cdots & a_{j,n} \\ & \vdots & \\ a_{j,1} & \cdots & a_{j,n} \\ & \vdots & \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix}.\end{aligned}$$

Vi har att vänsterledet $\det(B) = 0$. Av de fyra matriserna som förekommer i högerledet är rad i lika med rad j i den första och den fjärde matrisen. Av påstående 2) i satsen ovan är deras determinanter därför noll. Vi har därmed att determinanten av andra matrisen i högerledet adderat till determinanten av tredje matrisen i högerledet är lika med noll. Detta visar satsen. □

Lemma 10.1.4. *Låt E vara en elementär $(n \times n)$-matris och A en $(n \times n)$-matris. Då är*

$$\det(EA) = \det(E)\det(A).$$

Bevis. Det finns tre klasser av elementära matriser. Låt E vara en elementär matris sådan att EA byter plats på raderna i och j i matrisen A. Det vill säga att $E = E_{i,j}$ med notationen från föreläsning 7. Av Sats 10.1.3 följer att $\det(EA) = -\det(A)$. Då identitetsmatrisen har determinant 1 har vi också att $\det(E) = -1$. Vi har därmed att $\det(E)\det(A) = -\det(A)$ och vi har visat påståendet för denna klass av elementära matriser.

Låt $E = E_i(k)$ vara den elementära matris vi får genom att multiplicera rad i av identitetsmatrisen med talet $k \neq 0$. Av Sats 10.1.2, påstående 1), har

vi att $\det(EA) = k\det(A)$ och att $\det(E) = k$. Detta visar att $\det(EA) = \det(E)\det(A)$ för alla elementära matriser i denna klassen.

Den sista klassen är elementära matriser $E = E_{i,j}(c)$. Vi har att $E_{i,j}(c)A$ ger en ny matris där vi ändrar rad i av matrisen A genom att addera c gånger rad j. Från påstående 3) i Sats 10.1.2 följer det att $\det(E_{i,j}(c)A) = \det(A)$ och att $\det(E_{i,j}(c)) = 1$. Vi har visat satsen. □

Sats 10.1.5 (Fundamentala egenskapen till determinantfunktionen)**.** *Låt A vara en $(n \times n)$-matris. Då är matrisen A inverterbar om och endast om* $\det(A) \neq 0$.

Bevis. Vi kan skriva matrisen A som en produkt $A = E_1 \cdots E_r R$ med elementära matriser $E_1, \ldots, E_r$ och där R är den reducerade trappstegsformen till matrisen A. Av Lemma 10.1.4 följer det att

$$\det(A) = \det(E_1)\det(E_2 \cdots E_r R) = \det(E_1) \cdots \det(E_r) \cdot \det(R).$$

Vi har tidigare visat att en matris A är inverterbar om och endast om R är identitetsmatrisen. Om A är inverterbar, då har vi att $A = E_1 \cdots E_r$ är en produkt av elementära matriser. Varje elementär matris har en nollskild determinant och det följer att $\det(A) \neq 0$. Är däremot matrisen A inte inverterbar så är den reducerade trappstegsformen R inte identitetsmatrisen. Man beräknar (se uppgift 10.2) att $\det(R) = 0$ och vi har att $\det(A) = 0$. □

Exempel 10.1.6. För varje tal t betraktar vi ekvationssystemet i tre okända x, y, z

$$(\star) \quad \begin{cases} tx + 2y + z &= 3 \\ -y &= 2 \\ x + y + tz &= 1. \end{cases}$$

Vi vill avgöra för vilka t ekvationssystemet har en unik lösning. Vi skriver om $(\star)$ på matrisform $AX = B$, där

$$A = \begin{bmatrix} t & 2 & 1 \\ 0 & -1 & 0 \\ 1 & 1 & t \end{bmatrix} \quad X = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \quad B = \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}.$$

Systemet $(\star)$ har en unik lösning om och endast om matrisekvationen $AX = B$ har en unik lösning. Ekvationen $AX = B$ har en unik lösning om och endast om A^{-1} finns (se uppgift 10.3), vilket är ekvivalent med att $\det(A) \neq 0$. Vi beräknar determinanten av matrisen A och erhåller att

$$\det(A) = t(-t) + 1 = -t^2 + 1.$$

Determinanten är nollskild om $t \neq \pm 1$ och systemet $(\star)$ har en unik lösning om $t \neq \pm 1$.

Sats 10.1.7. *Låt A och B vara två $(n \times n)$-matriser. Vi har att*

$$\det(AB) = \det(A)\det(B).$$

Bevis. Vi påminner om att en matris C är singulär om och endast om det finns en nollskild vektor X sådan att $CX = 0$. Vi ser nu att om matrisen B är singulär då finns en nollskild vektor X sådan att $BX = 0$. Då är också $(AB)X = 0$ och matrisen AB är singulär. Om istället A är singulär och B är inverterbar (icke singulär), då påstår vi att matrisen AB också är singulär. Vi vet att det finns en nollskild vektor X sådan att $AX = 0$. Låt $W = B^{-1}X$, som också är nollskild. Vi har då att $ABW = ABB^{-1}X = AX = 0$.

Med andra ord har vi att om A eller B är singulära då är också produkten AB singulär. Av Sats 10.1.5 har vi därmed att $\det(AB) = 0$ och att minst en av faktorerna i $\det(A)\det(B)$ är noll. Vi har därmed visat satsen när antingen A eller B är singulär. Det fall som kvarstår är när både A och B är inverterbara. Men då är $A = E_1 \cdots E_r$ och $B = F_1 \cdots F_s$ produkter av elementära matriser. Av Lemma 10.1.4 följer det nu att $\det(AB) = \det(A)\det(B)$ och detta visar satsen. □

Följdsats 10.1.8. *Om matrisen A är inverterbar har vi att*

$$\det(A^{-1}) = \frac{1}{\det(A)}.$$

Bevis. Vi har att AA^{-1} är lika med identitetsmatrisen. Determinanten av identitetsmatrisen är 1 och av satsen erhåller vi att

$$\det(A)\det(A^{-1}) = 1.$$

□

10.2 Uppgifter

Uppgift 10.1. Visa Lemma 10.1.1. Detta kan göras på följande sätt. Notera först att permutationen $\tau_{i,i+i}$ har en enda inversion och följaktligen är $\operatorname{sign}(\tau_{i,i+1}) = -1$. Därefter verifierar du att antalet inversioner i $\sigma\tau_{i,i+1}$ är ett mindre eller mera än antalet inversioner i σ. Speciellt har du då visat att

$$\operatorname{sign}(\sigma\tau_{i,i+1}) = -\operatorname{sign}(\sigma). \tag{10.2.0.1}$$

Du är nu klar med transpositioner på formen $\tau_{i,i+1}$. För att behandla godtyckliga transpositioner $\tau_{i,j}$ kan vi anta att $j > i$. Vi skriver $j = i + p$ för något tal $p > 0$. Visa att vi har

$$\tau_{i,i+p} = \tau_{i,i+1} \cdots \tau_{i+p-2,i+p-1}\tau_{i+p-1,i+p}\tau_{i+p-2,i+p-1} \cdots \tau_{i+1,i+2}\tau_{i,i+1}.$$

Kom ihåg att läsa funktionssammansättning från höger. Gör ett litet exempel, $p = 3$, om det är svårt att förstå likheten ovan. Notera att $\tau_{i,i+p}$ alltså kan skrivas som en sammansättning av $2(p-1)+1$ stycken transpositioner på formen $\tau_{j,j+1}$. För att bestämma $\operatorname{sign}(\sigma\tau_{i,i+p})$ använder vi nu identiteten ovan och identiteten (10.2.0.1). Detta ger

$$\operatorname{sign}(\sigma\tau_{i,i+p}) = (-1)^{2(p-1)+1}\operatorname{sign}(\sigma).$$

Uppgift 10.2. Låt A vara en $(n \times n)$-matris och låt R vara dess reducerade trappstegsform. Antag att R *inte* är identitetsmatrisen. Visa att $\det(R) = 0$.

Uppgift 10.3. Förklara varför matrisekvationen $AX = B$ har en unik lösning $X = A^{-1}B$ om och endast om inversen A^{-1} finns (Notera att om X och Y är två lösningar då är $A(X - Y) = 0$ och använd sedan Sats 8.1.2).

Föreläsning 11

Markovkedjor

11.1 Iterativ fördelning

Vi skall idag titta på ett exempel av något som kallas Markovkedjor. Exemplet vi tittar på är kanske inte helt realistiskt och vi skall senare se mera realistiska användningar. Exemplet nedanför är en nedskalad version där huvudsyftet är att förklara Markovkedjor.

11.1.1. Vi tänker oss följande problem. På Campus finns det två pubar A och B. Det finns 9000 studenter och varje fredag går alla studenter på en pub.[1] Den första fredagen väljer hälften av studenterna pub A och den andra hälften pub B. Men nästa fredag fördelas studenterna efter följande mönster. Hela 60% av studenterna som förra fredagen var på pub A väljer att gå tillbaka till pub A och de resterande 40% går följaktligen till pub B. Av de som var på pub B förra fredagen väljer 80% att gå till pub A. Detta betyder att enbart 20% av studenterna som förra fredagen valde pub B återgår till pub B. Detta fördelningsmönster upprepas varje fredag. Det enda som betyder något för valet av pub är vilken pub man besökte förra fredagen.

Vi är intresserade av att veta hur fördelningen av studenterna ser ut efter studietiden. Studietiden är mycket lång som ni säkerligen vet.

Exempel 11.1.2. Låt oss beräkna fördelningen de första fredagarna. Den första fredagen F_1 är det 4500 studenter på varje pub. Vi skriver detta som en vektor $F_1 = (4500, 4500)$. Fredagen därefter har

$$4500 \cdot \frac{60}{100} + 4500 \cdot \frac{80}{100} = 450 \cdot 14 = 4500 + 1600 + 200 = 6300$$

[1] Till alla upprörda moralister kan jag tillägga att det enbart serveras alkoholfri läsk.

studenter valt pub A och de resterande 2700 har valt pub B. På vektorform har vi att $F_2 = (6300, 2700)$. Den tredje fredagen F_3 har vi följande fördelning

$$F_3 = (5940, 3060).$$

Komponenterna till vektorn F_3 var beräknade som följer

$$6300 \cdot \frac{60}{100} + 2700 \cdot \frac{80}{100} = 630 \cdot 6 + 270 \cdot 8 = 5940,$$

och $9000 - 5940 = 3060$.

11.1.3. Vi kommer nu att ge en beskrivning av problemet med hjälp av matriser och matrismultiplikation. För varje positivt heltal $n \geq 0$, låt

$$F_n = \begin{bmatrix} a_n \\ b_n \end{bmatrix}$$

vara vektorn där a_n är antalet studenter vid pub A, den n:te fredagen, och där b_n är antalet studenter vid pub B. Av beskrivningen av problemet har vi att för varje $n \geq 1$ så är

$$F_n = \begin{bmatrix} \frac{6}{10} & \frac{8}{10} \\ \frac{4}{10} & \frac{2}{10} \end{bmatrix} F_{n-1}. \tag{11.1.3.1}$$

Att ekvationen (11.1.3.1) verkligen stämmer ser vi om vi utför matrisprodukten. Vi har att $F_{n-1} = (a_{n-1}, b_{n-1})$ och detta ger

$$\begin{bmatrix} \frac{6}{10} & \frac{8}{10} \\ \frac{4}{10} & \frac{2}{10} \end{bmatrix} F_{n-1} = \begin{bmatrix} a_{n-1}\frac{6}{10} + b_{n-1}\frac{8}{10} \\ a_{n-1}\frac{4}{10} + b_{n-1}\frac{2}{10} \end{bmatrix}.$$

Den första komponenten i produktmatrisen ges av 60% av de som var i pub A fredagen $(n-1)$ samt 80% av de som var i pub B. Den andra komponenten i matrisen ges av 40% av de som var i pub A samt 20% av de som var i pub B. Detta är fördelningen fredagen n, med andra ord vektorn F_n.

Definition 11.1.4. En $(m \times m)$-matris $A = (a_{i,j})$ är en *stokastisk matris* om följande två krav är uppfyllda.

1) Varje element i matrisen A är icke-negativt, det vill säga att $a_{i,j} \geq 0$ för alla par $1 \leq i, j \leq m$.

2) Varje kolumn i matrisen A summerar till 1, det vill säga att $\sum_{i=1}^{m} a_{i,j} = 1$, för alla $1 \leq j \leq m$.

Exempel 11.1.5. Matrisen

$$A = \begin{bmatrix} \frac{6}{10} & \frac{8}{10} \\ \frac{4}{10} & \frac{2}{10} \end{bmatrix}$$

som vi har från beskrivning (11.1.3.1) är en stokastisk matris.

11.1.6. Om vi återgår till problemet med fördelningen av studenter vid pubarna A och B har vi att $F_n = AF_{n-1}$ för alla $n > 1$. Det betyder att $F_2 = AF_1$ och att $F_3 = AF_2$ men också att

$$F_3 = AF_2 = A(AF_1) = A^2F_1.$$

Allmänt har vi att

$$F_n = AF_{n-1} = AA \cdots AF_1 = A^{n-1}F_1.$$

Vi är intresserade av F_n när n blir mycket stor. Låt oss kalla fördelningen vid slutet av studietiden för F_∞. Vi har att

$$F_\infty = \lim_{n\to\infty} F_n = \lim_{n\to\infty} (A^{n-1}F_1).$$

11.1.7. Input från teorin om egenrum. När man har läst litet mera linjär algebra och behärskar teorin om egenrum, då är det inte svårt att producera följande matrisfaktorisering

$$A = \begin{bmatrix} 2 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -\frac{1}{5} \end{bmatrix} \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{2}{3} \end{bmatrix}.$$

Vi behöver inte något om egenrum; vi verifierar bara att vi har matrisfaktorisering ovan. Låt

$$P = \begin{bmatrix} 2 & 1 \\ 1 & -1 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 0 \\ 0 & -\frac{1}{5} \end{bmatrix} \quad Q = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{2}{3} \end{bmatrix}.$$

Vi beräknar att

$$PD = \begin{bmatrix} 2 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -\frac{1}{5} \end{bmatrix} = \begin{bmatrix} 2 & -\frac{1}{5} \\ 1 & \frac{1}{5} \end{bmatrix}$$

och att

$$PDQ = \begin{bmatrix} 2 & -\frac{1}{5} \\ 1 & \frac{1}{5} \end{bmatrix} \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{2}{3} \end{bmatrix} = \begin{bmatrix} \frac{2}{3} - \frac{1}{15} & \frac{2}{3} + \frac{2}{15} \\ \frac{1}{3} + \frac{1}{15} & \frac{1}{3} - \frac{2}{15} \end{bmatrix}.$$

Om man nu förenklar bråkuttrycken i matrisen ovan så ser man att $PDQ = A$. Eller hur? Vi har att

$$\frac{2}{3} - \frac{1}{15} = \frac{10}{15} - \frac{1}{15} = \frac{9}{15} = \frac{6}{10},$$

vilket är elementet $a_{1,1}$ i matrisen A och så vidare.

11.1.8. En formel för matrisprodukten A^n. Vi har sett att matrisen A kan skrivas som en produkt PDQ. Det betyder att

$$A^n = (PDQ)^n = PDQ \cdot PDQ \cdots PDQ.$$

Man kan undra hur detta kan hjälpa oss att beräkna A^n. Om vi nu tittar närmare på matrisen

$$P = \begin{bmatrix} 2 & 1 \\ 1 & -1 \end{bmatrix}$$

så ser vi att determinanten är -3 och alltså nollskild. Det betyder att P^{-1} existerar och en formel för inversen till (2×2)-matriser har vi. Vi ser nu att $Q = P^{-1}$. Alltså är $QP = 1$ och använder vi detta erhåller vi att

$$A^n = PDQ \cdot PDQ \cdots PDQ = PD^nQ.$$

Slutligen har vi att matrisen D är en diagonalmatris och produkter av diagonalmatriser är enkla att utföra. Vi har att

$$D^n = \begin{bmatrix} 1 & 0 \\ 0 & \frac{-1}{5} \end{bmatrix}^n = \begin{bmatrix} 1 & 0 \\ 0 & (\frac{-1}{5})^n \end{bmatrix}.$$

Detta ger nu att matrisprodukten A^n blir produkten av *tre* matriser

$$\begin{aligned} A^n &= \begin{bmatrix} 2 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & (\frac{-1}{5})^n \end{bmatrix} \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{2}{3} \end{bmatrix} \\ &= \begin{bmatrix} 2 & \frac{(-1)^n}{5^n} \\ 1 & \frac{(-1)^{n+1}}{5^n} \end{bmatrix} \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{2}{3} \end{bmatrix} \\ &= \begin{bmatrix} \frac{2}{3} + \frac{1}{3}\frac{(-1)^n}{5^n} & \frac{2}{3} + \frac{2}{3}\frac{(-1)^{n+1}}{5^n} \\ \frac{1}{3} + \frac{1}{3}\frac{(-1)^{n+1}}{5^n} & \frac{1}{3} + \frac{2}{3}\frac{(-1)^n}{5^n} \end{bmatrix}. \end{aligned}$$

Vi har nu beräknat A^n för godtyckliga positiva heltal n.

11.2 Slutfördelningen

Nu har vi beräknat A^n och fördelningen fredagen F_{n+1} blir

$$\begin{aligned} F_{n+1} = A^n \cdot F_1 &= \begin{bmatrix} \frac{2}{3} + \frac{1}{3}\frac{(-1)^n}{5^n} & \frac{2}{3} + \frac{2}{3}\frac{(-1)^{n+1}}{5^n} \\ \frac{1}{3} + \frac{1}{3}\frac{(-1)^{n+1}}{5^n} & \frac{1}{3} + \frac{2}{3}\frac{(-1)^n}{5^n} \end{bmatrix} \begin{bmatrix} 4500 \\ 4500 \end{bmatrix} \\ &= \begin{bmatrix} 3000 + \frac{(-1)^n}{5^n}1500 + 3000 + \frac{(-1)^{n+1}}{5^n}3000 \\ 1500 + \frac{(-1)^{n+1}}{5^n}1500 + 1500 + \frac{(-1)^n}{5^n}3000 \end{bmatrix} \end{aligned}$$

Låter vi $n \gg 0$ bli mycket stor då blir $(1/5^n)$ mycket liten och vi kan bortse från dess bidrag. Detta ger att

$$F_\infty = \begin{bmatrix} 6000 \\ 3000 \end{bmatrix}.$$

Vid slutet av studietiden är det alltså, ungefär, 6000 studenter vid pub A, och 3000 studenter vid pub B.

11.2.1. Utfallsvektorer. Istället för att titta på antalet studenter vid varje pub, kan man istället titta på andelen studenter. En vektor $X = (x_1, \ldots, x_m)$ i $\mathbf{R}^m$ kallas en *utfallsvektor* om $x_i \geq 0$, för alla $i = 1, \ldots, m$, och om

$$x_1 + x_2 + \cdots + x_m = 1.$$

Exempel 11.2.2. Som exempel kan vi ta fördelningen av studenter till de två pubarna A och B. Den första fredagen valde hälften pub A och andra hälften pub B. Detta kan beskrivas med utfallsvektorn $F_1 = (\frac{1}{2}, \frac{1}{2})$. Och slutfördelningen F_∞ gav att $2/3$ valde pub A och $1/3$ valde pub B. Som utfallsvektor kan vi skriva $F_\infty = (\frac{2}{3}, \frac{1}{3})$.

Lemma 11.2.3. *Låt A vara en stokastisk matris och X en utfallsvektor. Då är också AX en utfallsvektor.*

Bevis. Kan du visa detta? □

Definition 11.2.4. Låt $\{X_1, X_2, X_3, \ldots\}$ vara en sekvens av utfallsvektorer i $\mathbf{R}^m$, där talet m är fixerad. Om det finns en stokastisk matris A sådan att $X_n = AX_{n-1}$, för alla $n > 1$, då kallas sekvensen $\{X_n\}_{n\geq 1}$ en Markovkedja.

Exempel 11.2.5. Vektorerna $F_n = (a_n, b_n)$ som anger antalet studenter vid pub A och pub B, den n:te fredagen är en sekvens av vektorer i $\mathbf{R}^2$. Sekvensen $\{F_n\}_{n\geq 1}$ är en Markovkedja då vi har sambandet $F_n = AF_{n-1}$ givet i (11.1.3.1) och matrisen A är en stokastisk matris.

11.3 Oberoende av initialvärdet

I exemplet vi har diskuterat i dag började vi med initialvärdet $F_1 = (\frac{1}{2}, \frac{1}{2})$. Fördelningen vid slutet av studietiden blev $F_\infty = (\frac{2}{3}, \frac{1}{3})$. Det lustiga är dock att vi inte behöver läsa av initialvärdet F_1; slutfördelningen blir oavsett $(\frac{2}{3}, \frac{1}{3})$. Låt $F_1 = (p, q)$ vara en godtycklig utfallsvektor. Det betyder att p andel av studenterna väljer pub A och q andel av studenterna väljer pub B den första fredagen. Vi har att p och q är icke-negativa tal sådana att $p + q = 1$.

Fördelningen vid slutet av studietiden blir

$$F_\infty = \lim_{n\to\infty} A^n \begin{bmatrix} p \\ q \end{bmatrix}.$$

Nu beräknar vi $A^n F_1$ och sätter sedan $(1/5)^n$ lika med noll. Detta ger

$$F_\infty = \begin{bmatrix} \frac{2}{3}p + \frac{2}{3}q \\ \frac{1}{3}p + \frac{1}{3}q \end{bmatrix} = \begin{bmatrix} \frac{2}{3}(p+q) \\ \frac{1}{3}(p+q) \end{bmatrix}.$$

Vi har att $p+q = 1$ och det följer att $F_\infty = (\frac{2}{3}, \frac{1}{3})$. Vi får samma slutresultat F_∞ oberoende av initialvärdet till utfallsvektorn F_1.

11.3.1. Ibland, som i exemplet ovan, beror inte slutresultatet F_∞ på initialvärdet. Dock finns det exempel på stokastiska matriser där slutresultatet beror av initialvärdet och det finns stokastiska matriser där det inte finns något slutvärde alls. Kan du konstruera sådana exempel? Konstruera en stokastisk (2×2)-matris A sådan att $X_\infty = \lim_{n\to\infty} A^n X_1$ beror på vilken utfallsvektor X_1 man börjar med. Lite svårare är att hitta en stokastisk matris B sådan att $X_\infty = \lim_{n\to\infty} B^n X_1$ inte finns. Prova!

Forelesning 12

Google og informasjonssortering

Nettet[1] som vi alle kjenner til er en enorm hop av hjemmesider inneholdende all mulig tenkelig og utenkelig informasjon. Det er en fantastisk følelse å ha tilgang til all den informasjon som finnes på nettet. Et umiddelbart problem som dykker opp er hvordan man skal finne relevant informasjon. Vi skal her beskrive hvordan søkmotoren Google finner nålen i høystakken.

12.1 Nettet

Internett består av hjemmesider. Hver hjemmeside har en unik adresse, og sidene inneholder tekst samt pekere (linker) til andre hjemmesider. En nettleser gjør det mulig å åpne og lese en hjemmeside, og problemet som søkmotorene skal hjelpe oss med er å sortere ut hjemmesidene som er relevante for en gitt søkning.

For å forstå kompleksiteten i problemet gjeldende informasjonssorteringen er det verdt å merke seg følgende. Nettet er veldig stort, og faktisk er det vanskelig å bestemme antallet hjemmesider. Et estimat gjort januar 2004 (se [2]) indikererer at det dengang fantes 10 milliarder hjemmesider som i snitt inneholdt 500 KB informasjon. Vidre har vi at nettet er dynamisk. Ikke bare dukker det opp kontinuerlig nye hjemmesider, men gamle sider endres ved at ny tekst og nye pekere legges til.

Blåkopi Før man begynner å sortere informasjonen, så tar man først en slags blåkopi av nettet. Små avanserte program (såkalte webcrawlers) søker opp nettets hjemmesider, leser av informasjonen og følger opp pekerne

[1] Detta kapitel har jag inte hunnit översätta till svenska, eventuelt svorska.

for å finne fler hjemmesider. Siden nettet hele tiden endrer seg blir disse programmene aldri avsluttede, men går til stadighet gjennom eksisterende hjemmesider. Det tar omtrent (se [1]) tre hele uker for å søke gjennom nettet!

Informasjonen som disse programmene henter blir lagret i en stor indekseringsfil. I indekseringsfilen lagres alle typer av ord som blir funnet på hjemmesiden, samt informasjon om hvilke hjemmesider som inneholder de respektive ordene. Om vi tenker oss hjemmesidene nummererte som $1, 2, \ldots$, da kan en del av indekseringsfilen se ut som

- matrimonium 8, 24
- matrise 3, 11, 15, 879, 1000032
- matrose 6, 11, 3059.

Dette betyr at ordet "matrise" forekommer på hjemmesidene nummerert som 3, 11, 15, 879 og 1000032, mens hjemmeside 11 inneholdt både termen matrise og matrose. Denne indekseringsfilen er selvsagt enorm da alle typer av ord, innefor alle tenkelige språk forekommer. Året 2003 var denne indekseringsfilen omkring 4 milliarder stor og Google hadde en maskinpark bestående av 15000 datamaskiner for å lagre indekseringsfilen. Men, poenget er at selv om denne filen er stor så tar det ikke langt tid for en datamaskin å søke igjennom en slik liste.

12.2 Rangering

Når vi bruker en søkmotor så skriver vi inn en tekst eller bare et ord som beskriver vårt interesse. Deretter vil søkmotoren liste opp alle hjemmesider som inneholder vår søkte tekst. Disse hjemmesider blir listet etter en gitt rangering, der hjemmeside med høyest rang kommer først. Grunnen til at de fleste av oss bruker søkmotoren Google er fordi den har en rangering som vi opplever som fornuftig; de mest relevante sidene kommer først.

For eksempel, om du gjør et søk på ordet "matrise" så for du ikke bare 5 treff som eksemplet vårt over indikerer, men hele 175 000 treff. Det tar Google cirka 0.2 sekunder for å bestemme en ordnet liste av de 175 000 hjemmesider som inneholder ordet matrise, og høyest opp kommer Wikipedia. Hvordan er dette mulig?

Popularitetsrangering Et menneske kan fort avgjøre hvorvidt en hjemmeside virker relevant eller ikke, men en søkmotor har ingen kvalitativ forståelse

av tekst. I prinisippet kan et program bare telle hvor mange ganger et gitt ord forekommer.

I tiden før soekmotoren Google var det vanlig å rangere hjemmesidene etter hvor mange pekere en side hadde, en såkalt *popularitetsrangering*. En hjemmeside som hadde mange pekere til seg måtte være viktig siden mange eiere av hjemmesider hadde lagt til en peker dit. En annen rangering som var brukt telte kun hvor mange ganger et gitt ord forekom på siden. Her tenkte man seg at en viktig side ville anvende det gitte ordet flere ganger. Popularitetsrangeringen gir en bedre rangering enn å kun telle antallet forekomster av et ord per side, men popularitetsrangeringen er lett å manipulere. For å fremheve sin side under denne rangeringen lager man en million nye hjemmesider som inneholder en peker til sin side. Man skal ikke glemme at det finnes mange kommersielle aktører ute på nettet som er veldig interesserte i å få sine sider synlige. En god og fornuftig rangering må være vanskelig å manipulere.

Blant annet ryktes det om at en av pre-Google tidens store søkemotorer, Alta Vista, ikke ville returnerer sin egen hjemmesiden som den viktigste når man søkte på "Alta Vista". Et beskrivende eksempel på at rangeringsordningen ikke fungerte.

PageRank For å rangere hjemmesider skapte Sergey Brin og Larry Page en rangering som siden 1998 har dominert markedet for søkmotorer. Å gjøre et nettsøk med en søkmotor heter idag simpelthen å google.

Selv grunnideen som vi skal beskrive er enkel. Hver peker til en hjemmeside P skal vi tenke på som et rekommendasjonsbrev for P. En hjemmeside med mange rekommendasjonsbrev bør i utgangspunktet være mere viktig en en hjemmeside med få rekommendasjonsbrev. Men, som vi indikerte over er dette alene ikke nok for å gi en god rangering. Vi skal også ta hensyn til hvem som sender rekommendasjonsbrevene, dvs. hvilke sider som peker til hjemmesiden P.

Eksempel 12.2.1. Vi tenker oss personer som søker jobb. Deres rekommendasjonsbrev vil være avgjørende for rangeringen av de søkende, og i dette eksemplet tenker vi oss at de ikke har noen andre merittlister. Her kan vi tenke oss at en søker X har 1000 rekommendasjonsbrev, mens en annen søker Y har et brev. Om jobben for eksempel handlet om IT og programmering og Y har rekommendasjonsbrev fra Bill Gates, da er det rimelig å rangere Y før X, til tross for det store antallet rekommendasjonsbrev X har. Et rekommendasjonsbrev fra Bill Gates vil regnes som viktig. Men om det viste seg at en person som regnes som viktig, skriver veldig mange rekommendasjonsbrev da blir dennes brev med en gang mindre viktige.

Matematisk formalisering La oss gjøre om ideen i Eksempel 12.2.1 til en matematisk modell for rangering av hjemmesider. Vi tenker oss at nettets hjemmesider er nummererte som $P_1, P_2, \ldots P_n$. Vi leser av antallet pekere $|P_j|$ fra hjemmeside P_j; denne informasjonen har vi også lagret på indekseringsfilen. Viktigheten, eller rangen, til hjemmeside P_j skriver vi som $r(P_j)$ og er ennå et ubestemt tall. Basert på eksemplet med rekommendasjonsbrev vil vi at rangen til en hjemmeside P skal baseres på pekere fra andre hjemmesider til hjemmeside P. Pekerne tenker vi på som rekommendasjonsbrev. Hver hjemmeside Q som peker til hjemmesiden P har selv en viktighet, dvs rang. Rangen til hjemmesiden Q skal vekte pekeren, men vi vil også ta hensyn til hvorvidt hjemmesiden Q har mange pekerer til andre hjemmesider. Dette gir at rangen til en hjemmeside P_i skal tilfredstille ligningen

$$r(P_i) = \sum_{j \mapsto i} \frac{r(P_j)}{|P_j|}, \tag{12.2.1.1}$$

der vi summerer over alle hjemmesider $j \mapsto i$ som peker til hjemmesiden P_i. Rangen til P_i bestemmes som summen av rangen av innpekende hjemmesider delt på deres totale antall pekere.[2]

Det er verdt å bemerket at rangen $r(P)$ til en hjemmeside er enn så lenge en ubestemte verdi. Vi har kun satt opp ligningssystemet (12.2.1.1) som vi ønsker skal bestemme rangeringsvektoren. Det er ingenting som garanterer at ligningssystemet har, ikke trivielle, løsninger.

Hyperlinkmatrisen Vi vil nå vise hvordan vi løser PageRank ligningen (12.2.1.1). Vi lar $P_1, P_2, \ldots, P_n$ være hjemmesidene, og vi lar $|P_j|$ være antallet pekere fra hjemmeside P_j. Vi teller antallet pekere fra P_j til P_i som maksimalt en. Vi konstruerer deretter hyperlinkmatrisen H som er en $(n \times n)$-matrise, og der koeffisient (i, j) er

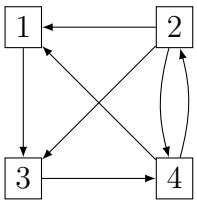
$$H_{i,j} = \begin{cases} \frac{1}{|P_j|} & \text{om hjemmeside } j \text{ peker til hjemmeside } i, \\ 0 & \text{ellers.} \end{cases}$$

Merk at definisjonen av hyperlinkmatrisen H bare gir mening hvis alle hjemmesidene $P_1, P_2, \ldots, P_n$ har pekere. Vi vil av tekniske grunner ikke her ta med hjemmesider som ikke har pekere.

Vi merker oss at hyperlinkmatrisen konstrueres baseres kun på informasjon som søkmotorene kan lese av.

[2]Om du er interessert i å se en gitt hjemmesides pagerank, ihvertfall tilnærmelsesvis, kan du besøke `www.seochat.com/seo-tools/pagerank-lookup/`.

Eksempel 12.2.2. Betrakt følgende mikro-nett bestående av fire hjemmesider $1, 2, 3$ och 4. Disse hjemmesidene har pekere som pilene i diagrammet nedenfor indikerer. Hjemmeside 1 har en peker til hjemmeside 3, og hjemme-



side 3 har en peker til hjemmeside 4. Hjemmeside 4 har en peker til hjemmeside 1 og hjemmeside 2, mens hjemmeside 2 har en peker til de andre tre. Vi har at $|P_1| = 1, |P_2| = 3, |P_3| = 1$ og $|P_4| = 2$. Ligningssystemet som gir rangeringen av de forskjellige hjemmesidene blir dermed

$$\begin{aligned} r(P_1) &= \frac{r(P_2)}{3} + \frac{r(P_4)}{2} \\ r(P_2) &= \frac{r(P_4)}{2} \\ r(P_3) &= r(P_1) + \frac{r(P_2)}{3} \\ r(P_4) &= \frac{r(P_2)}{3} + r(P_3) \end{aligned}$$

Hyperlinkmatrisen til dette eksemplet blir

$$H = \begin{bmatrix} 0 & \frac{1}{3} & 0 & \frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{2} \\ 1 & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 1 & 0 \end{bmatrix}.$$

Det er ingen tilfeldighet at kolonnene summerer opp til verdien 1.

Proposisjon 12.2.3. *Hyperlinkmatrisen H er en stokastisk matrise.*

Bevis. Vi har at alle koeffisientene i H er ikke-negative, og må kun verifiere at kolonne elementene summerer til 1. Vi har, for fiksert j, at koeffisient $H_{i,j}$ i hyperlinkmatrisen er null hvis hjemmeside j ikke peker til hjemmeside i. Og, per definisjon vil det finnes nøyaktig $|P_j|$ nullskilte koeffisienter $H_{i,j} = \frac{1}{|P_j|}$, slik at

$$\sum_{i=1}^{n} H_{i,j} = \sum_{\alpha=1}^{|P_j|} \frac{1}{|P_j|} = 1. \qquad \square$$

Rangeringsvektoren La n være antallet hjemmesider, og la $X = (x_1, \ldots, x_n)$ være en vektor i $\mathbf{R}^n$. Vi merker oss PageRank ligningen (12.2.1.1) er ingeting annet enn i'te rad i matriseproduket HX. Med andre ord har vi

$$HX = X.$$

Rangeringsvektoren som vi søker skal være en vektor $R = (r_1, r_2, \ldots, r_n)$ med positive koeffisienter $r_i > 0$, som satisfierer $HR = R$. Vi kan anta at koeffisientene summerer opp til 1, slik at R er en utfallsvektor. Koeffesient r_i i rangeringsvektoren vil gi rangen til hjemmeside P_i. Den koeffisient som er størst peker ut den hjemmesiden som rangerest høyest, og som anses mest viktig.

Vi har ennå ikke funnet en slik rangeringsvektor. Vi vet engang ikke hvorvidt det finnes løsninger, eller om det finnes om de er unike. For å garantere løsninger til systemet introduserer vi en ubestemt skalær λ, og betrakter

$$HX = \lambda X.$$

En vektor X som tilfredstiller ligningen $HX = \lambda X$ kalles en egenvektor til H, med egenverdi λ.

Proposisjon 12.2.4. *La X være en vektor slik at $HX = \lambda X$ for et gitt tall λ. Anta at koeffisientene til $X = (x_1, \ldots, x_n)$ er slik at summen* ikke *summerer opp til null, $\sum_{i=1}^n x_i \neq 0$. Da er egenverdien $\lambda = 1$.*

Bevis. Av Proposisjon 12.2.3 har vi H er en stokastisk matrisen. Det følger at koordinatene til X summerer opp til samme verdi som koordinatene til HX. La $r = \sum_{i=1}^n x_i$. Av ligningen $HX = \lambda X$ får vi ved å summere opp koordinaterne til de to matrisene at $r = \lambda r$. Ved antagelsen er $r \neq 0$, og det følger derav at $\lambda = 1$. □

Proposisjonen ovenfor gir i prinsippet eksistens av rangeringsvektorer. Egenvektorer vil det alltid finnes, og det eneste vi mener med i prinsippet er kravet om at koordinatene summerer opp til et tall forskjellig fra null.

Eksempel 12.2.5. La oss gå tilbake til mikronettet diskutert i Eksempel 12.2.2. Vi satte der opp hyperlinkmatrisen, og vi vil her finne rangeringsvektoren. Ligningssystemet $HX = X$ skriver vi som $(I_4 - H)X = 0$, og dette blir

$$\begin{bmatrix} 1 & -\frac{1}{3} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & -\frac{1}{2} \\ -1 & -\frac{1}{3} & 1 & 0 \\ 0 & -\frac{1}{3} & -1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = 0.$$

Gauss–Jordan eliminasjon gir trappeformen

$$\begin{bmatrix} 1 & -\frac{1}{3} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & -\frac{5}{6} \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Løsninger til dette systemet er $w = t$, $z = \frac{5}{6}t$, $y = \frac{1}{2}t$, $x = \frac{2}{3}t$, med t et villkårlig tall. Kravet om at vektoren også skal være en utfallsvektor gir

$$\frac{2}{3}t + \frac{1}{2}t + \frac{5}{6}t + t = t \cdot \frac{4+3+5+6}{6} = 3t = 1,$$

og det unike utfallet $(\frac{2}{9}, \frac{1}{6}, \frac{5}{18}, \frac{1}{3})$. Dette gir at hjemmeside P_4 er den viktigste, P_3 den nest viktigste. Mens hjemmeside P_2 er den minst viktige.

12.3 Iterering

Diagonaliseringstrikset vi gjorde for å finne det stabile utfallet i eksempel med studentpuben (Forelesning 11) er helt umulig å applisere til hyperlinkmatrisen. Å konstruere en diagonaliseringsmatrise, og dets invers, krever mange beregninger. Størrelsen til hyperlinkmatrisen gjør at kompleksiteten i disse beregningene blir uoverkommelige. Det man gjør, og som gjøres veldig raskt, er å tilnærme utfallsvektoren X med iterasjoner. La X_1 være en vilkårlig utfallsvektor. Da vil $X_{n+1} = H^n X_1$ være en approksimasjon til X, og det viser seg at omtrent 50 iterasjoner er nok. Dvs, med $n = 50$ så får vi en rangeringsvektor X_{51} som er en god nok tilnærmelse for at vi brukere skal oppleve søkmotoren som god, om ikke utmerket.

12.3.1. Det er klart at vi i beskrivelsen av søkmotoren Google gir en grov skisse av hvordan den fungerer. Søkmotoren inneholder blant annet en hel del finere delrutiner hvor blant annet nettsurferens klikkinger registreres og siden brukes for å bestemme rangeringen. Vidre så er hyperlinkmatrisen H så stor at flere praktiske problemer må overvinnes for i det hele tatt skrive opp denne, for å ikke nevne hvordan man skal kunne foreta 50 iterasjoner.

En annen ting man kan merke seg er at rangeringsvektoren som søkmotoren Google produserer gir en absolutt rangering. Rangeringen bestemmes kun av pekere, og ikke av innehold. Dette har visse uheldige konsekvenser. For eksempel, en høyt rangert side kanskje inneholder mye av interesse om et spesifikt tema, men har null interesse for en som vil lese om matriser. Om denne høyt rangerte siden skulle inneholde ordet "matrise" da ville denne sannsynlig komme først ved søk på dette ord.

Referanser

[1] Dan Laksov “Matematikk og informasjonssøkning på nettet” Normat 51, nr. 3 (2003) pp 119–131.

[2] Amy Langville & Carl Meyer “Google’s PageRank and Beyond. The science of search engine rankings.” Princeton University Press 2006.

[3] L. Page, S. Brin, R. Motvani, T. Winograd “The PageRank Citation Ranking: Bringing Order to the Web” http://ilpubs.stanford.edu:8090/422/

Appendix A

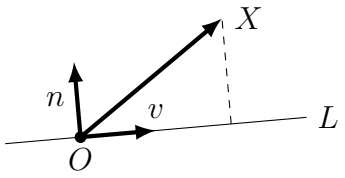
Ortogonal dekomposition

A.1 Avståndsformeln

Det vi använde för att härleda formeln för avståndet mellan en punkt Q i planet och en linje L, Sats 4.5.1, var följande observation. Låt $n = (a, b)$ vara en (nollskild) normalvektor till linjen L och antag nu att linjen L går genom origo. Varje vektor $X = (x, y)$ kan skrivas som en summa

$$X = tv + sn,$$

där v är en riktningsvektor till linjen L, och s och t är skalärer. Vektorerna v och n är vinkelräta och vi säger att vi har gjort en ortogonal dekomposition av X. Längden av vektorn sn var precis avståndet.



Låt oss göra detta en gång till. Vi har en ortogonal dekomposition av vektor X på formen

$$X = w + sn,$$

där $w = tv$ är någon vektor i linjen och s är något tal. Vektorn w som är i linjen L skriver vi som

$$w = \text{proj}_L(X) = X - sn$$

och kallas projektionen av X ned på linjen L. När vi tar skalärprodukten med n får vi

$$\langle X, n\rangle = 0 + s\|n\|^2, \tag{A.1.0.1}$$

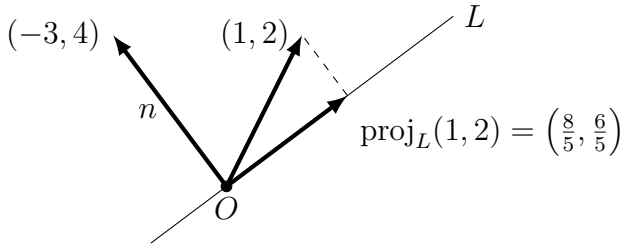
vilket leder oss till avståndsformeln. Nu använder vi enbart att talet s bestäms av uttrycket (A.1.0.1). Detta betyder att

$$\mathrm{proj}_L(X) = X - s \cdot n = X - \frac{\langle X, n\rangle}{\|n\|^2} \cdot n. \tag{A.1.0.2}$$

A.1.1. Notera att vi inte har använt att L är en linje, men enbart att n är en normalvektor till L. Vi återkommer till detta i högre dimensioner.

Exempel A.1.2. Betrakta linjen L som ges av ekvationen $-3x + 4y = 0$. En normalvektor till linjen är $n = (-3, 4)$. Den ortogonala projektionen av punkten $(1, 2)$ ges av uttrycket (A.1.0.2) som

$$\mathrm{proj}_L(1,2) = (1,2) - \frac{\big\langle (1,2), (-3,4)\big\rangle}{25}(-3,4) = \frac{1}{5}(8,6).$$



Proposition A.1.3. *Låt L vara en linje i planet som går genom origo. Avbildningen $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ som skickar en godtycklig punkt X till* $\mathrm{proj}_L(X)$ *är en linjär avbildning. Om $n = (a, b)$ är en nollskild normalvektor till L då ges T av matrismultiplikation med matrisen*

$$A = \frac{1}{a^2 + b^2}\begin{bmatrix} b^2 & -ab \\ -ab & a^2 \end{bmatrix}.$$

Bevis. Linjäriteten till avbildningen T följer av uttrycket (A.1.0.2) och definitionen av skalärprodukt. För att bestämma matrisen A beräknar vi $T(1, 0)$ och $T(0, 1)$. Vi har

$$T(1,0) = (1,0) - \frac{a}{a^2 + b^2}(a,b) = \frac{1}{a^2 + b^2}(b^2, -ab),$$

vilket ger den första *kolumnen* i A. En liknande beräkning för $T(0, 1)$ ger den andra kolumnen. □

Exempel A.1.4. Betrakta linjen L som ges av $-3x + 4y = 0$. Projektionen ned på linjen L ges som matrismultiplikation med

$$A = \begin{bmatrix} \frac{16}{25} & \frac{12}{25} \\ \frac{12}{25} & \frac{9}{25} \end{bmatrix}.$$

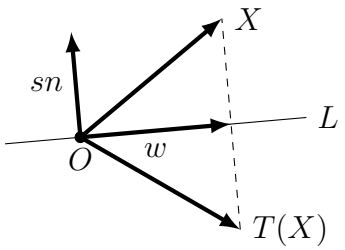
Speciellt har vi att punkten $(1, 2)$ skickas till

$$\text{proj}_L(1, 2) = A \cdot \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \left(\frac{40}{25}, \frac{30}{25}\right) = \left(\frac{8}{5}, \frac{6}{5}\right).$$

A.2 Spegling

Låt L vara en linje genom origo. För varje punkt X har vi en ortogonal dekomposition $X = w + sn$, där n är någon nollskild normalvektor till linjen L. Speglingen i linjen L är avbildningen $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ som skickar X till

$$\begin{aligned} T(X) &= \text{proj}_L(X) - sn \\ &= w - sn \\ &= (X - sn) - sn \\ &= X - 2sn. \end{aligned}$$



Proposition A.2.1. *Låt L vara en linje som går genom origo och betrakta avbildningen $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ som ges som spegling i linjen L. Avbildningen T är en linjär avbildning och vi har att*

$$T(X) = X - 2\frac{\langle X, n\rangle}{\|n\|^2}n.$$

Speciellt har vi att avbildningen ges av matrismultiplikation med matrisen

$$A = \frac{1}{a^2 + b^2}\begin{bmatrix} b^2 - a^2 & -2ab \\ -2ab & a^2 - b^2 \end{bmatrix},$$

där $n = (a, b)$ är någon nollskild normalvektor till linjen L.

Bevis. Av definitionen samt linjäriteten till projektionen följer det att speglingen är linjär. Av definitionen av projektionen (A.1.0.2) har vi att

$$\text{proj}_L(X) = X - sn,$$

vilket ger att $T(X) = X - 2sn$. Talet s har vi träffat på tidigare och denna bestäms av (A.1.0.1) som

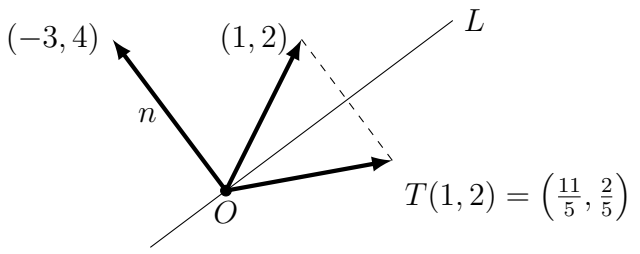
$$s = \frac{\langle X, n\rangle}{\|n\|^2}.$$

Därmed har vi visat det andra påståendet i propositionen. Slutligen för att bestämma matrisen A använder vi uttrycket för $T(X)$, som vi precis har visat, på vektorerna $X = (1, 0)$ och $X = (0, 1)$. Detta ger de två kolumnerna i matrisen A. □

Exempel A.2.2. Betrakta igen linjen L som ges av ekvationen $-3x+4y = 0$. Speglingen i linjen L ges av matrisen

$$A = \frac{1}{25}\begin{bmatrix} 7 & 24 \\ 24 & -7 \end{bmatrix}.$$

Punkten $(1, 2)$ skickas under speglingen till punkten $(\frac{55}{25}, \frac{10}{25}) = (\frac{11}{5}, \frac{2}{5})$.



A.3 Uppgifter

Uppgift A.1. Betrakta linjen L som ges av ekvationen $2x - 5y = 0$. Bestäm matrisen som representerar speglingen i linjen L och matrisen som representerar projektionen i linjen L.

Uppgift A.2. Betrakta linjen L som ges av $2x - 5y = 0$ och linjen N som ges av $3x + 7y = 0$. Bestäm matrisrepresentationen till avbildningen $T\colon \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ när T är

a) avbildningen som först speglar i linjen L och sedan speglar i linjen N.

b) avbildningen som först speglar i linjen N och sedan i linjen L.

c) avbildningen som först speglar i linjen N och sedan i linjen N (uh!).

d) avbildningen som först speglar i linjen N och sedan tar projektionen ned på linjen L.

e) avbildningen som först tar projektionen ned på linjen N och sedan speglar i linjen L.

f) avbildningen som först tar projektionen ned på linjen N och sedan projektionen ned på linjen L (uhu!).

Uppgift A.3. I beviset av Proposition A.1.3 skrev jag ”En liknande beräkning för $T(0,1)$ ger den andra kolumnen.” och i beviset av Proposition A.2.1 skrev jag ”... använder vi uttrycket för $T(X)$, som vi precis har visat, på vektorerna $X = (1,0)$ och $X(0,1)$. Detta ger de två kolumnerna i matrisen A”. Gör dessa detaljer som jag utelämnade.

Uppgift A.4. Bestäm koordinaterna till $T(2,3)$ där T är de sex olika avbildningarna i Uppgift A.2. Rita, för varje T, en bild som bekräftar rimligheten i ditt svar.

Appendix B

Linjära avbildningar

B.1 Avbildningar

B.1.1. Vi har att det euklidiska n-rummet $\mathbf{R}^n$ är mängden av alla ordnade reella tal

$$\mathbf{R}^n = \{(x_1, \ldots, x_n) \mid \text{ reella tal } x_i, \quad i = 1, \ldots, n\}.$$

Elementen $x = (x_1, \ldots, x_n)$ i $\mathbf{R}^n$ kallas för punkter eller vektorer.

En avbildning $f\colon \mathbf{R}^n \longrightarrow \mathbf{R}^m$ är en tillordning som till varje punkt $x = (x_1, \ldots, x_n)$ i $\mathbf{R}^n$ anger en punkt $f(x)$ i $\mathbf{R}^m$. Avbildningar kallas också för funktioner.

Exempel B.1.2. Ett exempel på en avbildning $f\colon \mathbf{R}^{101} \longrightarrow \mathbf{R}^{17}$ är avbildningen som skickar $x = (x_1, \ldots, x_{101})$ till dess 17 första komponenter: $f(x) = (x_1, \ldots, x_{17})$.

Exempel B.1.3. Ett annat exempel på en avbildning $f\colon \mathbf{R}^{101} \longrightarrow \mathbf{R}^{17}$ är avbildningen som skickar $(x_1, \ldots, x_{101})$ till punkten $(1, 0, \ldots, 0, 17)$.

B.1.4. Matrisavbildningar. De avbildningar vi är intresserade av kommer från matriser. Låt $A = (a_{i,j})$ vara en $(m \times n)$-matris. Som brukligt skriver vi element i $\mathbf{R}^n$ som $(n \times 1)$-matriser, dvs kolumnvektorer. Matrisen A ger genom matrismultiplikation en avbildning $T_A\colon \mathbf{R}^n \longrightarrow \mathbf{R}^m$. Avbildningen skickar en vektor $x = (x_1, \ldots, x_n)$ till

$$A \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{1,1}x_1 + \cdots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n \end{bmatrix}.$$

Detta skall tolkas som att $x = (x_1, \ldots, x_n)$ skickas till

$$T_A(x) = (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n, \ldots, a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n).$$

Notera att matrisen har storlek $(m \times n)$ och att avbildningen går från $\mathbf{R}^n$ till $\mathbf{R}^m$.

Exempel B.1.5. Betrakta matrisen

$$A = \begin{bmatrix} 1 & 2 & -4 & -4 \\ 2 & 4 & 0 & 0 \\ 2 & 3 & 2 & 1 \end{bmatrix}.$$

Detta ger en avbildning $T_A \colon \mathbf{R}^4 \longrightarrow \mathbf{R}^3$ som skickar (x, y, z, w) till

$$\begin{bmatrix} 1 & 2 & -4 & -4 \\ 2 & 4 & 0 & 0 \\ 2 & 3 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}.$$

Skriver vi ut detta får vi att avbildningen skickar (x, y, z, w) till

$$(x + 2y - 4z - 4w, 2x + 4y, 2x + 3y + 2z + w).$$

Speciellt har vi att vektorn $(1, 0, 1, -1)$ skickas till $(1, 2, 3)$.

Definition B.1.6. En avbildning $f \colon \mathbf{R}^n \longrightarrow \mathbf{R}^m$ är *linjär* om

$$f(av + bw) = af(v) + bf(w),$$

för alla tal a och b och alla vektorer v och w i $\mathbf{R}^n$.

B.1.7. Notera att en vektor $v = (v_1, \ldots, v_n)$ i $\mathbf{R}^n$ kan skrivas som

$$v = v_1e_1 + v_2e_2 + \cdots + v_ne_n,$$

där $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ är vektorn med 1 på i:te komponent, och noll på alla de andra komponenterna. Om avbildningen f är linjär har vi att

$$f(v) = v_1f(e_1) + v_2f(e_2) + \cdots + v_nf(e_n). \tag{B.1.7.1}$$

Detta är en ekvivalent beskrivning av linjäritet som vi använde i Definition 3.3.4.

Lemma B.1.8. *Låt $f \colon \mathbf{R}^n \longrightarrow \mathbf{R}^m$ vara en avbildning. Att avbildningen är linjär är ekvivalent med att avbildningen satisfierar* (B.1.7.1) *för alla vektorer v i $\mathbf{R}^n$.*

Bevis. Se uppgifterna. □

Exempel B.1.9. Visa att avbildningen i Exempel B.1.2 är linjär och att avbildningen i Exempel B.1.3 inte är linjär.

Notera också att en linjär avbildning är bestämd av sin verkan på vektorerna $e_1, \ldots, e_n$. Om vi känner $f(e_1), \ldots, f(e_n)$ då kan vi använda (B.1.7.1) för att bestämma $f(v)$ för godtyckliga vektorer v i $\mathbf{R}^n$.

Lemma B.1.10. *Låt $f\colon \mathbf{R}^n \longrightarrow \mathbf{R}^m$ vara en linjär avbildning. Låt A vara $(m \times n)$ matrisen*

$$A = \begin{bmatrix} f(e_1) & \cdots & f(e_n) \end{bmatrix},$$

där kolumn i är vektorn $f(e_i)$ i $\mathbf{R}^m$, för $i = 1, \ldots, n$. Då har vi att $f = T_A$, dvs den linjära avbildningen f ges av multiplikation med matrisen A.

Bevis. Se uppgifterna. □

Exempel B.1.11. Låt $T_A\colon \mathbf{R}^4 \longrightarrow \mathbf{R}^3$ vara den linjära avbildning som ges av matrisen A i Exempel B.1.5. Vi har att vektorn $e_3 = (0, 0, 1, 0)$ skickas till $T_A(e_3) = (-4, 0, 2)$, vilket är kolumn 3 i matrisen A.

B.2 Bildrum

Givet en matris A låter vi $T_A\colon \mathbf{R}^n \longrightarrow \mathbf{R}^m$ vara den tillhörande linjära avbildning. Fixera en vektor $b = (b_1, \ldots, b_m)$ i $\mathbf{R}^m$. Vi vill bestämma vilka vektorer $x = (x_1, \ldots, x_n)$ i $\mathbf{R}^n$ som skickas till b under avbildningen T_A, det vill säga

$$T_A(x) = b.$$

Skriver vi ut detta erhåller vi

$$T_A(x) = A \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{1,1}x_1 + \cdots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

För att dessa två matriser skall vara lika måste de vara lika elementvis. Detta ger oss ekvationssystemet

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + d_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ \qquad\qquad \vdots & \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m. \end{cases}$$

Detta vet vi hur vi löser.

Exempel B.2.1. Låt $T_A\colon \mathbf{R}^4 \longrightarrow \mathbf{R}^3$ vara den linjära avbildningen vi får från matrisen A i Exempel B.1.5. Låt $b = (b_1, b_2, b_3)$ vara en fixerad, men godtycklig, vektor i $\mathbf{R}^3$. Vi skall nu bestämma alla vektorer (x, y, z, w) i $\mathbf{R}^4$ som skickas till b under avbildningen T_A. Vi har att $T_A(x, y, z, w) = b$ ger ekvationssystemet

$$\begin{cases} x + 2y - 4y - 4w &= b_1 \\ 2x + 4y &= b_2 \\ 2x + 3y + 2z + w &= b_3. \end{cases}$$

Vi skriver ekvationssystemet som

$$\left[\begin{array}{cccc|c} 1 & 2 & -4 & -4 & b_1 \\ 2 & 4 & 0 & 0 & b_2 \\ 2 & 3 & 2 & 1 & b_3 \end{array}\right]$$

och detta löser vi med Gauss–Jordanelimination. Vi tar och adderar -2 gånger första raden till andra och tredje raden. Detta ger

$$\left[\begin{array}{cccc|c} 1 & 2 & -4 & -4 & b_1 \\ 0 & 0 & 8 & 8 & b_2 - 2b_1 \\ 0 & -1 & 10 & 9 & b_3 - 2b_1 \end{array}\right].$$

Vi byter plats på andra och tredje raden och multiplicerar den nya andra raden med -1. Sedan adderar vi -2 gånger andra raden till första raden. Detta borde ge

$$\left[\begin{array}{cccc|c} 1 & 0 & 16 & 14 & -3b_1 + 2b_3 \\ 0 & 1 & -10 & -9 & 2b_1 - b_3 \\ 0 & 0 & 8 & 8 & b_2 - 2b_1 \end{array}\right].$$

Slutligen delar vi tredje raden med 8, multiplicerar med -16 och adderar till första raden och multiplicerar med 10 och adderar till andra raden. Detta ger

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & -2 & b_1 - 2b_2 + 2b_3 \\ 0 & 1 & 0 & 1 & -\frac{1}{2}b_1 + \frac{5}{4}b_2 - b_3 \\ 0 & 0 & 1 & 1 & \frac{1}{8}b_2 - \frac{1}{4}b_1 \end{array}\right].$$

Detta betyder att

$$\begin{aligned} w &= t, \quad \text{där } t \text{ är ett godtyckligt reellt tal,} \\ z &= \frac{1}{8}b_2 - \frac{1}{4}b_1 - t, \\ y &= -\frac{1}{2}b_1 + \frac{5}{4}b_2 - b_3 - t, \\ x &= b_1 - 2b_2 + 2b_3 + 2t. \end{aligned}$$

För fixerad $b = (b_1, b_2, b_3)$ har vi att de vektorer (x, y, z, w) i $\mathbf{R}^4$ som skickas till b via avbildningen T_A är

$$(b_1 - 2b_2 + 2b_3 + 2t, -\frac{1}{2}b_1 + \frac{5}{4}b_2 - b_3 - t, \frac{1}{8}b_2 - \frac{1}{4}b_1 - t, t), \qquad \text{(B.2.1.1)}$$

med godtyckliga t. Vi verifierar att detta är korrekt genom att ta en punkt a i $\mathbf{R}^4$ som är på formen ovan (B.2.1.1) och beräkna vad avbildningen T_A skickar den:

$$\begin{aligned} T_A(a) &= \begin{bmatrix} 1 & 2 & -4 & -4 \\ 2 & 4 & 0 & 0 \\ 2 & 3 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} b_1 - 2b_2 + 2b_3 + 2t \\ -\frac{1}{2}b_1 + \frac{5}{4}b_2 - b_3 - t \\ \frac{1}{8}b_2 - \frac{1}{4}b_1 - t \\ t \end{bmatrix} \\ &= \begin{bmatrix} b_1 - 2b_2 + 2b_3 + 2t + 2(-\frac{1}{2}b_1 + \frac{5}{4}b_2 - b_3 - t) - 4(\frac{1}{8}b_2 - \frac{1}{4}b_1 - t) - 4t \\ 2(b_1 - 2b_2 + 2b_3 + 2t) + 4(-\frac{1}{2}b_1 + \frac{5}{4}b_2 - b_3 - t) \\ 2(b_1 - 2b_2 + 2b_3 + 2t) + 3(-\frac{1}{2}b_1 + \frac{5}{4}b_2 - b_3 - t) + 2(\frac{1}{8}b_2 - \frac{1}{4}b_1 - t) + t \end{bmatrix} \\ &= \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}. \end{aligned}$$

Exempel B.2.2. Vi återgår till Exempel B.2.1 ovan. Notera att om vi låter

$$P = (b_1 - 2b_2 + 2b_3, -\frac{1}{2}b_1 + \frac{5}{4}b_2 - b_3, \frac{1}{8}b_2 - \frac{1}{4}b_1, 0)$$

så är detta en fixerad punkt i $\mathbf{R}^4$ och $v = (2, -1, -1, 1)$ är en fixerad vektor i $\mathbf{R}^4$. Mängden (B.2.1.1) kan vi skriva som

$$P + t \cdot v,$$

med godtyckliga reella tal t. Med andra ord beskriver detta en linje i $\mathbf{R}^4$. För varje vald punkt $b = (b_1, b_2, b_3)$ finns det en linje i $\mathbf{R}^4$ som kollapsar till denna fixerade punkt under avbildningen T_A.

B.3 Uppgifter

Uppgift B.1. Visa Lemma B.1.8.

Uppgift B.2. Visa Lemma B.1.10.

Appendix C

Komplexa tal

C.1 Representation av tal

C.1.1. De reella talen betecknas ofta med symbolen $\mathbf{R}$. Vi kommer inte att definiera de reella talen här, men vi noterar att för varje par av reella tal a och b så är även $a+b$ och ab reella tal. Med andra ord är mängden $\mathbf{R}$ sluten under addition och multiplikation. Vidare har vi att till varje tal a finns det ett tal $-a$ sådant att $a+(-a)=0$ och till varje nollskilt tal $a \neq 0$ finns talet a^{-1} sådant att $aa^{-1}=1$.

C.2 Reella talen som matriser

Vi börjar med att presentera de reella talen på ett lite annorlunda sätt. Varje tal a kan skrivas som $a \cdot 1$, och nu kommer vi med 1 mena (2×2)-identitetsmatrisen. Vi skriver

$$a = a \cdot 1 = a \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.$$

Att skriva reella tal som en speciell klass av (2×2)-matriser skall vi snart se är ett smart drag. Notera först att addition och multiplikation av matriser är kompatibel med den vanliga additionen och multiplikationen av reella tal. Med detta menas följande. Om a är ett reellt tal, låter vi $T_a = a \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Vi har då att

$$T_a + T_b = T_{a+b} \quad \text{och} \quad T_a T_b = T_{ab}.$$

Detta betyder att vi verkligen kan betrakta de reella talen som diagonalmatriser med ett och samma diagonalelement.

C.2.1. Betrakta nu alla (2×2)-matriser på formen

$$\mathbf{C} = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid \text{reella tal } a \text{ och } b \right\}.$$

Delmängden av sådana matriser skriver vi som $\mathbf{C}$. Notera att nollmatrisen 0 och identitetsmatrisen 1 finns med i mängden $\mathbf{C}$. Och, med $b = 0$, har vi också alla reella tal inuti mängden $\mathbf{C}$. Vi kontrollerar nu att mängden är sluten under addition och multiplikation. Låt Z och W vara två godtyckliga element i mängden $\mathbf{C}$. Vi har att

$$Z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \quad \text{och} \quad W = \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$$

för några reella tal a, b, c och d. Vi har att

$$Z + W = W + Z = \begin{bmatrix} a+c & -(b+d) \\ b+d & a+c \end{bmatrix} \tag{C.2.1.1}$$

$$Z \cdot W = W \cdot Z = \begin{bmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{bmatrix}. \tag{C.2.1.2}$$

Vi har att $Z+W$ och $Z \cdot W$ är matriser på den speciella formen som krävs för att vara med i mängden $\mathbf{C}$. Observera även att för matriser i $\mathbf{C}$ blir matrisprodukten kommutativ (härligt!). Mängden $\mathbf{C}$ är sluten under addition och multiplikation. Hur är det med de andra egenskaperna för tal. Uppenbarligen har vi att för varje matris Z att $Z + (-Z) = 0$. Hur är det med Z^{-1}?

Sats C.2.2. *Låt Z vara ett nollskilt element i $\mathbf{C}$. Då finns det en matris Z^{-1} i $\mathbf{C}$ sådan att $ZZ^{-1} = 1$. Mera precist, om*

$$Z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

då har vi determinanten $\det(Z) = a^2 + b^2$. *Om $Z \neq 0$, då är determinanten nollskild och vi har inversen*

$$Z^{-1} = \begin{bmatrix} \frac{a}{a^2+b^2} & -\frac{-b}{a^2+b^2} \\ \frac{-b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix}.$$

Bevis. Vi har att $\det(Z) = a^2 + b^2$. Determinanten är noll om och endast om $a = 0$ och $b = 0$. Med andra ord är determinanten nollskild om och endast om $Z \neq 0$. Vi har tidigare visat att en matris är inverterbar om och endast om determinanten är nollskild och formeln för inverser för (2×2)-matriser ger slutligen satsen. □

C.2.3. De tre första egenskaperna: att mängden är sluten under addition, sluten under multiplikation och att varje matris Z har en additiv invers $-Z$; gäller inte bara för mängden $\mathbf{C}$. Dessa tre egenskaper gäller också för mängden av alla (2×2)-matriser, för att ta ett exempel. Det är egenskapen att varje matris $Z \neq 0$ har en multiplikativ invers som kräver att vi måste betrakta en delmängd.

C.2.4. Komplexa talen. Vi kallar mängden $\mathbf{C}$ av matriser definierad ovan, för *de komplexa talen*. Termen komplex kan man diskutera, men anledningen att vi kallar elementen i $\mathbf{C}$ för tal är att dessa matriser har alla egenskaper vi förväntar att tal skall ha. Speciellt har vi den trevliga egenskapen att varje nollskilt tal $Z \neq 0$ har en multiplikativ invers Z^{-1}.

Notera att det finns komplexa tal som inte är reella, det vill säga det finns matriser i $\mathbf{C}$ som inte är på formen $a \cdot 1$. Ett exempel är talet

$$\Omega = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{C.2.4.1}$$

Detta talet betecknar vi med symbolen Ω och det kallas ibland för den imaginära enheten. Notera att

$$\Omega^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \tag{C.2.4.2}$$

vilket betyder att $\Omega^2 = -1$.

Exempel C.2.5. Låt oss lösa några ekvationer inom talen $\mathbf{C}$. Vi börjar med ekvationen

$$X^2 = 5.$$

Notera nu att den okända X är alla matriser inom mängden $\mathbf{C}$ sådana att X^2 är lika med matrisen $5 \cdot 1$, matrisen med talet 5 på diagonalen. Låt X vara en godtycklig matris i mängden $\mathbf{C}$. Vi har

$$X = \begin{bmatrix} x & -y \\ y & x \end{bmatrix},$$

där x och y är okända reella tal. Vi får att

$$X^2 = \begin{bmatrix} x^2 - y^2 & -2xy \\ 2xy & x^2 - y^2 \end{bmatrix},$$

vilket skall vara lika med matrisen

$$5 = \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}.$$

Detta ger, elementvis, att $x^2 - y^2 = 5$ och $-2xy = 0$. Den andra ekvationen ger att antingen är $x = 0$ eller så är $y = 0$. Insätter vi $x = 0$ i den första ekvationen får vi $-y^2 = 5$, vilket saknar lösning. Insätter vi istället $y = 0$ i den första ekvationen får vi $x^2 = 5$, vilket har lösningarna $\pm\sqrt{5}$. Vi har nu visat att ekvationen $X^2 = 5$ har lösningarna $X = -\sqrt{5}$ och $X = \sqrt{5}$. Inget ovanligt med andra ord.

Exempel C.2.6. Betrakta ekvationen $X^2 = -4$ i $\mathbf{C}$. Låt $X = \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$ vara en okänd matris som ovan. Vi söker lösningar till

$$X^2 = \begin{bmatrix} x^2 - y^2 & -2xy \\ 2xy & x^2 - y^2 \end{bmatrix} = -4 = \begin{bmatrix} -4 & 0 \\ 0 & -4 \end{bmatrix}.$$

Vi jämför elementen och erhåller att $x^2 - y^2 = -4$ och $-2xy = 0$. Insätter vi $x = 0$ i den första ekvationen får vi $-y^2 = -4$, vilket ger $y = \pm 2$. Insätter vi $y = 0$ i den första ekvationen får vi $x^2 = -4$ och denna saknar lösning. Vi har visat att ekvationen $X^2 = -4$ har lösningarna

$$X = -2\Omega \quad \text{och} \quad X = 2\Omega,$$

där Ω är matrisen (C.2.4.1). Här ser vi att vissa ekvationer, som $X^2 = -4$, som saknar lösning i $\mathbf{R}$, har lösning i $\mathbf{C}$.

C.3 Komplexa talen som talplanet

Det reella talplanet $\mathbf{R}^2$ är mängden av alla ordnade talpar $z = (a, b)$. Till varje element $z = (a, b)$ i talplanet kan vi tillordna matrisen $Z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ i $\mathbf{C}$ och omvänt. Den första kolumnen till en godtycklig matris $Z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ i $\mathbf{C}$ ger det ordnade talparet $z = (a, b)$. Detta betyder att vi kan identifiera mängden $\mathbf{C}$ med mängden $\mathbf{R}^2$.

C.3.1. Notera att under den givna identifikationen av de komplexa talen med talplanet, identifieras de reella talen med x-axeln. Vi kallar därför x-axeln för den reella axeln. Talet Ω identifieras med talparet $\omega = (0, 1)$ och y-axeln kallas den imaginära axeln.

C.3.2. Addition och multiplikation av talpar. Vi har att $\mathbf{C}$ är tal och speciellt kan vi addera och multiplicera tal. Detta betyder att vi nu också kan addera och multiplicera element i $\mathbf{R}^2$. Låt $z = (a, b)$ och $w = (c, d)$ vara

två element i talplanet. För att addera och multiplicera dessa måste vi först betrakta dessa som element Z och W i $\mathbf{C}$. Sedan adderar och multiplicerar vi Z och W och får $Z+W$ och ZW. Dessa två nya matriser $Z+W$ och ZW identifieras med två talpar, och vi erhåller addition och multiplikation av z och w.

Lemma C.3.3. *Låt $z=(a,b)$ och $w=(c,d)$ vara två talpar. Den inducerade additionen från $\mathbf{C}$ ger komponentvis addition*

$$z+w=(a,b)+(c,d)=(a+c,b+d).$$

Den inducerade multiplikationen ges av formeln

$$z\cdot w=(a,b)\cdot(c,d)=(ac-bd,ad+bc).$$

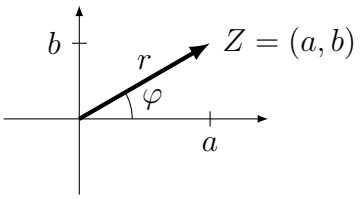
Bevis. Additionsformeln följer från (C.2.1.1) och multiplikationen följer från (C.2.1.2). □

Exempel C.3.4. Betrakta talparet $\omega=(0,1)$ som motsvarar matrisen Ω. Formeln ger att $\omega^2=(0,1)^2=(-1,0)$, vilket vi redan visste från beräkningarna i C.2.4. Ett annat exempel är produkten

$$(0,1)\cdot(-1,1)=(0-1,0-1)=(-1,-1).$$

C.4 Geometrisk tolkning av produkt

Vi kommer nu att tolka produkten zw av två talpar z och w geometriskt. Vi börjar med att beskriva ett talpar $z=(a,b)$ i polära koordinater. Vinklar mäts i radianer, moturs, och från den positiva horisontella x-axeln. Avståndet



från origo till (a,b) ges av Pythagoras Sats som $r=\sqrt{a^2+b^2}$. Om $(a,b)\neq(0,0)$ finns det en unik vinkel $\varphi\in[0,2\pi)$ sådan att

$$r\cos(\varphi)=a \quad \text{och} \quad r\sin(\varphi)=b.$$

Detta betyder att varje talpar $z=(a,b)$ kan beskrivas med ett avstånd r och en vinkel φ. Talparet $(0,0)$ har avståndet noll och vinkeln noll. Sambandet ges av $z=(a,b)=(r\cos(\varphi),r\sin(\varphi))$.

C.4.1. Rotationsmatrisen. Om vi skriver ett talpar $z = (a, b)$ i polära koordinater med avstånd r och vinkel φ, har vi $z = (r\cos(\varphi), r\sin(\varphi))$. Detta betyder att matrisen Z som motsvarar talparet z ges av

$$Z = \begin{bmatrix} r\cos(\varphi) & -r\sin(\varphi) \\ r\sin(\varphi) & r\cos(\varphi) \end{bmatrix}.$$

Notera nu att Z är rT_φ, där T_φ är matrisen som representerar den linjära avbildning som beskriver en rotation med φ grader, moturs omkring origo. Jämför med Uppgift 3.4.

Exempel C.4.2. Positiva reella tal a har avståndet $a = |a|$ och vinkeln är noll. Negativa tal a har avståndet $|a|$ och vinkeln är π. Till exempel har vi talparet

$$(-5, 0) = (5\cos(\pi), 5\sin(\pi)).$$

Talparet $\omega = (0, 1)$ har avståndet 1 och vinkeln är $\pi/2$. Detta betyder att talparet som motsvarar Ω ges som $(1\cos(\pi/2), 1\sin(\pi/2))$.

Lemma C.4.3. *Låt $z = (r\cos(\varphi), r\sin(\varphi))$ och $w = (s\cos(\vartheta), s\sin(\vartheta))$ vara två talpar. Multiplikationen zw ges av talparet*

$$(rs\cos(\varphi + \vartheta), rs\sin(\varphi + \vartheta)).$$

Bevis. Låt Z och W vara matriserna som motsvarar punkterna z och w. Då är

$$Z = \begin{bmatrix} r\cos(\varphi) & -r\sin(\varphi) \\ r\sin(\varphi) & r\cos(\varphi) \end{bmatrix}, \quad W = \begin{bmatrix} s\cos(\vartheta) & -s\sin(\vartheta) \\ s\sin(\vartheta) & s\cos(\vartheta) \end{bmatrix}.$$

Vi beräknar nu produkten ZW. Vi har att $Z = rT_\varphi$ och $W = sT_\vartheta$, där T_α är rotationsmatrisen med vinkel α. Vi har tidigare visat att sammansättning av två linjära avbildningar ges av produktmatrisen. Detta betyder att rotera först med ϑ radianer, och därefter rotera med φ radianer, ges av matrisprodukten $T_\varphi T_\vartheta$. Men, att först rotera med ϑ och därefter med φ, är att rotera med totalt $\vartheta + \varphi$ radianer. Det vill säga att

$$T_\varphi T_\vartheta = T_{\varphi+\vartheta} = \begin{bmatrix} \cos(\varphi + \vartheta) & -\sin(\varphi + \vartheta) \\ \sin(\varphi + \vartheta) & \cos(\varphi + \vartheta) \end{bmatrix}$$

Detta ger nu att $ZW = rT_\varphi sT_\vartheta = rsT_{\varphi+\vartheta}$, vilket vi skulle visa. □

C.4.4. Notera nu att vi geometriskt förstår hur produkten zw går till. Vi multiplicerar avståndet r till $z = (a, b)$ med avståndet s till $w = (c, d)$, och får avståndet rs till zw. Vinkeln till z adderas till vinkeln till w och ger vinkeln till zw.

Lemma C.4.5. *Om* $z = (r\cos(\varphi), r\sin(\varphi))$ *är nollskild, då ges inversen som*

$$z^{-1} = \left(\frac{1}{r}\cos(-\varphi), \frac{1}{r}\sin(-\varphi)\right).$$

Bevis. Påståendet följer från Lemma C.4.3 och det faktum att $(1,0) = (1\cos(0), 1\sin(0))$ är identitetselementet. □

Exempel C.4.6. Betrakta talparet $z = (1,1)$. Vi vill beräkna z^n, för olika heltal $n > 0$. I polära koordinater har vi att z har avståndet $\sqrt{2}$ och vinkeln är $\pi/4$. Detta ger att

$$z^n = \left(\sqrt{2}^n \cos(\pi n/4), \sqrt{2}^n \sin(\pi n/4)\right).$$

Appendix D

PS3 och krypteringsmissar

D.1 Kryptering

Vi skall[1] idag titta lite på kryptering, och mera specifikt hur elliptiska kurvor används i kryptering, så kallad ECDSA. Vi skall också se ett aktuellt exempel på hur detta **inte** skall användas.

D.1.1. Vi har följande problem. En användare A kontaktar en nätsida N. Användaren vill spela ett spel som nätsidan N har producerat, och nätsidan vill kontrollera att användaren A har betalat sin licens för att spela. Problemet är att en hacker H övervakar och läser av all informationsutväxling mellan A och N. Så om A visar fram ett kvitto, då kommer säkerligen hackern H att kopiera kvittot. På sådant sätt kan hackern H få möjlighet att spela utan att ha betalat licens, och detta tycker inte N om.

D.1.2. Lösningen som används på problemet ovan är att användaren A krypterar sitt kvitto på ett sätt som nätsidan N kan verifiera, men som hackern H inte kan dekryptera.

Det finns flera olika sätt att kryptera. Ett av de vanligaste är att använda par av stora primtal som krypteringsnycklar, så kallad RSA-kryptering. Ett annat sätt är att använda elliptiska kurvor, som i ECDSA.

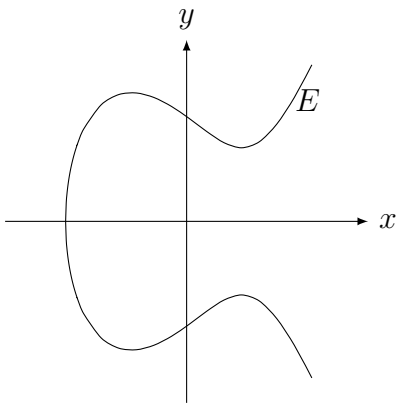
D.2 Elliptisk kurva

En elliptisk kurva är nollställemängden till en ekvation på formen

$$E = \{(x, y) \in \mathbf{R}^2 \mid y^2 = x^3 + ax + b\},$$

där a och b är givna tal. Här är en typisk bild av en elliptisk kurva:

[1] Jag själv lärde om detta av en kollega som, kanske, heter Joel Andersson



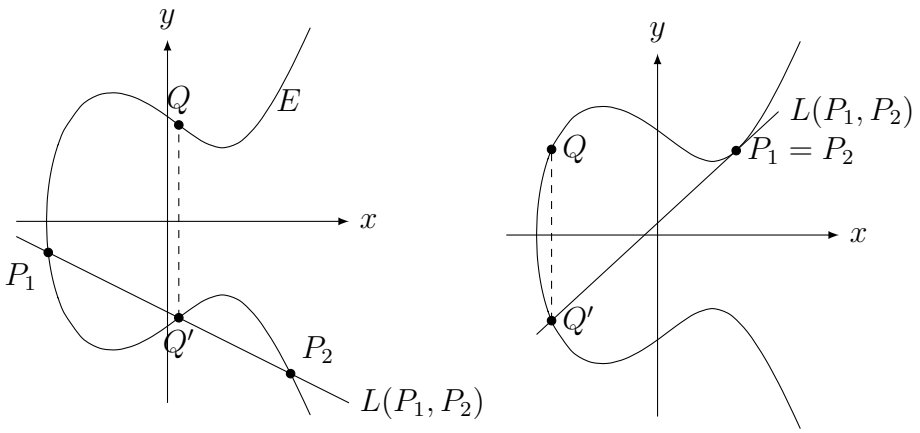
D.2.1. Konjugering. Vi observerar att om $P = (p, q)$ är en punkt på kurvan E då är också punkten $(p, -q)$ en punkt på kurvan E. Vi har att $q^2 = p^3 + ap + b = (-q)^2$, vilket betyder att kurvan är symmetrisk om x-axeln. Vi kommer att använda detta nedan och inför därför notationen $\overline{P}$ för konjugatet till punkten P. Vi har alltså att om $P = (p, q)$ då är $\overline{P} = (p, -q)$.

D.2.2. Addition av punkt. Vi tänker oss nu att den elliptiska kurva E är given. Vi kommer nu att göra följande geometriska konstruktion, och för denna använder vi oss av den typiska bilden ovan. Låt P_1 och P_2 vara två punkter på kurvan E. Vi kan dra linjen $L(P_1, P_2)$ genom P_1 och P_2. Denna linje $L(P_1, P_2)$ skär kurvan i en tredje punkt[2] Q' om inte P_1 och P_2 ligger på samma vertikala linje. Vi låter Q vara punkten som vi får om vi tar och skär kurvan E med en vertikal linje genom Q', det vill säga att $Q = \overline{Q'}$. Se figuren nedan. Fina illustrativa figurer finns även under länken `http://en.wikipedia.org/wiki/Elliptic_curve`.

D.2.3. Tangentlinjen. Om $P_1 = P_2$ avser vi med linjen $L(P_1, P_1)$ genom punkten $P_1 = P_2$ tangentlinjen till kurvan E i punkten P_1.

D.2.4. Oändlighetspunkt. Konstruktionen ovan fungerar dock inte om punkterna P_1 och P_2 ligger på samma vertikala linje, vilket betyder att $P_1 = \overline{P_2}$. För att bota detta problem skall vi föreställa oss att kurvan E har en punkt i oändligheten. Denna punkt kallar vi O. Vi skall tänka på de vertikala linjerna som meridianer på sfären; dessa linjer är parallella, men ändå så möts linjerna i nordpolen. Och faktisk så möts de parallella vertikala linjerna också i sydpolen, men på den elliptiska kurvan E är sydpol och nordpol en och samma punkt O. Därför låter vi $\overline{O} = O$.

[2]Detta gäller egentligen endast om vi tillåter lösningar med *komplexa* koordinater. Att det alltid finns en lösning beror på att skärningen mellan en linje och den elliptiska kurvan beskrivs av en tredjegradsekvation i en variabel. En sådan ekvation har alltid 3 komplexa lösningar.



Vi låter E_O vara den elliptiska kurvan E union oändlighetspunkten O. Vi definierar addition av punkterna till E_O på det sättet som vi angav i D.2.2. Detta ger en avbildning $E_O \times E_O \longrightarrow E_O$, som skickar ett par av punkter P_1 och P_2 på E_O till punkten $P_1 \oplus P_2$.

Exempel D.2.5. Låt P_1 och P_2 vara två punkter på kurvan E. Vi har att $P_1 \oplus P_2 = Q$, där Q ges som konjugering av punkten Q' som i sin tur ges av skärningen av kurvan E och linjen $L(P_1, P_2)$ genom P_1 och P_2.

Exempel D.2.6. Låt P vara en punkt på kurvan E. Vi skall bestämma $P \oplus O$. Linjen $L(P, O)$ genom P och oändlighetspunkten O ges av den vertikala linjen genom P. Linjen $L(P, O)$ skär kurvan E punkten P' där $P' = \overline{P}$. Vi har att $\overline{P'} = \overline{\overline{P}} = P$. Detta betyder att

$$P \oplus O = P.$$

Vi ser att addition med punkten O till en annan punkt P inte gör något. Symbolen O för oändlighetspunkten har inget med första bokstaven i oändlighet, men refererar till begreppet noll.

D.2.7. Notera att för att erhålla $P \oplus O = P$ var det nödvändigt att vi i definitionen av addition tog konjugatet av punkten Q' vilken ges som skärningen av linjen $L(P_1, P_2)$ med kurvan E, och inte punkten Q' som kunde tyckas mera naturligt.

Exempel D.2.8. Additionen av punkter D.2.2 är såpass naturlig att följande egenskap håller

$$(P_1 \oplus P_2) \oplus P_3 = P_1 \oplus (P_2 \oplus P_3),$$

för alla punkter P_1, P_2 och P_3 på kurvan. Vi kan med andra ord slopa parenteserna vid addition av punkter.

Exempel D.2.9. Vi har uppenbarligen att $P_1 \oplus P_2 = P_2 \oplus P_1$ för alla punkter P_1 och P_2 på den elliptiska kurvan.

Exempel D.2.10. Låt P vara en punkt på kurvan E, och låt $\overline{P}$ vara punkten som ligger på kurvan E och under samma vertikala linje som P. Vi har av konstruktion att linjen $L(P, \overline{P})$ är den vertikala linjen och denna linje skär kurvan E i oändlighetspunkten O, dvs $L(P, \overline{P})$ skär inte kurvan E men kurvan E_O. Eftersom $\overline{O} = O$ erhåller vi att

$$P \oplus \overline{P} = O.$$

Med andra ord är $\overline{P}$ den additiva inversen till P.

D.3 Gruppen till en elliptisk kurva

Det vi har indikerat med exemplen ovan är att punkterna på den elliptiska kurvan E_O med additionen $\oplus$ är en *grupp*, en kommutativ grupp. I ECDSA använder man gruppstrukturen på den elliptiska kurvan för krypteringen.

D.4 Primtalskroppar

Vi har givit den elliptiska kurvan E som en kurva i planet $\mathbf{R}^2$. I den verkliga världen vill man göra situationen lite mer "ändlig". Det betyder att koordinaterna till punkter P på kurvan E inte tillåts vara alla reella tal, men enbart element i en ändlig primtalskropp.

Om p är ett givet primtal så består primtalskroppen av heltalen $\mathbf{F}_p = \{0, 1, \ldots, p-1\}$. Addition och multiplikation sker modulo restklasserna. Subtraktion fungerar, och då p är ett primtal kommer även division att fungera.

Primtalen kan i praktiken vara mycket stora, men för att få en känsla för primtalskroppar kan man titta på små primtal.

Exempel D.4.1. Primtalskroppen $\mathbf{F}_5$ består av elementen $\{0, 1, 2, 3, 4\}$. Addition sker modulo restklasserna, så t ex är $3 + 4$ lika med 2. Subtraktion sker på samma sätt. Om vi vill lösa ekvationen $3 + x = 2$ i $\mathbf{F}_5$ så subtraherar vi 3 från båda sidor och erhåller

$$x = 2 - 3 = -1.$$

Talet -1 finns inte med i mängden $\mathbf{F}_5$, men lägger vi till 5 får vi 4. Detta betyder att $2 - 3 = 4$, vilket också är lösningen till ekvationen $3 + x = 2$. Multiplikation sker också modulo restklasser. Vi har att $4 \cdot 4 = 1$ då $16 = 3 \cdot 5 + 1$. Detta betyder också att $4 = \frac{1}{4}$ i $\mathbf{F}_5$. Vi har att $2 \cdot 3 = 1$ vilket betyder att $3 = \frac{1}{2}$ och att $2 = \frac{1}{3}$.

D.4.2. Vi tar för givet att om P_1 och P_2 är punkter på en elliptisk kurva E och koordinaterna till P_1 och P_2 båda ligger i en primtalskropp $\mathbf{F}_p$, då kommer även punkten $Q = P_1 \oplus P_2$ att ha koordinater i primtalskroppen $\mathbf{F}_p$. Speciellt har vi att punkterna på den elliptiska kurvan E_O med koordinater i primtalskroppen $\mathbf{F}_p$ bildar en grupp.

Om k är ett heltal och P är en punkt så definierar vi

$$k \cdot P = \underbrace{P \oplus P \oplus \cdots \oplus P}_{k \text{ kopior}}.$$

Observera att även om P är en punkt med koordinater i $\mathbf{F}_p$ så är inte nödvändigtvis $p \cdot P = 0$. Det finns dock oftast (om kurven inte är en så kallad supersingulär kurva) punkter P sådana att $p \cdot P = 0$. För en sådan punkt tillåter vi även att k är ett element i primtalskroppen $\mathbf{F}_p$, betraktat som ett heltal. Då är nämligen $(k_1 + k_2) \cdot P = k_1 \cdot P \oplus k_2 \cdot P$ där vi beräknar $k_1 + k_2$ i $\mathbf{F}_p$.

D.4.3. Notera att om k är ett nollskilt tal i primtalskroppen då är också $\frac{1}{k}$ ett heltal/element i primtalskroppen.

D.5 Krypteringsalgoritmen

Användaren A har vid betalningen av licensen till nätsidan N blivit tilldelad en elliptisk kurva E, en primtalskropp $\mathbf{F}_p$, en punkt P på den elliptiska kurvan, och en krypteringsnyckel c. Krypteringsnyckeln c är ett tal i primtalskroppen $\mathbf{F}_p$. Denna information är inte tillgänglig för andra.

När användaren A kontaktar nätsidan N utförs följande beräkningar av användaren A.

Steg 1

Först beräknas, av användaren A, punkten $c \cdot P = Q$ på kurvan E. Denna punkt kallas den offentliga nyckeln, och skickas till nätsidan N. Med hjälp av punkten Q identifierar nätsidan N vilken användare det handlar om. Det vill säga vilken kurva E, vilken punkt P, och vilken krypteringsnyckel c som användaren borde ha.

Steg 2

Användaren A skickar ett medelande till nätsidan N, typ "jag vill spela". Detta meddelandet blir omgjord till ett tal e. Hur denna funktion fungerar är inte så viktig. Det som är viktig är att talet e ändras med meddelandet. Man

kan tänka sig att meddelandet "jag vill spela" också innehåller information om klockslag mm, sådan att när användaren A vill spela dagen efter så kommer meddelandet e att vara ett annat.

Steg 3

En godtycklig, men stor, konstant k i primtalskroppen $\mathbf{F}_p$ väljes, och användaren A beräknar $k \cdot P$. Vi låter r vara x-koordinaten till punkten $k \cdot P = (r, r_2)$.

Steg 4

Vi beräknar talet $s = \frac{e+cr}{k}$ i primtalskroppen $\mathbf{F}_p$.

Informationsutväxlingen

Informationen som användaren A skickar till nätsidan N är alltså punkten Q, meddelandet e, och signaturen (r, s). Denna information kan avläsas av en tredje part, hackern H. Men, denna information kan inte återanvändas.

Verifieringsalgoritmen

När användaren A kontaktar nätsidan N kommer det besked om offentlig nyckel Q, meddelandet e och slutligen bifogas signaturen (r, s). Den offentliga nyckeln identifierar vem den tänkta användaren borde vara, och slutligen kontrollerar nätsidan N signaturen. Kontrollen görs på följande sätt.

Beräkning av punkten R

Nätsidan beräknar punkten

$$R = \frac{e}{s} \cdot P \oplus \frac{r}{s} \cdot Q.$$

Detta är möjligt då nätsiden N från punkten Q vet punkten P, och talen e, r och s skickades med kontakten från A.

Verifiering

Nu skall nätsidan verifiera att signaturen är korrekt, och detta görs genom att kontrollera att x-koordinaten till punkten R är det första talet r i signaturen som användaren A skickade. Vi har nämligen att $s = \frac{e+cr}{k}$, och detta ger

$$R = \frac{k}{e + cr}(e \cdot P \oplus r \cdot Q).$$

Vi har vidare att $Q = c \cdot P$, vilket ger att

$$R = \frac{k}{e + cr}(e + cr) \cdot P = k \cdot P.$$

Det var precis $k \cdot P$ som A beräknade för att bestämma r.

D.6 Felaktig implementering

När Playstation 3 (PS3) lanserades 2006/2007 var den betraktad som att inneha en mycket säker kryptering. PS3 användes sig av kryptering via elliptiska kurvor. Men, i december 2010 blev maskinernas krypteringskoder tillgängliga. Hackers lyckades bryta koden och det hela baserades på att PS3 hade implementerad krypteringskoden fel.

När PS3 gav ut licenser till användare så var det meningen att varje användare fick en programvara som hade en krypteringsalgoritm enligt ovan. Skillnaden var dock i Steg 3 där man istället för att slumpa ett godtyckligt tal k varje gång man kontaktade nätsidan N, använde sig av ett och samma tal k.

Betrakta en och samma användare A. Denna kontaktar nätsidan N med ett meddelande e_1 och en signatur (r_1, s_1). Dessa tre tal fångar hackern H upp. Vi har ekvationen $s_1 = \frac{(e_1 + cr_1)}{k}$, som vi också kan skriva som

$$s_1 k - r_1 c = e_1.$$

Talen e_1, r_1 och s_1 har vi, men inte de två okända k och c. Ni kan tänka på detta som en linje i ett plan där de två okända är k och c.

Men, dagen efter skickar användaren A ett nytt meddelande till nätsidan N. Hackern H fångar nu upp talet e_2 och signaturen (r_2, s_2). Nu får vi en linje till, nämligen

$$s_2 k - r_2 c = e_2.$$

Nu har vi ett ekvationssystem i två okända k och c som vi kan lösa. Ekvationssystemet skriver vi upp som matrisekvationen

$$\begin{bmatrix} s_1 & -r_1 \\ s_2 & -r_2 \end{bmatrix} \begin{bmatrix} k \\ c \end{bmatrix} = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix}.$$

Inversen till matrisen till vänster är

$$\frac{1}{-s_1 r_2 + r_1 s_2} \begin{bmatrix} -r_2 & r_1 \\ -s_2 & s_1 \end{bmatrix}.$$

Detta ger nu att

$$\begin{bmatrix} k \\ c \end{bmatrix} = \frac{1}{r_1 s_2 - s_1 r_2} \begin{bmatrix} -r_2 e_1 + r_1 e_2 \\ -s_2 e_1 + s_1 e_2 \end{bmatrix}.$$

Speciellt har vi att den hemliga krypteringsnyckeln till användaren A är

$$c = \frac{s_1 e_2 - s_2 e_1}{r_1 s_2 - s_1 r_2}.$$

Notera också att om k är konstant då blir $r_1 = r_2$. Detta betyder att

$$c = \frac{s_1 e_2 - s_2 e_1}{r_1 (s_2 - s_1)}.$$

Appendix E

LaTeX

E.1 Att skriva matematisk text

Vi började föreläsningen med LaTeX programmering. I sin enkelhet ser ett LaTeX-dokument ut så här:

```
\documentclass{article}

\begin{document}

Här kommer din text.

\end{document}
```

Filen sparas som namn.tex, och kompileras sedan med kommandot
`> pdflatex namn.tex`
som skapar filen namn.pdf. Försök gärna göra ett enkelt dokument i LaTeX. Häftet The Not So Short Introduction to LaTeX 2_ε finns under

`http://tobi.oetiker.ch/lshort/lshort.pdf`

och är vad jag själv använder. Möjligen är det första stället att börja på hemsidan

`http://www.latex-project.org/intro.html`

Detta är inte svårt att lära sig, och ni kommer att ha stor användning för detta i framtiden. Lycka till.