

Insinöörimatematiikkaa tiivistettynä

eli muistiinpanoja TKK:n matematiikan kursseilta

JARNO ELONEN

EMAIL: elonen@iki.fi

versio 1.1.0

7.6.2005

URN:NBN:fi-fe20044218

Hyvä lukija,

Olen kirjoittanut nämä muistiinpanot alunperin itselleni ja julkaisen ne nyt yksinkertaisesti siltä varalta, että niistä sattuisi olemaan jollekulle muullekin jotain iloa.

Kyseessä ei ole oppikirja vaan asioita on jätetty pois, oiottu ja yksinkertaistettu sen mukaan miten olen niitä itse katsonut tarvitsevani ja kuinka hyvin olen muistanut asiat entuudestaan. Tarkoituksena on ollut lähinnä luetteloida erilaisten ongelmien ratkaisutapoja käytännön (tietotekniikka-)insinöörintyötä ajatellen eikä niinkään osoittaa tai johtaa niitä. En myöskään väitä ymmärtäväni kaikkea kirjoittamaani – mikä on tietysti harmi, sillä matematiikka on kiinnostavaa vaikka ainakin itselläni muut työt ovat aina vieneet ajan ja energian paneutua siihen kunolla.

Tekstiä saa kopioida, muokata ja vaikka myydä vapaasti kunhan minut mainitaan alkupe-
räisen version toimittajana ja kerrotaan, että alkuperäinen on vapaasti kopioitavaa materiaalia.
Uusin versio löytyy osoitteesta:

`http://iki.fi/elonon/articles/insimat/`

Valituksille finglishistä ja muista muotoseikoista en luultavasti lotkauta korvaanikaan ellei valitusten mukana tule korjaustiedostoa, sillä tämän dokumentin päivittämiseen käytetty aika on aina pois muilta, tärkeämmiltä, asioilta. Tekstiin on epäilemättä kuitenkin jäänyt myös varsinaisia asiavirheitä – niistä saa mielellään huomauttaa sähköpostitse. GNU Diff:llä muodostetut korjaustiedostot suoraan .tm-tiedostoon ovat tietysti vieläkin tervetulleempia.

– JARNO ELONEN

Sisältö

1 Lineaarialgebra	6
1.1 Matriisien perusteet	6
1.1.1 Tulo	6
1.1.2 Käänteismatriisi	7
1.1.3 Gaussin eliminaatio	7
1.1.4 Determinantti	8
1.1.5 Kanta	8
1.1.6 Gram-Smidth-ortonormalisointi	9
1.1.7 Ominaisarvot ja -vektorit (eigenvalues & vectors)	9
1.1.8 Matriisifunktiot	9
1.2 Vektorit ja analyyttinen geometria	10
1.2.1 Vektoritulot	10
1.2.2 Suora	11
1.2.3 Taso	11
1.2.4 Tetraedri	11
1.2.5 Projektio	11
1.3 Homogeeniset koordinaatit	12
1.3.1 Ideaalipisteet, -suorat ja tasot	12
1.3.2 Duaalisuus ja lauseiden dualisointi	12
1.4 Kuvaukset (transformaatiot)	12
1.4.1 Lineaarikuvaus	12
1.4.2 Affiniteetti (affinikuvaus)	13
1.5 Matriisien sekalaisia sovelluksia	13
1.5.1 Pienimmän neliösumman sovitus (least squares fit)	13
1.5.2 Markovin ketjut	13
2 Differentiaalilaskentaa yleisesti	14
2.1 Differentiaali	14
2.2 Jacobian-matriisi	14
2.3 Monen muuttujan ketjusääntö	14
3 ODEt - ”tavalliset” differentiaaliyhtälöt	15
3.1 Peruskäsitteitä	15
3.2 Yksittäisen ODEn tarkka ratkaiseminen	15
3.2.1 Separoituva: integrointi puolittain	15
3.2.2 Tasa-asteinen: muuttujan vaihto	15
3.2.3 Eksakti: osittaisderivointi	15
3.2.4 Eksaktiksi muuttaminen: integroiva tekijä	16
3.2.5 1. kertaluvun lineaarinen ODE: yleinen ratkaisu	16
3.3 Yksittäisen yhtälön likiarvoratkaisut	16
3.3.1 Suuntakenttä - erikoisratkaisu graafisesti	16
3.3.2 Picardin iteraatio - approksimoiva algebrallinen erikoisratkaisu	17
3.4 2. asteen ODE	17
3.5 1. asteen lineaarinen homogeeninen ODE-ryhmä	17
3.5.1 Vaihekuvaaja	17
3.6 Laplace-muunnos	18
4 Sarjat	19
4.1 Suppenemisen testaus	19
4.2 Yleisimpiä sarjoja	19

4.3	Potenssisarjat	20
4.4	Fourier-sarja	20
5	Monen muuttujan analyysi	21
5.1	Avaruuspinta	21
5.2	Raja-arvo	21
5.3	Monen muuttujan funktion differentiaalit	21
5.3.1	Osittaisderivaatta	21
5.3.2	Gradientti ja suunnattu derivaatta	21
5.4	Napakoordinaatisto	22
5.5	Monen muuttujan ääriarvotehtävät	22
5.5.1	Ääriarvopisteiden luokittelu (Hessian)	22
5.5.2	Rajoitetut ääriarvotehtävät (Lagrange-kertoimet)	22
6	Skalaari- ja vektorikentät	22
6.1	Viivaintegraali	23
6.1.1	Greenin lause (suljetun käyrän viivaintegraali)	23
6.1.2	Stokesin lause (moniulotteiset pinnat)	24
6.2	”Vektoriderivaatat” - grad, div, curl	24
6.3	Divergenssilause (aka. Gaussin laki)	24
7	Kompleksiluvut	26
7.1	Kompleksiset funktiot	26
8	Abstrakti algebra	27
8.1	Ryhmät (groups) ja monoidit (monoids)	27
8.2	Renkaat (ring) ja kunnat (field)	28
8.3	Polynomirenkaat	29
8.4	Kooditeoria	30
9	Kombinatoriikka	31
9.1	Permutaatiot ja kombinaatiot	31
9.2	Inklusio-eksklusio-periaate	31
9.3	Binomi- ja multinomikertoimet	32
9.4	Generoivat funktiot eli emäfunktiot	32
9.5	Tornipolynomit (rook polynomials)	34
9.6	Differenssiyhtälöt eli rekursiot	35
9.6.1	Lineaariset ja vakiokertoimiset	35
9.6.2	Ratkaisu emäfunktiolla	36
9.7	Permutaatioryhmät ja ekvivalenssiluokat	36
10	Jaollisuus ja moduloaritmetiikka	39
10.1	Jaollisuussääntöjä	39
10.1.1	Suurin yhteinen tekijä (GCD) ja pienin yhteinen jaettava (LCM)	39
10.1.2	Lineaariset Diophanteen yhtälöt	40
10.2	Kongruenssi eli moduloaritmetiikka	40
10.3	Suuret alkuluvut	41
10.3.1	RSA-salakirjoitus	41
11	Graafit	42
11.1	Lauseita	42
11.2	Algoritmeja (ei-negatiivisesti) painotetuille graafeille	43
11.3	Kaksijakoinen graafi (bipartite graph)	43
12	Sekalaisia laskutekniikoita	44

12.1	Induktiotodistus	44
12.2	Neliöksi täydentäminen	44
12.3	Osamurtokehiteelmä	45
12.3.1	Tapa 1: $x:n$ valitseminen strategisesti	45
12.3.2	Tapa 2: yhtälöryhmä eri asteisista termeistä	46
12.3.3	Tapa 3: Heavisiden peittomenetelmä	46
12.4	Logaritmi	47
12.5	Raja-arvo	47
12.6	Trigonometrinen funktioiden ominaisuuksia	48
13	Merkintätapoja	48
13.1	Tavalliset lukujärjestelmät	48
13.2	Kreikkalaiset kirjaimet	48
	Hakemisto	49

1 Linearialgebra

Tässä kappaleessa käsitellään lähinnä reaalisia avaruuksia \mathbb{R}^n mutta suurin osa kohdista pätee myös myös kompleksisille avaruuksille tai vaikka alkiot olisivat funktioita (*funktioavaruus*). Oleellista on vain, että alkiot toteuttavat *linearialgebran aksioomat*, joiden mukaan mm. täytyy löytyä nolla-alkio ja ykkösalkio, jokaiselle alkion täytyy olla vasta-alkio, alkion kertominen skalaarilla täytyy kommutoida yms.

1.1 Matriisien perusteet

- *transpoosi* A^T on A :n peilaus *diagonaalin* (lävistäjän) suhteen
- *säännöllinen* vs. *singulaarinen matriisi*: on olemassa käänteismatriisi vs. ei ole olemassa. Älä sekoita säännöllistä ja **symmetristä** (ts. $A = A^T$).
- *ortogonaalinen matriisi*: $M^{-1} = M^T$ (pystyvektorit ovat kohtisuorassa eli ortogonaaliset)
- *ortonormeeratut vektorit*: toisiaan vastaan kohtisuorassa (ortogonaalimatriisi) **ja** normit (pituus) ovat 1
- *rangi* tai *rankki* (*rank*) eli *säännöllisyysaste*: yhtälöryhmän ratkaisun ei-vapaiden muuttujien määrä eli Gaussin eliminaation tuloksen $\left(\begin{array}{cc|c} I & P & b_1 \\ O & O & b_2 \end{array} \right)$ yksikköneliömatrisiin I koko.
- *lineaarikuvaus* on funktio, jolle a) $f(x) + f(y) = f(x + y)$ ja b) $\lambda f(x) = f(\lambda x)$ ja koska molemmat pitävät paikkansa matriisikertolaskussa: $f(x) = Fx$ kun $x \in \mathbb{R}^n$.
- lineaarikuvauksen *ydin* (*kernel*) on $Fx = 0$:n ratkaisujoukko.
- avaruuden *dimensio*: vapaiden muuttujien määrä, esim. \mathbb{R}^2 :lle 2 ja \mathbb{R}^3 :lle 3.
- *linearikombinaatio* tai -yhdistely on vektoreiden painotettu summa. Älä sekoita lineaarikombinaatiota lineaarikuvauksen kanssa!
- *kanta*: n kappaletta avaruuden \mathbb{R}^n lineaarisesti riippumatonta vektoria (mitkä tahansa). Sanonta: "*koordinaatit kannan B suhteen*".
- *luonnollinen kanta*: avaruuden \mathbb{R}^n vektorit $I_{n \times n}$ (eli tavallinen koordinaatisto).
- *matriisin normi* on mikä tahansa eräät ehdot täyttävä skalaari-"mittari" matriisille. Tässä kolme tärkeintä (vastaavista vektorinormeista johdettua) matriisnormia:

$$\|A\|_2 = \sqrt{\max(\text{ominaisarvot}(A^T A))}$$

$$\|A\|_1 = \max_{j=1 \dots n} (\sum_{i=1}^n |a_{ij}|) = \max(\text{absolute column sum})$$

$$\|A\|_\infty = \max_{j=1 \dots n} (\sum_{i=1}^n |a_{ji}|) = \max(\text{absolute row sum})$$

1.1.1 Tulo

Matriisien tulo tapahtuu "*kertomalla rivit sarakkeisiin*" ja $AB = C$:ssä, C :n korkeus on A :n korkeus ja leveys B :n leveys. Jos A :n leveys $\neq B$:n korkeus, tulo on määrittelemätön. Esim:

$$\begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}_{3 \times 2} \begin{pmatrix} g \\ h \end{pmatrix}_{2 \times 1} = \begin{pmatrix} ag + bh \\ cg + dh \\ eg + fh \end{pmatrix}_{3 \times 1}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix}_{2 \times 3} \begin{pmatrix} g \\ h \\ i \end{pmatrix}_{3 \times 1} = \begin{pmatrix} ag + bh + ci \\ dg + eh + fi \end{pmatrix}_{2 \times 1}$$

Toisin sanoen: matriisi \times vektori -operaatio on siis **matriisin leveys** -kokoisen vektorin kuvaus **matriisin korkeus** -kokoiseksi vektoriksi.

Pystyvektorien pistetulo $\vec{a} \cdot \vec{b} = |\vec{a}| |\vec{b}| \cos(\vec{a}, \vec{b}) = a^T b = (a_0 \ a_1 \ \dots) \begin{pmatrix} b_0 \\ b_1 \\ \vdots \end{pmatrix}$

1.1.2 Käänteismatriisi

Määritelmä: $MM^{-1} = I \wedge M^{-1}M = I$. Vain neliömatriiseilla voi olla käänteismatriisi niilläkin vain **joss** sarakkeet/rivit ovat lineaarisesti rippumattomia (sama asia). Sääntöjä:

$$\begin{aligned} (M^{-1})^{-1} &= M \\ (\lambda M)^{-1} &= \frac{1}{\lambda} M^{-1} \\ (AB)^{-1} &= A^{-1}B^{-1} \\ (M^T)^{-1} &= (M^{-1})^T \end{aligned}$$

Käänteismatriisin voi laskea *Gauss-Jordan-algoritmi*lla (ks. alempana)...

$$\begin{array}{c} \text{u} \\ \left. \begin{array}{ccc|ccc} a & b & c & 1 & 0 & 0 \\ d & e & f & 0 & 1 & 0 \\ g & h & i & 0 & 0 & 1 \end{array} \right\} \Rightarrow \begin{array}{c} \text{u} \\ \left. \begin{array}{ccc|ccc} 1 & 0 & 0 & J & K & L \\ 0 & 1 & 0 & M & N & O \\ 0 & 0 & 1 & P & Q & R \end{array} \right\} \end{array}$$

...tai hitaasti determinantin (ks. alempana) avulla (*Cramerin sääntö*):

$$M = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \Rightarrow M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} + \begin{vmatrix} e & f \\ h & i \end{vmatrix} & - \begin{vmatrix} d & f \\ g & i \end{vmatrix} & + \begin{vmatrix} d & e \\ g & h \end{vmatrix} \\ - \begin{vmatrix} b & c \\ h & i \end{vmatrix} & + \begin{vmatrix} a & c \\ g & i \end{vmatrix} & - \begin{vmatrix} a & b \\ g & h \end{vmatrix} \\ + \begin{vmatrix} b & c \\ e & f \end{vmatrix} & - \begin{vmatrix} a & c \\ d & f \end{vmatrix} & + \begin{vmatrix} a & b \\ d & e \end{vmatrix} \end{pmatrix}^T$$

2x2-kokoiselle matriisille Cramerin sääntö tosin on vielä selvästi helpompi: $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1} \Rightarrow M^{-1} = \frac{1}{AD - BC} \begin{pmatrix} D & -B \\ -C & A \end{pmatrix}$.

1.1.3 Gaussin eliminaatio

Yhtälöryhmä $Ax = b$ kirjoitetaan matriisiksi...

$$\begin{cases} A_{11}x_1 + A_{12}x_2 + A_{13}x_3 = b_1 \\ A_{21}x_1 + A_{22}x_2 + A_{23}x_3 = b_2 \\ A_{31}x_1 + A_{32}x_2 + A_{33}x_3 = b_3 \end{cases} \Rightarrow \begin{array}{ccc|c} A_{11} & A_{12} & A_{13} & b_1 \\ A_{21} & A_{22} & A_{23} & b_2 \\ A_{31} & A_{32} & A_{33} & b_3 \end{array}$$

...ja väännetään sitten yläkolmiomuotoon vähentämällä "nykyinen" rivi alemmista riveistä aina kerrottuna ylänurkan sopivasti kerrotulla tukialkiolla...

$$\begin{array}{ccc|c} A_{11} & A_{12} & A_{13} & b_1 \\ A_{21} & A_{22} & A_{23} & b_2 \\ A_{31} & A_{32} & A_{33} & b_3 \end{array} \Rightarrow \begin{array}{ccc|c} A_{11} & A_{12} & A_{13} & b_1 \\ 0 & C & D & E \\ 0 & F & G & H \end{array} \Rightarrow \begin{array}{ccc|c} A_{11} & A_{12} & A_{13} & b_1 \\ 0 & C & D & E \\ 0 & 0 & I & J \end{array}$$

...ja soveltamalla sitten alhaalta ylöspäin *peräkkäisiä sijoituksia* tai toistamalla eliminointi alhaalta ylös, jolloin saadaan yksikkömatriisi (kuten Gauss-Jordan:ssa). Huom:

- rivin vaihto ei muuta tulosta
- sarakkeen vaihto muuttaa muuttujien järjestystä \Rightarrow kirjanpito tarpeen
- Tulorivi $0=0$ **EI** tarkoita, että ryhmä olisi ratkaisematon vaan se poistetaan ja tulkitaan jäljelle jääneitä rivejä yhtälöryhmänä
- **Ristiriitainen** tulorivi (esim. $0=4$) tarkoittaa ratkaisematonta ryhmää

- Jos tuloksia on äärettömästi, esitetään ratkaisu vapaan muuttujan (tai useamman) avulla:

$$x = \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} + \tau \begin{pmatrix} -1 \\ 0 \\ 7 \end{pmatrix} \text{ eli } \begin{cases} x_0 = -\tau \\ x_1 = 2 \\ x_3 = 1 + 7\tau \end{cases}$$

1.1.4 Determinantti

Determinantti on neliömatriisin vektorien määräämän suoran/suunnikkaan/särmiön pituus/ala/tilavuus (ja vastaava luku moniulotteisemmille avaruuksille). Yksinkertaisin tapaus, 2×2 -determinantti on helppo laskea: $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$. Yleisiä sääntöjä:

- rivin/sarakkeen vaihto muuttaa etumerkin
- determinantin kertominen skalaarilla kertoo yhden rivin tai sarakkeen: $\lambda \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} \lambda a & \lambda b \\ c & d \end{vmatrix}$ ja esim. $\lambda^3 \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} \lambda a & \lambda^2 b \\ \lambda c & \lambda^2 d \end{vmatrix} = \begin{vmatrix} a & b \\ \lambda^3 c & \lambda^3 d \end{vmatrix}$ jne.
- rivin/sarakkeen lisääminen toiseen skaalattuna ei muuta tulosta (\Rightarrow Gauss toimii)
- transponointi ei muuta determinanttia (ts. $\det(A) = \det(A^T)$)
- $\det(AB) = \det(A) \det(B)$
- $\det(M) \neq 0 \Rightarrow$ sarakkeet/rivit ovat lin. riippumattomia \Rightarrow on olemassa käänteismatriisi

Ison determinantin voi laskea vääntämällä se Gaussin algoritmilla yläkolmiomuotoon ja laske-
malla lävistäjän tulo...

$$\begin{vmatrix} a & ? & ? \\ 0 & b & ? \\ 0 & 0 & c \end{vmatrix} = abc$$

...tai hitaammin *alideterminanttikehitelmän* avulla minkä tahansa rivin tai sarakkeen suhteen...

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = -b \cdot \begin{vmatrix} d & f \\ g & i \end{vmatrix} + e \cdot \begin{vmatrix} a & c \\ g & i \end{vmatrix} - h \cdot \begin{vmatrix} a & c \\ d & f \end{vmatrix}$$

...missä termien etumerkit määräytyvät elementin koordinaateista näin:

$$(-1)^{i+j} \Rightarrow \begin{vmatrix} + & - & + \\ - & + & - \\ + & - & + \end{vmatrix}$$

Vektorien ristitulo $\vec{a} \times \vec{b} = |\vec{a}| |\vec{b}| \sin(\vec{a}, \vec{b}) \vec{e} = \begin{vmatrix} \vec{i} & \vec{j} & \dots \\ a_0 & a_1 & \dots \\ b_0 & b_1 & \dots \end{vmatrix}$, missä $\vec{e} \perp \vec{a}, \vec{b}$.

1.1.5 Kanta

Avaruuden \mathbb{R}^n kanta (koordinaatisto) muodostuu mistä tahansa n :stä, lineaarisesti riippumattomasta vektorista. *Luonnollinen kanta* on "tavallinen koordinaatisto" $\{(1 \ 0 \ 0 \ \dots)^T, (0 \ 1 \ 0 \ \dots)^T, (0 \ 0 \ 1 \ \dots)^T, \dots\}$. Kannan vaihto luonnollisesta kantaan $\{b_1 (= b_{11}\vec{i} + b_{12}\vec{j} + \dots), b_2, \dots, b_n\}$ on...

$$\begin{aligned} b_1 \hat{x}_1 + b_2 \hat{x}_2 + \dots &= x \text{ eli} \\ \begin{pmatrix} b_{11} \\ b_{12} \\ \vdots \end{pmatrix} \hat{x}_1 + \begin{pmatrix} b_{21} \\ b_{22} \\ \vdots \end{pmatrix} \hat{x}_2 &= x \text{ eli} \\ \begin{pmatrix} b_{11} & b_{21} & \dots \\ b_{12} & b_{22} & \dots \\ \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \vdots \end{pmatrix} &= \begin{pmatrix} x_1 \\ x_2 \\ \vdots \end{pmatrix} \text{ eli} \\ B \hat{x} &= x \Leftrightarrow \\ \hat{x} &= B^{-1}x \end{aligned}$$

...eli tehdään kantamatriisi B **pysty**vektoreista $b_{1,\dots,n}$ ja ratkaistaan \hat{x} - tai jos halutaan kannanvaihtomatriisi, lasketaan B :n käänteismatriisi.

1.1.6 Gram-Smidth-ortonormalisointi

Kanta on *ortonormaali*, jos sen kaikki vektorit ovat kohtisuorassa toisiaan vastaan ja jokainen vektorin on 1:n mittainen (kuten luonnollisella kannalla). Minkä tahansa kannan voi pakottaa ortonormaaliksi *Gram-Smidth ortonormalisointi*-algoritmeilla. Sitä käytetään erityisesti numeerisessa laskennassa hieman ”epävireeseen” menneen kannan korjaamiseen. Merkitään alkuperäisiä vektoreita w_n ja uusia v_n :

1. merkitään $i = 1$ ja $v'_1 = w_1$ ja aloitetaan kohdasta 3
2. vähennetään i :nnestä vektorista kaikkien jo ortonormalisoitujen vektorien projektiot: $v'_i = w_i - \sum_{j=1}^{i-1} (w_i \cdot v_j) v_j$
3. normalisoidaan i :s vektori: $v_i = \frac{v'_i}{|v'_i|}$
4. Lisätään i :tä yhdellä eli siirrytään seuraavaan vektoriin. Jos $i < n$, jatketaan kohdasta 2.

1.1.7 Ominaisarvot ja -vektorit (eigenvalues & vectors)

Neliömatriisin ominaisarvon määritelmä: $Ax = \lambda x$, eli koska **A:lla transformointi ei muuta ominaisvektorin x suuntaa** (paitsi ehkä negatoid), transformaation voi (kaikille x :n suuntaisille vektoreille) tiivistää skalaariksi: *ominaisarvoksi* λ . Koska $Ax = \lambda x \Leftrightarrow (A - \lambda I)x = o$, löytää ominaisarvot ratkaisemalla $\det(A - \lambda I) = 0$ ja -vektorit ratkaisemalla tuloksen perusteella yhtälöryhmä $(A - \lambda I)x = o$. Siis:

1. laske $\det(A - \lambda I)$ eli λ :stä riippuva A :n *karakteristinen polynomi*
2. ratkaise polynomin juuret (eli A :n ominaisarvot)
3. muodosta nyt tunnetuista ominaisarvoista yhtälöryhmät $(A - \lambda_n I)x_n = 0$ ja ratkaise x_n :t (Huom: matriisi $(A - \lambda_n I)$ on singularinen, joten x_n :t eivät ole yksiselitteisiä, vaan ne voi skaalata mielivaltaisella vakiolla)

Matriisin on *diagonalisoituva*, jos sillä on n ominaisarvoa. Diagonalisoitu matriisi on koottu ominaisarvoista: $\Lambda = \begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \ddots \end{pmatrix}$. Vastaavasti sen *similariteettimuunnos* (-matriisi) on koottu ominais(pysty)vektoreista $X = (x_1 \ x_2 \ \dots)$. Matriisit A ja B ovat *similaariset*, jos on olemassa T siten, että $AT = TB$, joten A ja Λ ovat aina similaariset: $AX = X\Lambda \Leftrightarrow X^{-1}AX = \Lambda$. Esimerkki ominaisarvojen laskemista, diagonalisoinnista ja similaarisuuden hyödyntämisestä on seuraavassa kappaleessa.

1.1.8 Matriisifunktiot

Matriisifunktiot on määritelty $n \times n$ -neliömatriisille seuraavasti:

$$f(A) = \sum_{r=0}^{n-1} \alpha_r A^r$$

...josta α_r :t voi laskea ominaisarvojen avulla, sillä:

$$f(\lambda_i) = \sum_{r=0}^{n-1} \alpha_r \lambda_i^r \Rightarrow \begin{pmatrix} 1 & \lambda_0 & \lambda_0^2 \\ 1 & \lambda_1 & \lambda_1^2 \\ 1 & \lambda_2 & \lambda_2^2 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} f(\lambda_0) \\ f(\lambda_1) \\ f(\lambda_2) \end{pmatrix}$$

Toisaalta, jos ominaisarvot eivät ole moninkertaisia (**onko välttämätön ehto?**), voi saman laskea diagonalisoimalla avullakin:

$$f(\mathbf{\Lambda}) = \begin{pmatrix} f(\lambda_0) & & \\ & \ddots & \\ & & f(\lambda_{n-1}) \end{pmatrix}$$

$$f(\mathbf{A}) = \mathbf{X} f(\mathbf{\Lambda}) \mathbf{X}^{-1}$$

Tällä tavalla voidaan laskea esim. *matriisiekspONENTTI* $\exp(\mathbf{A}) = e^{\mathbf{A}} (= \mathbf{X} e^{\mathbf{\Lambda}} \mathbf{X}^{-1})$, $\sin(\mathbf{A})$, mielivaltaisen suuri matriisipotenssi \mathbf{A}^r tai vaikka neliöjuurimatriisi ($\mathbf{M}^2 = \mathbf{A}$). Esimerkki:

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \Leftrightarrow A^{-1} = \begin{pmatrix} -1/3 & 2/3 \\ 2/3 & -1/3 \end{pmatrix}$$

$$\begin{vmatrix} 1-\lambda & 2 \\ 2 & 1-\lambda \end{vmatrix} = 0 \Rightarrow \lambda_0 = 3, \lambda_1 = -1$$

$$\Lambda = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow \begin{cases} (1-3)x_{11} + 2x_{21} = 0 \Rightarrow x_{21} = x_{11} \\ 2x_{21} + (1-3)x_{22} = 0 \Rightarrow x_{22} = -x_{21} \end{cases} \Rightarrow$$

$$X = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \Leftrightarrow X^{-1} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

$$\Lambda^{11} = \begin{pmatrix} 3^{11} & 0 \\ 0 & (-1)^{11} \end{pmatrix} \Rightarrow \mathbf{A}^{11} = X \Lambda^{11} X^{-1} = \begin{pmatrix} 88573 & 88574 \\ 88574 & 88573 \end{pmatrix}$$

$$e^{\Lambda} = \begin{pmatrix} e^3 & 0 \\ 0 & e^{-1} \end{pmatrix} \Rightarrow e^{\mathbf{A}} = X e^{\Lambda} X^{-1} \approx \begin{pmatrix} 10.2 & 9.9 \\ 9.9 & 10.2 \end{pmatrix}$$

Huom: *matriisin derivaatta* ja integraali lasketaan kuitenkin ottamalla ne erikseen jokaiselle alkionle.

1.2 Vektorit ja analyyttinen geometria

1.2.1 Vektoritulot

- *Pistetulo* eli *skalaaritulo* eli *sisätulo* $a \cdot b = |a||b|\cos(a, b) = \mathbf{a}^T \mathbf{b} = (a_0 \ a_1 \ \dots) \begin{pmatrix} b_0 \\ b_1 \\ \vdots \end{pmatrix}$.

- Yhdensuuntaisuus: $a \perp b \Leftrightarrow a \cdot b = 0$
- Skalaariprojektio: a :n pituus b :llä on $\frac{a \cdot b}{|b|}$.

- *Ristitulo* eli *vektoritulo* $a \times b$ on määritelty vain 3-vektoreille:

(Huom: sanotaan, että *ristitulomatriisi* A^\times saadaan a :sta *ristiopeattorilla*)

$$a \times b = |a||b|\sin(a, b)\vec{e} \quad \|\vec{e} \perp a, b \text{ ja } |\vec{e}| = 1$$

$$= \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ a_x & a_y & a_z \\ b_x & b_y & b_z \end{vmatrix}$$

$$= A^\times \cdot b = \begin{pmatrix} 0 & -a_z & a_y \\ a_z & 0 & -a_x \\ -a_y & a_x & 0 \end{pmatrix} \cdot b$$

- Suunnikkaan ala: $A_{\text{suunnikas}} = |a \times b|$, **kolmion ala** $= A_{\text{kolmio}} = \frac{|a \times b|}{2}$.

- *Skalaarikolmitulo*: $\overline{abc} = a \cdot b \times c = a \times b \cdot c$.
Särmiön tilavuus: $|\overline{abc}|$, tetraedrin tilavuus: $\frac{|\overline{abc}|}{6}$.
Huom: alat voi laskea myös determinantilla: $|\overline{abc}| = \begin{vmatrix} a_x & b_x & c_x \\ a_y & b_y & c_y \\ a_z & b_z & c_z \end{vmatrix}$.

1.2.2 Suora

- *Parametrimuoto*: $\vec{p} = \vec{p}_0 + \tau \vec{s}$, missä \vec{s} on suoran suunta
- *Normaalimuoto*: koska jokainen p_0 :sta pisteeseen johtava vektori on kohtisuorassa normaalia vastaan, on \mathbb{R}^2 :ssa:
 $(\vec{p} - \vec{p}_0) \cdot \vec{n} = 0$ eli $n_1x + n_2y = \vec{n} \cdot \vec{p}$ eli $ax + by = c$, missä **a, b ovat \vec{n} :n komponentit ja c on normaalin ja \vec{p}_0 :n pistetulo** (eli \vec{p}_0 :n projektio \vec{n} :lle, suoran siirto origosta).
- *Painopistekoordinaatit*: $\vec{p} = a\vec{p}_0 + b\vec{p}_1$, missä $a + b = 1$
Jos $a > 0 \wedge b > 0$, piste on p_0 :n ja p_1 :n välissä. Keskipisteessä $a = b = 1/2$.
- *Suoraparvi* on usemman suoran ryhmä ja *suoraviuhka* kulkee tietyn pisteen läpi.
- Avaruudessa \mathbb{R}^3 suoran voi esittää parametrimuodossa tai kahden tason leikkauksena:
$$\begin{cases} \vec{n}_a \cdot (\vec{p} - \vec{p}_a) = 0 \\ \vec{n}_b \cdot (\vec{p} - \vec{p}_b) = 0 \end{cases}$$

1.2.3 Taso

- *Parametrimuoto*: $\vec{p} = \vec{p}_0 + \sigma \vec{s} + \tau \vec{t}$, missä tietysti $\vec{s} \nparallel \vec{t}$
- *Normaalimuoto*: koska jokainen p_0 :sta pisteeseen johtava vektori on kohtisuorassa normaalia vastaan, on (\mathbb{R}^3 :ssa!): $(\vec{p} - \vec{p}_0) \cdot \vec{n} = 0$ eli $n_1x + n_2y + n_3z = \vec{n} \cdot \vec{p}_0$ eli
 $ax + by + cz = d$, missä **a, b, c ovat \vec{n} :n komponentit ja d on normaalin ja \vec{p}_0 :n pistetulo**.
- *Painopistekoordinaatit*: vektoreilla $\vec{p} = a(\vec{p}_1 - \vec{p}_0) + b(\vec{p}_2 - \vec{p}_0)$ tai $\vec{p} = a\vec{p}_0 + b\vec{p}_1 + c\vec{p}_2$, missä $a + b + c = 1$.
Annetun pisteen sijainnin p -pisteiden muodostamaan kolmioon nähden voi päätellä painokertoimien merkistä - kolmion sisällä se on " + + + ". Kolmion *painopisteessä* $a = b = c = 1/3$.

1.2.4 Tetraedri

- Tetraedrissä on 4 tahkoa ja 4 kärkipistettä ("kolmiopohjainen pyramidi"):
- Kun kärkipisteistä p_0, p_1, p_2, p_3 johdetaan kolme särmävektoria $(p_1 - p_0), (p_2 - p_0), (p_3 - p_0)$ saadaan sekä kanta, että auki kertomalla painopistekoordinaattiesitys:
 $\vec{p} = a\vec{p}_0 + b\vec{p}_1 + c\vec{p}_2 + d\vec{p}_3$, missä $a + b + c + d = 1$. Kuten 3D-tason ja 2D-suoran tapauksissakin, painopisteessä on $a = b = c = d = 1/4$ ja annetun pisteen paikan tetraedrin suhteen voi päätellä a, b, c, d :n etumerkeistä - tetraedrin sisällä se on " + + + + ".

1.2.5 Projektio

- *Yhdensuuntaisprojektion* määrittää *projektiotason* normaali n ja *projektiiosäteiden* suuntavektori s . Laskukaava: $x' = x - \frac{n \cdot x}{n \cdot s} s$ tai matriisina $x' = P x$, $P = I - \frac{1}{n^T s} s n^T$. P on yhdensuuntaisprojektiio joss $P = P^2$.

- Jos suuntavektori on lisäksi kohtisuorassa tasoon nähden, on kyseessä *ortogonaalinen projektiio* (joss $P = P^T$).

1.3 Homogeeniset koordinaatit

projektiivinen taso, projektiivinen avaruus, Pappuksen lause, projektiviteetti, kiintopiste

Euklidisen tason \mathbb{R}^2 pistettä $p = \{x, y\}$ vastaa *projektiivisen tason* \mathbb{P}^2 piste, eli *homogeeninen koordinaatti* $P = \begin{pmatrix} 1 \\ x \\ y \end{pmatrix} = \begin{pmatrix} P_0 \\ P_1 \\ P_2 \end{pmatrix} \hat{=} \begin{pmatrix} 1 \\ P_1/P_0 \\ P_2/P_0 \end{pmatrix} \hat{=} \begin{pmatrix} \lambda \\ \lambda x \\ \lambda y \end{pmatrix} \hat{=} \{x/\lambda, y/\lambda\}$. Grafiikkakirjoissa ylimääräinen ("nollas") elementti kirjoitetaan usein viimeiseksi: [x,y,w].

Sekä affinitransformaatiot (siirto, peilaus, rotaatio, skaalaus, skew) **että projektiio** ovat homogeenisissa koordinaateissa palautettavissa (projektiiossa $z = 0$ aiheuttaa tavallisen pisteen muuttumisen ideaalipisteeksi, $z = \infty$ ideaalipisteen muuttumisen tavalliseksi ja lopuissa z koodautuu w :hen) – siitkö lienee nimi "projektiivinen taso"? Molemmat voidaan esittää esim. \mathbb{P}^3 :n tapauksessa 4×4 -matriisilla.

1.3.1 Ideaalipisteet, -suorat ja tasot

Pystyvektorilla esitetään pisteitä ja vaakavektorilla (transponoiduilla) suoria: $w^T = (\omega_0 \ \omega_1 \ \omega_2)$. Suoran tavallinen yhtälö on $\omega_1 x + \omega_2 y + \omega_0 = 0$. *Ideaalipisteet* $\begin{pmatrix} 0 \\ \xi_1 \\ \xi_2 \end{pmatrix}$ ovat kuviteltuja "ääretömän kaukana sijaitsevien samansuuntaisten suorien leikkauksia", toimivat laskennassa aivan kuten muutkin pisteet ja sijaitseva *ideaalisuoralla* $(1 \ 0 \ 0)^T$ (tai *projektiivisessä avaruudessa* \mathbb{P}^3 *ideaalitasolla*).

1.3.2 Duaalisuus ja lauseiden dualisointi

Projektiivisen tason pisteet ja suorat ovat *duaalisia* eli niitä koskevissa lauseissa sanan "suora" ja "piste" (\mathbb{P}^3 :ssa "taso" ja "piste") voi vaihtaa keskenään (eli lause voidaan *dualisoida*):

- suora kahdesta pisteestä: $w^T = p_1 \times p_2$ / (leikkaus-)piste kahdesta suorasta: $p = w_1^T \times w_2^T$.
- piste on suoralla / suora on pisteellä: $w^T p = \vec{w} \cdot \vec{p} = 0$
- pisteet samalla suoralla: $|p_1 \ p_2 \ \dots| = 0$ / suorat yhdensuuntaisia: $|w_1 \ w_2 \ \dots| = 0$

1.4 Kuvaukset (transformaatiot)

1.4.1 Lineaarikuvaus

Lineaarikuvaus tai tuttavallisesti matriisikertolasku $f(x) = Ax$ (ilman homogeenisia koordinaatteja), on määritelty kahdella ehdolla:

- $f(x) + f(y) = f(x + y)$
- $\lambda f(x) = f(\lambda x)$

Lineaarikuvauksen *ydin* (*kernel*) on $Ax = 0$:n ratkaisujoukko.

Yleisiä lineaarikuvauksia:

- Skaalaus: $A = \begin{pmatrix} s_x & 0 & 0 \\ 0 & s_y & 0 \\ 0 & 0 & s_z \end{pmatrix}$ tai symmetrisessä (uniform) tapauksessa $A = \begin{pmatrix} s & 0 & 0 \\ 0 & s & 0 \\ 0 & 0 & s \end{pmatrix}$

- Kierro (rotaatio): rotaatiomatriisilla \Leftrightarrow ortogonaalisella matriisilla on aina $\det(A) = \pm 1$ ($1 \Rightarrow$ oikeakätinen, $-1 \Rightarrow$ vasenkätinen) ja yksi ominaisarvo $\lambda = 1$. Kyseistä ominaisarvoa vastaava ominaisvektori on rotaatioakseli (koska M :n ominaisvektori = vektori, jonka suunta ei muutu M :llä kerrottaessa). Toisaalta on:

- akseli + kulma: $A(x, \omega) = I + X^\times \sin(\omega) + (X^\times)^2 (1 - \cos(\omega))$, missä $X^\times = \begin{pmatrix} 0 & -x_2 & x_1 \\ x_2 & 0 & -x_0 \\ -x_1 & x_0 & 0 \end{pmatrix}$, kun $|x| = 1$
- kolme akselia: $A(i, j, k) = \begin{pmatrix} i_x & j_x & k_x \\ i_y & j_y & k_y \\ i_z & j_z & k_z \end{pmatrix}$

1.4.2 Affiniteetti (affinikuvaus)

Affiniteetti on kahden tason (\mathbb{R}^2) tai avaruuden (\mathbb{R}^3) välinen kuvaus $x' = A x + b$. Tasot/ava-ruudet, jotka saadaan affiniteetillä toisistaan ovat *affinisia*.

Suunnikkaan pinta-ala tai *yhdensuuntaissärmiön* tilavuus kertoutuvat affinikuvauksessa $\det(A)$:lla.

Projektiivisessä avaruudessa/tasossa affiniteetin voi kuvata matriisikertolaskulla:

$$x = \begin{pmatrix} 1 & x & y & z \end{pmatrix}^T \Rightarrow x' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ b_x & A_{11} & A_{12} & A_{13} \\ b_y & A_{21} & A_{22} & A_{23} \\ b_z & A_{31} & A_{32} & A_{33} \end{pmatrix} x$$

tai

$$x = \begin{pmatrix} x & y & z & 1 \end{pmatrix}^T \Rightarrow x' = \begin{pmatrix} A_{11} & A_{12} & A_{13} & b_x \\ A_{21} & A_{22} & A_{23} & b_y \\ A_{31} & A_{32} & A_{33} & b_z \\ 0 & 0 & 0 & 1 \end{pmatrix} x$$

1.5 Matriisien sekalaisia sovelluksia

1.5.1 Pienimmän neliösumman sovitus (least squares fit)

Jos yritetään sovittaa n -kertoiminen funktio $y(x) = f(x, a_0, \dots, a_n)$ liian moneen havaintoon $x \rightarrow y$ (k kappaletta, $k > n$), saadaan sijoittamalla havainnot x polynomiin *ylimäärätty* yhtälöryhmä:

$$\begin{matrix} A & \cdot & u & = & y \\ k \times n & n \times q & k \times 1 & & k \times 1 \end{matrix}, \text{ missä } A = \text{sijoittamalla saadut kertoimet}, u = (a_0 \dots a_n)^T \text{ ja } y \text{ funktion havaitut}$$

arvot. *Pienimmän neliösumman sovitus*: haetaan A :lle neliömatriisi $M = A^T A$, y :lle pienempi vektori $b = A^T y$ ja ratkaistaan $M u = b$ tavalliseen tapaan.

1.5.2 Markovin ketjut

Markovin ketju (Markov Chain) on joukko tiloja, joiden välisten siirtymien todennäköisyys ei riipu toteutuneesta siirtymä-historiasta. Yksi kätevä esitystapa on *stokastinen matriisi*: neliömatriisi, jossa jokaisen rivin summa on 1. Esim:

Lyhyt mies saa lyhyen pojan todennäköisyydellä 0.75 ja pitkän todennäköisyydellä 0.25. Pitkä taas saa lyhyen todennäköisyydellä 0.1 ja pitkän varmuudella 0.9. Lyhyitä ja pitkiä on aluksi saman verran: $u = (0.5 \ 0.5)$. Stokastinen matriisi $M = \begin{pmatrix} 0.75 & 0.25 \\ 0.1 & 0.9 \end{pmatrix}$. Toisen sukupolven jakauma on $u M = (0.5 \ 0.5) \begin{pmatrix} 0.75 & 0.25 \\ 0.1 & 0.9 \end{pmatrix} = (0.425 \ 0.575)$, kolmannen sukupolven jakauma on $u M^2$ jne.

Stokastisella matriisilla on aina ominaisarvo 1 ja stabiili tila äärettömän monen siirtymän jälkeen voidaan laskea diagonalisoimalla.

2 Differentiaalilaskentaa yleisesti

2.1 Differentiaali

Differentiaali on funktion *linearisaation* (yhden muuttujan funktion tapauksessa tangentin, kahden tapauksessa 3D-tason jne.) kasvun määrä muuttujansa/muuttujiensa muutoksen suhteen. Esim. $dy = f'(x) \Delta x$. Jos $y = x$, saadaan kaavasta $dx = f'(x) \Delta x = 1 \cdot \Delta x$ eli $dx = \Delta x$. Siksi voidaan kirjoittaa $dy = f'(x) dx$. Huom: differentiaalini **ei** välttämättä tarvitse olla pieni, koska kyse on **linearisaation** kasvusta (siis esim. $f'(x) \Delta x$ eikä $f(x + \Delta x)$)!

Kahden muuttujan tapauksessa differentiaali on määritelty osittaisderivaattojen avulla seuraavasti: $df = \frac{\partial f}{\partial x} \Delta x + \frac{\partial f}{\partial y} \Delta y$ eli $df = \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy$ ja samalla tavalla useammille muuttujille.

Differentiointi (vs. derivointi) tarkoittaa differentiaalini (siis esim. $dy = f'(x) dx$) laskemista ja siinä käytetään derivointia (tai osittaisderivointia) ja jos halutaan arvo, eikä kaavaa, x :n muutos $dx (= \Delta x)$. Esim. jos $\Delta x = 0.2, \Delta y = -0.1, f(x, y) = x^2 y$, niin

$$\begin{aligned} df(x, y) &= \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy = (2yx) \Delta x + (x^2) \Delta y \Rightarrow \\ df(1, 3) &= (2 \cdot 3 \cdot 1) \cdot 0.2 + (1^2) \cdot -0.1 = 1.1 \end{aligned}$$

2.2 Jacobian-matriisi

Jacobian-matriisi on usean muuttujan vektoriarvoisen funktion derivaatta eli käytännössä matriisi, joka sisältää funktion tulosvektorin \mathbf{y} jokaisen elementin (m kpl.) derivaatat jokaisen sisääntulevan vektorin \mathbf{x} elementin (n kpl.) suhteen:

$$d\mathbf{y} = D\mathbf{f}(\mathbf{x}) d\mathbf{x}$$

$$\begin{pmatrix} y_0 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} \frac{\partial y_0}{\partial x_0} & \dots & \frac{\partial y_0}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial y_m}{\partial x_0} & \dots & \frac{\partial y_m}{\partial x_n} \end{pmatrix} \begin{pmatrix} dx_0 \\ \vdots \\ dx_n \end{pmatrix}$$

Jacobian-matriisille mm. pätee ketjusääntö $D(\mathbf{f} \circ \mathbf{g})(\mathbf{x}) = \mathbf{f}'(\mathbf{g}(\mathbf{x})) D(\mathbf{g}(\mathbf{x}))$.

Huom! älä sekoita Jacobian-matriisia yhtälöryhmien implisiittisessä derivoinnissa käytettävään Jacobian-determinanttiin $\frac{\partial(F, G)}{\partial(x, y)} = \begin{vmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} \\ \frac{\partial G}{\partial x} & \frac{\partial G}{\partial y} \end{vmatrix} = \begin{vmatrix} F_1 & F_2 \\ G_1 & G_2 \end{vmatrix}$.

2.3 Monen muuttujan ketjusääntö

Yhden muuttujan ketjusäännön $Df(u(x)) = f'(u(x)) u'(x)$ yleistettyjä versioita:

- Jos $z = f(x, y)$ ja x ja y riippuvat molemmat muuttujasta t (eli $x = u(t), y = v(t)$), on:

$$\frac{dz}{dt} = \frac{\partial z}{\partial x} \frac{dx}{dt} + \frac{\partial z}{\partial y} \frac{dy}{dt}$$

- Jos $z = f(x, y)$ ja x, y riippuvat kahdesta muuttujasta s, t (eli $x = u(s, t), y = v(s, t)$), on:

$$\begin{cases} \frac{\partial z}{\partial s} = \frac{\partial z}{\partial x} \frac{\partial x}{\partial s} + \frac{\partial z}{\partial y} \frac{\partial y}{\partial s} \\ \frac{\partial z}{\partial t} = \frac{\partial z}{\partial x} \frac{\partial x}{\partial t} + \frac{\partial z}{\partial y} \frac{\partial y}{\partial t} \end{cases}$$

3 ODEt - "tavalliset" differentiaaliyhtälöt

Tiivistelmä: lineaariselle, 1. asteen ODElle on ratkaisukaava, samoin kuin (vakio kertomiselle) ryhmälle niitä. Muissa tapauksissa Laplace-muunnos on usein kätevin tapa ellei likiarvoratkaisu riitä.

Tässä kappaleessa käytetään vapaana muuttujana välillä x :ää ja välillä t :ta – älä hämäännä. Kirjain t on yleinen käytäntö, koska differentiaaliyhtälöitä käytetään usein ajasta riippuvien ilmiöiden mallintamiseen.

3.1 Peruskäsitteitä

- *Tavallinen differentiaaliyhtälö*: $y = f(x)$ (yhden muuttujan funktio)
- *Kertaluku* (tässä k): $f(x, y, y', y'', y''', \dots, y^{(k)}) = 0$, ts. monenettako derivaattaa funktiosta löytyy
- *Eksplisiittinen ODE*: yhtälö on muodossa $y = \hat{f}(x, y)$ (**eikä** esim. $xy' = 2y$)
- *Osittaisdifferentiaali*: $u = f(x, y)$ on differentiaali yhden muuttujan suhteen (monen muuttujan funktiossa)
- *Yleinen ratkaisu* vs. *erityisratkaisu/erikoisratkaisu* (eng. particular/special solution)
- *Alkuarvo-ongelma*: määritetty y :n ja derivaattojen arvot yhdessä pisteessä
- *Reuna-arvo-ongelma*: määritetty y :n ja derivaattojen arvot kahdessa pisteessä

3.2 Yksittäisen ODE:n tarkka ratkaiseminen

3.2.1 Separoituva: integrointi puolittain

ODE on *separoituva*, jos x ja y ovat erotettavissa eri puolille yhtälöä kohtelemalla differentiaalia dx :n dy :n osamääränä:

$$\frac{dy}{dx} = \frac{f(x)}{g(y)} \Rightarrow \int g(y) dy = \int f(x) dx$$

Kun molemmat puolet on integroitu, ratkaistaan y . Toisinaan vakiofunktio $y(x) = y_0$ tuotta, esim. tapauksessa: $\frac{dy}{dx} = f(x)g(y)$ kun $g(y_0) = 0$. (Huom: separoituva ODE on itse asiassa eksaktin ODE:n erikoistapaus $M_y = 0 = N_x$)

3.2.2 Tasa-asteinen: muuttujan vaihto

ODE on *tasa-asteinen*, jos sen voi saattaa muotoon $y' = f(\frac{x}{y})$, jolloin sen voi ratkaista vaihtamalla $\frac{y}{x}$:n ja y' :n seuraavasti:

$$z(x) = \frac{y(x)}{x} \Leftrightarrow y(x) = x \cdot z(x) \Rightarrow y'(x) = 1 \cdot z(x) + x \cdot z'(x) \text{ eli}$$

$$z = \frac{y}{x} \Rightarrow y' = z + x z'$$

Vaihdon jälkeen yhtälö on separoituva. Ratkaistaan z saadusta yhtälöstä $z + x z' = f(z)$, sijoitetaan takaisin $z = y/x$ ja ratkaistaan y . Huom. triviaaliratkaisu: $z = z_0$, jos $f(z_0) - z_0 = 0$.

3.2.3 Eksakti: osittaisderivointi

ODE on eksakti, jos se on muotoa $M(x, y) dx + N(x, y) dy = 0$ eli $M(x, y) + N(x, y)y' = 0$ eli $\frac{dy}{dx} = -\frac{M(x, y)}{N(x, y)}$ ja on olemassa funktio $f(x, y)$, jolle $\frac{\partial f}{\partial x} = M(x, y) \wedge \frac{\partial f}{\partial y} = N(x, y)$.

Jos M ja N ovat tiedossa, eksaktiuden voi tarkistaa kaavalla $M_y = N_x$ eli $\frac{\partial M}{\partial y} = \frac{\partial N}{\partial x}$ (kyllä, derivaatat "menevät ristiin" aiemman kanssa) ja ratkaista seuraavasti:

$$f(x, y) = \underbrace{\int M(x, y) dx}_{Q(x, y)} + g(y) \quad \Bigg\| \quad g(y) \text{ korvaa integrointivakion}$$

$$N(x, y) = f_y(x, y) = Q_y(x, y) + g'(y) \Rightarrow$$

$$g(y) = \int N(x, y) - Q_y(x, y) dy \quad \Bigg\| \quad \text{muista nyt} + C$$

Lopuksi ratkaistaan y yhtälöstä $f(x, y) = 0$. Ideana on siis soveltaa peräkkäin

$$\frac{\partial f(x, y)}{\partial x} = M(x, y)$$

ja

$$\frac{\partial f(x, y)}{\partial y} = N(x, y)$$

3.2.4 Eksaktiksi muuttaminen: integroiva tekijä

Jos ODE:n voi muuttaa eksaktiksi kertomalla funktiolla $u(x, y)$, on u ODE:n *integroiva tekijä*. Sellaisen voi löytää systemaattisesti jos se riippuu vain joko x :stä tai y :stä:

$$\frac{1}{u(x)} du = \frac{M_y - N_x}{N} dx$$

tai

$$\frac{1}{u(y)} du = \frac{N_x - M_y}{M} dy$$

Sekä y :stä että x :stä riippuvia tekijöitäkin voi olla, mutta niitä ei tällä kaavalla löydä.

3.2.5 1. kertaluvun lineaarinen ODE: yleinen ratkaisu

- Homogeeninen ($y' + p(x) \cdot y = 0$, ts. ei y :stä riippumattomia termejä) separoituu. Yleinen ratkaisu: $y = C e^{-\int p(x) dx}$ ja vakiokertoimiselle ($y' + a y = 0$): $y = C e^{-ax}$, missä C on mielivaltainen vakio (integrointivakio). Johto:

$$\begin{aligned} \frac{dy}{dx} + p(x) \cdot y &= 0 \Leftrightarrow \\ \frac{1}{y} dy &= -p(x) dx \Rightarrow \\ \int \frac{1}{y} dy &= -\int p(x) dx \Rightarrow \\ \ln|y| &= -P(x) + \hat{C} \Rightarrow \\ y &= e^{-P(x) + \hat{C}} = e^{\hat{C}} e^{-P(x)} = C e^{-P(x)} \end{aligned}$$

- Homogeenisen (mutta **ei** epähomogeenisen) ODEn erikoisratkaisujen lineaarikombinaatio on myös ratkaisu \Rightarrow yleinen ratkaisu on $y = c_1 y_1 + c_2 y_2$. Sanotaan, että (y_1, y_2) on *ratkaisun kanta* kun $\{y_n\}$ ovat lineaarisesti riippumattomia. *Funktioiden lineaarinen riippumattomuus* selviää, kun lasketaan *Wronskian-determinantti* (esimerkin vuoksi kolmella funktiolla): $\begin{vmatrix} u & v & w \\ u' & v' & w' \\ u'' & v'' & w'' \end{vmatrix}$, joka on 0 joss funktiot ovat lineaarisesti riippuvia.
- Ei-homogeeniselle ($y' = p(x) \cdot y + q(x)$) on aina integroiva tekijä: $e^{\int p(x) dx}$. Jos $p(x) = a$ eli vakio, on yleinen ratkaisu $y(x) = e^{ax} \int e^{-ax} q(x) dt + c e^{ax}$.

3.3 Yksittäisen yhtälön likiarvoratkaisut

3.3.1 Suuntakenttä - erikoisratkaisu graafisesti

Valitaan sopiva ruudukollinen $(x, y) \in \mathbb{R}$, ratkaistaan ODEsta kullekin ruudukon pisteelle $y' = f(x, y)$ ja piirretään vastaava nuoli tai viiva. Alkuarvo-ongelman ratkaisun voi hahmotella seuraamalla kenttää alkuarvopisteestä. Tietokoneella voi käyttää tämän (huonon) ns. Eulerin menetelmän sijaan vaikkapa 4. asteen Runge-Kuttaa.

Isocline (tasa-arvokäyrä) on jokin y' :n suhteen vakioarvoinen käyrä suuntakentällä (esim. ns. *nullcline* eli käyrä $y' = 0$).

3.3.2 Picardin iteraatio - approksimoiva algebrallinen erikoisratkaisu

Picardin iteraatiolla saadaan tarkentuva approksimaatio alkuarvo-ongelman $y'(x) = f(x, y(x))$, $y'(x_0) = y_0$ ratkaisulle

$$\begin{aligned}\phi_0(x) &= y_0 \\ \phi_{n+1}(x) &= \phi_0 + \int_{x_0}^x f(t, \phi_n(t)) dt\end{aligned}$$

...eli joka askeleella integroidaan välillä $x_0 \dots x$ funktiolle $f(x, y)$, missä x on korvattu t :llä ja y edellisen iteraation tuloksella.

Ratkaisun olemassaolon testaus suljetulla välillä eli *Picardin lause*: jos $y' = f(x, y)$ on jatkuva laatikon $|x - x_0| \leq a \wedge |y - y_0| \leq b$ sisällä, iteraatio suppenee yksikäsitteiseen ratkaisuun välillä $|x - x_0| \leq \min \{a, b/M\}$.

3.4 2. asteen ODE

Muotoa $f(y'', y', x) = 0$ oleva ODE ratkeaa muuttujaa vaihtamalla: $u(x) = y(x)'$. Korkeamman asteen ODE:n voi tällä tavalla muuttaa ensimmäisen asteen ODE-ryhmäksi jonka voi sitten ratkaista vaikka Laplace-muunnoksella tai ominaisarvojen avulla. Esim:

$$a y''' + b y'' + c y' + d y + e = 0 \parallel y = y(x) \Rightarrow \begin{cases} y' = y_1 \\ y_1' = y_2 \\ y_2' = y_3 \\ a y_3' = -b y_2 - c y_1 - d y - e \end{cases}$$

Toisen asteen homogeenisessa tapauksessa: $a y'' + b y' + c y = 0 \Rightarrow \begin{pmatrix} u \\ v \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ -c/a & -b/a \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$.

3.5 1. asteen lineaarinen homogeeninen ODE-ryhmä

Ryhmä voidaan esittää matriisimuodossa:

$$\mathbf{y}' = A \mathbf{y} \equiv \begin{pmatrix} y_1' \\ y_2' \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

Matriisin e^{At} sarakkeet ovat ryhmän erikoisratkaisuja ja kun \mathbf{y}_0 on vektorillinen alkuarvoja, $\mathbf{y} = \mathbf{y}_0 e^{At}$ on alkuarvo-ongelman ratkaisu. Yleinen ratkaisu saadaan myös suoraan ominaisarvoista ja -vektoreista jos ne ovat erillisiä (ei-moninkertaisia) tai A on symmetrinen:

$$\mathbf{y}(t) = c_1 \mathbf{x}_1 e^{\lambda_1 t} + c_2 \mathbf{x}_2 e^{\lambda_2 t} + \dots + c_n \mathbf{x}_n e^{\lambda_n t}$$

...missä c_n ovat mielivaltaisia vakioita, λ_n matriisin A ominaisarvoja ja \mathbf{x}_n niitä vastaavia ominaisvektoreita. Kaksinkertaisen ominaisarvon tapauksessa toinen ratkaisu saadaan kaavalla $\mathbf{y}_2(t) = t \mathbf{x}_1 + \mathbf{c} e^{\mu t}$, missä $(A - \mu I) \mathbf{c} = \mathbf{x}_1$ ja $\mu = \lambda_1$. (**Epäselvä:** onko varmasti $\mu = \lambda_1$?)

Epähomogeenisessa tapauksessa $\mathbf{y}(t)' = A \mathbf{y}(t) + \mathbf{f}(t)$ ja erikoisratkaisun saa kaavalla $\mathbf{y}_p = e^{At} \int e^{-At} \mathbf{f}(t) dt$. (**Epäselvä:** saako yleisen ratkaisun lisäämällä $\mathbf{c} e^{At}$ ja mikä silloin on \mathbf{c} ?) Yleisen saa (muun muassa) *ODE:n diagonalisointimenetelmällä*: ratkaistaan ensin uuden yhtälöryhmän, $\mathbf{z}' = \Lambda \mathbf{z} + \mathbf{g}$ (Λ on A :n diagonalisoitu versio eli ominaisarvomatriisi ja $\mathbf{g} = X^{-1} \mathbf{f}$, missä X on vastaavista ominaispystyvektoreista koottu matriisi), diagonalisoinnin ansiosta nyt toisistaan riippumattomat, yhtälöt yksittäisen yhtälön ratkaisukaavalla $z_i(x) = e^{\lambda_i x} \int e^{-\lambda_i x} g_i(x) dt + c_i e^{\lambda_i x}$ (tai vaikka Laplace-muunnoksella) ja sitten ”epädiagonalisoidaan” tulos: $\mathbf{y} = X \mathbf{z}$.

3.5.1 Vaihekuvaaja

Kahden muuttujan lineaariselle 1. asteen ODE-ryhmälle voidaan piirtää kaksiulotteinen *vaihekuvaaja*, jossa on parvi erikoisratkaisukäyriä: $\begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix}$. Kohtia, joissa $y_1' = 0$, $y_2' = 0$ sanotaan *tasapainopisteiksi* (myös: *kriittinen piste*). Homogeenisessä tapauksessa piste on aina $(0, 0)$. Tasapainopisteiden luokittelu riippuu A :n ominaisarvoista:

- Piste on *stabiili* jos molempien reaalinen osa on ≤ 0 , muuten *epästabiili*. Jos ne reaaliosat on nolla, piste on *attraktiivisesti stabiili* (piste on napa tai spiraali ja lähistön ratkaisut päätyvät siihen) ja muuten *orbitaalisesti stabiili* (lähistön ratkaisut pysyvät pisteen lähellä kun $t \rightarrow \infty$).

- Lähiympäristön käytöksestä voidaan sanoa enemmänkin: reaaliset ja samanmerkkiset \Rightarrow napa (stabiili \Rightarrow sisäänpäin tai epästabiili \Rightarrow ulospäin), reaaliset ja erimerkkiset \Rightarrow satulapiste (kaksi käyrää sisään, kaksi ulos, muut "hipovat"), $\text{Re}(\lambda_1) = \text{Re}(\lambda_2) = 0 \Rightarrow$ keskus (soikion tai ympyrän) ja $\lambda_1 = \lambda_2 = 0 \Rightarrow$ spiraali (sisään tai ulos).

ODEn *linearisointi* mahdollistaa myös epälineaarisen ODEn tasapainopisteiden luokittelun: yhtälöiden $x' = F(x, y)$, $y' = G(x, y)$ tasapainopiste $F(a, b) = G(a, b) = 0$ luokitellaan matriisin $\begin{pmatrix} F_x(a, b) & F_y(a, b) \\ G_x(a, b) & G_y(a, b) \end{pmatrix}$ mukaan em. tavalla paitsi, että 1) ympyräpisteet voivat olla myös spiraaleja ja 2) tapaus $\text{Im}(\lambda_1) = \text{Im}(\lambda_2) = 0 \wedge \lambda_1 = \lambda_2$ voi olla joko spiraali tai napa.

3.6 Laplace-muunnos

Laplace-muunnoksessa differentiaaliyhtälö (tai -ryhmä) muunnetaan ensin *aika-alueesta s-tasoon* (kirjoitetaan: $\mathcal{L}(f(t)) = F(s)$), ratkaistaan sitten saadusta yhtälöstä F ja tehdään lopuksi käänteismuunnos (kirj. $\mathcal{L}^{-1}(F(s)) = f(t)$). Usein käänteismuunnosta varten tarvitaan osamurtokehitelmää. Tulos pätee (tässä annetulla määritelmällä) vain alueella $t \geq 0$! Alla muutamia tärkeimpiä muunnoksia:

$f(t)$	$\iff F(s) = \mathcal{L}(f(t)) = \int_0^\infty e^{-st} f(t) dt$	\mathcal{L} :n määritelmä
$f + g$	$\iff F + G$	
αf	$\iff \alpha F$	
$f'(t)$	$\iff sF - f(0)$	Derivointi
$f''(t)$	$\iff s^2 F - s f(0) - f'(0)$	2. derivaatta
$\int_0^t f(t) dt$	$\iff \frac{1}{s} F$	Määrätty integraali
$t f(t)$	$\iff -F'$	Derivointi taajuusalueessa
$f(\alpha t)$	$\iff \frac{1}{\alpha} F(s/\alpha)$	t:n skaalaus
$f g$	$\iff F * G$	Konvoluutio, $\int_0^t f(t-z) g(z) dz$
$f * g$	$\iff FG$	Konvoluutiolause toiseen suuntaan
$\delta(t)$	$\iff 1$	Diracin delta"funktio", $\int_{-\epsilon}^\epsilon \delta(t) dt = 1$
$u(t) \hat{=} 1$	$\iff \frac{1}{s}$	Heavisiden askelfunktio (1, kun $t \geq 0$)
$e^{at} f(t)$	$\iff F(s-a)$	Siirto taajuusalueessa
$u(t-a) f(t-a)$	$\iff e^{-as} F(s)$	Aikasiirto, huomaa $u!$
t	$\iff \frac{1}{s^2}$	
$\frac{1}{n!} t^n$	$\iff \frac{1}{s^{n+1}}$	huom: $n \geq 0$
e^{at}	$\iff \frac{1}{s-a}$	
$\sin(\omega t)$	$\iff \frac{\omega}{s^2 + \omega^2} = \frac{1}{2} \left(\frac{1}{s-i\omega} + \frac{1}{s+i\omega} \right)$	
$\cos(\omega t)$	$\iff \frac{s}{s^2 + \omega^2} = \frac{1}{2} i \left(\frac{1}{s-i\omega} + \frac{1}{s+i\omega} \right)$	

Esimerkki: ratkaistaan yksinkertainen epähomogeeninen ODE:

$$\begin{aligned}
 y(t)' &= 2y(t) + 1, \text{ kun } y(0) = 3 \\
 sY - 3 &= 2Y + \frac{1}{s} \\
 (s-2)Y &= \frac{1}{s} + 3 \\
 Y &= \frac{1}{s(s-2)} + \frac{3}{s-2} \\
 &= \frac{-1/2}{s} + \frac{1/2+3}{s-2} \Bigg\| = \text{osamurtokeh. Heavisiden menet.} \\
 \Rightarrow y(t) &= -\frac{1}{2}t + \frac{7}{2}e^{2t} \Bigg\| \text{ huom: } t \geq 0!
 \end{aligned}$$

4 Sarjat

- Luku**jono** *suppenee*, jos sillä on raja-arvo äärettömydessä, muuten *hajaantuu*. Vaihtoehtoinen määritelmä: suppenee, jos on $|y| < \epsilon$, missä ϵ voidaan valita mielivaltaisen pieneksi, ja aina löytyy $f(n)$ sen sisältä.
- *Sarja* on äärettömän lukujonon summa. Se *suppenee*, jos sen osasumista muodostettu jono suppenee. Tällöin $\lim_{n \rightarrow \infty} a_n = 0$.
- Eikö luku ei kasva äärettömäksi äärettömällä summauksella vaikka summattava pieneniikin? Vastaus: ei, koska esim. $a_n = \frac{3}{10^n}: 0.3 + 0.03 + 0.003 + \dots = 0.333\dots$
- Äärettömät sarjat ovat usein ratkaisuja differentiaaliyhtälöihin, joita ei voi muuten esittää alkeisfunktioilla.

Koska sarja voidaan tulkita jonon osasummasarjan raja-arvoksi äärettömydessä, saadaan raja-arvon laskusäännöistä (kun $\sum a_n = A$ ja $\sum b_n = B$):

- $\sum c a_n = c A$
- $\sum (a_n \pm b_n) = A \pm B$
- Jos $a_n \leq b_n$ kaikille n , niin $A \leq B$

4.1 Suppenemisen testaus

Suppenemista voi testata helpommin kuin laskea summan, ja positiivis-termisen sarjan suppeneminen on helpompi laskea kuin vaihtelevatermisen. Jos $a_n > 0$:

Integraalitest. $\sum a_n$ suppenee joss $\int_N^\infty a(x) dx$ suppenee. (N voidaan valita mielivaltaisesti, koska suppeneminen ei koskaan riipu jonon alusta.)

Osamäärätesti. $r_a = \lim_{n \rightarrow \infty} \frac{a_{n+1}}{a_n}$, eli perättäisten termien osamäärä

n:s juuri-testi. $r_b = \lim_{n \rightarrow \infty} (a_n)^{\frac{1}{n}}$, eli alkion äärettömäs juuri äärettömässä

Molemmille sarja suppenee, jos $r < 1$, saattaa hajaantua, jos $r = 1$ ja hajaantuu varmasti, jos $r = 1$. Luku r_b on olemassa useammin kuin r_a , mutta kun molemmat ovat olemassa, on $r_a = r_b$.

Jos taas summassa on sekä positiivisia että negatiivisia termejä, se suppenee *ainakin* jos $\sum |a_n|$ suppenee (suppenee *absoluuttisesti*), ja toisinaan muulloinkin (suppenee *ehdollisesti*). Eriytyisesti: $\sum (-1)^n a_n$ (eli joka toinen termi negatiivinen) suppenee, jos $\lim_{n \rightarrow \infty} a_n = 0$ ja $a_n \leq a_{n+1}$ (*Leibnizin lause*).

4.2 Yleisimpiä sarjoja

Aritmeettinen sarja. $\sum a_1 + (n-1)d$ (ts. $a_n = a_{n-1} + d$). Perättäisten termien erotus on vakio. Hajaantuu aina, mutta osasumma on $n \frac{a_1 + a_n}{2}$.

Geometrinen sarja. $\sum a r^{n-1}$. Perättäisten termien osamäärä on vakio.

Suppenee arvoon $\frac{a}{1-r}$, kun $|r| < 1$. Osasumma $\frac{a(1-r^n)}{1-r}$.

p-sarja. $\sum \frac{1}{n^p}$. Suppenee, kun $p > 1$ ja hajaantuu muuten. Huomaa erityisesti, että $p = 1$ eli *harmoninen sarja* ($\frac{1}{1} + \frac{1}{2} + \frac{1}{3} \dots$), hajaantuu (vaikkakin hitaasti). Summan *yleistä* kaavaa ei ole, mutta $\sum \frac{1}{n^2} = \frac{\pi^2}{6}$.

4.3 Potenssisarjat

Potenssisarja on muotoa $P(x) = \sum_{n=0}^{\infty} a_n (x-c)^n$, missä c on sarjan *suppenemiskeskus*.

Potenssisarja suppenee aina ja vain suppenemiskeskuksensa ympäristössä säteellä R ($\in [0, \infty[$), missä $R = \frac{1}{L}$, $L = \lim_{n \rightarrow \infty} \left| \frac{a_{n+1}}{a_n} \right|$ (kts. ”osamäärätesti” ylempää). Päätepisteet voivat joko kuulua tai olla kuulumatta R :n määräämään *suppenemisintervalliin*.

Yhteenlaskettujen potenssisarjojen suppenemissäde on $R \geq \min \{R_a, R_b\}$. Sama pätee myös keskenään kerrotuille potenssisarjoille (*Cauchyn tulo*):

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} c_n x^n \quad \left\| \quad c_n = \sum_{i=0}^n a_i b_{n-i} \right.$$

Huom: *Taylorin sarja* on potenssisarja, jolle $a_n = \frac{f^{(n)}(c)}{n!}$.

Erityisen tärkeä (geometrinen/Taylorin/McLaurinin) potenssisarja on:

$$\frac{1}{1-x} = 1 + x + x^2 + \dots x^n, |x| \leq 1$$

4.4 Fourier-sarjat

- Määritelmä: $2L$ -jaksoisen funktion Fourier-sarja (alueella $[-L, L]$) on:

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} \left(a_n \cos \frac{n\pi x}{L} + b_n \sin \frac{n\pi x}{L} \right)$$

$$a_n = \frac{1}{L} \int_{-L}^L f(x) \cos \left(\frac{n\pi x}{L} \right) dx \quad \left\| \quad n = 0, 1, 2, \dots \right.$$

$$b_n = \frac{1}{L} \int_{-L}^L f(x) \sin \left(\frac{n\pi x}{L} \right) dx \quad \left\| \quad n = 1, 2, \dots \right.$$

...tai kompleksimuodossa lyhyemmin:

$$f(x) = \sum_{n=-\infty}^{\infty} c_n e^{i\pi n x/L}$$

$$c_n = \frac{1}{2L} \int_{-L}^L f(x) e^{-i\pi n x/L} dx$$

- Jos $f(x)$ on *parillinen funktio* (eli $f(-x) = f(x)$), $b_n = 0$ aina ja sarja supistuu ”*fourier-kosinisarjaksi*”: $f(x) = a_0 + \sum_{n=1}^{\infty} a_n \cos \frac{n\pi x}{L}$
- Jos $f(x)$ on *pariton funktio* (eli $f(-x) = -f(x)$), $a_n = 0$ aina ja sarja supistuu ”*fourier-sinisarjaksi*”: $f(x) = \sum_{n=1}^{\infty} b_n \sin \frac{n\pi x}{L}$. (Huom: parittomuuden seuraus: $f(0) = 0$)
- Kertoimien skaalaaminen vakiolla vasta $f(x)$:n skaalaamista

5 Monen muuttujan analyysi

5.1 Avaruuspinta

Kahdella muuttujalla parametrisoitu avaruuspinta:

$$\mathbf{p}(u, v) = \begin{pmatrix} x(u, v) \\ y(u, v) \\ z(u, v) \end{pmatrix}$$

Normaali:

$$\mathbf{n}(u, v) = \frac{\partial(y, z)}{\partial(u, v)} \mathbf{i} + \frac{\partial(z, x)}{\partial(u, v)} \mathbf{j} + \frac{\partial(x, y)}{\partial(u, v)} \mathbf{k}$$

$$\frac{\partial(x, y)}{\partial(u, v)} = \begin{vmatrix} \frac{\partial x}{\partial u} & \frac{\partial x}{\partial v} \\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v} \end{vmatrix} \quad (= \text{Jacobian})$$

Pinta-ala lasketaan seuraavasti:

$$A = \int_{v_0}^{v_1} \int_{u_0}^{u_1} dA(u, v),$$

$$dA(u, v) = |\mathbf{n}(u, v)| du dv$$

5.2 Raja-arvo

- Monen muuttujan funktion raja-arvo määritellään n -ulotteisen, rajatta pienenevän pallon avulla
- Yleinen raja-arvo on olemassa vain, jos se on *sama lähestymissuunnasta riippumatta*. Esim. funktiolle $\frac{2xy}{x^2+y^2}$, $\lim_{(x,y) \rightarrow (0,0)} = 0$ x -akselia ja y -akselia pitkin lähestyessä, mutta 1 suoraa $x = y$ pitkin lähestyessä, sillä $f(x, 0) = f(0, y) = 0$, mutta $f(x, x) = 1$.
- Raja-arvo voi myös olla olemassa kaikkia suoria $y = kx$ pitkinä lähestyessä, mutta **ei** muita käyriä pitkin. Esim. $f(x, y) = \frac{2x^2y}{x^4+y^2} \Rightarrow \lim_{(x,y) \rightarrow (0,0)} f(x, kx) \rightarrow 0$, mutta $f(x, x^2) = 1$.
- Funktio on jatkuva tietyssä pisteessä joss raja-arvo on siinä sama kuin funktion arvo. Funktiosta voi siksi *tehdä jatkuvan* määrittelemällä arvo epäjatkuvassa pisteessä sopivasti, joss raja-arvo on olemassa.
- Määritelmä: raja-arvo pisteessä (a, b) on olemassa, joss **MITÄ???**

5.3 Monen muuttujan funktion differentiaalit

5.3.1 Osittaisderivaatta

- Osittaisderivaatta on derivaatta jonkin muuttujan suhteen ja sitä merkitään "doo":lla, esim. $\frac{\partial f(x, y)}{\partial x}$.
- *Korkeamman kertaluvun osittaisderivaatat* voivat olla myös ns. sekaderivaattoja, esim. $f_{21} = f_{yx} = \frac{\partial}{\partial x} \cdot \frac{\partial f(x, y)}{\partial y} = \frac{\partial^2 f}{\partial x \partial y}$ on f derivoituna ensin y :n ja sitten x :n suhteen.
- **Jos** itse funktio ja sen alemman kertaluvun osittaisderivaatat ovat jatkuvia tietyssä pisteessä, eri järjestyksessä otetut sekaderivaatat ovat samoja. Epäjatkuvassa tapauksessa näin ei ole.

5.3.2 Gradientti ja suunnattu derivaatta

N :n muuttujan funktion *gradientti* on n -ulotteinen vektori, joka on koottu funktion osittaisderivaatioista. Gradienttia merkitään nabla- eli del-symbolilla:

$$\nabla f(x, y, z) = \frac{\partial f}{\partial x} \mathbf{i} + \frac{\partial f}{\partial y} \mathbf{j} + \frac{\partial f}{\partial z} \mathbf{k}$$

- Funktio kasvaa aina nopeiten gradienttinsa suuntaan. Derivaatta k.o. suuntaan on $|\nabla f|$.

- Gradienttivektori on aina tasokäyrän normaali (vrt. kukkula, jonka huipulta valuu vettä)
- Funktion derivaatta (kasvunopeus) mielivaltaiseen suuntaan \mathbf{u} on $D_{\mathbf{u}}f(a, b) = \mathbf{u} \cdot \nabla f(x, y)$
- Liikkuvan tarkkailijan kokema kasvunopeus (nopeus \mathbf{v} ei välttämättä yksikkövektori!) on samoin $D_{\mathbf{v}}f(a, b) = \mathbf{v} \cdot \nabla f(x, y)$

5.4 Napakoordinaatisto

Kahden muuttujan funktioiden tasa-arvokäyriä voi toisinaan esittää kätevästi napakoordinaateilla. Muunnokset karteesisten ja napakoordinaattien välillä sujuvat seuraavilla kaavoilla:

$$\begin{aligned} r^2 &= x^2 + y^2 & \varphi &= \tan^{-1} \frac{y}{x} \\ x &= r \cos \varphi & y &= r \sin \varphi \end{aligned}$$

5.5 Monen muuttujan ääriarvot

5.5.1 Ääriarvopisteiden luokittelu (Hessian)

Ääriarvopisteitä voivat myös monen muuttujan tapauksessa olla derivaatan (gradientin) nollakohdat ($\nabla f = \mathbf{0}$) tai reunapisteet. Yhden muuttujan tapauksessa *kriittisen pisteen* tyyppin voi määrittellä toisesta derivaatasta:

- $f''(x) < 0 \Rightarrow$ maksimi
- $f''(x) > 0 \Rightarrow$ minimi
- $f''(x) = 0 \Rightarrow$ ei tietoa (jos vaihtaa merkkiä x :n kohdalla \Rightarrow satulapiste)

Monen muuttujan tapauksessa luokittelu hoituu kyseisessä pisteessä lasketun *Hessian*-matriisin ominaisarvojen ($\det(A - \lambda I) = 0$) avulla:

$$\mathbf{H} = \begin{pmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{pmatrix}$$

- kaikki $\lambda_k \leq 0 \Rightarrow$ maksimi
- kaikki $\lambda_k \geq 0 \Rightarrow$ minimi
- osa λ_k positiivisia, osa negatiivisia \Rightarrow ei tietoa

5.5.2 Rajoitetut ääriarvot (Lagrange-kertoimet)

Jos ääriarvot tehtävässä vastauksiksi kelpaa vain osa kriittisistä pisteistä, voidaan tehtävä ratkaista muotoilemalla rajoitusfunktio $g(\mathbf{x}) = 0$ ja minimoimalla/maksimoimalla alkuperäisen sijaan *Lagrangen funktio*...

$$L(\mathbf{x}, \lambda) = f(\mathbf{x}) + \lambda g(\mathbf{x})$$

...missä $\lambda \in \mathbb{R}$ on nimeltään *Lagrangen kerroin*. Jos rajoituksia on enemmän, myös kertoimia ja rajoitusfunktioita voidaan ottaa mukaan enemmän. Esim:

$$L(x, y, z, \lambda, \mu) = f(x, y, z) + \lambda g(x, y, z) + \mu h(x, y, z)$$

6 Skalaari- ja vektorikentät

- *skalaarikenttä* on $f(x, y, \dots) \in \mathbb{R}$ ja *vektorikenttä* on $f(x, y, \dots) \in \mathbb{R}^n$.
- Skalaarikenttä S on vektorikentän V *potentiaali*, joss $\nabla S = V$ kaikissa pisteissä. (On ilmeisesti olemassa myös kaikille kentille määritelty *vektoripotentiaali* \mathbf{G} , jolle $\mathbf{F} = \nabla \times \mathbf{G}$. Käyttötavasta ei käsitystä.)

- Vektorikenttä (tai esim. voima) on *konservatiivinen*, jos sillä on potentiaalienttä (kai-killalla vektorikentällä ei ole). Integraalin tapaan potentiaali ei ole yksikäsitteinen, vaan siihen voi lisätä mielivaltaisen vakion. Konservatiiviselle vektorikentälle $\mathbf{F}(x, y, z) = F_a(x, y, z)\mathbf{i} + F_b(x, y, z)\mathbf{j} + F_c(x, y, z)\mathbf{k}$ pätee:

$$2D : \frac{\partial}{\partial y} F_a(x, y) = \frac{\partial}{\partial x} F_b(x, y)$$

$$3D : \begin{cases} \frac{\partial}{\partial y} F_a(x, y) = \frac{\partial}{\partial x} F_b(x, y) \\ \frac{\partial}{\partial z} F_a(x, y) = \frac{\partial}{\partial x} F_c(x, y) \\ \frac{\partial}{\partial z} F_b(x, y) = \frac{\partial}{\partial y} F_c(x, y) \end{cases}$$

Tai toisaalta: F on konservatiivinen $\Leftrightarrow \text{curl}(F) = 0$. Jos kenttä on konservatiivinen, potentiaalin voi laskea seuraavasti:

$$U(x, y, z) = \int_a^x f(t, b, c) dt + \int_b^y f(x, t, c) dt + \int_c^z f(x, y, t) dt$$

(lopuksi ilmeisesti voi merkitä $a = b = c = 0$ ja lisätä integrointivakion C)

- *Vuo (Flux)* on vektorikentän vektoreiden ja käyrän (2D) tai pinnan (3D) normaalin pistetulon summa (ts. paljonko vektoreita “virtaa” käyrän/pinnan läpi sen suuntaisesti). $\text{Flux}_{2D} = \int_C \mathbf{F} \cdot \mathbf{N} ds$ ja $\text{Flux}_{3D} = \int_A \mathbf{F} \cdot \mathbf{N} dA$.

6.1 Viivaintegraali

Viivaintegraali on viivan differentiaalisten tangenttivektoreiden ($d\mathbf{r}$) ja kentän tulon summa. Skalaarikentän tapauksessa tulo $S(x, y)d\mathbf{R}$ ja vektorikentän tapauksessa $\mathbf{F}(x, y) \cdot d\mathbf{R}$.

Viivaintegraali lasketaan parametrisoimalla \mathbf{r} :n x , y -komponentin, derivoimalla ne t :n suhteen, ottamalla tulo (piste- tai skalaari) ja integroimalla. Esim:

$$\begin{aligned} x(t) &= t^2 \\ y(t) &= 4t \\ t &\in [-2, 7] \\ \mathbf{r}(t) &= t^2\mathbf{i} + 4t\mathbf{j} \Rightarrow \\ d\mathbf{r} &= 2t\mathbf{i} + 4\mathbf{j} dt \\ \mathbf{F}(x, y) &= 5x\mathbf{i} + 3y^2\mathbf{j} \Rightarrow \\ \mathbf{F}(t) &= 5t^2\mathbf{i} + 3(4t)^2\mathbf{j} \Rightarrow \\ \mathbf{F} \cdot d\mathbf{r} &= 10t^3 + 48t^2 dt \\ \int_C \mathbf{F} \cdot d\mathbf{r} &= \int_{-2}^7 10t^3 + 48t^2 dt = \frac{23157}{2} \end{aligned}$$

Joskus vektorikentän yli viivaintegraalia merkitään $\int_C F_a(x, y) dx + F_b(x, y) dy$, mikä tarkoittaa samaa kuin $\mathbf{F} = F_a\mathbf{i} + F_b\mathbf{j} \Rightarrow \int_C \mathbf{F} \cdot d\mathbf{r}$ ja se lasketaan samalla tavalla parametrisoitua \mathbf{r} :n ja \mathbf{F} :n pistetulona kuin yllä.

Tyypillinen esimerkki viivaintegraalista vektorikentän yli on fysikaalinen *työ*, jonka voima \mathbf{F} tekee kuljettaessaan pistemäistä kappaletta käyrää C pitkin.

6.1.1 Greenin lause (suljetun käyrän viivaintegraali)

Tasolla suljetun käyrän viivaintegraalin voi joskus laskea helpommin seuraavasti:

$$\oint_C F_a(x, y) dx + F_b(x, y) dy = \iint_R \left(\frac{\partial F_b}{\partial x} - \frac{\partial F_a}{\partial y} \right) dA$$

...missä R on käyrän C sisään jäävä alue ja C käydään läpi vastapäivään. Oikea puoli on siis pinta-integraali, jossa lasketaan ensin vaakasuuntainen integraali ja sitten pystysuuntainen (tai päinvastoin). Jos R on reikäinen, lasketaan reikien seintän mukaan, mutta myötäpäivään.

6.1.2 Stokesin lause (moniulotteiset pinnat)

Stokesin lause on Greenin lauseen laajennus moniulotteisille pinnoille:

$$\oint_C \mathbf{F} \bullet d\mathbf{r} = \iint_S \text{curl } \mathbf{F} \bullet \hat{\mathbf{N}} \, dS$$

6.2 ”Vektoriderivaatat” - grad, div, curl

Kentille voidaan määritellä kolme eri ”derivaattaa”, joista jokainen on eri kerto-operaattorin ja *nabla*-operaattorin ”formaali tulo”:

- *Gradientti* on vektorikenttä, joka osoittaa skalaarikentän nopeimman kasvun suunnan (kasvunopeus on k.o. vektorin pituus):

$$\nabla f(x, y, z) = \left(\frac{\partial}{\partial x} \mathbf{i} + \frac{\partial}{\partial y} \mathbf{j} + \frac{\partial}{\partial z} \mathbf{k} \right) f(x, y, z) = \frac{\partial f}{\partial x} \mathbf{i} + \frac{\partial f}{\partial y} \mathbf{j} + \frac{\partial f}{\partial z} \mathbf{k}$$

- *Divergenssi* on skalaarikenttä, joka kertoo kuinka paljon toinen vektorikenttä ”etäännyy pisteestä p ” eli tarkemmin sanottuna vuo äärettömän pienen p -keskisen pallon (tasossa kiekon) sisältä:

$$\text{div } \mathbf{F} = \nabla \bullet \mathbf{F} = \frac{\partial F_a}{\partial x} + \frac{\partial F_b}{\partial y} + \frac{\partial F_c}{\partial z}$$

Divergenssin voi siis myös tulkita *lähteen* (esim. pistevarausten tapauksessa Diracin delta-funktio tai jatkavassa tapauksessa varaustiheys) voimakkuudeksi yksikkötilavuutta kohti.

- *Curl* (karmeasti suomennettuna *roottori*) on vektorikenttä, joka kertoo kuinka paljon kenttä ”pyörii pisteen p ympäri” eli tarkemmin sanottuna kiekon reunan muodostavien äärettömän monen tangenttivektorin ($d\mathbf{r}$) ja vektorikentän vektorien pistetulo kerrottuna kiekon (C) yksikkönormaalilla ($\hat{\mathbf{N}}$):

$$\hat{\mathbf{N}} \bullet \text{curl } \mathbf{F} = \oint_C \mathbf{F} \bullet d\mathbf{r}$$

$$3D : \text{curl } \mathbf{F} = \nabla \times \mathbf{F} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ \frac{\partial}{\partial x} & \frac{\partial}{\partial y} & \frac{\partial}{\partial z} \\ F_a & F_b & F_c \end{vmatrix}$$

$$2D : \text{curl } \mathbf{F} = \left(\frac{\partial F_b}{\partial x} - \frac{\partial F_a}{\partial y} \right) \mathbf{k}$$

Näille pätee kaikenlaisia yhtälöitä, mm.:

- $\text{div curl} = 0$ eli $\nabla \bullet (\nabla \times \mathbf{F}) = 0$
- $\text{curl grad} = \mathbf{0}$ eli $\nabla \times (\nabla S) = \mathbf{0}$
- ns. *laplacian*: $\nabla^2 S = \text{div grad } S = \nabla \bullet \nabla S$ tai vektorikentälle: $\nabla^2 \mathbf{F} = (\nabla^2 F_a) \mathbf{i} + (\nabla^2 F_b) \mathbf{j} + (\nabla^2 F_c) \mathbf{k}$. Skalaarikenttä on *harmoninen* jollain alueella, jossa siellä pätee *laplace-yhtälö* $\nabla^2 S = 0$.

6.3 Divergenssilause (aka. Gaussin laki)

Vuo jonkin alueen D pinnan S läpi on yhtä suuri kuin kaikkien sen pisteiden divergenssien summa (=tilavuusintegraali):

$$\int_D \text{div } \mathbf{F} \, dV = \oint_S \mathbf{F} \bullet \hat{\mathbf{N}} \, dS$$

Erityisesti: jos suljetun pinnan sisällä ei ole yhtään lähdeettä (positiivista tai negatiivista, *source* tai *sink*), on *kokonaisvuo* sen läpi 0 kentästä riippumatta (mikä tulee sisään, menee myös ulos). Huomaa, että esim. pistevarausten tapauksessa lähteet ovat pistemäisiä Diracin delta-funktioita, joiden integraalilla on arvo vaikka niitä ympäröivä kiekko pienennettäisiin kuinka pieneksi tahansa.

Variaatioita ("curl-lause" ja "gradienttilause"?), joiden tulos on vektori:

$$\int_D \operatorname{curl} \mathbf{F} \, dV = - \oint_S \mathbf{F} \times \hat{\mathbf{N}} \, dS$$
$$\int_D \operatorname{grad} S \, dV = \oint_S S \hat{\mathbf{N}} \, dS$$

7 Kompleksiluvut

- Imaginääriyksikkö $i = (0, 1)$ ja $i^2 = -1$
- *moduli* = $\text{mod } z = r = |z| = \sqrt{z\bar{z}}$, *argumentti* = *vaihekulma* = $\arg z$
- *polaarisitys*: $z = r \cdot (\cos \varphi + i \cdot \sin \varphi) = r e^{i\varphi}$ (*Eulerin kaava*, muistisääntö: $r \text{ cis}(\varphi)$)
 $r = \sqrt{x^2 + y^2}$ ja $\varphi = \text{atan} \frac{y}{x} + 2n\pi$
- *pääarvo* = $\arg z = \varphi$:n se arvo, joka on välillä $-\pi < \text{Arg } z \leq \pi$
- *liittoluku* eli *konjugaatti* on $\bar{z} = x - iy$. Sille pätee:
 $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$, $\overline{z_1 - z_2} = \bar{z}_1 - \bar{z}_2$, $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$, $\overline{z_1/z_2} = \bar{z}_1/\bar{z}_2$
- kertolasku: $z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1) =$
 $r_1 r_2 [\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)]$
- jakolasku: $\frac{z_1}{z_2} = \frac{x_1 + iy_1}{x_2 + iy_2} = \frac{x_1 x_2 + y_1 y_2}{x_2^2 + y_2^2} + i \cdot \frac{x_2 y_1 - x_1 y_2}{x_2^2 + y_2^2} = \frac{(x_1 + iy_1)(x_2 - iy_2)}{(x_2 + iy_2)(x_2 - iy_2)} =$
 $\frac{r_1}{r_2} [\cos(\varphi_1 - \varphi_2) + i \sin(\varphi_1 - \varphi_2)]$. Huom. erityisesti: $\frac{1}{i} = -i$
- käänteisluku: $z' = \frac{1}{z} = \frac{x}{x^2 + y^2} + i \frac{y}{x^2 + y^2}$ tai $\frac{1}{\text{mod } z} e^{-i \cdot \arg z}$
- potenssiin korotus (\mathbb{Z}) (*De Moivre'n kaava*): $z^n = r^n \cdot e^{in\varphi}$
- $\ln z = \ln(r) + i\varphi (+ i 2k\pi)$, $k \in \mathbb{N}$
- n :s juuri: $\sqrt[n]{z} = \sqrt[n]{r} \cdot e^{i \frac{\varphi + 2k\pi}{n}} | k = 0, 1, \dots, n-1$
 Arvoja on siis n kappaletta ja ne sijaitsevat tasaisin välein $\sqrt[n]{r}$ -säteisellä ympyrällä.
- kolmioepäyhtälö: $\|z_1\| - \|z_2\| \leq \|z_1 + z_2\| \leq \|z_1\| + \|z_2\|$

7.1 Kompleksiset funktiot

- Merkitään $f(z) = U(x, y) + iV(x, y)$, missä $z = x + iy$
- Jos $f(z)$ on differentioituva tietyssä pisteessä $\Rightarrow f'(z) = U_x(x, y) + iV_x(x, y) = U_y(x, y) + iV_y(x, y)$. Lisäksi $U_x = V_y \wedge U_y = -V_x$ (*Cauchy-Riemann-ositteisderivaattayhtälö*).
- Jos $U_x = V_y \wedge U_y = -V_x$ **ja** $f(z)$ on jatkuva $\Rightarrow f(z)$ on differentioituva.
- $f(z)$ on *analyttinen*, jos se on differentioituva z :n naapurustossa (ϵ -säteisen kiekon sisällä kaikissa pisteissä). Lisäksi: $f(z)$ on differentioituva äärettömässä jos $f(1/z)$ on analyttinen origossa.
- Jos $f(z)$ on analyttinen $\Rightarrow U$ ja V ovat harmonisia (ks. kahden muuttujan funktiot).
- $\sin(z) = (\sin x \cosh y) + i(\cos x \sinh y)$
- Ns. *conformal mapping* $w = \frac{az + b}{cz + d}$, $ad - bc \neq 0 \Leftrightarrow z = \frac{-dw + b}{cw - a}$ määräytyy yksiselitteisesti kolmella pisteellä: $\frac{w - w_1}{w - w_3} \cdot \frac{w_2 - w_3}{w_2 - w_1} = \frac{z - z_1}{z - z_3} \cdot \frac{z_2 - z_3}{z_2 - z_1}$ (∞ :n sisältävät osamäärät korvataan 1:llä!). K.o. kuvaus muuttaa suoria ympyröiksi ja päinvastoin.
- Suljetun polun viivaintegraalin laskemiseen on kasa erilaisia sääntöjä, joista residuaalimetelmä vaikuttaa erityisen hyödylliseltä. Kun polku ei leikkaa itseään ja on *positiivisesti orientoitu* ja f on polun sisällä muuten analyttinen, mutta k :ssa pisteessä on singularaarinen *napa* (eng. *pole*), pätee *Cauchyn residuaalilause*:

$$\oint_C f(z) dz = 2\pi i \sum_{j=1}^n \text{Res } f(z)_{z=z_j}$$

$$\text{Res } f(z)_{z=z_0} = \lim_{z \rightarrow z_0} f(z - z_0) (z - z_0)$$

$$\left(= \frac{p(z_0)}{q'(z_0)}, \text{ jos } f = \frac{p}{q} \right)$$

Jos polku on negatiivisesti orientoitu, lasketaan residuaalit negatiivisina. Huom: jos singulariteettejä ei ole, on integraali 0.

8 Abstrakti algebra

= algebrallisia rakenteita (eli alkioiden ja niihin kohdistuvien operaatioiden yhdistelmiä) aksiomaattisesti (eli pieneen määrään perusoletuksia nojaavasti) käsittelevä oppi.

8.1 Ryhmät (groups) ja monoidit (monoids)

Joukon G ja siihen vaikuttavan jonkin operaation \circ yhdistelmä, (G, \circ) , on nimeltään:

- *puoliryhmä* (semigroup), jos \circ on assosiatiiivinen eli $a \circ (b \circ c) = (a \circ b) \circ c$
- *monoidi*, jos lisäksi on olemassa *neutraalialkio* $e \in G$, jolle $e \circ a = a \circ e = a$
 - jos \circ on $+$ (additiivinen ryhmä), niin e merkitään 0
 - jos \circ on \cdot (multiplikaatiivinen ryhmä), niin e merk. 1 . Merkitään myös $ab = a \cdot b$.
- *ryhmä* (group), jos lisäksi kaikille alkioille on käänteisalkio: $a^{-1} \circ a = a \circ a^{-1} = e$
 - jos \circ on $+$, niin käänteisalkiota nimitetään *vasta-alkioksi* ja merkitään $-a$
 - jos \circ on \cdot , niin voidaan merkitä myös $a^{-1} = \frac{1}{a}$ ja $a^{-1}b = \frac{b}{a}$
- *abelin ryhmä*, jos se on lisäksi *kommutatiivinen* eli $a \circ b = b \circ a$ kaikille a, b . Huom: myös puoliryhmä ja monoidi voivat olla kommutatiivisia.

Jos G on äärellinen niin \circ välttämättä ”pyörähtää ympäri” (kongruenssin tapaan) koska kaikille $a, b \in G \Rightarrow (a \circ b) \in G$. Esim. ryhmässä $(\{0, 2, 4\}, +)$ on $2 + 2 = 4$ mutta $4 + 2 = 0$.

Lisää määritelmiä ja lauseita:

- alkion *potenssi* $a^n, n \in \mathbb{Z} = a \circ a \circ a \dots$ yhteensä n kertaa.
 - jos \circ on $+$, niin potenssia merkitään na
- ryhmän *kertaluku* (*order*) $|G|$ on sen alkioiden määrä
- *aliryhmä* on G :n jonkin **ei-tyhjän** osajoukon ja ryhmän operaattorin yhdistelmä, jos myös kyseinen osajoukko on ryhmä kyseisellä operaattorilla (joss $H \subseteq G$ on ko. alijoukko ja $a, b \in H \Rightarrow ab \in H \wedge a^{-1} \in H$).
- *triviaali aliryhmä* on nimitys aliryhmille $(\{e\}, \circ)$ ja (G, \circ)
- *suora tulo* $(G, \circ) \times (H, *)$, on uusi ryhmä (jolla on uusi operaattori \bullet) siten, että: $(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$
- *homomorfismi* on funktio $f: G \rightarrow H$ ryhmien $(G, \circ), (H, *)$ välillä, jos kaikille $a, b \in G$ pätee $f(a \circ b) = f(a) * f(b)$.
- *isomorfismi* on homomorfismi, joka on lisäksi bijektio (eli kääntäen yksikäsitteinen, ts. on olemassa myös isomorfismi $f^{-1}: H \rightarrow G$). (esim. $\log(x), x \in \mathbb{R}$ on isomorfismi $(\mathbb{R}^+, \cdot) \rightarrow (\mathbb{R}, +)$, koska $f(ab) = \log(ab) = \log(a) + \log(b) = f(a) + f(b)$ – ts. logaritmillä voidaan muuttaa \mathbb{R}^+ :n kertolasku \mathbb{R} :n yhteenlaskuksi (kuten oli tapana ennen laskimia).
- ryhmiä sanotaan isomorfisiksi, jos niiden välillä olemassa isomorfismi ja ne voidaan tällöin samaistaa (rakenteellisesti).
- *syklinen ryhmä* on ryhmä, jonka kaikki alkiot ovat jonkin sen alkion potensseja. Kyseinen alkio *virittää ryhmän* (generates the group) ja merkitään $\langle a \rangle \subseteq (G, \circ)$. Viritetyn (usein ali-)ryhmän suuruus eli *alkion kertaluku* on $|\langle a \rangle|$.
 - jos $|G|$ on ääretön, syklinen ryhmä on isomorfinen $(\mathbb{Z}, +)$:n kanssa
 - jos taas äärellinen ja $|G| = n \geq 2$, niin $(\mathbb{Z}_n, +)$:n kanssa.
 - virittävälle alkioille on $a^{|\langle a \rangle|} = e$
 - Syklisen ryhmän kaikki aliryhmät ovat syklisiä.

- *Kleinin ryhmä* on pienin ei-syklinen ryhmä (yksikäsitteinen, kertaluku 4, en piirrä tähän).
- Jokainen ryhmä, jonka $|G|$ on alkuluku, on syklinen. Syy:
- *Lagrange'n lause*: jos H on ryhmän G aliryhmä, niin $|H|$ jakaa $|G|$:n (eli $\frac{|G|}{|H|} \in \mathbb{Z}^+$)

Esimerkki: syklinen ryhmä $(\{1, -1, i, -i\}, \cdot)$, virittäjänä i , on isomorfinen $(\mathbb{Z}_4, +)$:n kanssa kun määritellään: $f(1) = [0], f(-1) = [2], f(i) = [1], f(-i) = [3]$:

$$\begin{array}{ccccc|ccccc}
 \cdot & 1 & -1 & i & -i & + & 0 & 2 & 1 & 3 \\
 1 & 1 & -1 & i & -i & 0 & 0 & 2 & 1 & 3 \\
 -1 & -1 & 1 & -i & i & 2 & 2 & 0 & 3 & 1 \\
 i & i & -i & -1 & 1 & 1 & 0 & 3 & 2 & 1 \\
 -i & -i & i & 1 & -1 & 3 & 3 & 1 & 0 & 2
 \end{array}
 \quad \text{ja aliryhmät } \langle -1 \rangle, \langle 2 \rangle:
 \begin{array}{ccc|ccc}
 \cdot & 1 & -1 & + & 0 & 2 \\
 1 & 1 & -1 & 0 & 0 & 2 \\
 -1 & -1 & 1 & 2 & 2 & 0
 \end{array}$$

8.2 Renkaat (ring) ja kunnat (field)

Joukon G ja sen kahden operaation $+$ ja \cdot yhdistelmä, $(G, +, \cdot)$, on algebrallinen *renkas*, jos:

- I. $(G, +)$ on kommutatiivinen ryhmä ja
- II. (G, \cdot) on puoliryhmä ja
- III. *distributiivisäännöt* pätevät:
 - $(a + b) \cdot c = a \cdot c + b \cdot c$
 - $a \cdot (b + c) = a \cdot b + a \cdot c$

Lisäksi:

- Renkaan *ykkösalkio* (ei aina olemassa) merkitään 1 ja määritellään $1 \cdot a = a \cdot 1 = a$
- Alkio $a \neq 0$ on *aito nollatekijä* jos on olemassa $b \neq 0$, jolle $a \cdot b = 0$ tai $b \cdot a = 0$.
- *Yksikkö* (unit) on alkio a , jolla on jokin käänteisalkio a^{-1} (missä $a \cdot a^{-1} = a^{-1} \cdot a = 1$).
Huom: "yksikkö" \neq "ykkösalkio" (\cdot :n neutraali-alkio, unity)
- *Kommutatiivinen renkas* on renkas, jolle $a \cdot b = b \cdot a$ (ei esim. matriisirenkaissa).
- *Kunta* (field) on kommutatiivinen renkas jonka kaikki $a \neq 0$ ovat yksiköitä. (Esim. \mathbb{Q} on kunta, mutta \mathbb{Z} ei, koska esim. $4^{-1} = \frac{1}{4} \notin \mathbb{Z}$ eli 4 ei ole yksikkö eli sillä ei ole kokonaisluku-käänteisalkiota.)
- *Kokonaisalue* (integral domain) on kommutatiivinen renkas, jolla ei ole nollatekijöitä (ekvivalentti ehto: $xy = xz \Rightarrow y = z$).
- Kaikki kunnat ovat kokonaisalueita ja kaikki **äärelliset** kokonaisalueet ovat kuntia.
- Jos alkiolla on käänteisalkio, se ei voi olla nollatekijä \Rightarrow kunnassa ei ole lainkaan aitoja nollatekijöitä.
- $(\mathbb{Z}_n, +, \cdot)$ on kommutatiivinen, ykkösalkiolla varustettu renkas ja sen alkiolla a on käänteisluokka joss $\text{sy}(a, n) = 1$. Joss n on alkuluku, on \mathbb{Z}_n (myös) kunta (eli kaikilla alkiolla, ts. kongruenssiluokilla, on käänteisalkio).
- Kaikkien äärellisten kuntien koko on muotoa p^h , missä p on alkuluku ja $h \in \mathbb{Z}^+$.
- *Alirenkas* on renkas, jonka alkiaina on jonkin toisen renkaan alkioiden osajoukko.
- *Ideaali alirenkas* I on R :n alirenkas, jolle 1) kaikkien sen alkioiden erotuksetkin kuuluvat I :hin (ts. $(a - b) \in I$ kaikille $a, b \in I$) ja 2) myös kaikille $r \in R, a \in I$ pätee $r \cdot a, a \cdot r \in I$.
- Kaikki \mathbb{Z} :n alirenkaat ovat ideaaleja ja niiden S alkiot ovat muotoa $y \in S = nx \mid x \in \mathbb{Z}$.
Tästä johtuu: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.
- Renkaan *karasteristika* $\text{char } R$ on on pienin $n \in \mathbb{Z}^+$, jolle $\underbrace{a + a + \dots + a}_{n \text{ kpl.}} = 0 \in R$. Jos yhtään tällaista lukua ei ole olemassa, $\text{char } R = 0$.

- Jos kyseessä on kunta ja $n = \text{char } R > 0$, n on alkuluku. Kuntien \mathbb{Q} , \mathbb{R} ja \mathbb{C} karaktererika on 0, mutta on olemassa äärettömiä kuntia, joiden $\text{char} > 0$ (esim. $\text{char GF}(\mathbb{Z}_3[x]) = 3$).
- *Rengashomomorfismi* on funktio $f: R \rightarrow S$ (missä $(R, +, \cdot)$ ja (S, \oplus, \odot) ovat renkaita), jos kaikille $a, b \in R$ on $f(a + b) = f(a) \oplus f(b)$ ja $f(a \cdot b) = f(a) \odot f(b)$. Jos f on lisäksi bijektio (kääntäen yksikäsitteinen kuvaus), se on *isomorfismi*. Renkaat ovat keskenään isomorfisia jos niiden välillä on olemassa isomorfismi.
- "*Matriisirengas* renkaan R yli" eli $M_n(R)$ on $n \times n$ -neliomatriiseista koottu rengas, jonka matriisialkiot ovat R :n alkioita. Matriisikertolaskun epäkommutatiivisuudesta johtuen M_n on harvoin kommutatiivinen vaikka R olisikin.

8.3 Polynomirenkaat

Jos $(R, +, \cdot)$ on rengas (vaika \mathbb{Q} -kunta, tai äärellinen \mathbb{Z} -rengas tai vaikka matriisirengas):

- "Muuttujan x R -polynomi" on muotoa $a_n x^n + \dots + a_2 x^2 + a_1 x^1 + a_0 x^0$, missä $a_i \in R$.
- *Johtokerroin* on polynomin korkeinta astetta oleva termin kerroin a_n .
- *Vakiotermi* on $a_0 x^0 = a_0$ (*nollapolynomi*, jos $a_0 = 0$).
- Merkintätapa: $R[x]$ = muuttujan x kaikkien R -polynomien (ääretön) joukko.
- Äärettömällekin joukolle $R[x]$:n polynomeja on yleisessä tapauksessa useita esitystapoja. Esim. jos $R = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ niin $5x^2 + 3x^1 - 2x^0 \equiv 5x^2 + 3x^1 + 4x^0$, koska $-2 \equiv 4 \pmod{6}$.
- Jos polynomin $f(x)$ kertoimet ovat a_j ja $g(x)$:n kertoimet b_j niin $f(x) \cdot g(x)$:n tulon termien kertoimet ovat $c_i = \sum_{k=0}^i a_k b_{i-k}$. **Huom:** jos R -renkaassa on aitoja nollatekijöitä, tulon aste saattaa olla pienempi kuin f :n ja g :n asteiden summa.
- "*Polynomirengas* yli R " on rengas $(R[x], +, \cdot)$.
- Juuri on x :n arvo, jolla polynomin arvoksi tulee nolla-alkio. **Huom:** yleisessä tapauksessa (kun R -rengas ei ole kokonaisalue) $R[x]$:n polynomeilla voi siis olla niiden astetta enemmän juuria.
- $p(x) \in R[x]$ on *redusoituva* eli jaollinen, jos sen aste on ≥ 2 ja $p(x) = f(x) \cdot g(x)$ joillekin f, g , joiden aste on ≥ 1 . Jaoton polynomi on *redusoimaton*. **Huom:** redusoituvuus riippuu R :stä: esim. $(x^2 + 1) \in \mathbb{R}[x]$ on jaoton, mutta $(x^2 + 1) \in \mathbb{C}[x]$ jaollinen: $(x - i)(x + i)$.
- Jos R on kunta ja polynomi on astetta 2 tai 3, se on redusoituva/jaollinen joss sillä on juuri R :ssä.
- Polynomien *suhteellinen redusoimattomuus*: $\text{sy}(p(x), g(x)) = \text{vakio}$ (eli astetta nolla).
- *Normeerattu polynomitulo* on tekijöihin jaetun polynomin yksikäsitteinen esitysmuoto, jossa koko lauseke on kerrottu vakiolla ja kaikkien tekijöiden (redusoimattomia, ts. jaottomia polynomeja) johtokerroin on 1: $p(x) = a_n \cdot (x^n + b_{n-1} x^{n-1} + \dots + b_1) \cdot \dots \cdot (x^m + c_{m-1} x^{m-1} + \dots + c_1)$.
- Eri polynomirakenteiden määrä voidaan rajata (tavallisesti äärettömästä $R[x]$:stä) äärelliseksi kongruenssilla: valitaan jokin polynomi $s(x)$ ja määrätään, että kaikkien renkaan operaatioiden tuloksesta otetaan lopuksi jakojäännös $s(x)$:llä. Merkitään: $R[x]/s(x)$. Jos $s(x)$ on redusoituva, tulos on rengas ja jos taas redusoimaton niin kunta. Esim. polynomikunnan $\mathbb{Z}_2[x]/(x^2 + x + 1)$ operaatiot ovat:

+	0	1	x	$x + 1$	ja	·	0	1	x	$x + 1$
0	0	1	x	$x + 1$		0	0	0	0	0
1	1	0	$x + 1$	x		1	0	1	x	$x + 1$
x	x	$x + 1$	0	1		x	0	x	$x + 1$	1
$x + 1$	$x + 1$	x	1	0		$x + 1$	0	$x + 1$	1	x

Jos R on ääretön, on tietysti myös $R[x]/s(x)$ ääretön vaikka eri polynomimuotoja onkin rajallisesti. Esim. $\mathbb{R}[x]/(x^2 + 1)$ on isomorfinen \mathbb{C} :n kanssa.

- *Galois-kunta* $\text{GF}(q) = \text{GF}(p^h) = \text{polynomikunta } \mathbb{Z}_p[x]/s(x)$, missä $s(x)$ on, kertalkua $h \in \mathbb{Z}^+$ oleva redusoimaton, normeerattu polynomi. $s(x)$:n löytäminen ei ole yleensä helppoa, mutta siihen on olemassa algoritmeja. Galois-kunnan karakteristika $\text{char GF}(p^h) = p$.
- $\text{GF}(p^h)$:n *fundamentaalikunta* on sen alikunta \mathbb{Z}_p . Erityistapaus: $\text{GF}(p) = \mathbb{Z}_p$ eli yksinkertaisen (siis ”ei-moninkertaisen”) alkuluvun Galois-kunta on oma fundamentaalikuntansa.
- Jokainen $q = p^h$ kokoinen (eli ”kertalukua q oleva”) kunta on isomorfinen $\text{GF}(p^h)$:n kanssa.

8.4 Kooditeoria

Boolean algebran (symbolien 0, 1 jonoista sekä operaatioista $+$, \cdot koottu logiikka-algebra) sovellus: siirretään n -bittisiä viestejä ($\in \mathbb{Z}_2^n$) häiriöisellä linjalla, joka voi aiheuttaa mihin tahansa siirrettävään bittiin virheen (ts. $0 \leftrightarrow 1$) todennäköisyydellä p , bitin sijainnista ja alkuperäisestä arvosta riipumatta.

- *Virherakenne* $e \in \mathbb{Z}_2^n$:ssä on 1 niissä kohdissa joissa siirretyissä viestissä on virhe ja 0 niissä, joissa bitti siirtyi oikein. Kun k =virhebittien (1-bittien) määrä eli *virheen paino*:
 - Tietyn virherakenteen esiintymisen todennäköisyys on $p^k(1-p)^{n-k}$
 - Tasan k virhettä sisältävän siirron todennäköisyys on $\binom{n}{k} p^k(1-p)^{n-k}$
- (n, m) -*blokkikoodaus* muuttaa m -bittiset viestit n -bittisiksi jonoksi lisäämällä niihin $(n - m)$ kpl. tarkistusbittejä jolloin *koodauksen tehosuhte* on $\frac{m}{n}$ ($m < n$).
- *Hamming-etäisyys* on kahdessa bittijonossa toisistaan eroavien bittien määrä.
- Kun viestejä välitetään käyttäen joukkoa *koodisanoja*, kaikki painoa $\leq k$ olevat virheet voidaan:
 - havaita, jos eri koodisanojen minimietäisyys on vähintään $k + 1$
 - korjata, jos eri koodisanojen minimietäisyys on vähintään $2k + 1$
- Koodaus $E: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$ on *ryhmäkoodi* joss sen tuottamat koodisanat ovat $(\mathbb{Z}_2^n, +)$:n aliryhmä. Ryhmäkoodeilla koodisanojen Hamming-minimietäisyys on niiden nolasta eriävien koodisanojen minimipaino (eli niiden keskinäisiä etäisyyksiä ei tarvitsekaan laskea).
- Koodauksen $E: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$ *generoiva matriisi* on G jolla **oikealta** kertominen tuottaa viestisanoista koodisanat: $E(w \in \mathbb{Z}_2^m) = w \cdot G = c \in \mathbb{Z}_2^n$ (missä w on m -**vaakavektorina** esitetty viesti ja c on n -vektorina esitetty koodisana). Esim: eräs $\mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^3$ -koodaus:

$$\begin{pmatrix} 0 & 1 \end{pmatrix} \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right) = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

- Generoiva matriisi on *normalisoitu* eli *systemaattinen* jos se on muotoa $[I_m|A]$ eli vasemmallalla on alimatriisina yksikkömatriisi. Minkä tahansa generoivan matriisin voi normalisoida ja tuloksena on *ekvivalentti koodaus*.
- *Tarkistusmatriisi* on H , jolle c :n *syndrooma* eli $H \cdot c^T = 0^T \in \mathbb{Z}_2^{n-m}$ joss c on jokin käytettyistä koodisanoista. Normalisoitu muoto on $[B|I_{n-m}]$. Huom: syndrooman laskussa **pystyvektorina** esitetty viesti kerrotaan H :lla **vasemmalta**.
- Jos vastaanotetussa viestissä r on virhe vain yhdessä bitissä, i , $H \cdot r^T$ on H :n i :s pystyriivi. (Yleisesti: syndrooma on virhebittien vastaavien H :n pystyriivien summa.)
- Generoivalla matriisilla esitetty koodaus on ryhmäkoodi.
- *Hamming-koodaus*: tarkistusmatriisi $H = [B|I_k]$ eli *Hammingin matriisi* on kokoa $k \times (2^k - 1)$ ja sen pystyriivit on koottu lukujen $1, 2, \dots, 2^k - 1$ binääriesityksistä jossain järjestyksessä. Vastaava generoiva (eli koodaus-) matriisi on $G = [I_{2^k-1-k}|B^T]$. Hamming-koodauksella siirretään $m = 2^k - 1 - k$ -mittaisia viestejä, sillä voidaan korjata yksi virhe ja sen tehosuhte on $\frac{2^k - 1 - k}{2^k - 1} = 1 - \frac{k}{2^k - 1}$.

9 Kombinatoriikka

9.1 Permutaatiot ja kombinaatiot

- *permutaatio* = uudelleenjärjestely/sekoitus
- *kombinaatio* = yhdistelmä, jossa järjestyksellä ei ole väliä
- *R-permutaatioiden* määrä = “montako erilaista r :n pituista järjestettyä jonoa voidaan muodostaa n :stä eri alkioista” = $P(n, r) = \frac{n!}{(n-r)!}$. Huom: $P(n, n) = P(n) = n!$
- *R-kombinaatioiden* määrä = “montako erilaista r :n kokoista joukkoa voidaan valita n :stä eri alkioista kun järjestyksellä ei ole väliä” = $C(n, r) = \binom{n}{r} = \frac{P(n, r)}{r!} = \frac{n!}{r!(n-r)!}$. Huom: $C(n, n) = 1$
- *Toistopermutaatioiden* määrä = “monellako toisistaan erottuvalla tavalla voidaan järjestää n kpl. k :sta eri luokasta valittua alkioita, kun luokasta 1 valitaan r_1 kpl, luokasta 2 valitaan r_2 jne.” =

$$P(n, r_1, r_2, \dots, r_k) = \frac{n!}{r_1! \cdot r_2! \cdot \dots \cdot r_k!}$$
 (missä siis $n = \sum r_i$)
- *Kyyhkyslakkaperiaate*: “Jos on $n + 1$ kyyhkystä ja n pesää, vähintään yhdessä pesässä on 2 kyyhkystä” (kaikki voivat olla myös samassa pesässä!)
- “ n :n eri alkion mahdollisten luokittelujen määrä k :hon luokkaan jaettaessa kun osa luokista saa olla tyhjiä” =
“ k :sta eri merkistä koottujen n :n pituisten merkkijonojen pituus” = k^n
- Yhtälön $x_1 + x_2 + \dots + x_k = n$ ratkaisujen määrä, kun $x, n \in \mathbb{N} =$
“Monellako tapaa voidaan järjestää n pallon ja $k - 1$ erottimen muodostama jono” =

$$P(n + k - 1, n, k - 1) = \frac{(n + (k - 1))!}{n! \cdot (k - 1)!} =$$
“Monellako tavalla voidaan valita pallojen paikat” = $C(n + (k - 1), n) =$
“Monellako tavalla voidaan valita erotinten paikat” = $C(n + (k - 1), (k - 1))$.
Esim:
“Monellako tavalla 7 eri henkilöä voi valita 4:stä eri ruokalajista?” =
“Montako ratkaisua on positiivisella kokonaislukuyhtälöllä $x_1 + x_2 + x_3 + x_4 = 7$?” =
“Monellako (erottuvalla) tavalla voidaan järjestää jono ’|||ooooo?’” = $\frac{10!}{7! \cdot 3!} = \binom{10}{7}$
- *Väärinjärjestysten* määrä = “Monellako tapaa voi järjestää n alkioita niin, ettei mikään ole omalla paikallaan” = $\sum_{k=0}^n \frac{(-1)^k n!}{k!} \approx n! \cdot e^{-1}$
- “ n :n eri alkion mahdollisten luokittelujen määrä k :hon ei-tyhjään luokkaan jaettaessa” (esim. $n = 3, k = 2: \{1, 2, 3\} \Rightarrow \{1\}\{2, 3\}, \{1, 2\}\{3\}, \{1, 3\}\{2\}$) eli *2. lajin Strilingin luvut* =

$$S(n, k) = \frac{1}{k!} \sum_{r=1}^k (-1)^{k-r} \binom{k}{r} r^n$$
 (rekursiokaavana: $S(n + 1, k) = k S(n, k) + S(n, k - 1)$)
- “ n :n eri alkion kaikkien mahdollisten luokittelujen määrä” eli *Bellin luvut* = $B(n) = \sum_{k=1}^n S(n, k)$

9.2 Inklusio-eksklusio-periaate

Inklusio-eksklusio-periaatteella lasketaan osittain päällekkäisiä ehtoja täyttävien alkioiden / tapausten määriä: ensin päällekkäisten joukkojen koot lasketaan yhteen ja sitten tuloksesta vähennetään niille yhteisten alkioiden määrä (ettei sitä oteta mukaan kahteen kertaan). Ongelmia kannattaa visualisoida Venn-diagrammilla. Merkintätapoja:

Joukko S , jonka koko $|S| = N$, koostuu alkioista, jotka toteuttavat kukin joitain (tai vaikka kaikki tai ei yhtään) t :stä eri ehdosta c_1, \dots, c_t (esim. N esinettä ja 4 ehtoa: c_1 = “alkio on pallo”, c_2 = “alkio on vihreä”, c_3 = “alkio on sininen”, c_4 = “alkio on painava” jne). Vähintään yhden ehdoista c_i, c_j, \dots toteuttavien alkioiden määrää merkitään $N(c_i c_j \dots)$ ja niitä, jotka eivät toteuta niistä mitään (mutta voivat toteuttaa jotain muita!) merkitään $N(\bar{c}_i \bar{c}_j \dots)$.

Ei yhtään ehtoa täyttäviä alkioita on:

$$E_0 = \bar{N} = S_0 - S_1 + S_2 - S_3 + \dots = \sum_{i=0}^t (-1)^i S_i$$

$$\dots \text{kun} \begin{cases} S_0 = N \\ S_1 = N(c_1) + N(c_2) + N(c_3) + \dots \\ S_2 = N(c_1 c_2) + N(c_1 c_3) + \dots + N(c_2 c_3) + N(c_2 c_4) + \dots \\ S_3 = N(c_1 c_2 c_3) + N(c_1 c_2 c_4) + \dots + N(c_2 c_3 c_4) + \dots \end{cases}$$

Yleisesti: tasan m ehtoa täyttäviä alkioita on:

$$E_m = S_m - \binom{m+1}{1} S_{m+1} + \binom{m+2}{2} S_{m+2} - \dots$$

$$= \sum_{i=0}^{t-m} (-1)^i \binom{m+i}{i} S_{m+i} = \sum_{i=0}^{t-m} (-1)^i \frac{(m+i)!}{i! m!} S_{m+i}$$

9.3 Binomi- ja multinomikertoimet

Binomilause määrää termien kertoimet kun binomi kerrotaan auki polynomiksi:

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

Kerroin k :nnen asteen x :lle on siis n :n k -kombinaatio. Binomikertoimia kuvataan usein *Pascalin kolmiolla*, jonka jokainen reuna-alkio on 1 ja jokainen sisäalkio aina kahden heti sen yläpuolella olevan alkion summa. *Multinomilause* yleistää tuloksen:

$$\text{Tulossa } (x_1 + x_2 + \dots + x_k)^n, \text{ termin } x_1^{r_1} \cdot x_2^{r_2} \cdot \dots \cdot x_k^{r_k} \text{ kerroin on } \binom{n}{r_1 r_2 \dots r_k} = \frac{n!}{r_1! \cdot r_2! \cdot \dots \cdot r_k!}$$

Joskus tarvitaan "binomikertoimia", joissa $n \in \mathbb{Z}^-$ tai $n \in \mathbb{R}$: *yleistetyt binomikertoimet*:

$$\binom{s}{k} = \frac{s \cdot (s-1) \cdot \dots \cdot (s-k+1)}{k!}, \quad s \in \mathbb{R}, k \in \mathbb{Z}$$

...tai jos s :n tilalla onkin negatiivinen kokonaisluku (\mathbb{Z}^-) eikä desimaaliluku, niin:

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k} = (-1)^k \frac{(n+k-1)!}{k!(n-1)!}$$

9.4 Generoivat funktiot eli emäfunktiot

Emäfunktiolla voi ratkaista mekaanisesti erilaisia kombinatorisia tehtäviä ("montako erilaista / monellako tavalla" ja jopa "luettele kaikki" eli *enumerointi*) esittämällä jonot polynomeina. Algebrallisen pyörityksen jälkeen tulos katsotaan suoraan polynomien halutun asteisten termien kertoimista *eikä itse polynomiin sijoiteta mitään!*

- tavallinen emäfunktio $g(x) = a_0 + a_1 x + a_2 x^2 + \dots = \sum_{k=0}^{\infty} a_k x^k$ (sopii kombinaatiolle)
- eksponentiaalinen emäfunktio $G(x) = a_0 + a_1 x + a_2 \frac{x^2}{2!} + \dots = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!}$ (permutaatioille)
- muitakin emäfunktioita on (esim. kahden muuttujan versio)

Esim. (tavallinen emäfunktio): "Montako positiivista kokonaislukuratkaisua on yhtälöllä $a + b + c = 12$, kun $a \in [4, 8]$, $b \in [2, 6]$ ja $c \in [2, 5]$?" Tämä ratkeaa kertomalla auki polynomi (tavallinen emäfunktio)...

$$\underbrace{(x^4 + x^5 + x^6 + x^7 + x^8)}_a \underbrace{(x^2 + x^3 + x^4 + x^5 + x^6)}_b \underbrace{(x^2 + x^3 + x^4 + x^5)}_c = x^8 + \dots + 14x^{12} + 16x^{13} + \dots$$

...ja ottamalla siitä x^{12} :n kerroin (14). Muuttujan x potenssit esittävät a :n, b :n ja c :n arvoja ja niiden kertoimet (a_i , tässä tapauksessa 1 kaikille mainituille ja muille 0) merkitsevät "monellako tavalla kyseinen arvo voi tulla valituksi kyseiselle muuttujalle". Ym. lauseen voi siis lukea tulkitsemalla $+$ ="tai", \cdot ="ja" (kuten Boolean algebrassa): "jos ($a=4$ tai $a=5$ tai ...) ja ($b=2$ tai $b=3$ tai ...) ja ...". Auki kerrottu polynomi esittää näiden eri kombinaatioita ja siitä näkee myös, että esim. $a + b + c = 13$ ratkaisuja olisi 16 kpl.

Polynomien kertominen keskenään on työlästä, joten laskemisessa hyödyllisiä ovat *potenssi-sarjojen laskusäännöt* (Huom: suppeneuusehdoilla ei tässä ole mitään väliä, koska x :ään ei oikeasti sijoiteta mitään):

A) äärettömät jonot (sarjat):

$$\begin{aligned} (a_n = 1, 1, 1, 1, \dots) \frac{1}{1-x} &= 1 + x + x^2 + x^3 + \dots = \sum_{i=0}^{\infty} x^i \\ (a_n = 1, -1, 1, -1, \dots) \frac{1}{1+x} &= 1 - x + x^2 - x^3 + \dots = \sum_{i=0}^{\infty} (-1)^i x^i \\ (a_n = 1, 2, 3, 4, \dots) \frac{x}{(1-x)^2} &= x + 2x^2 + 3x^3 + \dots = \sum_{i=0}^{\infty} i x^i \left(= \frac{d}{dx} \sum_{i=0}^{\infty} x^{i+1} = \frac{d}{dx} x \frac{1}{1-x} \right) \\ \frac{1}{(1+x)^n} &= \sum_{i=0}^{\infty} \binom{-n}{i} x^i = \sum_{i=0}^{\infty} (-1)^i \binom{n+i-1}{i} x^i \\ \frac{1}{(1-x)^n} &= \sum_{i=0}^{\infty} \binom{-n}{i} (-x)^i = \sum_{i=0}^{\infty} \binom{n+i-1}{i} x^i \\ g_a(x) \cdot g_b(x) &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^k a_i b_{k-i} \right) x^k \text{ eli jonojen konvoluutio} \end{aligned}$$

B) äärelliset jonot:

$$\begin{aligned} (a_n = \underbrace{1, 1, 1, \dots, 1}_{n \text{ kpl.}}) \frac{1-x^{n+1}}{1-x} &= 1 + x + x^2 + \dots + x^n \\ (1+x)^n &= \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \dots + \binom{n}{n} x^n \\ & \quad [\text{esim. } (1+x)^4 = 1 + 4x + 6x^2 + 4x^3 + 1x^4] \\ (1+ax)^n &= \binom{n}{0} + \binom{n}{1} ax + \binom{n}{2} a^2 x^2 + \dots + \binom{n}{n} a^n x^n \\ (1+x^m)^n &= \binom{n}{0} + \binom{n}{1} x^m + \binom{n}{2} x^{2m} + \dots + \binom{n}{n} x^{nm} \end{aligned}$$

C) (permutaatioiden laskemista varten) eksponenttifunktiot:

$$\begin{aligned} e^x &= 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \dots = \sum_{k=0}^{\infty} \frac{x^k}{k!} \\ e^{ax} &= 1 + ax + a^2 \frac{x^2}{2} + a^3 \frac{x^3}{6} + \dots = \sum_{k=0}^{\infty} a^k \frac{x^k}{k!} \\ \cosh x &= \sum_{k=0}^{\infty} \frac{x^{2k}}{(2k)!} \\ \sinh x &= \sum_{k=0}^{\infty} \frac{x^{2k+1}}{(2k+1)!} \\ \cos x &= \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k}}{(2k)!} \\ \sin x &= \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{(2k+1)!} \end{aligned}$$

Epäsäännöllisempiä sarjoja voi esittää laskemalla eri emäfunktioita yhteen tai vähentämällä yksittäisiä termejä, esim. $42, 0, -2, 1, 1, 1, 1, \dots \sim \frac{1}{1-x} + 41x^0 - 1x^1 - 3x^2$.

Ongelmassa esiintyvät jonot kirjoitetaan ensin emäfunktioiksi (eli ”siirrytään taulukossa oikealta vasemmalle”), sievennetään sitten niiden yhdistelmä (esim. summa) ja muutetaan tulos sitten takaisin sarjamuotoon (ts. ”taulukossa takaisin vasemmalta oikealle”). Menettely muistuttaa siis hieman Laplace-muunnoksen käyttöä ja myös emäfunktioissa ”käänteismuunnos” vaatii usein osamurtokehitemää (esimerkki differenssiyhtälöt-kappaleen lopussa).

Joitain generoivia funktioita (Huom! nämä siis *määrittelevät lukujonoja*, eivätkä annan itse määriä!):

- Väärinjärjestysten määrä: $D(x) = \frac{e^{-x}}{1-x}$
- *Fibonacciin luvut* ($a_n = a_{n-1} + a_{n-2}$): $F(x) = \frac{x}{1-x-x^2}$ ($\Rightarrow F_n = \frac{1}{\sqrt{5}}(r_+^n - r_-^n)$ || $r_{\pm} = (1 \pm \sqrt{5})/2$)
- *Catalanin luvut* ($a_{n+1} = a_0 a_n + a_1 a_{n-1} + \dots + a_n a_0$ eli esim. ”Eriolaisten n -kärkisten binääripuiden määrä”): $C(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$ ($\Rightarrow a_n = \frac{1}{n+1} \binom{2n}{n}$)
- ”Luvun n ositusten määrä $p(n)$ ”: $P(x) = \prod_{k=1}^{\infty} \frac{1}{(1-x^k)}$. Ositus = luvun kokoaminen termeistä $k \leq n$ (esim. $4=1+3=1+1+2=2+2=4$). Tekijät $k > n$ eivät vaikuta vastaukseen, joten äärettömän tulon voi katkaista ja käyttää (kertomalla versiot $k = 1 \dots n$ yhteen) sarjaa $\frac{1}{1-x^k} = \sum_{i=0}^{\infty} x^{ik}$.

9.5 Tornipolynomit (rook polynomials)

- *Tornipolynomi* = emäfunktio, jolla lasketaan ”Monellako tavalla voidaan asettaa k toisiaan uhkaamatonta (nontaking) tornia tietyn muotoiselle shakkilaudalle kun osa ruuduista on kiellettyjä (\otimes)?”
- ”Uhkaamaton” = mikään nappula ei saa olla samalla rivillä eikä sarakkeella toisen kanssa.
- Vastausta merkitään $r_k(C)$ kun C on lauta. Esim. $r_2(E) = 8$ ja $r_3(E) = 2$, kun $E = \begin{array}{|c|c|c|} \hline \square & \square & \square \\ \hline \square & \otimes & \square \\ \hline \otimes & \square & \square \\ \hline \end{array}$.
- Tornipolynomi $r(C, x)$ generoi r_k :n kaikille k . Esim: $R(E, x) = 1 + 6x + 8x^2 + 2x^3$ (tarkoittaa: 1 tapaa asettaa 0 tornia, 6 tapaa 1 torni, 8 tapaa 2 ja 2 tapaa 3 tornia)
- Jos kiellettyjä ruutuja on vähemmän kuin sallittuja, voidaan laskea käänteisen (vaihdetaan kielletyt \leftrightarrow sallitut) laudan polynomi ja selvittää inklusio-eksklusio-kaavaa:

$$r_h(C) = \sum_{i=0}^h (-1)^i \cdot r_i(C^{-1}) \cdot (w-i)! \left\| \begin{array}{l} w = \text{laudan leveys} \\ h = k = \text{laudan korkeus} \end{array} \right.$$

Esimerkki:

$$\begin{aligned} R(E^{-1}, x) &= 1 + 3x + 2x^2 \Rightarrow \\ r_3 &= (1 \cdot (3-0)! - 3 \cdot (3-1)! + 2 \cdot (3-2)! - 0 \cdot (3-3)!) \\ &= 1 \cdot 3! - 3 \cdot 2! + 2 \cdot 1! - 0 \cdot 0! \\ &= 6 - 6 + 2 - 0 = 2 \end{aligned}$$

(**MUTTA**: miten saa r_k :n mielivaltaiselle k eikä vain tapaukselle $k = h$??)

- Jos lauta koostuu erillisistä osista C_1, \dots, C_n (ts. ei yhteisiä rivejä eikä sarakkeita), on koko laudan polynomi sen erillisten osien polynomien tulo:

$$r(C, x) = r(C_1, x) \cdot r(C_2, x) \cdot \dots \cdot r(C_n, x)$$

- Lautaa voidaan jakaa kahdella tekniikalla vaikka erillisiä osia ei heti näkyisikään:

1. siirtelemällä rivejä ja sarakkeita (ei vaikuta tulokseen)

2. valitsemalla yksi rutuu jostain strategisesta paikasta ja laskemalla yhteen tapaukset, joissa siinä a) on nappula [poistetaan myös kaikki sen uhkaamat ruudut] tai b) ei ole nappulaa [poistetaan vain kyseinen ruutu]

$$r(C, x) = x \cdot \underbrace{r(C_a, x)}_{\text{on nappula}} + \underbrace{r(C_b, x)}_{\text{ei nappulaa}}$$

Esimerkki: Johdetaan ym. E :n tornipolynomi ilman käänteisen laudan temppea, sijoittamalla kokeeksi nappula vasemmalle ylös laudanjakotekniikan 2 mukaisesti:

$$\begin{aligned} E_a &= \begin{array}{cc} \otimes \otimes \\ \otimes \otimes \otimes \\ \otimes \square \square \end{array} \wedge E_b = \begin{array}{cc} \otimes \square \square & \otimes \square \square \\ \square \otimes \otimes & = \otimes \square \square \\ \otimes \square \square & \square \otimes \otimes \end{array} \text{ (erilliset osat!) } \Rightarrow \\ r(E_a, x) &= (1 + 2x) \wedge r(E_b, x) = (1 + x) \cdot (1 + 4x + 2x^2) \\ &\Rightarrow \\ r(E, x) &= x(1 + 2x) + (1 + x)(1 + 4x + 2x^2) \\ &= 1 + 6x + 8x^2 + 2x^3 \end{aligned}$$

9.6 Differenssiyhtälöt eli rekursiot

(...eli *rekurrenssiyhtälöt* eli *palautuskaavat*)

- Alkion a_n arvo riippuu k :sta edellisestä alkioista ja n :stä: $a_n = g(a_{n-1}, a_{n-2}, \dots, a_{n-k}, n)$, $n \geq k$. Vakio k on differenssiyhtälön *kertaluku*.
- Terminologia pitkälti samaa kuin differentiaaliyhtälöissä
- Homogeenisten, lineaaristen yhtälöiden yleiset ratkaisut saa erityisratkaisujen lineaarikombinaationa (kuten differentiaaliyhtälöissäkin)
- Helpoille tapauksille on ratkaisukaavoja ja hankalampiin voi usein käyttää emäfunktioita

9.6.1 Lineaariset ja vakiokertoimiset

Ratkaisukaavoja:

- Ensimmäisen kertaluvun vakiokertoimisen, lineaarisen ja homogeenisen yhtälön eli $a_n = r a_{n-1}$ (tai $a_{n+1} = r a_n$) yleinen ratkaisu on $a_n = c r^n$ (kun $n \geq 0$). Huom: $c = a_0$.
- Toisen kertaluvun vakiokertoiminen, lineaarinen ja homogeeninen yhtälö (kuten Fibonaccin luvut) eli $C_n a_n + C_{n-1} a_{n-1} + C_{n-2} a_{n-2} = 0$ (missä $n \geq 2$) ratkeaa sijoittamalla a_n :n tilalle *yritefunktioksi* ensimmäisen kertaluvun ratkaisu $a_n = c r^n$:

$$\begin{aligned} C_n c r^n + C_{n-1} c r^{n-1} + C_{n-2} c r^{n-2} &= 0 \parallel : c r^{n-2} \Rightarrow \\ C_n r^2 + C_{n-1} r + C_{n-2} &= 0 \end{aligned}$$

Tämä on *karakteristinen polynomi* ja rekursion ratkaisu riippuu sen juurista r_1 ja r_2 lineaarikombinaatiolla:

- 2 reaalista, erisuurta juurta $\Rightarrow a_n = c_1 r_1^n + c_2 r_2^n$ ($c_{\{1,2\}}$ ovat mielivaltaisia vakioita)
- kompleksikonjugaatit \Rightarrow samalla tavalla (r_1 ja r_2 eliminoivat toistensa imaginääriosat), mutta laskeminen on vähän hankalampaa ja se kannattaa tehdä polaarikoordinaateissa kompleksiluvun potenssiin korotuksen takia
- kaksinkertainen juuri (eli $r_1 = r_2$) $\Rightarrow a_n = (c_1 + c_2 n) r^n$

Sama konsti toimii korkeammankin kertaluvun yhtälöille, mutta polynomin ratkaisu menee turhan hankalaksi.

- Epähomogeenisten versioiden ratkaisut saa kaavasta $a_n = a_n^{(H)} + a_n^{(P)}$ eli homogeenisen version yleinen ratkaisu + epähomogeenisen jokin yksittäisratkaisu. Jos epähomogeeninen osa $f(n)$ sattuu olemaan muotoa $k r^n$, niin:
 - Ensimmäinen kertaluku (eli $a_n + C a_{n-1} = f(n)$):
 1. $a_n^{(P)} = A r^n$ jos se ei satu olemaan myös $a_n^{(H)}$:n ratkaisu tai

2. $a_n^{(P)} = A n r^n$, jos sattuu
- o Toinen kertaluku:
 1. $a_n^{(P)} = A r^n$ jos se ei satu olemaan myös $a_n^{(H)}$:n ratkaisu tai
 2. $a_n^{(P)} = A n r^n$ jos sattuu, ja $a_n^{(H)}$ on muotoa $c_1 r_1^n + c_2 r_2^n$ tai
 3. $a_n^{(P)} = A n^2 r^n$ jos sattuu, ja $a_n^{(H)}$ on muotoa $(c_1 + c_2 n) r^n$

9.6.2 Ratkaisu emäfunctioilla

Ideana on etsiä ensin rekursiota esittävä emäfunctio suljetussa muodossa (potenssisarjojen laskusäännöllä) ja sitten etsiä toiseen suuntaan sitä vastaava sarja.

Esimerkki: “Mikä on sarjan $a_{n+1} = 2a_n + 1 \parallel n \geq 0 \wedge a_0 = 0$ n :s alkio?”

1. Valitaan ja nimetään sarjaan “sovitettava” emäfunctio – valitaan tässä: $A(x) = \sum_{n=0}^{\infty} a_n x^n$ (eli tavallinen emäfunctio)
2. Esitetään molemmat puolet $A(x)$:n avulla (sitien, ettei yhtään a_n :ää jää jäljelle). Aloiteetaan kertomalla x^n :llä ja summataan sitten $[0, \infty]$ yli.

$$\text{(vasen)} a_{n+1} : \sum_{n \geq 0} (a_{n+1}) x^n = \left(\sum_{n \geq 0} a_n x^n - a_0 \right) / x = \frac{1}{x} \sum_{n \geq 0} a_n x^n = A(x) / x$$

$$\text{(oikea)} 2a_n + 1 : 2 \sum_{n \geq 0} a_n x^n + \sum_{n \geq 0} x^n = 2A(x) + \frac{1}{1-x}$$

3. Ratkaistaan $A(x)$:n suhteen:

$$\begin{aligned} A(x)/x &= 2A(x) + \frac{1}{1-x} \Rightarrow \left\| \cdot x \right. \\ (1-2x)A(x) &= \frac{x}{1-x} \Rightarrow \\ A(x) &= \frac{x}{(1-x)(1-2x)} \end{aligned}$$

4. Etsitään saadulle emäfunctiolle sarjaesitys. Käytetään osamurtokehitelmää (Heaviside) ja potenssisarjojen laskusääntöjä:

$$\begin{aligned} \frac{x}{(1-x)(1-2x)} &= x \left(\frac{A}{1-x} + \frac{B}{1-2x} \right) \\ &= x \left(\frac{-1}{1-x} + \frac{2}{1-2x} \right) \left\| y=2x: \frac{1}{1-y} \Rightarrow \sum_{n \geq 0} y^n = \sum_{n \geq 0} (2x)^n \right. \\ &= x \left(- \sum_{n \geq 0} x^n + 2 \sum_{n \geq 0} 2^n x^n \right) = x \left(\sum_{n \geq 0} 2^{n+1} x^n - \sum_{n \geq 0} x^n \right) \\ &= \sum_{n \geq 0} (2^{n+1} - 1) x^{n+1} = \sum_{n \geq 0} (2^n - 1) x^n \end{aligned}$$

Viimeisestä summasta nähdään suoraan, että emäfunctio sarjaesityksen n :s kerroin, eli alkuperäisen sarjan a_n , on $2^n - 1$.

9.7 Permutaatioryhmät ja ekvivalenssiluokat

Tulkitaan geometrisen objektin (esim. neliön) eri värisiksi värjättyjen kärkien kiertoja ja peilauksia/3D-rotatiota (eli *liikeryhmää*) permutaatioina ja lasketaan montako erinäköistä objektia voidaan tehdä jos niitä saadaan pyöritellä vapaasti. Määritelmiä:

- *symmetrinen ryhmä* S_n on bijektioiden $\pi: A \rightarrow A$, kun $|A| = n$ muodostama algebrallinen ryhmä (ts. n :n alkion kaikkien erilaisten permutaatiofunktioiden ryhmä)

- *permutaatioryhmä* tarkoittaa S_n :n aliryhmää, ts. $G = \{\pi_1, \dots, \pi_k\}$, vaikka olisikin $k < n$
- tulo $\pi_1 \pi_2$ ("tyhjä operaattori") tarkoittaa yhdistettyä (2 peräkkäin tehtyä) permutaatiota
- permutaatioryhmä ei ole kommutatiivinen (aabelin ryhmä), jos $n \geq 3$. Suomeksi: permutaatioiden järjestyksen vaihtaminen voi muuttaa tulosta.
- *Caley'n lause*: "jokainen ryhmä voidaan esittää permutaatioryhmänä" eli sille on isomorfismi viimeistään S_n :ään (ja usein jo S_m :ään, missä $m < n$).
- *permutaation matriisiesitys*: $\pi = \begin{pmatrix} 12345 \\ 23154 \end{pmatrix}$, josta näkee mikä alkio vaihtuu minkäkin paikalle.
- Toinen esitystapa: *erillisten syklien tulo* eli *erilliset esittäjät*: $\pi = (123)(45)$ (sama permutaatio π kuin edellisen esimerkin matriisissa). Tässä edellinen vaihtuu aina seuraavan paikalle ja viimeinen pyörähtää ensimmäisen tilalle. Esim: $(1234) = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix}$. Yhden mittainen sykli = alkio ei vaihda paikkaa.

Kun merkitään kärkien eri väritystapoja (konfiguraatioita) C_i :llä (neliön ja kahden värin tapauksessa niitä on yhteensä $2^4 = 16$ kpl: $S = \{c_1, \dots, c_{16}\}$) ja permutaatioita π_i :llä (neliön tapauksessa 8 kpl, kun lasketaan erilaiset kierrot ja peilaukset: $G = \{\pi_0, \dots, \pi_7\}$, missä $\pi_0 = 360^\circ$ kierto = "ei muutosta"), niin:

- *Ekvivalenssiluokka* on niiden väritystapojen c_i joukko, jotka voidaan muttaa toistensa näköisiksi G :n permutaatioilla. Ts. ekvivalenssiluokkien määrä = "oikeasti erilaisten" väritysten määrä.
- Väritystavan $c \in S$ *G-rata* on niiden väritystapojen joukko, joiden näköisiksi G :n permutaatiot voivat c :n muuttaa. Sen π -rata ($\pi \in G$) taas on niiden väritysten joukko, joiksi ryhmä $\langle \pi \rangle$ (eli π :n potenssien muodostama G :n aliryhmä) voi sen muuttaa.
- Värityksen/konfiguraation c *stabilisaattori* on aliryhmä $G_x \subseteq G$, jonka sisältämät permutaatiot eivät muuta c :stä lainkaan
- G :n *kiintopiste* on jokin c , joka ei muutu millään permutaatiolla $\pi_i \in G$. Tasaväritykset ovat tietysti aina kiintopisteitä.
- *Burnsiden lemma*: $\frac{1}{|G|} \sum_{\pi \in G} \Psi(\pi) =$ ekvivalenssiluokkien määrä, kun $\Psi(\pi) =$ " π :tä sovellettaessa muuttumattomien konfiguraatioiden määrä".
Esimerkki: "monellako tavalla 6 ihmistä voi sijoittaa pyöreän pöydän ympärille?". $\pi_i = i \cdot 60^\circ$ kierto, kun $i = [0, 5]$. Erilaisia konfiguraatioita pyörittämättömälle pöydälle on $6!$, joten $\pi_0 = 0^\circ \Rightarrow \Psi(\pi_0) = 6!$ ja koska kukaan ei pysy paikallaan vähänkään pyöritettäessä, $\Psi(\pi_{i>0}) = 0$. Vastaus: $\frac{1}{6} (6! + 0 + 0 + 0 + 0 + 0) = 5! = 120$. (Yleisesti: *syklinen järjestys* voidaan valita $(n-1)!$ tavalla.)
- *Sykli-indeksi* helpottaa laskemista: $\pi = (1)(2)(3)(4)$:n sykli-indeksiesitys on x_1^4 , $\pi = (1234)$:n esitys on x_4^1 ja esim. $\pi = (12)(3)(4)(5)$:n on $x_2^1 x_1^3$. Sykli-indeksi...

$$P_G(x_1, \dots, x_k) = \frac{1}{|G|} [\text{esitysten summa}]$$

...antaa m :n eri värin värityksen ekvivalenssiluokkien määrän sijoituksella $P_G(m, m, \dots)$.

- *Polyan lause*: kun on käytettävissä m eri väriä, erilaisten väritysten *inventaarille*, eli eri kombinaatioiden määrien luetteloinnille, saadaan emäfunktio sijoituksella...

$$P_G((v_1 + \dots + v_m), (v_1^2 + \dots + v_m^2), \dots, (v_1^k + \dots + v_m^k))$$

...missä v_i on väriä i esittävä muuttuja. Huom: v_i :n ei sijoiteta mitään vaan tulos katsotaan kertoimista, koska kyseessä on emäfunktio.

Esim.: "Montako eri tapaa on värittää 3-lapainen potkuri kun väreinä on r,g ja b?"
 Permutaatioryhmä $G = \{(1)(2)(3), (123), (132)\}$ eli kierrot 0° , 120° ja 240° , joiden sykli-
 indeksiesitykset ovat x_1^3, x_3^1 ja x_3^1 . Inventaario-emäfunktio saadaan siis seuraavasti:

$$\begin{aligned} P_G(x_1, x_2, x_3) &= \frac{1}{3}(x_1^3 + 2x_3) \Rightarrow \\ P_G((r+g+b), (r^2+g^2+b^2), (r^3+g^3+b^3)) &= \frac{1}{3} \left((r+g+b)^3 + 2(r^3+g^3+b^3) \right) \\ &= r^3 + r^2g + r^2b + rg^2 + 2rgb + rb^2 + \\ &\quad g^3 + g^2b + gb^2 + b^3 \end{aligned}$$

Polynomista nähdään, että on 2 eri tapaa (termi $2rgb$) kun käytetään kaikkia kolmea väriä (ja 1 tapa kaikilla muilla värikombinaatioilla). Termien kertoimia voi usein laskea multinomilauseen avulla kertomatta koko polynomia auki.

10 Jaollisuus ja moduloaritmetiikka

- Jos a on jaollinen b :llä, sanotaan " b jakaa a :n" ja merkitään: $b|a$. Jos $a \neq b$, jakaa sanotaan b :n jakavan a *aidosti* (vrt. "aito osajoukko (\subset vs. \subseteq)").
- *Alkuluku* on luku, jolla ei ole yhtään 1:stä poikkeavaa aitoa tekijää.
- *Aritmetiikan peruslause*: jokainen positiivinen kokonaisluku $n \in \mathbb{Z}^+$ voidaan esittää yksikäsitteisesti alkulukujen tulona (eli $n = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_k^{s_k} \parallel s_k \in \mathbb{Z}^+$) \Rightarrow jokainen ei-alkuluku on jaollinen jollain alkuluvu(i)lla

10.1 Jaollisuussääntöjä

- $(a|b) \wedge (b|c) \Rightarrow (a|c)$
- $(a|b) \Rightarrow (a|bc)$
- Jos $x = y + z$ ja a jakaa kaksi muuttujista, jakaa se kaikki kolme.
- Jos a jakaa luvut $c_1 \dots c_n$, jakaa se myös näiden lineaarikombinaatiot: $a|(c_1 x_1 + \dots + c_n x_n)$.
- Luvut a ja b ovat *suhteellisia alkulukuja* eli keskenään jaottomia, jos niiden suurin yhteinen tekijä on 1 eli $(a, b) = 1$ eli on olemassa $x, y \in \mathbb{Z}$ siten, että $ax + by = 1$.

10.1.1 Suurin yhteinen tekijä (GCD) ja pienin yhteinen jaettava (LCM)

Suurin yhteinen tekijä (*sy*t tai *gcd*, Greatest Common Denominator) merkitään (a_1, \dots, a_n) tai $\text{sy}(a_1, \dots, a_n)$ ja on suurin luku d , joka jakaa kaikki a_i eli $\forall i: d|a_i$. Kahdelle muuttujalle voidaan merkitä myös $d = ax + by$, missä $x, y \in \mathbb{Z}$.

S.y.t löytyy *Euklideen algoritmilla*: jaetaan joka askeleella jäljellä oleva luku edellisen askeleen jakojäännöksellä ja lopetetaan kun jäännöksestä tulee 0. Viimeinen ei-nolla jäännös on s.y.t. Algoritmi toimii myös useammalle kuin kahdelle luvulle, sillä $(a, b, c) = ((a, b), c)$. Esim. $d = (116298, 461952) = 18$:

$$\begin{aligned} 461952 &= 3 \cdot 116298 + 113058 \\ 116298 &= 1 \cdot 113058 + 3240 \\ 113058 &= 34 \cdot 3240 + 2898 \\ 3240 &= 1 \cdot 2898 + 342 \\ 2898 &= 8 \cdot 342 + 162 \\ 342 &= 2 \cdot 162 + 18 \\ 162 &= 9 \cdot 18 + 0 \end{aligned}$$

Lineaarikombinaatioesityksen $d = ax + by$ kertoimet x ja y (ja sen avulla Diophanteen yhtälön ratkaisun) löytää tästä peruuttamalla. Aluksi ratkaistaan ketjun toiseksi viimeinen rivi jakojäännöksen suhteen, sitten ratkaistaan edellinen rivi samalla tavalla, yhdistetään ne ja supistetaan, ratkaistaan kolmanneksi viimeinen rivi ja jatketaan samaan tapaan alkuun asti:

$$\begin{aligned} 342 - 2 \cdot 162 &= 18 \\ 2898 - 8 \cdot 342 &= 162 \Rightarrow 342 - 2 \cdot (2898 - 8 \cdot 342) = 18 \\ &\Rightarrow -2 \cdot 2898 + 17 \cdot 342 = 18 \\ 3240 - 1 \cdot 2898 &= 342 \Rightarrow -2 \cdot 2898 + 17 \cdot (3240 - 1 \cdot 2898) = 18 \\ &\Rightarrow 17 \cdot 3240 - 19 \cdot 2898 = 18 \\ 113058 - 34 \cdot 3240 &= 2898 \Rightarrow 17 \cdot 3240 - 19 \cdot (113058 - 34 \cdot 3240) = 18 \\ &\Rightarrow -19 \cdot 113058 + 663 \cdot 3240 = 18 \\ 116298 - 1 \cdot 113058 &= 3240 \Rightarrow -19 \cdot 113058 + 663 \cdot (116298 - 1 \cdot 113058) = 18 \\ &\Rightarrow 663 \cdot 116298 - 682 \cdot 113058 = 18 \\ 461952 - 3 \cdot 116298 &= 113058 \Rightarrow 663 \cdot 116298 - 682 \cdot (461952 - 3 \cdot 116298) = 18 \\ &\Rightarrow -682 \cdot 461952 + 2709 \cdot 116298 = 18 \\ &\Rightarrow x = 2709 \wedge y = -682 \end{aligned}$$

Pienin yhteinen jaettava (*pyj* tai *lcm*, Least Common Multiple) merkitään $[a_1, \dots, a_n]$ tai $\text{pyj}(a_1, \dots, a_n)$ ja on pienin luku, jonka kaikki a_i jakavat eli $\forall i: a_i | c$.

$$\bullet \quad a \cdot b = \text{syt}(a, b) \cdot \text{pyj}[a, b] \Rightarrow \text{pyj}[a, b] = \frac{a \cdot b}{\text{syt}(a, b)}$$

10.1.2 Lineaariset Diophanteen yhtälöt

Diophanteen yhtälö on yhtälö, jonka ratkaisuksi sallitaan vain kokonaislukuja. Lineaarinen kahden muuttujan versio: $ax + by = c$, jossa $a, b, c \in \mathbb{Z}$.

- Ratkaisuja on olemassa (äärettömästi) joss $\text{syt}(a, b) | c$.
- Yksittäisratkaisun $x = x_0, y = y_0$ jälkeen yleisen ratkaisun saa kaavalla

$$\begin{cases} x = x_0 + n b' \\ y = y_0 - n a' \end{cases}$$

...missä a' ja b' tarkoittavat s.y.t:llä (a, b) jaettuja versioita kertoimista. Huom! x :n kohdalla on b ja y :n kohdalla a eikä päinvastoin!

- Yksittäisratkaisun saa mekaanisesti ratkomalla Euklideen algoritmin jälkeen peruutuksella x :n ja y :n yhtälöstä $ax + by = \text{syt}(a, b)$ ja kertomalla ne sitten $c/\text{syt}(a, b)$:llä. Esim: ratkaistaan $116298x + 461952y = 2754$:
 1. Etsitään edellisen kappaleen Euklid-esimerkin mukaan $\text{syt}(116298, 461952) = 18$
 2. Etsitään peruutustekniikalla ratkaisut $x = 2709 \wedge y = -682$ väliaikaiselle yhtälölle $116298x + 461952y = 18$ (myöskin edellisen kappaleen esimerkin mukaan)
 3. Todetaan, että $2754/18 = 153$ ja sen perusteella, että $153 \cdot (-682 \cdot 461952 + 2709 \cdot 116298) = 18 \cdot 153$ eli $x = 2709 \cdot 153 = 414477 \wedge y = -682 \cdot 153 = -104346$

10.2 Kongruenssi eli moduloaritmetiikka

- "*kongruenssi modulo n* " merkitään $a \equiv b \pmod{n}$ ja tarkoittaa, että $a \pmod{n} = b \pmod{n}$ eli $n | (a - b)$
- *Kongruenssiluokka* (eli *jäännösluokka* eli *ekvivalenssiluokka*) merkitään $[n]$, ja se tarkoittaa kongruenssiaritmetiikan numeroa. Esim: $[3] \cdot [8] = [6]$ modulin 9 suhteen (koska $3 \cdot 8 = 24$ ja $24 \pmod{9} = 6$)
- Kongruenssiluokan *käänteisloukka* $[x]^{-1}$ on $[y]$ siten, että $[x] \cdot [y] = [1]$. Esim: $[3]^{-1} = [5] \pmod{7}$, koska $(3 \cdot 5) \pmod{7} = 1$
- *Kongruenssiyhtälö* $ax \equiv b \pmod{n}$ vastaa Diophanteen yhtälöä $ax - ny = b$.
- Kongruenssiaritmetiikka tietyllä modulolla n vastaa algebrallista rengasta (tai kun n on alkuluku niin kuntaa) \mathbb{Z}_n (ks. "renkaat ja kunnat" kappaleesta "abstrakti algebra").
- Käänteisloukka on olemassa kaikille luokille joss n (=moduli) on alkuluku. Tällöin vain 1 ja -1 ovat itsensä käänteisalkioita (ts. $a^2 \equiv 1 \pmod{n}$). Muillakin moduleilla voi kyllä olla yksittäisiä käänteistyviä luokkia.
- *Korkea potenssi modulo m* lasketaan ottamalla välituloksista jakojäännös ja jatkamalla siitä. Tehokas tapa $a^N \pmod{m}$:n laskemiseen on laskea ensin $a^2, a^4, a^8, a^{16}, \dots$ peräkkäisillä neliöinneillä ja kertoa niitä sitten yhteen N :n binääriesityksen mukaan ottamalla mod m joka askeleen jälkeen.
- *Wilsonin lause*: $(p - 1)! \equiv -1 \pmod{p}$, kun p on alkuluku. Ei ole käytännöllinen alkulukutesti, koska kertoman laskeminen on hidasta.
- *Fermat'n pieni lause*: $a^{p-1} \equiv 1 \pmod{p}$, kun (ei joss!) p on alkuluku ja $p \nmid a$ (ts. p ei ole a :n tekijä, ts. $\text{syt}(a, p) = 1$)
- *Eulerin φ -funktio* $\varphi(n)$ on alkoiden $a_i \leq n$, joille $\text{syt}(a_i, n) = 1$, eli n :ää pienempien suhteellisten alkulukujen, määrä. Sääntöjä:
 - $\varphi(p) = p - 1$ joss p on alkuluku. Tällöin myös: $\varphi(p^a) = p^a - p^{a-1}$

- jos $\text{syt}(m, n) = 1$, niin $\varphi(mn) = \varphi(m)\varphi(n)$
- $\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$ (kun $n = \prod_1^k p_i^{a_i}$) eli n :n alkutekijöistä
- *Eulerin lause*: $a^{\varphi(n)} \equiv 1 \pmod{n}$, kun $\text{syt}(a, n) = 1$. (Jos $n = p$, saadaan $a^{p-1} \equiv 1 \pmod{p}$.)

10.3 Suuret alkuluvut

- Alkulukuja on äärettömän paljon.
- On olemassa sekä *alkulukukaksosia*, joiden erotus on 2, että mielivaltaisen pitkiä lukujoja joissa ei ole yhtään alkulukua.
- Luvun $n \in \mathbb{Z}$ hajottaminen alkutekijöihin on erittäin raskas operaatio. Huomioita:
 - Jos pienillä alkuluvuilla testatessa tulee osuma, ts. $\frac{n}{p} = k \in \mathbb{Z}$, hakua k :lle pitää jatkaa p :stä (sama tekijä voi esiintyä useita kertoja)
 - n :n alkutekijöissä voi olla max. 1 alkuluku $p > \sqrt{n}$. Kaikki muut ovat tätä pienempiä $\Rightarrow n$ on alkuluku ellei \sqrt{n} mukaan lukien ole löytynyt yhtään tekijää
 - Tehokkain tunnettu tekijöintialgoritmi on työmäärältään $O(e^{\sqrt{\log n \cdot \log(\log n)}})$
- Fermat'n pienellä lauseella ($b^{n-1} \equiv 1 \pmod{n}$, kun n on alkuluku) voi usein todeta, että n ei ole alkuluku, mutta se ei ole pitävä testi.
- ”*Pseudoalkuluku* kannassa b ” on jaollinen luku n , joka läpäisee Fermat'n pienen lauseen testin ja jolle $\text{syt}(n, b) = 1$. Niitäkin on äärettömän monta, mutta paljon harvemmassa kuin oikeita alkulukuja.
- *Carmichaelin luku* on pseudoalkuluku kaikissa kannoissa $b \geq 2$. Erittäin harvinaisia, mutta niitäkin oletetaan olevan äärettömästi. \Rightarrow Fermat'n pieni lause ei teoriassakaan ole aivan täydellinen alkulukutesti.
- *Millerin testi*: pariton n ei ole alkuluku jos, kun $d \in \mathbb{N}^+$ on pariton, joko:
 1. $b^d \not\equiv 1 \pmod{n}$ tai
 2. $b^{d \cdot 2^s} \not\equiv -1 \pmod{n}$ jollekin $s \in \mathbb{N}^+$
- ”*Vahva pseudoalkuluku* kannassa b ” on jaollinen luku n , joka läpäisee Millerin testin kannassa b . Vain oikeat alkuluvut läpäisevät testin kaikissa kannoissa $\text{syt}(b, n) = 1$.
- *Rabinin todennäköisyystesti*: todennäköisyys sille, että jaollinen luku n on vahva pseudoalkuluku kaikissa kannoissa $b_i < n \parallel i \in [1, k]$ on pienempi kuin $1/4^k$.

10.3.1 RSA-salakirjoitus

- Avaimien luonti: valitaan kaksi alkulukua $q \neq r$ ja lasketaan niiden tulo $n = q \cdot r$.
 - Julkinen avain eli salakirjoitusavain on pari (e, n) , missä e on jokin luku, jolle $\text{syt}(e, \varphi(n)) = 1$.
 - Salainen avain eli purkuavain on pari (d, n) , missä $d \equiv e^{-1} \pmod{\varphi(n)}$.
- Viesti muutetaan/jaetaan lohkoiksi $0 \leq P < n$
- Salaus: $E(P) \equiv P^e \pmod{n}$
- Purku: $P \equiv E(P)^d \pmod{n}$
- Allekirjoituksessa käytetään avaimia nurinperin: salataan purkuavaimella ja puretaan salausavaimella.
- Luvuilla $q - 1$ ja $r - 1$ pitää olla suuria tekijöitä ja q :n ja r :n on oltava jonkin verran eri pituisia, ettei $\varphi(n) = (q - 1)(r - 1)$ ratkea liian helposti. Luvut ovat niin suuria, että käytännössä sovelletaan Rabinin todennäköisyystestiä, koska täydellisen Millerin testin ajo kestäisi liian kauan.

11 Graafit

- *Silmukka* (loop) on sivu, joka alkaa ja päättyy samaan solmuun (**älä** sekoita kierrokseen (cycle)!)
- *Kierros* on *polku*, jonka alku- ja loppusolmu ovat samat
- *Lineaarinen* eli *yksinkertainen* graafi on sellainen, jossa jokaista mahdollista sivua on korkeintaan yksi eikä siinä ole yhtään silmukkaa - ei-lineaarinen graafi on *multigraafi*
- Kaksi solmua ovat *naapureita*, jos niiden välillä on sivu
- Kaksi solmua on *yhdistetty*, jos niiden välillä on jokin polku
- Graafi on *täydellinen*, joss kaikki kärjet on yhdistetty kaikkiin muihin kärkiin
- Graafin G ja sen aligraafin $G_1 \subset G$ *komplementti* $G - G_1$ on muuten sama kuin G , mutta siitä on poistettu G_1 :n sivut
- Graafi on *yhtenäinen*, jos kaikkien solmujen välillä on polku
- *Puu* on suunnistamaton, lineaarinen, yhtenäinen, kierrokseton graafi, *metsä* muuten sama, mutta ei yhtenäinen
- Suunnistamattoman graafin *kärjen aste* on siihen tulevien sivujen määrä - suunnistetulle on määritely erikseen *tuloaste* ja *lähtöaste*.
- Graafit ovat *isomorfisia* ($G_1 \sim G_2$), jos niillä on sama rakenne (eli voidaan määritellä kääntäen yksikäsitteiset funktiot, jotka mappaavat solmut ja sivut graafista toiseen)
- Graafin *sulkeuma* C^n on yleistetyn naapurimatriisin n :s potenssi ja ilmaisee solmusta toiseen olevien n -pituisten polkujen määrän
- Graafien *konfiguraatio* on sama, jos ne ovat isomorfisia kun molemmista poistetaan ne ja poistetaan astetta 2 olevat kärjet
- *Eulerin polku* käsittää kaikki **sivut** tasan kerran (vastaavasti *Eulerin kierros*)
- *Hamiltonin polku* käsittää kaikki **solmut** tasan kerran (vastaavasti *Hamiltonin kierros*)

11.1 Lauseita

- Eulerin *kierros* suunnistamattomassa graafissa on olemassa joss graafi on yhtenäinen ja kaikkien solmujen asteet ovat parillisia. Eulerin *polku* joss tasan kaksi paritonta kärkeä (jotka voitaisiin periaatteessa yhdistää, jolloin saadaan kierros).
- Hamiltonin polulle/kierrokselle ei ole yksikäsitteistä olemassaololausetta, mutta:
 - polkua ei ole ainakaan, jos on yli 2 kärkeä, joiden aste ≤ 1
 - kierros on olemassa ainakin, jos kaikkien kärkien aste $\geq \frac{\text{solmuja}}{2}$
- Graafi on *tasograafi* (eli levitettävissä tasoon ilman leikkaavia sivuja) joss se ei sisällä kaksijakoisen graafin $K_{3,3}$ (3+3 solmua kahdessa rivissä, ylärivin kaikki solmut yhdistetty kaikkiin alarivin solmuihin mutta ei toisiin ylärivin solmuihin, ts. 9 sivua) eikä täydellisen 5-graafin K_5 konfiguraatiota. (=Kuratowskin lause)
- Yhtenäinen tasograafi rajaa tasolle $r = e - v + 2$ aluetta, ääretön alue mukaan lukien (=Eulerin kaava)
- Jos tasograafissa on yli 1 sivu ja tasoalueita r kpl, on $3r \leq 2e$ ja $e \leq 3v - 6$.
- Jos graafin kaikkien kärkien aste on n , voi sivujen määrän laskea kaavalla $e = n v / 2$, sillä "jokainen kärki on yhteinen n :lle sivulle ja yhden sivun määräämiseen tarvitaan kaksi kärkeä".

11.2 Algoritmeja (ei-negatiivisesti) painotetuille graafeille

Seuraavat klassiset graafialgoritmit ovat ns. *ahneita algoritmeja*:

- *Primin algoritmi* minimaalisen virittäjäpuun hakemiseen (eli priority first search): ensin lisätään jonoon kaikki naapureihin johtavat sivut joiden paino on pienempi kuin jo jonossa ehkä olevan, samaan solmuun johtavan sivun, sitten valitaan jonosta pienimmän painoinen sivu ja toistetaan kunnes kaikki solmut on käyty läpi.
- *Dijkstran minimipolkualgoritmi*: kuin Primin algoritmi, mutta lähdetään tietyistä solmista, lisätään jonoon aina painojen *summa* (eikä pelkästään sivun omaa painoa) ja lopetetaan kun tultu kohdesolmuun.
- *Kruskalin algoritmi* minimaalisen viritäjäpuun hakemiseen: valitaan yksitellen pienin jäljellä oleva sivu, joka ei muodosta kierrosta jo valittujen kanssa. (Kierrostarkistus voidaan tehdä merkitsemällä jokaiseen sivuun mihin tulostetsän puuhun se kuuluu ja yhdistämällä vain eri alipuita keskenään. Alipuiden yhdistämisessä toisen puun tunnus aina hävitetään, joten lopuksi on jäljellä vain yksi puu.)

11.3 Kaksijakoinen graafi (bipartite graph)

- Graafi on kaksijakoinen joss se voidaan jakaa kahteen joukkoon siten, että sivuja on vain niihin kuuluvien kärkien välillä (ei siis saa olla esim. kierroksia)
- Kärjet piirretään yleensä kahteen riviin niin, että joukon 1 (X) kärjet ovat ylhäällä ja joukon 2 (Y) alhaalla.
- Tyypillinen käyttöesimerkki on avioliitto-/opiskelupaikkaongelma, jossa henkilöt X luettelevat heille kelpaavat puoliset/koulut Y :stä (ts. preferenssit esitetään sivuina) ja sitten yritetään löytää kaikille sopiva järjestely.
- Kaksijakoisen graafin *sovitus* on joukko sivuja, joilla ei ole yhteisiä kärkiä
- Sovitus on *maksimaalinen*, jos ei ole olemassa enemmän sivuja sisältäviä sovituksia.
- X :n jonkin osajoukon $A \subseteq X$ *ulottuvuus* $R(A)$ on kaikkien siihen sivuilla kytkettyjen Y -kärkien joukko.
- Osajoukon A *vaje* on kokonaisluku $\delta(A) = |A| - |R(A)|$. Huom: voi olla negatiivinen!
- Koko *graafin vaje* $\delta(G)$ on kaikkien X :n osajoukkojen vajeiden maksimi. Koska niihin kuuluu myös tyhjä joukko ja $\delta(\emptyset) = 0$, on $\delta(G) \geq 0$.
- Graafin *täydellinen sovitus* on sellainen, jossa jokaisesta X :n kärjestä lähtee sivu ja sellainen on olemassa joss $|R(A)| \geq |A|$ kaikille $A \subseteq X$ (eli $\delta(G) = 0$). Täydellisen sovituksen etsimiseen on olemassa useita ns. polunlaajennusalgoritmeja. Tässä eräs:

Käydään läpi kaikki kärjet $x \in X$:

Jos x :lle ei ole jo valittu esittäjä sivua:

Käydään läpi x :ään yhdistetyt kärjet $y \in Y$ jotka eivät jo kuulu sovitukseen:

Jos löytyy y :hyn yhdistetty kärki $x_2 \in X$ joka ei jo kuulu sovitukseen:

Lisätään sivu $x_2 \rightarrow y$ sovitukseen ja palataan uloimpaan silmukkaan

- Jos X -kärjet korvataan joukoilla ja Y -kärjet niistä yhteen tai useampaan kuuluvilla alkioilla (ts. ei käsitellä enää varsinaista graafia vaan merkitään "preferenssejä" esim. $x_1 \sim \{y_1, y_2\}$, $x_2 \sim \{y_1\}$), puhutaan täydellisen sovituksen sijaan joukkojen $x_{1\dots n}$ *esittäjäsystemistä*.
- Joskus sivuihin yhdistetään *painot*, jolloin yleinen ongelma on etsiä joko painojen summan maksimoiva (tai minimoiva) sovitus. Siihen sopii mm. *unkarilainen algoritmi*, joka iteroi graafin matriisiesitystä (sivujen painot matriisialkioina).

12 Sekalaisia laskutekniikoita

12.1 Induktiotodistus

1. Julistetaan *induktiohypoteesi* (esim. $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$)
2. *Induktion perusta*: osoitetaan, että $P(0)$ (tai $P(1)$ tai joku muu helppo tapaus) on tosi (esim. $[2^0 = 1] = [2^{0-1} + 1 = 2 - 1 = 1]$).
3. *Induktioaskel*: osoitetaan, että jos induktiohypoteesi (tai -oletus) $P(n)$ on tosi, myös $P(n + 1)$ on tosi sijoittamalla $P(n)$:n toinen puoli $P(n + 1)$:n sisään ja pyörittelemällä algebrallisesti. Esim.

$$\begin{aligned} \underbrace{2^0 + 2^1 + \dots + 2^n}_{\text{hypot. mukaan } 2^{n+1} - 1} + 2^{n+1} &= 2^{(n+1)+1} - 1 \\ (2^{n+1} - 1) + 2^{n+1} &= 2^{n+2} - 1 \parallel + 1 \\ 2^{n+1} + 2^{n+1} &= 2^{n+2} \\ 2^{(n+1)+1} &= 2^{n+2} \parallel \log_2 \\ n + 2 &= n + 2 \end{aligned}$$

12.2 Neliöksi täydentäminen

$$x^2 + bx = \left(x + \frac{b}{2}\right)^2 - \left(\frac{b}{2}\right)^2$$

Esim. *toisen asteen yhtälön ratkaisukaavan johtaminen*:

$$\begin{aligned} ax^2 + bx + c &= 0 \\ x^2 + \frac{b}{a}x &= -\frac{c}{a} \\ \left(x + \frac{b}{2a}\right)^2 &= \frac{b^2}{4a^2} - \frac{4a}{4a} \cdot \frac{c}{a} = \frac{b^2 - 4ac}{4a^2} \\ x + \frac{b}{2a} &= \pm \frac{\sqrt{b^2 - 4ac}}{\sqrt{4a^2}} \\ x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

12.3 Osamurtokehitemä

Jokaiselle rationaalifunktiolle $\frac{N(x)}{D(x)}$ (N on alemmaa astetta kuin D) voi muodostaa *osamurtokehitemän* $\frac{A_1}{P_1(x)} + \dots + \frac{A_n}{P_n(x)}$ missä termit ovat muotoa $\frac{a}{(x+b)^n}$ tai $\frac{bx+c}{(x^2+px+q)^m}$ ja $a, b, c, p, q \in \mathbb{R}$ ja $n, m \in \mathbb{N}$ (jos sallitaan $a, b \in \mathbb{C}$, jälkimmäistä muotoa ei tarvita). Kehitelmästä on hyötyä varsinkin integroinnissa.

Aluksi faktoroidaan nimittäjä ensimmäisen tai toisen asteen termeihin kaavalla $a x^2 + b x + c = a (x - x_1) (x - x_2)$ (tai sen suoraviivaisella laajennuksella korkeamman asteen polynomeille). Hajotelman termit määräytyvät saatujen tekijöiden mukaan – tapauksia on kolme:

1. reaalinen ($a \in \mathbb{R}$), ei-toistuva juuri \Rightarrow lineaarinen nimittäjä, vakioarvoinen osoittaja:

$$\frac{\dots}{\dots \cdot (x+a) \cdot \dots} = \dots + \frac{A}{x+a} + \dots$$

2. imaginäärinen juuri \Rightarrow toisen asteen nimittäjä, lineaarinen osoittaja:

$$\frac{\dots}{\dots \cdot (x^2+px+q) \cdot \dots} = \dots + \frac{Bx+C}{x^2+px+q} + \dots$$

3. n -kertainen juuri $\Rightarrow n$ termiä, joissa nimittäjän aste laskee:

$$\frac{\dots}{\dots \cdot (x+a)^n \cdot \dots} = \dots + \frac{A_1}{(x+a)^n} + \frac{A_2}{(x+a)^{n-1}} + \dots + \frac{A_n}{x+a} \text{ tai}$$

$$\frac{\dots}{\dots \cdot (x^2+px+q)^n \cdot \dots} = \dots + \frac{B_1x+C_1}{(x^2+px+q)^n} + \frac{B_2x+C_2}{(x^2+px+q)^{n-1}} + \dots + \frac{B_nx+C_n}{x^2+px+q}$$

Hajotelman termien osoittajiin tulevat vakiot (A, B, C) eli *residy* (eng. *residue*) voidaan laskea monella tavalla. Seuraavat kolme tapaa on esitetty kahden eri suuren, reaalisen juuren avulla (ts. $\frac{\dots}{(x+a)(x+b)}$, $a \neq b$), mutta ne toimivat myös korkeamman asteen tapauksissa (ts. $\frac{\dots}{(x-a_1)\dots(x-a_n)}$). Heavisiden menetelmää lukuunottamatta ne toimivat myös moninkertaisille ja epälinearisille tapauksille.

12.3.1 Tapa 1: $x:n$ valitseminen strategisesti

Lavennetaan osamurrot samannimisiksi alkuperäisen kanssa, eliminoidaan nimittäjät ja ratkaistaan osoittajista muodostuvan polynomin tuntemattomat (A, B) valitsemalla x aina siten, että se hävittää kerrallaan yhden muuttujista:

$$\frac{x-1}{(3x-5)(x-3)} = \frac{A}{(3x-5)} + \frac{B}{(x-3)} \left\| \text{lavennetaan oikea puoli} \right.$$

$$\frac{x-1}{(3x-5)(x-3)} = \frac{A(x-3)}{(3x-5)(x-3)} + \frac{B(3x-5)}{(3x-5)(x-3)} \left\| \cdot (3x-5)(x-3) \right.$$

$$x-1 = A(x-3) + B(3x-5)$$

Valitaan strategisesti $A(x-3)=0 \Rightarrow x=3$:

$$3-1 = A(3-3) + B(3 \times 3 - 5) \Leftrightarrow$$

$$2 = 4B$$

$$B = 1/2$$

Sama temppu B:lle: $B(3x - 5) = 0 \Rightarrow x = 5/3$:

$$\begin{aligned} 5/3 - 1 &= A(5/3 - 3) + B(3 \times 5/3 - 5) \Leftrightarrow \\ 2/3 &= -4/3 A \\ A &= -1/2 \end{aligned}$$

Eli:

$$\frac{x-1}{(3x-5)(x-3)} = -\frac{1}{2(3x-5)} + \frac{1}{2(x-3)}$$

12.3.2 Tapa 2: yhtälöryhmä eri asteisista termeistä

Etsitään murtofunktiota vastaava yhtälö kuten tavassa 1 ja ryhmitellään se x :n polynomiksi (tässä esimerkin vuoksi toisen asteen, vaikka ensimmäisen asteenkin riittäisi):

$$\begin{aligned} x-1 &= A(x-3) + B(3x-5) \Leftrightarrow \\ x-1 &= Ax - 3A + 3Bx - 5B \Leftrightarrow \\ 0x^2 + 1x - 1 &= 0x^2 + (A+3B)x + (-3A-5B) \end{aligned}$$

Sitten tehdään x :n eri asteisista termeistä (vakiot, x :t, x^2 :t yms) lineaarinen yhtälöryhmä:

$$\begin{aligned} 0x^2 + 1x - 1 &= 0x^2 + (A+3B)x + (-3A-5B) \parallel \text{turha} \\ 0x^2 + 1x - 1 &= 0x^2 + (A+3B)x + (-3A-5B) \\ 0x^2 + 1x - 1 &= 0x^2 + (A+3B)x + (-3A-5B) \end{aligned}$$

Ratkaistaan saatu lineaarinen yhtälöryhmä (esimerkkinä näytetty turha $x^2: 0=0$ on poistettu):

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ -3 & -5 \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 3 \\ -3 & -5 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} -1/2 \\ 1/2 \end{pmatrix}$$

12.3.3 Tapa 3: Heavisiden peittomenetelmä

Heavisiden menetelmä on helppo, mutta ei toimi moninkertaisten $((x+a)^n)$ eikä epälineaaristen $(x^2 + px + q)$ termien kanssa. Murtofunktiota ei tarvitse vääntää yhtälöksi kuten edellisissä tavoissa:

Pyyhitään vain aina yksi tekijä pois nimittäjästä ja sijoitetaan sen nolllaamiseen tarvittava vakio jäljelle jääneeseen kaavaan x :n tilalle. Poistettua tekijää vastaava residy saadaan suoraan:

$$\begin{aligned} \frac{x-1}{(3x-5)(x-3)} \parallel 3x-5=0 \Rightarrow x=5/3 \\ \frac{5/3-1}{5/3-3} = A = -1/2 \\ \frac{x-1}{(3x-5)(x-3)} \parallel x-3=0 \Rightarrow x=3 \\ \frac{3-1}{3 \cdot 3-5} = B = 1/2 \end{aligned}$$

12.4 Logaritmi

- Määritelmä: $\log_a x = y \Leftrightarrow a^y = x$ eli "mihin potenssiin a pitää korottaa, että saadaan x "
- Ehdot: *kantaluvulle* $a > 0, a \neq 1$ ja *numerukselle* $x > 0$
- $\log x^r = r \log x$
- $\log a b = \log a + \log b$
- $\log \frac{x}{y} = \log x - \log y$
- $a^{\log_a x} = x$. Esim. $e^{\ln x} = x$.
- $\log_a 1 = 0$
- $\log_a a = 1$
- $\log_a x = \frac{\log_b x}{\log_b a}$ (eli *kantaluvun vaihto*)

12.5 Raja-arvo

- Summa, erotus, tulo ja osamäärä ovat triviaaleja:

$$\lim_{x \rightarrow a} f(x) = L \wedge \lim_{x \rightarrow a} g(x) = M \Rightarrow \lim_{x \rightarrow a} f(x) \otimes g(x) = L \otimes M$$

- $\lim_{x \rightarrow \pm\infty} \frac{1}{x} = 0$
- $\lim_{x \rightarrow \pm\infty} \frac{P(x)}{Q(x)}$:n raja-arvon saa jakamalla molemmat polynomit nimittäjän korkeimman asteen muuttujalla. Esim: $\lim_{x \rightarrow \pm\infty} \frac{2x^2 - x + 3}{3x^2 + 5} = \lim_{x \rightarrow \pm\infty} \frac{2 - \frac{1}{x} + \frac{3}{x^2}}{3 + \frac{5}{x^2}} = \frac{2}{3}$
- ääretöntä lähestyttäessä myös neliöjuuresta voi usein päästä eroon vastaavalla jakolaskulla: $\lim_{x \rightarrow \infty} \frac{x}{\sqrt{x^2 + 1}} = \lim_{x \rightarrow \infty} \frac{x}{\sqrt{x^2(1 + \frac{1}{x^2})}} = \lim_{x \rightarrow \infty} \frac{x}{\sqrt{x^2} \sqrt{1 + \frac{1}{x^2}}} = \frac{x}{|x| \cdot 1} = 1$
- polynomien raja-arvo(n merkki: $\pm\infty$) äärettömyydessä määrätty vain ja ainoastaan korkeimman asteen tekijän mukaan, koska esim. $3x^3 - x^2 + 2x = 3x^2(1 - \frac{1}{3x} + \frac{2}{3x^2})$
- jotain ei-määrättyä arvoa lähestyvän raja-arvon saa yleensä joko faktoroiden polynomeja juuriensa avulla tai viimeistäänkin muuttamalla laskun raja-arvoksi äärettömyydessä:

$$\lim_{x \rightarrow 2} \frac{x-2}{x^2-4} = \lim_{x \rightarrow 2} \frac{(x-2)(x+2)}{(x-2)(x+2)} = \lim_{x \rightarrow 2} \frac{x^2/4}{(x^2/4)(x+2)} = \lim_{x \rightarrow 2} \frac{1}{x+2} = \frac{1}{4} \text{ tai}$$

$$\lim_{x \rightarrow 2} \frac{x-2}{x^2-4} = \lim_{a \rightarrow \infty} \frac{(2 + \frac{1}{a}) - 2}{(2 + \frac{1}{a})^2 - 4} = \lim_{a \rightarrow \infty} \frac{\frac{1}{a}}{(\frac{1}{a})^2 + 4\frac{1}{a}} = \lim_{a \rightarrow \infty} \frac{1}{\frac{1}{a} + 4} = \frac{1}{4}.$$

- $\lim_{x \rightarrow \infty} \frac{x^a}{e^x} = 0 \Big/ \lim_{x \rightarrow -\infty} |x|^a e^x = 0$ eli "eksponentti voittaa potenssiin korotuksen"
- $\lim_{x \rightarrow \infty} \frac{\ln x}{x^a} = 0 \Big/ \lim_{x \rightarrow 0+} x^a \ln x = 0$, eli "potenssiin korotus voittaa logaritmin"
- l'Hospitalin 1. sääntö: $\lim_{x \rightarrow a+} f(x) = \lim_{x \rightarrow a+} g(x) = 0 \Rightarrow \lim_{x \rightarrow a+} \frac{f(x)}{g(x)} = \lim_{x \rightarrow a+} \frac{f'(x)}{g'(x)}$. Huom: toimii **vain** $[0/0]$ -muotoisille lauseille!
- l'Hospitalin 2. sääntö: $\lim_{x \rightarrow a+} g(x) = \infty \Rightarrow \lim_{x \rightarrow a+} \frac{f(x)}{g(x)} = \lim_{x \rightarrow a+} \frac{f'(x)}{g'(x)}$. Huom: toimii **vain** $[?/\infty]$ -muotoisille lauseille **ja** on käytännöllinen vain $[\infty/\infty]$ -muotoisille! Tyyppien $[0^0]$, $[\infty^0]$, $[1^\infty]$ -muotoiset voi kuitenkin muuttaa muotoon $[0/0]$ tai $[\infty/\infty]$ ottamalla logaritmin.

12.6 Trigonometrinen funktioiden ominaisuuksia

- $\sin^2 x + \cos^2 x = 1$
- $D(\arcsin x) = \frac{1}{\sqrt{1-x^2}}$
- $D(\arctan x) = \frac{1}{1+x^2}$

13 Merkintätapoja

13.1 Tavalliset lukujärjestelmät

- \mathbb{Z} = kokonaisluvut = $] -\infty, \dots, -1, 0, 1, \dots, \infty[$
- \mathbb{Z}^+ = positiiviset kokonaisluvut = $[1, \dots, \infty[$
- \mathbb{N} = luonnolliset luvut = $\mathbb{Z}^+ \cup \{0\} = [0, 1, \dots, \infty[$
- \mathbb{Q} = rationaaliluvut $\frac{p \in \mathbb{Z}}{q \in \mathbb{Z}^+}$
- \mathbb{R} = reaaliluvut
- \mathbb{C} = kompleksiluvut = $(x \in \mathbb{R}) + i (y \in \mathbb{R})$

13.2 Kreikkalaiset kirjaimet

(Roomalaisten kirjainten kanssa yhteiset merkit harmaalla, etsimisen helpottamiseksi.)

α A alfa	ν N nyy
β B beeta	ξ Ξ ksii
γ Γ gamma	o O omikron
δ Δ delta	π Π pii
ε E epsilon	ρ P rhoo
ζ Z zeeta	σ Σ sigma
η H eeta	τ T tau
ϑ Θ theeta	v Υ ypsilon
ι I ioota	φ Φ fi
κ K kappa	χ X khii
λ Λ lambda	ψ Ψ psii
μ M myy	ω Ω omega

Hakemisto

ääriarvopisteiden luokittelu	22	eksaktiksi muuttaminen	16
ääriarvotettava		eksplisiittinen	15
monen muuttujan	22	linearisointi	18
rajoitettu	22	-ryhmä, 1. asteen lin. homog.	17
2. asteen yhtälön ratkaisukaava	44	separoituva	15
abelin ryhmä	27	tasa-asteinen (homogenous)	15
affininen	13	tavallinen	15
affiniteetti	13	tavallinen 2. asteen	17
ahne algoritmi	43	differentiointi	14
aika-alue	18	Dijkstran minimipolkualgoritmi	43
algebra	27	dimensio (avaruuden)	6
alideterminanttikehitelmä	8	Diophanteen yhtälö	40
alirangas	28	distributiiosäännöt	28
alirengas		divergenssi	24
ideaali	28	divergenssilause	24
aliryhmä	27	ekvivalenssiluokka	
triviaali	27	kongruenssi	40
alkuarvo-ongelma	15	permutaatioryhmän	37
alkuluku	39	ekvivalentti koodaus	30
pseudo-	41	emäfunktio	32
vahva	41	eksponentiaalinen	32
suuri	41	tavallinen	32
alkulukuja		enumerointi	32
suhteellinen	39	epästabiili piste	17
alkulukukaksoset	41	erillisten syklien tulo	37
analyttinen	26	esittäjäsystemi	43
argumentti (kompleksiluvun)	26	Euklideen algoritmi	39
aritmetiikan peruslause	39	Eulerin	
aste		fii-funktio	40
kärjen	42	kaava	26, 42
lähtö-	42	kierros	42
tulo-	42	lause	41
attraktiivisesti stabiili	17	polku	42
avaruuspinta	21	Fermat'n pieni lause	40
Bellin luvut	31	Fibonaccin luvut	34
binomikertoimet	32	field	28
yleistetyt	32	Fii-funktio	40
binomilause	32	flux	23
bipartite graph	43	Fourier-kosinisarja	20
blokkikoodaus	30	Fourier-sarja	20
Burnsiden lemma	37	Fourier-sinisarja	20
Caleyn lause	37	fundamentaalikunta	30
Carmichaelin luku	41	funktioavaruus	6
Catalanin luvut	34	Galois-kunta	30
Cauchyn residuaalilause	26	Gaussin eliminaatio	7
Cauchyn tulo	20	Gaussin laki	24
Cauchy-Riemann	26	Gauss-Jordan	7
conformal mapping	26	gcd	39
curl	24	generoiva funktio	32
determinantti	8	generoiva matriisi	30
Wronskian	16	graafi	42
diagonaali (matriisin)	6	algoritmeja painotetuille	43
diagonalisoituvuus	9	kaksijakoinen	43
differenssiyhtälö	35	komplementti	42
differentiaali	14	lineaarinen	42
monen muuttujan funktion	21	multi-	42
osittais-	15	painotettu	43
differentiaaliyhtälö		täydellinen	42
1. kertaluvun lineaarinen	16	taso-	42
eksakti	15		

yhtenäinen	42	kommutatiivinen	27
yksinkertainen	42	kompleksiluku	26
gradientti	21, 21, 24	kompleksiluvut	48
Gram-Smidth ortonormalisointi	9	kompleksinen funktio	26
Greenin lause	23	konfiguraatio	
group	27	graafin	42
hajaantuminen	19	kongruenssi	40
Hamiltonin kierros	42	-luokka	40
Hamiltonin polku	42	-yhtälö	40
Hamming-etäisyys	30	konjugaatti	26
Hammingin matriisi	30	konservatiivinen vektorikenttä	23
Hamming-koodaus	30	koodisana	30
harmoninen (skalaarikenttä)	24	kooditeoria	30
Heavisiden menetelmä	46	korkea potenssi	40
Hessian	22	kreikkalaiset kirjaimet	48
homogeeniset koordinaatit	12	kriittinen piste	17, 22
homomorfismi	27	Kruskalin algoritmi	43
rengas-	29	kunta	28
ideaalipiste	12	fundamentaali-	30
ideaalisuora	12	Galois-	30
ideaalitaso	12	Kuratowskin lause	42
induktio		kuvaus	12
-askel	44	affini	13
-hypoteesi	44	lineaari-	12
perusta	44	kyyhkyslakkaperiaate	31
-todistus	44	lähde	24
Inklusio-eksklusio-periaate	31	lähtöaste	42
integral domain	28	Lagrangen funktio	22
integroiva tekijä	16	Lagrangen kerroin	22
inventaario	37	Lagrangen lause	28
isocline	16	Laplace-muunnos	18
isomorfinen		laplace-yhtälö	24
graafi	42	laplacian	24
isomorfismi	27	lcm	40
rengas-	29	least squares fit	13
jäännösluokka	40	Leibnizin lause	19
Jacobian-matriisi	14	liikeryhmä	36
jaollisuus	39	liittoluku	26
-sääntöjä	39	lineaarialgebra	6
johtokerroin	29	lineaarialgebran aksioomat	6
käänteisluokka	40	lineaarikombinaatio	6
kärjen aste	42	lineaarikuvaus	6, 12
kanta	6, 8, 8	lineaarinen riippumattomuus (funktioiden)	16
luonnollinen	6, 8	linearisaatio	14
ratkaisun (ODE)	16	linearisointi	18
kantaluku (logaritmin)	47	logaritmi	
kantaluvun vaihto	47	laskusääntöjä	47
karakteristinen polynomi		luonnolliset luvut	48
rekursion	35	Markovin ketju	13
karakteristinen polynomi (matriisin)	9	matriisi	
karasteristika (renkaan)	28	derivaatta	10
kernel	6, 12	eksponentti	10
kertaluku		generoiva	30
alkion	27	normalisoitu	30
differentiaaliyhtälön	15	Hessian	22
rekursion	35	Jacobian	14
ryhmän	27	käänteis-	7
ketjusääntö		ortogonaalinen	6
monen muuttujan	14	-rengas	29
kierros	42	säännöllinen	6
kiintopiste	37	singulaarinen	6
Kleinin ryhmä	28	stokastinen	13
kokonaisalue	28	tarkistus-	30
kokonaisluvut	48	tulo	6
kombinaatio	31	matriisifunktiot	9
kombinatoriikka	31	metsä	42

Millerin testi	41	projektiivinen taso	12
moduli (kompleksiluvun)	26	projektio	11
moduloaritmetiikka	39, 40	ortogonaalinen	12
monoidi	27	-säde	11
multigraafi	42	-taso	11
multinomikertoimet	32	yhdensuuntais	11
multinomilause	32	pseudoalkuluku	41
naapurisolmu	42	puoliryhmä	27
nabla	24	puu	42
napa	26	pyj	40
napakoordinaatisto	22	Rabinin todennäköisyydesti	41
neliöksi täydentäminen	44	raja-arvo	
neutraalialkio	27	laskusääntöjä	47
nollapolynomi	29	monen muuttujan	21
nollatekijä		rangi	6
aito	28	rank	6
normi (matriisin)	6	rankki	6
nullcline	16	rata	37
numerus	47	rationaaliluvut	48
ODE	15	reaaliluvut	48
ominaisarvo	9	redusoimattomuus	29
ominaisvektori	9	suhteellinen	29
order	27	redusoituvuus	29
orbitaalisesti stabiili	17	rekurrenssiyhtälö	35
ortonormaali	9	rekursio	35
ortonormalisointi	9	rengas	28
ortonormeerattu	6	kommutatiivinen	28
osamurtokehitemä	45, 45	matriisi-	29
osittaisderivaatta	21	polynomi-	29
osittaisdifferentiaali	15	rengashomomorfismi	29
ositus	34	residue	45
pääarvo (kompleksiluvun)	26	residy	45
painopiste	11	reuna-arvo-ongelma	15
painopistekoordinaatit	11, 11	ring	28
palautuskaava	35	ristioperaattori	10
parillinen funktio	20	ristitulo	10
pariton funktio	20	-matriisi	10
Pascalin kolmio	32	rook polynomial	34
peräkkäiset sijoitukset	7	roottori	24
permutaatio	31	RSA-salakirjoitus	41
erilliset esittäjät	37	ryhmä	27
matriisiesitys	37	Kleinin	28
-ryhmä	37	syklinen	27
toisto-	31	ryhmäkoodi	30
permutaatioryhmä	36	säännöllisyysaste	6
Picardin iteraatio	17	sarja	19, 19
Picardin lause	17	Fourier-	20
pienimmän neliösumman sovitus	13	harmoninen	20
pienin yhteinen jaettava	40	potenssi-	20
pistetulo	10	Taylorin	20
polaariesitys (kompleksiluvun)	26	semigroup	27
pole	26	silmukka	42
polku	42	similaarisuus	9
Polyan lause	37	similariteettimuunnos	9
polynomirengas	29, 29	sink	24
polynomitulo		sisätulo	10
normeerattu	29	skalaarikenttä	22
positiivisesti orientoitu	26	harmoninen	24
potenssi	27	skalaarikolmitulo	11
korkea	40	skalaaritulo	10
potenssisarja	20	source	24
laskusäännöt	33	sovitus	
potentiaali	22	kaksijakoisen graafin	43
-vektori	22	stabiili piste	17
Primin algoritmi	43	stabilisaattori	37
projektiivinen avaruus	12	s-taso	18

Stokesin lause	24	transpoosi	6
Strilingin luvut, 2. lajin	31	tulo	
sulkeuma	42	Cauchy	20
suora	11	formaali	24
ideaali-	12	matriisi-	6
normaalimuoto	11	piste-/skalaari-/sisä-	10
painopistekoordinaatit	11	polynomi-	29
parametrimuoto	11	risti-	10
-parvi	11	skalaarikolmi-	11
-viuhka	11	suora	27
suora tulo	27	vektori-	10
suppeneminen	19, 19	tuloaste	42
absoluuttinen	19	työ	23
ehdollinen	19	ulottuvuus (osajoukon)	43
testaus	19	unkarilainen algoritmi	43
suppenemisintervalli	20	väärinjärjestys	31
suppenemiskeskus	20	vahva pseudoalkulukku	41
suuntakenttä	16	vaihekulma	26
suurin yhteinen tekijä	39	vaihekuvaaja	17, 17
sykli-indeksi	37	vaje	43
syklinen järjestys	37	vakiotermi	29
syklinen ryhmä	27	vasta-alkio	27
symmetrinen ryhmä	36	vektorikenttä	22
syndrooma	30	konservatiivinen	23
systemaattinen	30	vektoripotentiali	22
syt	39	vektoritulo	10, 10
täydellinen sovitus	43	viivaintegraali	23, 23
tarkistusmatriisi	30	suljetun käyrän)	23
tasa-arvokäyrä	16	virheen paino	30
tasapainopiste	17	virherakenne	30
taso	11	virittää (ryhmä)	27
ideaali-	12	vuo	23
normaalimuoto	11	Wilsonin lause	40
painopistekoordinaatit	11	Wronskian-determinantti	16
parametrimuoto	11	ydin	12
projektiivinen	12	ydin (lineaarikuvauksen)	6
Taylorin sarja	20	yhdensuuntaissärmiö	13
tehosuhde (koodauksen)	30	yhdistetty solmu	42
tetraedri	11	ykkösalkio	28
toistopermutaatio	31	yksikkö	28
tornipolynomi	34, 34	ylimäärätty yhtälöryhmä	13
transformaatio	12	yritefunktio	35