Savitauluista tietokoneisiin - klassista ja modernia algebraa

Markku Niemenmaa

Matemaattisten tieteiden laitos

Lokakuun 17., 2012

- Sana 'algebra' tulee 800 - luvulla eläneen matemaatikon Muhammad ibn Musa al-Khwarizmin teoksesta:
  Al - Kitab al mukhtasar fi hisab al - jabr wa - l - muqabala

- Sana 'algebra' tulee 800 - luvulla eläneen matemaatikon Muhammad ibn Musa al-Khwarizmin teoksesta:
  Al - Kitab al mukhtasar fi hisab al - jabr wa - l - muqabala

- 1100 - luvulla Robert of Chester käänsi kirjan latinaksi:
  Liber algebrae et almucabala

- Sana 'algebra' tulee 800 - luvulla eläneen matemaatikon Muhammad ibn Musa al-Khwarizmin teoksesta:
  Al - Kitab al mukhtasar fi hisab al - jabr wa - l - muqabala

- 1100 - luvulla Robert of Chester käänsi kirjan latinaksi:
  Liber algebrae et almucabala

- Klassinen algebra: tarkastelee yhtälöiden ratkaisemista ja siihen liittyviä menetelmiä

- Klassinen algebra: tarkastelee yhtälöiden ratkaisemista ja siihen liittyviä menetelmiä

- Moderni algebra: tarkastelee algebrallisia rakenteita, jotka selittävät, miksi joillakin yhtälöillä ei ole ratkaisuja. Algebrallisia rakenteita käytetään myös koodausteoriassa, salausmenetelmissä eli kryptografiassa ja tarkistusmerkkijärjestelmissä.

- Klassinen algebra: tarkastelee yhtälöiden ratkaisemista ja siihen liittyviä menetelmiä
- Moderni algebra: tarkastelee algebrallisia rakenteita, jotka selittävät, miksi joillakin yhtälöillä ei ole ratkaisuja. Algebrallisia rakenteita käytetään myös koodausteoriassa, salausmenetelmissä eli kryptografiassa ja tarkistusmerkkijärjestelmissä.
- Historiallisesti raja klassisen ja modernin algebran välillä kulkee 1800 - luvun alkupuolella

- Klassinen algebra: tarkastelee yhtälöiden ratkaisemista ja siihen liittyviä menetelmiä
- Moderni algebra: tarkastelee algebrallisia rakenteita, jotka selittävät, miksi joillakin yhtälöillä ei ole ratkaisuja. Algebrallisia rakenteita käytetään myös koodausteoriassa, salausmenetelmissä eli kryptografiassa ja tarkistusmerkkijärjestelmissä.
- Historiallisesti raja klassisen ja modernin algebran välillä kulkee 1800 - luvun alkupuolella

- Toisen asteen yhtälö: $x^2 + bx + c = 0$

- Toisen asteen yhtälö: $x^2 + bx + c = 0$
- Ratkaisu: $x = \frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$

- Toisen asteen yhtälö: $x^2 + bx + c = 0$
- Ratkaisu: $x = \frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$

- Babylonialainen (Kaksoisvirranmaan, Mesopotamian) matematiikka tunsi ratkaisumenetelmän tiettyihin lukuihin liittyvänä toimintaohjeena n. 2000 eaa. eli 4000 vuotta sitten !

- Toisen asteen yhtälö: $x^2 + bx + c = 0$
- Ratkaisu: $x = \frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$

- Babylonialainen (Kaksoisvirranmaan, Mesopotamian) matematiikka tunsi ratkaisumenetelmän tiettyihin lukuihin liittyvänä toimintaohjeena n. 2000 eaa. eli 4000 vuotta sitten !

- Tuolta ajalta on säilynyt noin 300 matematiikkaa käsittelevää savitaulua ja osa niistä liittyy em. ratkaisumenetelmään.

- Toisen asteen yhtälö: $x^2 + bx + c = 0$
- Ratkaisu: $x = \frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$

- Babylonialainen (Kaksoisvirranmaan, Mesopotamian) matematiikka tunsi ratkaisumenetelmän tiettyihin lukuihin liittyvänä toimintaohjeena n. 2000 eaa. eli 4000 vuotta sitten !

- Tuolta ajalta on säilynyt noin 300 matematiikkaa käsittelevää savitaulua ja osa niistä liittyy em. ratkaisumenetelmään.

- Otto Neugebauer (1899 - 1990) julkaisi saksankielisiä käännöksiä savitaulujen teksteistä, jotka käsittelivät matemaattisia ongelmia, niiden ratkaisuja sekä laskutaulukkoja.

- Otto Neugebauer (1899 - 1990) julkaisi saksankielisiä käännöksiä savitaulujen teksteistä, jotka käsittelivät matemaattisia ongelmia, niiden ratkaisuja sekä laskutaulukkoja.
- Savitauluissa on nuolenpääkirjoitusta, joka on laadittu akkadin kielellä. Neugebauer opetteli kyseisen kielen ja julkaisi vuonna 1935 kaksiosaisen kirjan savitaulujen teksteistä.

- Otto Neugebauer (1899 - 1990) julkaisi saksankielisiä käännöksiä savitaulujen teksteistä, jotka käsittelivät matemaattisia ongelmia, niiden ratkaisuja sekä laskutaulukkoja.
- Savitauluissa on nuolenpääkirjoitusta, joka on laadittu akkadin kielellä. Neugebauer opetteli kyseisen kielen ja julkaisi vuonna 1935 kaksiosaisen kirjan savitaulujen teksteistä.

- Exhibition: The Culture of Old Babylonian Mathematics (New York University, Nov. 2010 - Jan. 2011). Edelleen netissä!

- Kolmannen asteen yhtälön $x^3 + qx + r = 0$ ratkaisun keksi ensimmäisenä Niccolo Fontana (lempinimeltään 'Tartaglia' eli 'änkyttäjä') vuonna 1535.

- Kolmannen asteen yhtälön $x^3 + qx + r = 0$ ratkaisun keksi ensimmäisenä Niccolo Fontana (lempinimeltään 'Tartaglia' eli 'änkyttäjä') vuonna 1535.

- Vuonna 1545 Girolamo Cardano julkaisi ratkaisumenetelmän kirjassaan ' Ars magna, sive de regulis algebraicis '. Samana vuonna Cardanon oppilas Ludovico Ferrari keksi 4. asteen yhtälön ratkaisun.

- Kolmannen asteen yhtälön $x^3 + qx + r = 0$ ratkaisun keksi ensimmäisenä Niccolo Fontana (lempinimeltään 'Tartaglia' eli 'änkyttäjä') vuonna 1535.

- Vuonna 1545 Girolamo Cardano julkaisi ratkaisumenetelmän kirjassaan ' Ars magna, sive de regulis algebraicis '. Samana vuonna Cardanon oppilas Ludovico Ferrari keksi 4. asteen yhtälön ratkaisun.

- Cardanon kaava:

$$\sqrt[3]{-r/2 + \sqrt{r^2/4 + q^3/27}} + \sqrt[3]{-r/2 - \sqrt{r^2/4 + q^3/27}}$$

- Kolmannen asteen yhtälön $x^3 + qx + r = 0$ ratkaisun keksi ensimmäisenä Niccolo Fontana (lempinimeltään 'Tartaglia' eli 'änkyttäjä') vuonna 1535.

- Vuonna 1545 Girolamo Cardano julkaisi ratkaisumenetelmän kirjassaan ' Ars magna, sive de regulis algebraicis '. Samana vuonna Cardanon oppilas Ludovico Ferrari keksi 4. asteen yhtälön ratkaisun.

- Cardanon kaava:

$$\sqrt[3]{-r/2 + \sqrt{r^2/4 + q^3/27}} + \sqrt[3]{-r/2 - \sqrt{r^2/4 + q^3/27}}$$

- Tartaglia paljastaa ratkaisunsa Cardanolle runomuodossa:

- Tartaglia paljastaa ratkaisunsa Cardanolle runomuodossa:
- Quando che'l cubo con le cose appresso, Se agguaglia a qualche numero discreto ($x^3 + cx = d$)

- Tartaglia paljastaa ratkaisunsa Cardanolle runomuodossa:
- Quando che'l cubo con le cose appresso, Se agguaglia a qualche numero discreto ($x^3 + cx = d$)
- Trovati dui altre differenti in esso (hae sellaiset luvut u ja v, että $u - v = d$)

- Tartaglia paljastaa ratkaisunsa Cardanolle runomuodossa:
- Quando che'l cubo con le cose appresso, Se agguaglia a qualche numero discreto ($x^3 + cx = d$)
- Trovati dui altre differenti in esso (hae sellaiset luvut u ja v, että $u - v = d$)
- Dapoi terrai, questo per consueto, Che'l loro produtto, sempre sia eguale al terzo cubo delle cose netto ($uv = (c/3)^3$)

- Tartaglia paljastaa ratkaisunsa Cardanolle runomuodossa:
- Quando che'l cubo con le cose appresso, Se agguaglia a qualche numero discreto ($x^3 + cx = d$)
- Trovati dui altre differenti in esso (hae sellaiset luvut u ja v, että $u - v = d$)
- Dapoi terrai, questo per consueto, Che'l loro produtto, sempre sia eguale al terzo cubo delle cose netto ($uv = (c/3)^3$)
- El residuo poi sua generale, delle lor latti cubi, ben sottratti, varra la tua cosa principale ($x = \sqrt[3]{u} - \sqrt[3]{v}$)

- Tartaglia paljastaa ratkaisunsa Cardanolle runomuodossa:
- Quando che'l cubo con le cose appresso, Se agguaglia a qualche numero discreto ($x^3 + cx = d$)
- Trovati dui altre differenti in esso (hae sellaiset luvut u ja v, että $u - v = d$)
- Dapoi terrai, questo per consueto, Che'l loro produtto, sempre sia eguale al terzo cubo delle cose netto ($uv = (c/3)^3$)
- El residuo poi sua generale, delle lor latti cubi, ben sottratti, varra la tua cosa principale ($x = \sqrt[3]{u} - \sqrt[3]{v}$)

- Millainen olisi sitten 5. asteen yhtälön yleinen ratkaisukaava ? Tätä mietittiin Cardanon ja Ferrarin jälkeen n. 250 vuotta !

- Millainen olisi sitten 5. asteen yhtälön yleinen ratkaisukaava ? Tätä mietittiin Cardanon ja Ferrarin jälkeen n. 250 vuotta !

- Ensimmäisenä väitteen, että 5. asteen yhtälöllä ei ole yleistä ratkaisukaavaa, esitti Paolo Ruffini 1799. Niels Henrik Abel perusteli yo. väitettä permutaatioiden avulle vuonna 1824.

- Millainen olisi sitten 5. asteen yhtälön yleinen ratkaisukaava ? Tätä mietittiin Cardanon ja Ferrarin jälkeen n. 250 vuotta !

- Ensimmäisenä väitteen, että 5. asteen yhtälöllä ei ole yleistä ratkaisukaavaa, esitti Paolo Ruffini 1799. Niels Henrik Abel perusteli yo. väitettä permutaatioiden avulle vuonna 1824.

- Lopulta vuonna 1831 Evariste Galois (1811 - 1832) osoitti, että yhtälön ratkaisukaavan olemassaoloon liittyy permutaatioiden muodostama algebrallinen rakenne, 'le groupe' (group, Gruppe, ryhmä). Jos ratkaisukaava on olemassa, niin ryhmää sanotaan ratkeavaksi (solvable group). 'Ryhmä' on modernin (abstraktin) algebran peruskäsitteitä.

- Millainen olisi sitten 5. asteen yhtälön yleinen ratkaisukaava ? Tätä mietittiin Cardanon ja Ferrarin jälkeen n. 250 vuotta !

- Ensimmäisenä väitteen, että 5. asteen yhtälöllä ei ole yleistä ratkaisukaavaa, esitti Paolo Ruffini 1799. Niels Henrik Abel perusteli yo. väitettä permutaatioiden avulle vuonna 1824.

- Lopulta vuonna 1831 Evariste Galois (1811 - 1832) osoitti, että yhtälön ratkaisukaavan olemassaoloon liittyy permutaatioiden muodostama algebrallinen rakenne, 'le groupe' (group, Gruppe, ryhmä). Jos ratkaisukaava on olemassa, niin ryhmää sanotaan ratkeavaksi (solvable group). 'Ryhmä' on modernin (abstraktin) algebran peruskäsitteitä.

- Galois'n tutkimukset julkaistaan vasta 1846 lehdessä 'Journal de Mathematiques Pures et Appliquees'.

- Millainen olisi sitten 5. asteen yhtälön yleinen ratkaisukaava ? Tätä mietittiin Cardanon ja Ferrarin jälkeen n. 250 vuotta !

- Ensimmäisenä väitteen, että 5. asteen yhtälöllä ei ole yleistä ratkaisukaavaa, esitti Paolo Ruffini 1799. Niels Henrik Abel perusteli yo. väitettä permutaatioiden avulle vuonna 1824.

- Lopulta vuonna 1831 Evariste Galois (1811 - 1832) osoitti, että yhtälön ratkaisukaavan olemassaoloon liittyy permutaatioiden muodostama algebrallinen rakenne, 'le groupe' (group, Gruppe, ryhmä). Jos ratkaisukaava on olemassa, niin ryhmää sanotaan ratkeavaksi (solvable group). 'Ryhmä' on modernin (abstraktin) algebran peruskäsitteitä.

- Galois'n tutkimukset julkaistaan vasta 1846 lehdessä 'Journal de Mathematiques Pures et Appliquees'.

- Mitä sitten ovat nuo Galois'n ryhmät?

- Mitä sitten ovat nuo Galois'n ryhmät?
- Galois'n ryhmät koostuvat permutaatioista. Alkiot 1, 2 ja 3 voidaan permutoida kuudella eri tavalla:
  123, 132, 213, 231, 312, 321.

- Mitä sitten ovat nuo Galois'n ryhmät?
- Galois'n ryhmät koostuvat permutaatioista. Alkiot 1, 2 ja 3 voidaan permutoida kuudella eri tavalla:
  123, 132, 213, 231, 312, 321.
- Viidennen asteen yhtälöön

$$x^5 - 4x + 2 = 0$$

liittyy permutaatioryhmä, jonka alkioiden lukumäärä on 120. Tämä ryhmä on rakenteeltaan senverran 'hankala', että yhtälöllä ei ole klassista ratkaisukaavaa.

- Mitä sitten ovat nuo Galois'n ryhmät?
- Galois'n ryhmät koostuvat permutaatioista. Alkiot 1, 2 ja 3 voidaan permutoida kuudella eri tavalla:
  123, 132, 213, 231, 312, 321.
- Viidennen asteen yhtälöön

$$x^5 - 4x + 2 = 0$$

liittyy permutaatioryhmä, jonka alkioiden lukumäärä on 120. Tämä ryhmä on rakenteeltaan senverran 'hankala', että yhtälöllä ei ole klassista ratkaisukaavaa.

- 1800 - luvun lopulla ja 1900 - luvulla ryhmäteoriasta muodostuu oma itsenäinen algebrallinen teoria ja ryhmien rakenteellisia ominaisuuksia aletaan tutkia.

- 1800 - luvun lopulla ja 1900 - luvulla ryhmäteoriasta muodostuu oma itsenäinen algebrallinen teoria ja ryhmien rakenteellisia ominaisuuksia aletaan tutkia.

- Kysymys 1): Millaiset kertaluvut (siis ryhmän alkioiden lukumäärät) liittyvät ratkeaviin ryhmiin ?

- 1800 - luvun lopulla ja 1900 - luvulla ryhmäteoriasta muodostuu oma itsenäinen algebrallinen teoria ja ryhmien rakenteellisia ominaisuuksia aletaan tutkia.

- Kysymys 1): Millaiset kertaluvut (siis ryhmän alkioiden lukumäärät) liittyvät ratkeaviin ryhmiin ?

- Kysymys 2): Äärelliset ryhmät voidaan 'rakentaa' osista, joita kutsutaan yksinkertaisiksi ryhmiksi (simple group). Onko mahdollista antaa rakennekuvaus kaikista yksinkertaisista ryhmistä ?

- 1800 - luvun lopulla ja 1900 - luvulla ryhmäteoriasta muodostuu oma itsenäinen algebrallinen teoria ja ryhmien rakenteellisia ominaisuuksia aletaan tutkia.

- Kysymys 1): Millaiset kertaluvut (siis ryhmän alkioiden lukumäärät) liittyvät ratkeaviin ryhmiin ?

- Kysymys 2): Äärelliset ryhmät voidaan 'rakentaa' osista, joita kutsutaan yksinkertaisiksi ryhmiksi (simple group). Onko mahdollista antaa rakennekuvaus kaikista yksinkertaisista ryhmistä ?

- Ensimmäiseen kysymykseen antoivat tärkeän vastauksen Walter Feit ja John Thompson vuonna 1963 artikkelissaan:
  ' Solubility of groups of odd order ', Pacific Journal of Mathematics, 13(1963), 775 - 1029.
  Päätulos kertoo, että jokainen paritonta kertalukua oleva ryhmä on ratkeava. Thompson sai vuonna 1970 Fieldsin mitalin.

- Ensimmäiseen kysymykseen antoivat tärkeän vastauksen Walter Feit ja John Thompson vuonna 1963 artikkelissaan:
  ' Solubility of groups of odd order ', Pacific Journal of Mathematics, 13(1963), 775 - 1029.
  Päätulos kertoo, että jokainen paritonta kertalukua oleva ryhmä on ratkeava. Thompson sai vuonna 1970 Fieldsin mitalin.

- Äärellisten yksinkertaisten ryhmien luokittelu saatiin valmiiksi 1980 - luvun alussa. Luokittelu piti tuolloin sisällään 15000 sivua teoriaa (siis satoja artikkeleita) ja satoja tietokoneen avulla konstruoituja rakenteita.

- Ensimmäiseen kysymykseen antoivat tärkeän vastauksen Walter Feit ja John Thompson vuonna 1963 artikkelissaan:
  ' Solubility of groups of odd order ', Pacific Journal of Mathematics, 13(1963), 775 - 1029.
  Päätulos kertoo, että jokainen paritonta kertalukua oleva ryhmä on ratkeava. Thompson sai vuonna 1970 Fieldsin mitalin.

- Äärellisten yksinkertaisten ryhmien luokittelu saatiin valmiiksi 1980 - luvun alussa. Luokittelu piti tuolloin sisällään 15000 sivua teoriaa (siis satoja artikkeleita) ja satoja tietokoneen avulla konstruoituja rakenteita.

- Luokittelulauseen mukaan yksinkertaiset ryhmät muodostuvat kolmesta pääryhmästä (sykliset, alternoivat, Lien tyypin ryhmät) sekä 26:sta erikoistapauksesta (ns. sporadiset ryhmät).

- Luokittelulauseen mukaan yksinkertaiset ryhmät muodostuvat kolmesta pääryhmästä (sykliset, alternoivat, Lien tyypin ryhmät) sekä 26:sta erikoistapauksesta (ns. sporadiset ryhmät).
  Viimeksimainituista tunnetuin on Fischer - Griessin hirviö (tunnetaan myös nimellä Friendly Giant).Sen kertaluku on:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{2} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

- Luokittelulauseen mukaan yksinkertaiset ryhmät muodostuvat kolmesta pääryhmästä (sykliset, alternoivat, Lien tyypin ryhmät) sekä 26:sta erikoistapauksesta (ns. sporadiset ryhmät).
  Viimeksimainituista tunnetuin on Fischer - Griessin hirviö (tunnetaan myös nimellä Friendly Giant).Sen kertaluku on:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{2} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

- Luokittelulause on eräs ryhmäteorian merkittävimmistä saavutuksista. Gorenstein, Lyons ja Solomon alkoivat 1990 - luvulla koota luokitteluun liittyviä tuloksia ja niiden todistuksia yksiin kansiin. Yhdet kannet eivät kyllä riittäneet, sillä tuloksena on 11 - osainen kirjasarja, josta on tähän mennessä ilmestynyt kuusi osaa.

- Luokittelulauseen mukaan yksinkertaiset ryhmät muodostuvat kolmesta pääryhmästä (sykliset, alternoivat, Lien tyypin ryhmät) sekä 26:sta erikoistapauksesta (ns. sporadiset ryhmät).
  Viimeksimainituista tunnetuin on Fischer - Griessin hirviö (tunnetaan myös nimellä Friendly Giant).Sen kertaluku on:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{2} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

- Luokittelulause on eräs ryhmäteorian merkittävimmistä saavutuksista. Gorenstein, Lyons ja Solomon alkoivat 1990 - luvulla koota luokitteluun liittyviä tuloksia ja niiden todistuksia yksiin kansiin. Yhdet kannet eivät kyllä riittäneet, sillä tuloksena on 11 - osainen kirjasarja, josta on tähän mennessä ilmestynyt kuusi osaa.

- Miten ryhmäteoriaa voidaan sitten käyttää ?

- Miten ryhmäteoriaa voidaan sitten käyttää ?
- 1) Ryhmien avulla voidaan tutkia muiden algebrallisten rakenteiden ominaisuuksia.

- Miten ryhmäteoriaa voidaan sitten käyttää ?
- 1) Ryhmien avulla voidaan tutkia muiden algebrallisten rakenteiden ominaisuuksia.
- 2) Ryhmien avulla voidaan parantaa esim. tarkistusmerkkijärjestelmien laatua.

- Miten ryhmäteoriaa voidaan sitten käyttää ?
- 1) Ryhmien avulla voidaan tutkia muiden algebrallisten rakenteiden ominaisuuksia.
- 2) Ryhmien avulla voidaan parantaa esim. tarkistusmerkkijärjestelmien laatua.
- Tarkistusmerkit ??

- Miten ryhmäteoriaa voidaan sitten käyttää ?
- 1) Ryhmien avulla voidaan tutkia muiden algebrallisten rakenteiden ominaisuuksia.
- 2) Ryhmien avulla voidaan parantaa esim. tarkistusmerkkijärjestelmien laatua.
- Tarkistusmerkit ??
- Matkapuhelimet päälle ja näppäilkää: $*\#06\#$

- Miten ryhmäteoriaa voidaan sitten käyttää ?
- 1) Ryhmien avulla voidaan tutkia muiden algebrallisten rakenteiden ominaisuuksia.
- 2) Ryhmien avulla voidaan parantaa esim. tarkistusmerkkijärjestelmien laatua.
- Tarkistusmerkit ??
- Matkapuhelimet päälle ja näppäilkää: $*\#06\#$
- Yanling Chen, Danilo Gligoroski, MN, A.J. Han Vinck: On the properties of a check digit system based on group theory. Accepted presentation, ISIT 2012, Massachusetts Institute of Technology, July 2012.

- Algebran tutkimus rakentuu nelituhatvuotisen perinteen pohjalle ja sillä on suuri merkitys sekä matematiikan sisällä perustutkimuksessa että informaatioteknologiaan liittyvissä sovelluksissa. On mielenkiintoista nähdä mihin suuntaan algebra kehittyy!

- Algebran tutkimus rakentuu nelituhatvuotisen perinteen pohjalle ja sillä on suuri merkitys sekä matematiikan sisällä perustutkimuksessa että informaatioteknologiaan liittyvissä sovelluksissa. On mielenkiintoista nähdä mihin suuntaan algebra kehittyy!