

Leonhard Euler (1707-1783)



Theoremata circa residua ex
divisione potestatum relictia (1761)

“ Ik heb mij voorgenomen de resten die ontstaan bij deling van de termen in de meetkundige rij a^ν door een priemgetal p , onderling ondeelbaar met a , aandachtig te bekijken.”

Stelling:

$$\#\{0 < r \leq p - 1 : \exists \nu : a^\nu = r \pmod{p}\} \mid p - 1$$

Gevolg: Kleine Stelling van Fermat

Carl Friedrich Gauß (1707-1783)



Cirkeldeling in de Disquisitiones Arithmeticae (1801)

- “Er bestaat een primitieve wortel modulo p ”
- “Als $p - 1 = e \cdot f$, dan is $\langle g^e \rangle$ ondergroep van $\langle g \rangle$ van orde f . ”
- “De oplossingen van $X^p - 1$ vormen een cyclische groep van orde p ”

Carl Friedrich Gauß (1707-1783)

Kwadratische vormen in de DA (1801)

Definities.

- Kwadratische vorm is $(a, b, c) = ax^2 + 2bxy + cy^2$ $a, b, c \in \mathbf{Z}$
- Discriminant is $D = b^2 - ac$.
- Twee vormen zijn equivalent als ze door $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ in elkaar overgaan met $\alpha, \beta, \gamma, \delta \in \mathbf{Z}$ en inverse bestaat.

Probleem: Hoeveel inequivalente kwadratische vormen zijn er van gegeven discriminant?

Stelling: Eindig veel.

Definitie.

Als $(A, B, C) = (a, b, c)(a', b', c')$ door een transformatie

$$\begin{aligned} X &= pxx' + p'xy' + p''yx' + p'''yy', \\ Y &= qxx' + q'xy' + q''yx' + q'''yy' \end{aligned}$$

dan heet (A, B, C) transformeerbaar tot $(a, b, c)(a', b', c')$.

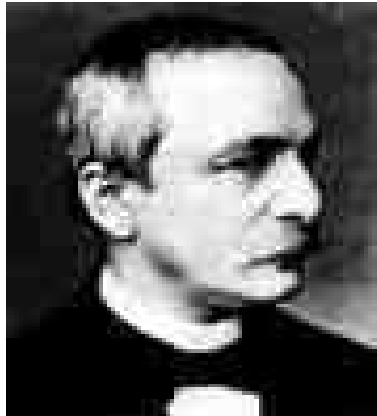
Dit definieert een produkt.

Stelling: • Als $(a, b, c) \sim (\alpha, \beta, \gamma)$ en $(a', b', c') \sim (\alpha', \beta', \gamma')$ dan ook $(a, b, c)(a', b', c') \sim (\alpha, \beta, \gamma)(\alpha', \beta', \gamma')$.

• $(a, b, c)(a', b', c') \sim (a', b', c')(a, b, c)$.

• $(a, b, c)(1, 0, -D) \sim (a, b, c)$.

Leopold Kronecker (1823-1891)



Auseinandersetzung einiger Eigenschaften der
Klassenanzahl idealer complexer Zahlen (1870)

Joseph-Louis Lagrange (1736-1813)



Réflexions sur la théorie algébrique des équations
(1770)

- Analyse van bekende oplossingsmethodes, bijv.:
als x_1, x_2, x_3 wortels zijn van $X^3 + pX + q = 0$, neemt de
rationale functie

$$R = (x_1 + \alpha x_2 + \alpha x_3)^3$$

maar **twee** waarden aan voor alle verwisselingen van
 x_1, x_2, x_3 .

- Definitie.

Stel $R(x_1, \dots, x_n)$ is een functie van de wortels van een
polynoom f dat onder $\sigma \in S_n$ maar d waarden $\{R_i\}_{i=1}^d$
aanneemt. Dan heet

$$\prod_{i=1}^d (X - R_i)$$

resolvent van graad d voor f .

Paolo Ruffini (1765-1822)



Teoria generale delle equazioni (1799)

Bestudeert S_n :

- zoekt voortbrengers.
- classificeert ondergroepen (eis: “inwendigheid”).
- Lagrange’s resolvent van graad $d \iff$ ondergroep van index d
- vindt alle ondergroepen van S_5 , i.h.b. zijn er geen van orde 15, 30 en 40 (dus $d = 8, 4, 3$ kan niet).

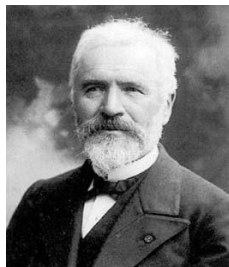
Augustin-Louis Cauchy (1789-1857)



diverse werken (1812-1846)

- abstracte theorie van S_n , o.a. **Stelling**. De index van een ondergroep van S_n is 2 of ten minste de grootste priemdelers van n .
- notaties: product, macht, inverse, orde
- σ en τ zijn **semblables** als ze dezelfde cykelstructuur hebben. **Stelling**. σ, τ semblables $\iff \exists \rho : \tau = \rho \sigma \rho^{-1}$.
- vindt voortbrengers.
- definitie normaaldeler (na Galois).

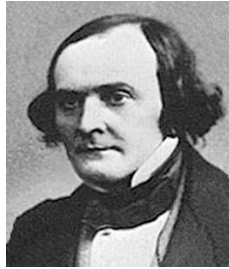
..., Abel, Galois, ..., **Camille Jordan (1838-1922)**



Traité des substitutions et des équations algébriques
(1870)

morfisme $G \rightarrow \Gamma$ heet **mériédrique** (surjectief) of **holoédrique** (bijectief)

Arthur Cayley (1821-1895)



Theory of Quantics (1854)

- 19e eeuwse crisis: vele soorten meetkunde (euclidisch, niet-euclidisch, projectief, ...)
- idee: bij een meetkunde hoort een verzameling (lineaire) transformaties
- “die” meetkunde is dan de studie van de invarianten onder die transformaties, bv. **dubbelverhouding**

Felix Klein (1849-1925)



- Erlangen programma (1872): consequente studie van transformatiegroepen
- automorfe vormen, elliptische functies, relatie tussen oplossen van vijfdegraadsvergelijking en symmetrieën van het vijfvlak, i.h.b. “**Sym(Icosaëder) $\cong A_5$** ”.
- (met Lie) noodzaak van oneindige groepen \Rightarrow eis dat inversen bestaan

De abstracte definitie

- voor het eerst bij Cayley (1854 en 1878), dan Burnside, von Dyck
- via Kronecker bij Heinrich Weber
- **inwendigheid**: meestal expliciet gevraagd
- **associativiteit + bestaan van eenheid**: meestal automatisch, want groepen van afbeeldingen onder samenstellen (wel bij Kronecker, niet bij Cayley)
- **commutativiteit**: in “getaltheorie” altijd, Cayley en Klein merken op dat het niet altijd hoeft in de meetkunde.
- **bestaan van inversen**:
 - meestal “schrappwet” $ab = ac \Rightarrow b = c$ (impliceert bestaan van inversen voor eindige groepen; bij Weber 1895)
 - expliciet pas bij **oneindige** groepen (Klein, Lie), nog niet bij oneindige groepen van Burnside.

20e eeuw:

Emmy Noether (1882-1935)

Bartel vd Waerden (1903-1996)

