

DE STELLING VAN CAUCHY OVER DE MOGELIJKE AANTALLEN WAARDEN VAN RATIONALE FUNCTIES.

NB CAUCHY GEBRUIKTE HET WOORD 'VALEUR' EN ABEL GEBRUIKTE 'WERTHE'; IK GEBRUIK DAAROM 'WAARDE'. BETER ZOU ZIJN OVER FUNCTIES TE SPREKEN OMDAT MEN FORMULES OPEREREDE.

ALS $f(x_1, x_2, \dots, x_n)$ EEN RATIONALE FUNCTIE IS DAN BEPAALT ELKE PERMUTATIE EEN NIEUWE FUNCTIE EN WE KYKEN EIGENLYK HOEVEEL VERSCHILLENDE FUNCTIES ZO GEMAAKT KUNNEN WORDEN.

WE BEZIGEN DE NOTATIE VAN CAUCHY (OVERGEGENOMEN DOOR ABEL); DIE IS WAT OMSLACHTIGER DAN DE CYKEL-NOTATIE MAAR OP EEN PAAR MOMENTEN WAT BEELDENDER.

CAUCHY GEBRUIKTE MEER TYPEN FUNCTIES, BIJVOORBEELD

$$f(x_1, x_2, x_3, x_4) = x_1 x_2^m \cos x_4 + x_4 \sin x_3$$

EEN SUBSTITUTIE: NOTEERDE MIJ ALS

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

HET EFFECT VAN DEZE OP f IS DAN

$$x_2 x_4^m \cos x_3 + x_3 \sin x_1$$

DIE BOVENSTE RIJ HOEFT OUS NIET OP VOLGORDE TE STAAN.

06/05/2025

IN ZIJN NOTATIE ZIJN BEREIK-
RYEN EEN PERMUTATIE VAN 1 2 3 4.
GEWOON DE RANGSCHIKKING NIET TE
VERWARREN MET DE CYKEL NOTATIE.

AFOORTINGEN ALS WE 1 2 4 3 ALS A_1 ,
NOTEREN EN 2 4 3 1 ALS A_2 .
DAN KRYGEN WE DE VOLGENDE
NOTATIE VOOR ONZE SUBSTITUTIE.

$$\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$$

LAAT f EEN FUNCTIE VAN m VARIABLEN
ZIJN. NOTER $N = 1 \cdot 2 \cdot 3 \cdots m$ ($m!$ dus).
EN NUMMER DE PERMUTATIES VAN
1 2 3 ... m ALS $A_1, A_2, A_3, \dots, A_N$.

DE FUNCTIES DIE WE KRYGEN ALS
WE DE SUBSTITUTIE $\begin{pmatrix} 1 & 2 & 3 & \dots & m \\ & & & & A_i \end{pmatrix}$

UITVOEREN NOEMEN WE f_i .

WE KRYGEN ZO N FUNCTIES/WAARDEN

$$f_1, f_2, f_3, \dots, f_N$$

ALS ALLE FUNCTIES VERSCHILLEN ZIJN
IER DUS N .

ALS NIET ALLE FUNCTIES VERSCHILLEN
IS HET AANTAL VERSCHILLENDE
FUNCTIES EEN DEELER VAN N .

NEEM AAN DAT M FUNCTIES,

$$\text{ZEG } f_\alpha, f_\beta, f_\gamma, \dots$$

GE LYK ZYN; DAAR HOEVEN DUS M
PERMUTATIES BIJ $A_\alpha, A_\beta, A_\gamma, \dots$

WE NEMEN M ZO GROOT MOGELIJK

DUS ELKE PERMUTATIE A DIE NIET

IN DE RIJ $A_\alpha, A_\beta, A_\gamma, \dots$ STAAT GEEFT EEN ANDERE
VERSIE VAN f DAN $f_{\alpha\beta\gamma} = f_\beta \dots$

06/05/2025

EERST EEN VOORBEELD MET $n=5$ EN $m=3$

STEL DAT $\alpha = (1\ 2\ 3\ 4\ 5)$, $\beta = (1\ 2\ 3\ 4\ 5)$

$A_\alpha = 1\ 3\ 2\ 4\ 5$, $A_\beta = 3\ 4\ 5\ 2\ 1$ EN $A_\gamma = 5\ 4\ 3\ 2\ 1$

DE ZELFDE FUNCTIES BEPALEN

STEL DAT $A = [i\ j\ k\ l\ m]$ EEN

ANDERE PERMUTATIE IS

VOER NU DE SUBSTITUTIE $\begin{pmatrix} A_\alpha \\ A \end{pmatrix}$ UIT

EN KOPIER DIE NAAR A_β EN A_γ

$\begin{pmatrix} 1\ 3\ 2\ 4\ 5 \\ [i\ j\ k\ l\ m] \end{pmatrix} \rightarrow \begin{pmatrix} 3\ 4\ 5\ 2\ 1 \\ [j\ l\ m\ k\ i] \end{pmatrix} = \begin{pmatrix} 5\ 4\ 3\ 2\ 1 \\ [m\ l\ j\ k\ i] \end{pmatrix}$

OMDAT $f(x_1, x_3, x_2, x_4, x_5) = f(x_3, x_4, x_5, x_2, x_1)$
 $= f(x_5, x_4, x_3, x_2, x_1)$

VOLOT NU DAT

$f(x_i, x_j, x_k, x_l, x_m) = f(x_j, x_l, x_m, x_k, x_i)$
 $= f(x_m, x_l, x_j, x_i, x_k)$

DUS A BEHOORT OOK TOT EEN GROEPJE
 VAN DRIE PERMUTATIES DIE EENZELFDE
 FUNCTIE OPLEVEREN

OP DEZE MANIER VERDELEN WE
 DE 120 PERMUTATIES IN GROEPEN
 VAN DRIE DIE DUS 40 VERSCHILLENDE
 FUNCTIES OPLEVEREN.

MET ALGEMEENE BEWYS GAAT OP
 DE ZELFDE MANIER: NEEM EEN
 ANDERE PERMUTATIE A (DIE DUS
 EEN ANDERE FUNCTIE OPLEVERT).

MAAK DE SUBSTITUTIE $\begin{pmatrix} A_\alpha \\ A \end{pmatrix}$

EN KOPIER DIE NAAR $A_\beta, A_\gamma, \dots$

DE RESULTERENDE m FUNCTIES

ZYN GELYK. OMDAT m MAXIMAAL IS
 BEHOORT A DUS TOT EEN GROEP VAN m

PERMUTATIES DIE EENZELFDE
FUNCTIE GENEREREN.

CONCLUSIE: ALS R HET AANTAL
VERSCHILLENDE FUNCTIES IS DAT
WE DOOR PERMUTEREN KUNNEN
MAKEN DAN GELDT $N = R \cdot M$.

NB VOOR DEGENEN DIE PERMUTATIE-
GROEPEN KENNEN: HET KUPIËREN
VAN $\binom{A_n}{A}$ NAAR $A_\beta, A_\gamma, \dots$ LEVERT
IN GROEPENTAAPE DE VOLGENDE
SUBSTITUTIES OP:

$$\begin{pmatrix} A_\beta \\ AA_\alpha^{-1}A_\beta \end{pmatrix}, \begin{pmatrix} A_\gamma \\ AA_\alpha^{-1}A_\gamma \end{pmatrix}, \dots$$

STEL NU DAT p EEN PRIEMGETAL
IS DAT $n!$ DEELT; DUS $p \leq n$.

NEEM AAN DAT $p \geq 5$ EN
DAT $\neq 20$ IS DAT WE DOOR
PERMUTEREN MINDER DAN p VEEL
FUNCTIES KRIJGEN.

DAN IS HET AANTAL VERSCHILLENDE
FUNCTIES TEN HOOGSTE 2.

WE GEBRUIKEN DE CYKELNOTATIE

NEEM EEN p -CYKEL $\sigma = (i_1, i_2, i_3, \dots, i_p)$
EN LAAT DIT OP $\neq$ WERKEN

VOORBEELD: $p = n = 5$ $\sigma = (1, 3, 2, 5, 4)$;

WE KRIJGEN

$\neq (x_3, x_5, x_2, x_1, x_4)$	σ
$\neq (x_2, x_4, x_5, x_3, x_1)$	$\sigma\sigma$
$\neq (x_5, x_1, x_4, x_2, x_3)$	$\sigma\sigma\sigma$
$\neq (x_4, x_3, x_1, x_5, x_2)$	$\sigma\sigma\sigma\sigma$
$\neq (x_1, x_2, x_3, x_4, x_5)$	$\sigma\sigma\sigma\sigma\sigma$

IN HET ALGEMEEN KRIJGEN WE ZO DUS
 p UITDRUKKINGEN WAARVAN DE p -DE
WEERGELIJK IS AAN f ZELF.

DE GEWOONTE IS f ZELF VOORAN
TE ZETTEN EN DE RIJ DE NUMMEREN
NAAR HET AANTAL MALEN DAT σ
GEBRUIKT IS:

$f_0 = f$ (σ NIET GEBRUIKT
EN DAN $f_1, f_2, \dots, f_{p-1}$

WE KUNNEN MAAR MINDER DAN p
VERSCHILLENDE FUNCTIES GEN
KRIJGEN, DUS ER ZIJN i EN j
MET $0 \leq i < j \leq p-1$

ZÖ DAT $f_i = f_j$
NOEM $j-i$ EVEN k .

BEWERING: OOK GELDT $f_0 = f_k$

IMMERS f_i EN f_j ONTSTAAN

UIT f_{i-1} EN f_{j-1} DOOR σ TOE TE PASSEN

MAAR DAT KUNNEN WE TERUG -
DRAGEN EN DAN VOLGT DAT OOK

$f_{i-1} = f_{j-1}$; DOOR i STAPPEN TERUG
TE DOEN KOMEN WE ZO UIT OP $f_0 = f_k$.

IN ONS VOORBEELD VINDEN WE
BIJVOORBEELD $p=3$ EN DUS

$f_0 = f_3$ OF WEL

$$f(x_1, x_2, x_3, x_4, x_5) = f(x_5, x_1, x_4, x_2, x_3)$$

DAT σ DRIE KEER TOE OP f_3

DAT IS σ ZES KEER TOE PASSEN OP

f ZELF; VIJF KEER GEEFT f ZELF
DUS ZES KEER GEEFT f_1 .

WE ZIEN $f = f_0 = f_3 = f_1$

NOG DRIE KEER GEEFT DAN $f_1 = f_4$

MEER DRIE KEER: $f_4 = f_2$

CONCLUSIE: $f = f_0 = f_3 = f_1 = f_4 = f_2$

ALLE VIJF FUNCTIES ZIJN GELIJK

DUS f VERANDERT NIET ALS WE 5-CYKELS GEBRUIKEN.

ALGEMEEN: WE HEBBEN $f_0 = f_R$

EN OOK $f_i = f_{i+p}$ OMDAT p KEER σ TOEPASSEN MEERKOMT OP NIETS DOEN.

NU GEBRUIKEN WE DAT p PRIEM IS:

DE RJ $0, R, 2R, 3R, \dots, (p-1)R$
DOORLOOPT MODULO p DE GETALLEN
 $0, 1, 2, \dots, p-1$

DUS VOLGT DAT $f_0 = f_1 = f_2 = \dots = f_{p-1}$.

ARGUMENT $\text{GGD}(R, p) = 1$ WANT $0 < R < p$

HET ALGORITME VAN EUCLIDES LEVERT,
MET WAT BOEKHOUDEN, TWEE GEMEELE
GETALLEN s EN t ZODAT

$$sR + tp = \text{GGD}(R, p) = 1$$

DUS $i s R \equiv i \pmod{p}$ VOOR ELKE i

NU BEWYZEN WE: ELK 3-CYKEL
LAAT f INVARIANT.

EERST EEN VOORBEELD $n = p = 5$:

WE WILLEN LATEN ZIEN DAT f
INVARIANT IS ONDER $(1\ 2\ 3)$

DUS $f(x_1, x_2, x_3, x_4, x_5) = f(x_2, x_3, x_1, x_4, x_5)$

HIER IS WAAR WE $p \geq 5$ GEBRUIKEN.

06/05/2025

NEEM DE TWEE 5-CYKELS

$$\sigma = (1 \ 3 \ 2 \ 4 \ 5) \text{ EN}$$

$$\tau = (1 \ 5 \ 4 \ 3 \ 2)$$

ALS WE EERST σ OP $\mathbb{F}$ TOEPASSEN
KRIJGEN WE

$$\mathbb{F}(x_1, x_2, x_3, x_4, x_5) = \mathbb{F}(x_3, x_4, x_2, x_5, x_1)$$

ALS WE DAARNA τ TOEPASSEN
KOMT ER

$$\mathbb{F}(x_3, x_4, x_2, x_5, x_1) = \mathbb{F}(x_2, x_3, x_1, x_4, x_5)$$

ANDERS VOORGESD

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\tau} 2$$

$$2 \xrightarrow{\sigma} 4 \xrightarrow{\tau} 3$$

$$3 \xrightarrow{\sigma} 2 \xrightarrow{\tau} 1$$

$$4 \xrightarrow{\sigma} 5 \xrightarrow{\tau} 4$$

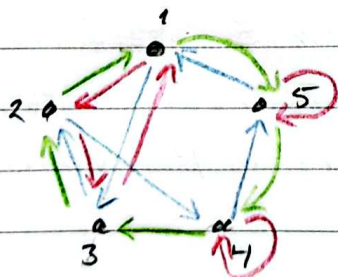
$$5 \xrightarrow{\sigma} 1 \xrightarrow{\tau} 5$$

DANKZIJ DE 4 EN DE 5 KUNNEN

WE 2 LANGS EEN OMWEG, VIA 4,

NAAR 3 STUREN EN 4 ZELF

VIA 5 TERUG OP ZIJN PLAATS KRIJGEN

 σ : BLAUW τ : GROEN $\tau \circ \sigma$: ROOD

ALGEMEEN: $\sigma = (\hat{c}_1 \ \hat{c}_3 \ \hat{c}_2 \ j_1 \ j_2 \dots j_{p-3})$

$$\tau = (\hat{c}_1 \ j_{p-2} j_{p-2} \dots j_1 \ \hat{c}_3 \ \hat{c}_2)$$

$$\hat{c}_1 \rightarrow \hat{c}_3 \rightarrow \hat{c}_2$$

$$\hat{c}_2 \rightarrow j_1 \rightarrow \hat{c}_3$$

$$\hat{c}_3 \rightarrow \hat{c}_2 \rightarrow \hat{c}_1$$

$$j_2 \rightarrow j_3 \rightarrow j_2$$

$$j_{p-2} \rightarrow \hat{c}_1 \rightarrow j_{p-2}$$

Nu: ELKE 3-CYKEL IS SAMEN TE STELLEN
UIT TWEE VERWISSELINGEN
 $(a b c) = \text{EERST } (b c) \text{ EN}$
 $\text{DAN } (a b)$

WANT: $a \rightarrow a \rightarrow b$
 $b \rightarrow c \rightarrow c$
 $c \rightarrow b \rightarrow a$

ELKE SAMENSTELLING VAN TWEE
VERWISSELINGEN IS SAMEN TE
STELLEN UIT 3-CYKELS

① $(a b)$ EN $(b c)$

EERST $(b c)$ DAN $(a b)$: $(a b c)$

EERST $(a b)$ DAN $(b c)$: $(a c b)$

② $(a b)$ EN $(c d)$ (ALLE VERSCHILLENDE)

DE VOLGORDE MAAKT NIET UIT

EN EERST $(a b)$ DAN $(c d)$

IS HET ZELFDE ALS ACHTEREEN-
VOLGENS $(a b)(b c)(b c)(c d)$

[ONDERWEG TWEE KEER b EN c

VERWISSELEN DOET NIETS]

MAAR EERST $(a b)$ DAN $(b c)$: $(a c b)$

EERST $(b c)$ DAN $(c d)$: $(b d c)$

DVS $(a b)$ EN $(c d)$ SAMEN

IS EERST $(a c b)$ DAN $(b d c)$.

EINDELYK: f IS INUSINVARIANT ONDER
ALLE PERMUTATIES DIE UIT EEN EVEN
AANTAL VERWISSELINGEN BESTAAN
DE ENIGE POTENTIËLE ANDERE WAARDE
ONTSTAAT DOOR EEN VERWISSELING

CONCLUSIE f BEPAALT HOOGUIT TWEE FUNKTIES