4

Notatie $n \in \mathbb{Z}_{>0}$, dan $[n] := \{1, \dots, n\}$

Def voor X verzameling is $S(X) := \{ f : X \to X \mid f \text{ bijectief} \}$
de permutatiegroep van X. elementen $f \in S(X)$ heten permutaties van X.
voor $n \in \mathbb{Z}_{>0}$ schrijven we $S_n := S([n])$, heet ook wel de symmetrische groep op n elementen.

Opm voor $n \geq 3$ is S_n niet-abels, immers (notatie wordt straks verklaard)
$$(12)(13) = (132) \neq (123) = (13)(12)$$

Notatie een $\sigma \in S_n$ kan als volgt worden geschreven:
$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$
VB $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in S_n$ n ofb $1 \mapsto 1$ $2 \mapsto 3$ $3 \mapsto 2$.

St. voor X, Y verz., $\#X = \#Y = n$, geldt dat er $n!$ bijecties $X \to Y$ zijn.

Gevolg: S_n heeft $n!$ elementen.

Def een permutatie $\sigma \in S_n$ heet een cykel als geldt voor
$\exists a_1, a_2, \dots, a_k \in [n]$, alle verschillend ($i \neq j \Rightarrow a_i \neq a_j$)
zdd
$$\sigma(x) = \begin{cases} a_{i+1} & \text{als } x = a_i, \ 1 \leq i < k \\ a_1 & \text{als } x = a_k \\ x & \text{als } x \notin \{a_1, a_2, \dots a_k\} \end{cases}$$
De cykel "heeft dan lengte k". Notatie cykel: $(a_1 \, a_2 \dots a_k)$

Opm twee cykels $(a_1 \, a_2 \dots a_k)$ en $(b_1 \, b_2 \dots b_\ell)$ heten disjunct als $\{a_1, \dots a_k\}$ en $\{b_1, \dots, b_\ell\}$ disjunct zijn.
<u>Belangrijk</u>: disjuncte cykels σ_1, σ_2 commuteren: $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$

St. 4.4 Elke $\sigma \in S_n$ kan worden geschreven als eindig product van $t \in \mathbb{Z}_{\geq 0}$ paarsgewijs disjuncte cykels $\sigma_1, \sigma_2, \dots, \sigma_t$
dus $\sigma = \sigma_1 \sigma_2 \dots \sigma_k$, en deze schrijfwijze is (vanwege commutativiteit van disjuncte cykels) <u>op volgorde</u> van $\sigma_1, \dots \sigma_k$ <u>na</u> uniek bepaald.
en <u>op</u> 1-cykels <u>na</u> (die kun je n.l. wel/niet opschrijven)

Def een inversie van $\sigma \in S_n$ is een paar $(i,j) \in [n] \times [n]$ zdd $i < j$ en $\sigma(i) > \sigma(j)$

Def Het teken van een permutatie $\sigma \in S_n$ is, voor N het aantal inversies van σ, $\mathcal{E}(\sigma) := (-1)^N$
dus $\mathcal{E}: S_n \longrightarrow \{\pm 1\}$ $\mathcal{E}(\sigma) = 1$ dan heet σ <u>even</u>, anders <u>oneven</u>

St. merk op dat $\{\pm 1\}$ een multiplicatieve groep is, en dat $\mathcal{E}: S_n \to \{\pm 1\}$ een homomorfisme vormt. Dwz
$$\mathcal{E}(\sigma\tau) = \mathcal{E}(\sigma)\mathcal{E}(\tau)$$

Def De alternerende groep A_n is de verzameling van alle even permutaties. Dit is een ondergroep, aangezien $A_n = \mathrm{Ker}(\mathcal{E})$

St. 4.10 $\sigma \in S_n$:

(a) is σ een verwisseling (2-cykel), dan $\mathcal{E}(\sigma) = -1$

(b) is σ een k-cykel, dan $\mathcal{E}(\sigma) = (-1)^{k-1}$

(c) is σ het product van k cykels met lengtes $l_1, l_2, \ldots l_k$, dan $\mathcal{E}(\sigma) = (-1)^{l_1 + l_2 + \cdots + l_k - k}$.

(d) elke $\sigma \in S_n$ kan geschreven worden als het product van een eindig aantal verwisselingen: voor m het aantal verwisselingen geldt m even $\Leftrightarrow$ σ even.

Opm voor $n \geq 2$ kunnen we nagaan dat $\# A_n = \frac{1}{2} \# S_n = \frac{1}{2} n!$
Want neem $(1\,2) \in S_n$, dan is $\lambda_{(12)}: S_n \to S_n$ een bijectie, en $\lambda_{(12)}(A_n)$ bestaat geheel uit oneven permutaties en alle $\sigma \in A_n$ zijn verschillend, ~~daar~~ en verder blijkt ook $S_n / A_n = \lambda_{(12)}(A_n)$ omdat voor σ met $\mathcal{E}(\sigma) = -1$ geldt $(1\,2)\sigma \in A_n$ dus $\sigma = (1\,2)((1\,2)\sigma) \in \lambda_{(12)}(A_n)$
dus $\lambda_{(12)}(A_n) \subset S_n / A_n$, $S_n / A_n \subset \lambda_{(12)}(A_n)$ en dus $S_n \setminus A_n = \lambda_{(12)}(A_n)$
Verder $\# A_n = \# \lambda_{(12)}(A_n)$ vanwege injectiviteit $\lambda_{(12)}$, dus
$\# S_n = \#(A_n \sqcup \lambda_{(12)}(A_n)) = \# A_n + \# \lambda_{(12)}(A_n) = \# A_n + \# A_n$
$\Rightarrow \# A_n = \frac{1}{2} \# S_n$ ■

St. elke $\sigma \in A_n$ kan worden geschreven als (evt leeg product) $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$
met $\sigma_1, \ldots \sigma_k$ 3-cykels, als $n \geq 3$ en als $n \leq 2$ is $A_n = \{(1)\}$.

Bew. schrijf σ met st. 4.10 als een even aantal verwisselingen
voor elk paar opeenvolgende verwisselingen $(ab)(cd)$ geldt:
$a = c,\ b = d \Rightarrow$ verwijder het paar, het is (1)
$a = c,\ b \neq d \Rightarrow (ab)(ad) = (adb)$
$a \neq c,\ b \neq d \Rightarrow (ab)(cd) = (ab)(ac)(ac)(cd)$
$= ((ab)(ac))((ca)(cd)) = (acb)(cda)$
we kunnen dit per tweetal doen, en aangezien er een even aantal verwisselingen is maken we zo van alle verwisselingen 3-cykels □

St. 4.14 (Stelling van Cayley) elke groep G is isomorf met een ondergroep van $S(G)$. I.h.b. als $\# G = n < \infty$, dan $G \cong S_n$

Bewijs definieer $f: G \to S(G)$ door $f: x \mapsto \lambda_x$
met λ_x linksvermenigvuldiging $G \to G$ door $y \mapsto xy$, $y \in G$
(zoals in Hoofdstuk 2).

Dan geldt $(\lambda_a \circ \lambda_b)(x) = a(bx) = (ab)x = \lambda_{ab}(x)$
$\forall x \in G$, dus $f(ab) = f(a)f(b)$, f is homomorfisme.
Bovendien is $x \in \mathrm{Ker}(f) \Leftrightarrow f(x) = \mathrm{id}$, de identiteit,
dus $x \mapsto x$, en $ax = x\ \forall x \in G \Leftrightarrow x = e$,
dus $\mathrm{ker}(f) = \{e\} \Rightarrow f$ is injectief.

Dus is $G / \mathrm{onder}\ f$ isomorf met $\mathrm{Im}(f)$, want $f: G \to \mathrm{Im}(f) \subseteq S_n$
is surjectief. Daarnaast is $f(G)$ voor elke G en homom. f
een ondergroep, dus G is isomorf met og. $\mathrm{Im}(f)$ in S_n. □

5

Def G groep, $S \subset G$ deelverzameling (niet leeg) dan zij
$\langle S \rangle := \{ x \in G : \exists s_1, s_2, \dots s_k \in S \; \exists r_1^{-1}, r_2^{-1}, \dots, r_l^{-1} \in S : x = s_1 s_2 \cdots s_k r_1 r_2 \cdots r_l \}$

Lemma $\langle S \rangle$ is een o.g. van G, want <u>Bewijs</u> $x \in \langle S \rangle, y \in \langle S \rangle$
dan $x = x_1 x_2 \cdots x_n$ $y = y_1 y_2 \cdots y_m$ met $x_i \in S$ of $x_i^{-1} \in S$, $y_i \in S$ of $y_i^{-1} \in S$, dus $xy^{-1} = x_1 x_2 \cdots x_n y_m^{-1} y_{m-1}^{-1} \cdots y_1^{-1}$ met x_i of $x_i^{-1} \in S$, y_i of $y_i^{-1} \in S$
en dus $xy^{-1} \in \langle S \rangle \Rightarrow (H1')$
Bovendien als $S \neq \emptyset$ dan neem $s \in S$, dan $s \in \langle S \rangle$ want $s = s$, $s \in S$
dus $\langle S \rangle \neq \emptyset$. als $S = \emptyset$, spreekt men meestal af $\langle \emptyset \rangle := \{e\}$. □

men noemt $\langle S \rangle$ de door S voortgebrachte ondergroep.

Vb als $x \in G$, G groep, dan zien we $\langle x \rangle = \{ x^n \in G \mid n \in \mathbb{Z} \}$

Def G heet cyclisch als $\exists x \in G : \langle x \rangle = G$

Vb stel $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, dan $\bar{a} = a\bar{1}$ (dit is additieve notatie voor $\bar{1} + \bar{1} + \dots + \bar{1}$ met a termen $\bar{1}$, in multiplicatieve notatie: $\bar{1}^a$) dus $\mathbb{Z}/n\mathbb{Z} \subseteq \langle \bar{1} \rangle$ de omkering geldt omdat $\langle \bar{1} \rangle$ een o.g. van zijn groep is, dus $\langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$, ihb is $\mathbb{Z}/n\mathbb{Z}$ cyclisch.

Def G groep, $x \in G$ als er een $n \in \mathbb{Z}_{>0}$ is zdd $x^n = e$,
dan definieert men $\text{orde}(x) := \min \{ n \in \mathbb{Z}_{>0} \mid x^n = e \}$
is er niet zo'n n, dan definieert men $\text{orde}(x) = \infty$

Vb als $\sigma \in S_n$, is σ te schrijven als $\sigma_1 \sigma_2 \cdots \sigma_k$, disjuncte cykels die dus kommuteren. Dus $\sigma^n = \sigma_1^n \sigma_2^n \cdots \sigma_k^n$
en dit is (1) desda elke $\sigma_i^n = (1)$, want de cykels werken op disjuncte deelverzamelingen van $[n]$ en kunnen dus nooit elkaars inversen worden of onderling effect hebben door machtverheffen.
Dus moet n een veelvoud van elke $\text{orde}(\sigma_i)$ zijn (dit volgt uit de te bewijzen stelling 5.5) en dus, omdat $\text{orde}(\sigma_i) = l(\sigma_i)$
met $l : \text{cykels} \to \mathbb{Z}_{\geq 0}$ de lengte van een cykel.

dus voor $\ell_1, \ell_2, \ldots \ell_k$ de lengtes van cykels $\sigma_1 \sigma_2 \ldots \sigma_k$,
geldt orde $(\sigma) = \text{kgv}(\ell_1, \ell_2, \ldots, \ell_k)$

in $\mathbb{Z}/n\mathbb{Z}$ geldt dat orde $(\bar{a})$ het kleinste getal m is
zdd $m\bar{a} = \bar{0}$, dus zdd $ma \equiv 0 \mod n$, dus zdd
$n \mid ma$. We zien $ma = \text{kgv}(a,n) \Rightarrow m = \frac{\text{kgv}(a,n)}{a}$
$= n/\text{ggd}(a,n) \Rightarrow$ orde $(\bar{a}) = n/\text{ggd}(a,n)$

|| immers

(Formule van Gauss) Omdat in $\mathbb{Z}/n\mathbb{Z}$ orde $(\bar{a})$ een
deler is van n, $n = \#(\mathbb{Z}/n\mathbb{Z})$ (dit blijkt algemeen te gelden,
zie de stelling van Lagrange & gevolgen), en voor $d \mid n$ kunnen we a's vinden
met: orde $(\bar{a}) = d \Leftrightarrow d = n/\text{ggd}(a,n) \Leftrightarrow \text{ggd}(a,n) = \frac{n}{d}$
$\Leftrightarrow a = b \cdot \frac{n}{d}$ en $\text{ggd}(b,d) = 1$ (immers $\text{ggd}(b.\frac{n}{d}, n) = \frac{n}{d}\,\text{ggd}(b, d)$)

we kijken nu naar alle verschillende a's, dus neem $1 \leq a \leq n$,
dan moet wel $1 \leq b \leq d$ om a's te vinden die niet
dezelfde restklasse $\bar{a}$ opleveren: dus

$a = b \cdot \frac{n}{d}$ met $\text{ggd}(b,d) = 1$ én $1 \leq b \leq d$.

Er zijn precies $\varphi(d)$ zulke b's, dus we zien
dat, omdat orde $(\bar{a}) \neq$ orde $(\bar{b}) \Rightarrow \bar{a} \neq \bar{b}$,

$$(\mathbb{Z}/n\mathbb{Z}) = \bigsqcup_{d \mid n} \{1 \leq b \leq d \mid \text{ggd}(b,d) = 1\}$$

$$\Rightarrow n = \#(\mathbb{Z}/n\mathbb{Z}) = \sum_{d \mid n} \varphi(d) \quad \text{Dus} \quad \sum_{d \mid n} \varphi(d) = n$$

Dit is de formule van Gauss, gevonden met GR.THEORIE.

St.5.5 G groep $x \in G$, orde $(x) = n < \infty$. Dan
$x^m = e \Leftrightarrow n$ deelt m

Bewijs: "$\Rightarrow$": schrijf $m = qn + r$, deling met rest (1.1). Dan $x^{qn+r} = e$
dus $(x^n)^q x^r = e \Rightarrow e^q x^r = e \Rightarrow x^r = e$
$0 \leq r < n$, moet als $r > 0$, dan zou n niet het minimale getal > 0
zijn zdd $x^n = e$, want dat is nu r. Contradictie. Dus $r = 0$
en $\Rightarrow m = qn$, dus n deelt m.
"$\Leftarrow$": schrijf $m = qn$, dan $x^m = x^{qn} = (x^n)^q = e^q = e$ □

Gevolg 5.6 G groep, $x \in G$. Dan
(a) als $\text{orde}(x) = n < \infty$, dan $\langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$, door $f: \bar{a} \mapsto x^a$
(b) als $\text{orde}(x) = \infty$, dan $\langle x \rangle \cong \mathbb{Z}$, door $f: a \mapsto x^a$

Bewijs (a) – f is welgedefinieerd: $\bar{a} = \bar{b}$, dan $f(\bar{a}) = x^a$ en omdat $a \equiv b \bmod n$, dus $a = b + qn$, $q \in \mathbb{Z}$: $x^a = x^{b+qn} = (x^n)^q x^b = e^q x^b = x^b = f(\bar{b})$

– f is injectief: $x^a = x^b \Rightarrow x^{a-b} = e \Rightarrow a - b \in n\mathbb{Z} \Rightarrow \bar{a} = \bar{b}$.

– f is surjectief: we zagen $\langle x \rangle = \{x^m \in G \mid m \in \mathbb{Z}\}$ maar voor $a, b \in \mathbb{Z}$ met $a \equiv b \bmod n$ geldt $x^a = x^b$ dus $\langle x \rangle = \{x^m \in G \mid m = 1, \dots, n\} = \text{im}(f)$.

– f is homomorfisme: $f(\bar{a} + \bar{b}) = f(\overline{a+b}) = x^{a+b} = x^a x^b = f(\bar{a}) f(\bar{b})$

(b) – f is homomorfisme: $f(a+b) = x^{a+b} = x^a x^b = f(a) f(b)$, $a, b \in \mathbb{Z}$

– f is injectief: $x^a = x^b \Rightarrow x^{a-b} = e$, maar $\text{orde}(x) = \infty$ dus als $a - b > 0$ dan levert dit een tegenspraak op, en als $a - b < 0$, dan $b - a > 0$ en $x^{b-a} = (x^{-1})^{a-b} = (x^{a-b})^{-1} = e^{-1} = e$, ook een tegenspraak. Dus $a - b = 0$ en dit geeft $a = b$

– f is surjectief: $\langle x \rangle = \{x^m \in G \mid m \in \mathbb{Z}\} = \text{im}(f)$ $\square$

Gevolg als G een groep is, eindig en met n elementen, $\exists x \in G$: $\langle x \rangle = G$, dan $G \cong \mathbb{Z}/n\mathbb{Z}$. Dus op isomorfie na is er maar één cyclische groep. Deze noteert men kortheidshalve ook wel als $C_n = \{e, \alpha, \alpha^2, \dots \alpha^{n-1}\}$ met $\alpha^n = e$.

Gevolg 5.7 $f: G_1 \longrightarrow G_2$ groepshomomorfisme. als $x \in G_1$ eindige orde heeft, dan $f(x) \in G_1$ ook, bovendien:
$\text{orde}(f(x))$ deelt $\text{orde}(x)$.
Als f injectief is, geldt $\text{orde}(f(x)) = \text{orde}(x)$

Bewijs: stel $x \in G_1$, $\text{orde}(x) = n < \infty$, dan $f(x)^n = f(x^n) = f(e_1) = e_2$ dus via St. 5.5 geldt $\text{orde}(f(x)) \mid \underbrace{n}_{= \text{orde}(x)}$.

stel dat f injectief is doorheen, dan $f(x)^p = e_2$

$\Rightarrow$ $f(x^p) = e_2 = f(e_1) \underset{\text{injectief}}{\Rightarrow} x^p = e_1$

dus $\{p \in \mathbb{Z}_{>0} \mid f(x)^p = e_2\} = \{p \in \mathbb{Z}_{>0} \mid x^p = e_1\}$

dus $\text{orde}(f(x)) = \min\{p \in \mathbb{Z}_{>0} \mid f(x)^p = e_2\} = \min\{p \in \mathbb{Z}_{>0} \mid x^p = e_1\} = \text{orde}(x)$. $\blacksquare$

Def de orde van een groep G, genoteerd orde(G) of $\#G$, is het aantal elementen van de verz. G. Hierdoor volgt nu uit gevolg 5.6 dat orde$(\langle x \rangle)$ = orde(x), (wat voor orde ∞ niet zo veel betekent, maar wel voor eindige orde).

St. 5.9 voor A eindige abelse groep geldt dat elke $x \in G$ een orde(x) heeft die $\#A$ deelt. Het bewijs is eenvoudig gegeven met voor $x \in G$ $\lambda_x(G)$ te bekijken ($G = \{g_1, \ldots g_n\}$) en te zien $G = \lambda_x(G)$ dus $g_1 \cdot \ldots \cdot g_n = xg_1 xg_2 \cdot xg_n \Rightarrow x^n = e \Rightarrow \text{orde}(x) | n$ □

Opm we gaan een veel algemener bewijs geven dat ook op niet-abelse groepen en elke ondergroep betrekking heeft, 5.30. Dus deze stelling is niet zo belangrijk nu. Gevolg is wel:

Gevolg (Stelling van Euler) $a, m \in \mathbb{Z}$, ggd$(a,m) = 1$, dan
$$a^{\varphi(m)} \equiv 1 \bmod m$$

Bewijs ggd$(a,m) = 1$, dus $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^*$. $(\mathbb{Z}/m\mathbb{Z})^*$ is een Abelse groep A, dus pas 5.9 (of 5.30..) toe met $n = \#(\mathbb{Z}/m\mathbb{Z})^* = \varphi(m)$ dan zien we orde$(\bar{a})$ deelt $\varphi(m)$, dus $\bar{a}^{\varphi(m)} \equiv \bar{1}$ via st. 5.5. Dus $a^{\varphi(m)} \equiv 1 \bmod m$

$\Longrightarrow$ voor p priem geldt voor elke $a \in \mathbb{Z}$ dat ggd$(a,p) = 1$ en $\varphi(p) = p-1$. Dit geeft $a^{p-1} \equiv 1 \bmod p$, oftewel
$a^p \equiv a \bmod p$, de (Kleine Stelling van Fermat).

Vb $a \in \mathbb{Z}$, dan $a^{11-1} \equiv 1 \bmod 11$, $a^{31} \equiv 1 \bmod 31$
uit $a^{10} \equiv 1 \bmod 11$ volgt $a^{30} \equiv 1^3 \bmod 11 \equiv 1 \bmod 11$
dus $a^{30} \equiv 1 \bmod 11$, $a^{30} \equiv 1 \bmod 31$. De Chinese reststelling zegt nu dat er modulo $11 \cdot 31$ (31 en 11 zijn beide priem dus relatief priem) een unieke n is zdd ($n \equiv 1 \bmod 11 \wedge n \equiv 1 \bmod 31$). Omdat $n = 1$ voldoet, is $n \equiv 1 \bmod 341$ $(341 = 31 \cdot 11)$.
Dus $a^{30} \equiv 1 \bmod 341 \Longrightarrow a^{31} \equiv a \bmod 341$ (Tentamenopgave)

Def $H \leq G$ o.g. en $a \in G$. De linkernevenklasse (LNK) van H in G met a is: $aH := \{a \cdot h \in G \mid h \in H\}$
de rechternevenklasse (RNK) is $Ha := \{h \cdot a \in G \mid h \in H\}$

De verz. $\{aH \subset G \mid a \in G\}$ schrijft men als G/H, die van de RNK's als $H \backslash G$. (Raak niet verward met de verschilverzameling $G \setminus H := G \cap H^c$.)

Opm als je G additief schrijft geeft dit $a + H$ en $H + a$
Ingeval G abels is, merk op $aH = Ha$ (H6: elke H is dan een normaaldeler)

Vb in S_n is er o.g. A_n. als $a \in A_n$, dan geldt
$a' \in A_n \Rightarrow aa' \in A_n$, $a'a \in A_n$, dus $aA_n \subset A_n \supset A_n a$,
anderzijds $\# aA_n = \# \lambda_a(A_n) = \# A_n$ vanwege injectiviteit (analoog $A_n a = \rho_a(A_n)$)
dus $aA_n = A_n a = A_n$.
Als $a \notin A_n$, dan is a oneven, dus voor $a' \in A_n$ is aa' en $a'a$ ook oneven, dus $aA_n = A_n a = S_n \setminus A_n$. Dus $S_n / A_n = \{A_n, S_n \setminus A_n\}$

zij $H \subset \mathbb{R}^2$ ($\mathbb{R}^2$ met $(a,b) + (c,d) := (a+c, b+d)$)
dan is een ondergroep bijvoorbeeld H, een rechte lijn door de oorsprong.
En $a + H$ is dan een lijn parallel aan H die door $a \in \mathbb{R}^2$ gaat, en $a + H = H + a$ (abels). Merk weer op, als $a \in H$, dan $a + H = H$.

St. 5.18 G groep $H \subset G$ ondergroep

(a) $\forall a,b \in G$: $aH = bH \Leftrightarrow a^{-1}b \in H$	$Ha = Hb \Leftrightarrow ab^{-1} \in H$
(b) $\forall a,b \in G$: $aH \cap bH = \emptyset$ óf $aH = bH$	$Ha \cap Hb = \emptyset$ óf $Ha = Hb$.
(c) $\forall x \in G : \exists!\, L \in G/H : x \in L$.	$\exists!\, R \in G/H : x \in R$

Bew. neem de relatie $\sim \subset G \times G$ door $a \sim b : a^{-1}b \in H$.
dan (1) $a^{-1}a = e \in H$ wegens H o.g. (G2) $\Rightarrow$ $\forall a \in G: a \sim a$
(2) $a^{-1}b$, $b^{-1}c \in H \Rightarrow (a^{-1}b)(b^{-1}c) \in H$ wegens (H1)
dus $a^{-1}c \in H \Rightarrow \forall a,b,c \in G$: $a \sim b$ $b \sim c \Rightarrow a \sim c$
(3) $a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H$ wegens (H2)
$\Rightarrow b^{-1}a \in H \Rightarrow$ $\forall a,b \in G$: $a \sim b \Rightarrow b \sim a$

dus $\sim$ is een equivalentierelatie. Zij $\bar{a}$ de equivalentieklasse van a. dan $b \in \bar{a} \Leftrightarrow \exists h \in H: a^{-1}b = h \Leftrightarrow \exists h \in H: b = ah$
$\Leftrightarrow b \in aH$. Dus de LNK's zijn precies de equivalentieklassen van $\sim$.
Hieruit volgt dat $G/H = G/\sim$, een partitie van H is, en
dat bewijst (b) en (c), alsook (a): $aH = bH \Leftrightarrow a \sim b$. ■

Bewijs voor RNK's gaat analoog, uiteraard.

St. 5.21 G groep, H o.g. dan $\# aH = \# Ha = \# H \quad \forall a \in G$.
Bewijs: ρ_a, λ_a is bijectief, en dus $\# \lambda_a(H) = \# H = \# \rho_a(H)$ ■

Def. $G \supset H$, H og. van g. G. Dan heet de index van H in G:
$[G:H] := \#(G/H)$ en $[H:G] := \#(H\backslash G)$

Def Een representantensysteem S voor G/H of $H\backslash G$ is een verz. $S \subset G$
zdd $\forall L \in G/H: \exists! s \in S: s \in L$, dus er bestaat een
bijectief $f: S \to G/H$ door $s \mapsto sH$.
Opm We zien dan $G = \bigsqcup_{s \in S} sH$. En ook $[G:H] = \# S$.

Vb. voor S_n en A_n: $S = \{(1), (12)\}$ als $n \geq 2$, dan zijn
er immers $S_n/A_n = \{A_n, (12)A_n\}$ en $(1) \in A_n$, $(12) = (12)(1) \in (12)A_n$

Vb voor $\mathbb{Z}/n\mathbb{Z}$ met ondergroep $n\mathbb{Z}$ en $\sim$: $a - b \in n\mathbb{Z}$
hebben we representanten $\{0, 1, \ldots, n-1\}$. ihb. $[\mathbb{Z}:n\mathbb{Z}] = n$.

St. 5.24 (Lagrange) g. $G \supset H$ og. dan $\# G = [G:H] \cdot \# H$
(in oneindige groepen kunnen hier kardinaliteitsgetallen worden gezien).

Bew. kies een representantensysteem S van G/H, dan $\# S = [G:H]$ en
$$G = \bigsqcup_{s \in S} sH \Rightarrow \# G = \sum_{s \in S} \# sH = \# S \cdot \# H$$
$\Rightarrow \# G = [G:H] \cdot \# H$. □

Gevolg H og. $\subset G$ g., G eindig. Dan deelt $\# H \mid \# G$
en ook $[G:H] \mid \# G$.

Gevolg. $H_1 \subset H_2 \subset G$, H_1, H_2 o.g., G $\overset{\text{eindig}}{\text{g.}}$ Dan H_1 ook o.g van H_2
en $[G : H_1] = [G : H_2] \cdot [H_2 : H_1]$

Gevolg 5.30 (zie 5.9 voor zwakkere uitspraak). G eindige g., $x \in G$
dan orde(x) | G, <u>want</u> $\# \langle x \rangle \mid \# G$

Gevolg 5.31 G groep, met $\# G = p$, p priem, is een cyclische
groep en isomorf met $\mathbb{Z}/p\mathbb{Z}$ (of C_p)

Bewijs: $p \geq 2$ dus neem een $x \in G$ zdd $x \neq e$, die bestaat.
dan deelt orde(x) p, maar p heeft delers $\{1, p\}$ en
orde$(x) = 1 \Rightarrow x = e$, dus orde$(x) = p$. Dus $\# \langle x \rangle = p \Rightarrow \langle x \rangle = G$.

St. 5.33 (Stelling van Cauchy) (Het bewijs is gruwelijk met de kennis die we nu hebben, in H8 wordt een bewijs op heel andere principes gegeven).
G eindige groep, p priemdeler van $\# G$. Dan
is er een $x \in G$ zdd orde$(x) = p$.

Opm dit is een gedeeltelijke omkering van: $x \in G$, dan orde$(x) \mid \# D$.
we moeten namelijk voor de deler aannemen dat deze priem is, en
dan kunnen we een $x \in G$ vinden zdd orde$(x) = p$.
Dus elke orde(x) deelt $\# G$, niet elke ~~orde~~ deler van $\# G$
is een orde van een $x \in G$. (Anders zou elke G cyclisch zijn!)

— Bewijs kennen van 5.5, 5.24 (lagrange), 5.18(b,c), 5.21

5.24 moet worden bewezen met 5.18 b,c en 5.21.