$sr^n s = ssr^{-n} = r^{6-n}$ $\quad sr^5 s = ssr^{-5} = r$

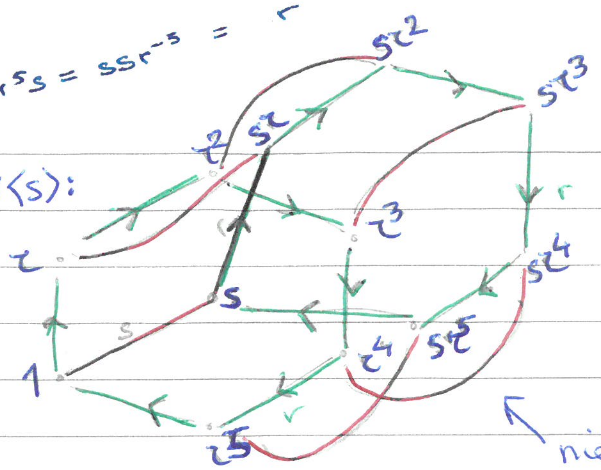
ind. $sr^n = r^{-1}sr^{n-1} = r^{-1}r^{-(n-1)}s = r^{-n}s$

$(sr)^2 = 1 \Rightarrow sr = r^{-1}s^{-1} = r^{-1}s$

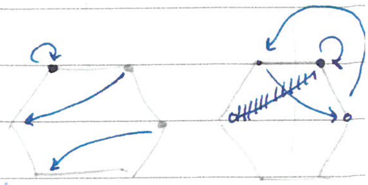
sr

rs

Dit is $\langle r \rangle \times \langle s \rangle$: want de groep is commutatief



niet D_6!



2 VRIJE GROEPEN

def neem een verzameling S van symbolen, geheten een alfabet. Voor $s \in S$ maken we ook het symbool s^{-1}, de 'formele inverse' van s, en we noteren $S^{-1} = \{s^{-1} \mid s \in S\}$. verder $S^{\pm} = S \cup S^{-1}$, dus $S \cap S^{-1} = \emptyset$ in h.b.

we noemen een rij w van $k \in \mathbb{N}$ symbolen uit $S^{\pm}$, schrijf $w = s_1 \dots s_k$, $s_i \in S^{\pm}$, een woord en noemen de lengte $|w|$ van w: k.

Het lege woord $\emptyset$ is het ~~woord~~ met 0 symbolen.
$S^* := \{\text{woorden over } S\}$

def twee woorden w, v heten equivalent, $w \sim v$, als ze in elkaar getransformeerd kunnen worden door een eindig aantal inserts / deletes van subwoorden van de vorm ss^{-1} of $s^{-1}s$, $s \in S$.

dit is een equivalentierelatie. We kunnen een bin. op. op $S^*/\sim$ definiëren door $[w]\cdot[v] := [wv]$ te zetten waarbij $wv \in S^*$ de concatenatie van w en v is. Probleem:

- aantonen dat dit welgedefinieerd is ; daarna
- aantonen dat dit associatief is. (dat is makkelijker want concatenatie is dat ook (met inductie naar woordlengte))

— het kan ook anders, geïnspireerd op Cayley graaf.

2.2

St. Elke equivalentieklasse $[w]$, $w \in S^*$, bevat een uniek "gereduceerd woord"

def een gereduceerd woord $w \in S^*$ is een woord waarin geen deelwoorden van de vorm ss^{-1} of $s^{-1}s$ voorkomen, $s \in S$

bew neem w en haal alle deelwoorden $s^{-1}s$ of ss^{-1} eruit. Dit is een eindig proces, want w maakt men elke keer korter en dus houd men een kortste woord $v \geq \emptyset$ over. Dit woord $v \sim w$ per definitie. $\Rightarrow$ existentie van v.

Uniciteit: stel $u \in [w]$ is ook gereduceerd. Dan kunnen we u en v in elkaar transformeren in eindig aantal inserts / deletes van $s^{-1}s$ of ss^{-1}, $s \in S$

in het pad $u \overset{=}{\to} u_1 \to u_2 \to \dots u_n \overset{=}{\to} v$, waarbij elke $u_i \to u_{i+1}$ een deletie/insertie heeft, en we aannemen dat $\sum_{i=1}^{n} |u_i|$ minimaal is over alle mogelijke paden $u \to .. \to v$, moet de ~~eerste~~ laatste stap een deletie en de ~~laatste~~ eerste een insertie zijn dus $|w_i|$ neemt een lokaal maximum aan voor een $1 < i < m$. $w_{i-1} \to w_i \to w_{i+1}$ door eerst een ss^{-1} te inserten en vervolgens een tt^{-1} te deleten, $s,t \in S^{\pm}$.

identiek en zelfde positie

$\Rightarrow$ 1) $tt^{-1} = ss^{-1}$ dan kunnen we $w_{i-1} = w_{i+1}$ en w_{i-1}, w_i geheel weglaten $\Rightarrow \sum_i |w_i|$ niet minimaal.

2.4 St De cayleygraaf $\Gamma = \Gamma(F(S), S)$ voor F de vrije groep over S, is een boom.

Bew. Het is duidelijk dat elke cayleygraaf samenhangend is want $\forall g \in V(\Gamma)$ heeft een product van voortbrengers in S en dat geeft een pad naar g vanuit e

Echter is het nu ook aan te tonen dat Γ geen cykels bevat. Laat Γ zo'n circuit van $s_i^{\pm} \in S$ bevatten, waarbij s_i^{-1} aanduidt dat lijn $s_i \in E(\Gamma)$ in omgekeerde oriëntatie $\bar{s}$ bewandeld wordt. noteer $w = s_1^{\pm} \cdots s_k^{\pm}$

Enerzijds bevat $[w]$ als het unieke gereduceerde woord het lege woord, dus $[w] = [\emptyset] = e$ dus w is één enkel punt en dus geen circuit. $\square$

Wanneer men machten van een gereduceerd woord neemt en deze uitschrijft als gereduceerd woord, kan het woord alleen korter worden als $w = s_1 \cdots s_k$ en $s_1 = s_k^{-1}$

def wanneer $s_1 \neq s_k^{-1}$ dan is w^m $m \in \mathbb{N}$ gereduceerd. Dan heet w cyclisch gereduceerd.

Deze terminologie omdat elke cyclische shift $s_i s_{i+1} \cdots s_k s_1 \cdots s_{i-1}$ $1 \leq i \leq k$ ook weer gereduceerd is

Anders, als $s_1 = s_k^{-1}$, dan $w = s_1 w' s_1^{-1}$ en dus $w^n = s_1 w'^n s_1^{-1}$ waar w'^n misschien gereduceerd is.

Omdat we dit willen structureren, schrijf $w = u\hat{w}u^{-1}$ voor u, woord en $\hat{w}$ cyclisch gereduceerd, w gereduceerd

prop deze notatie is uniek, want als $w = v\hat{x}v^{-1}$ voor $\hat{x}$ cyclisch gereduceerd, dan is v even lang als u want als één langer is dan is $\hat{x}$ of $\hat{w}$ juist niet cyclisch gereduceerd: en v is dus zo lang mogelijk dat $v = s_1 \cdots s_\ell$ en $w = s_1 \cdots s_\ell \hat{x} s_\ell^{-1} \cdots s_1^{-1}$
Hieruit zien we ook $2\ell < k$ als $w = s_1 \cdots s_k$.

St 2.5 $F(S)$ is torsie-vrij, dwz er zijn geen elementen van eindige orde behalve e.

Bew. Zij $[w] \in F(S)$, en neem zvva w gereduceerd. Dan schrijf $w = u\hat{w}u^{-1}$ voor $\hat{w}$ cyclisch gereduceerd. Er volgt $w^n = u\hat{w}^n u^{-1}$ en dit is een gereduceerd woord. Dus als $[w] \neq e$ dan $w \neq \emptyset$ dus $\hat{w} \neq \emptyset$ dus $|w^n| > |w| > 0$ dus $w^n \neq \emptyset$ en is gereduceerd, dus $w^n \notin [\emptyset] \Rightarrow [w]^n \neq e$ $\forall n \geq 0$ $\square$

2.6 St $g, h \in F(S) = F$ vrije groep over S. Dan
$gh = hg \iff g = x^m,\ h = x^n$ voor $x \in F$, $n, m \in \mathbb{Z}$

Bew. $\Leftarrow$ is triviaal $gh = x^m x^n = x^{m+n} = x^{n+m} = hg$ alle groepen.
$\Rightarrow$:
neem g, h gereduceerd. Dan met inductie op $|g| + |h|$ (≥ 0):

IB $|g|+|h| \leq 1 \Rightarrow$ dan $g = \emptyset$ of $h = \emptyset$ dus ~~$gh = ge = eg = hg$ of $gh = eh = he = hg$.~~
$g = g,\ h = g^0$ of $g = h^0,\ h = h$

IS stel het geldt voor $|g| + |h| < k$.
Dan neem g, h met $gh = hg$ en $|g| + |h| = k$

schrijf gh en hg als gereduceerde woorden:
dus $g = s_1 \cdots s_k$ gereduceerd $s_i \in S$
$h = t_1 \cdots t_\ell$ gereduceerd $t_i \in S$

dan $gh = s_1 \cdots s_{k-r} t_{r+1} \cdots t_\ell$ waarbij s_k tegen t_1 cancelt als $s_k = t_1^{-1}, \ldots$ s_{k-r+1} tegen t_r.
neem dus dat $s_1 \cdots s_{k-r} t_{r+1} \cdots t_\ell$ gereduceerd is.
Nu schrijven we hg ook zo: $hg = t_1 \cdots t_{\ell-p} s_{p+1} \cdots s_k$

merk echter op dat $[hg] = [gh]$ en deze equivalentieklassen bevatten slechts één uniek gereduceerd woord, dus

$s_1 \cdots s_{k-r} t_{r+1} \cdots t_\ell = t_1 \cdots t_{\ell-p} s_{p+1} \cdots s_k$ als gereduceerde woorden, en dus $r = p$ want ze zijn i.h.b. even lang!

er "valt nu $2r$ lengte weg" aan letters. We onderscheiden drie gevallen voor r:

— $r=0$: dan is gh gereduceerd als concatenatie
dus $s_1 \cdots s_k t_1 \cdots t_\ell$ en $t_1 \cdots t_\ell s_1 \cdots s_k$ zijn gereduceerd.

In dat geval zijn ze gelijk als woorden want $[gh] = [hg]$ en deze klassen hebben als uniek gereduceerd woord $s_1 \cdots s_k t_1 \cdots t_\ell$ en $t_1 \cdots t_\ell s_1 \cdots s_k$

neem zvva dat $k \leq \ell$. Dan is $s_1 \cdots s_k$ een "initial segment" van $t_1 \cdots t_\ell$. Dus $h = gu$ voor $u = t_{k+1} \cdots t_\ell$ gereduceerd

$\Rightarrow$ $gh = hg$ wordt $g^2 u = gug$
wordt $gu = ug$ dus u en g commuteren. Maar $|g| + |u| < |g| + |h|$, met IH volgt: $g = x^m$, $u = x^n$. Dus $h = gu = x^m x^n = x^{m+n}$ en dit was te bewijzen

— $r = \ell$: ~~dan is $[gh] \ni t_{r+1} \cdots t_\ell$ en $t_{r+1} \cdots t_\ell$ is gereduceerd want h is dat. tevens $t_1 \cdots t_{\ell-r} \in [hg] = [gh]$ dus $t_1 \cdots t_{\ell-r} = t_{r+1} \cdots t_\ell$ als gereduceerde woorden~~

g wordt volledig uitgedoofd door het voorste deel van h dus $h = g^{-1}u$ als gereduceerde woorden. Tevens $h = ug^{-1}$ als gereduceerde woorden $\Rightarrow$ $gh = hg$ geeft $u = g^{-1}ug$ dus $gu = ug$ en $|g| + |u| < |g| + |h|$ dus we zien weer $g = x^n$ $u = x^m$ dus $h = x^{m-n}$.

— $r < \ell$, $r > 0$: Gedeeltelijke cancellatie: we vergelijken de gereduceerde woorden en vinden
$s_1 = t_1, \ldots t_\ell = s_k$ en $s_k = t_1^{-1}$ en $t_\ell = s_1^{-1}$
vanwege cancellatie $\rightarrow$: dus $g = s_1 g' s_1^{-1}$, $h = s_1 h' s_1^{-1}$
voor g', h' gereduceerd.

vanwege $gh = hg$ geldt dus $s_1 g' h' s_1^{-1} = s_1 h' g' s_1^{-1}$
als gereduceerde woorden, dus $g'h' = h'g'$ en ook
als gereduceerde woorden, met $|g'| + |h'| < |g| + |h|$
$\Rightarrow$ $g' = x^n$, $h' = x^m$ en dus $g = s_1 x^n s_1^{-1}$, $h = s_1 x^m s_1^{-1}$.
maar $s_1 x^n s_1^{-1} = (s_1 x s_1^{-1})^n$, $s_1 x^m s_1^{-1} = (s_1 x s_1^{-1})^m$
dus $g = y^n$, $h = y^m$ voor $y = s_1 x s_1^{-1} \in F$ $\square$

2.2 UNIVERSELE EIGENSCHAP VAN VRYE GROEPEN.

2.7 Zij $F = F(S)$ de vrije groep over S en zij G een groep en $\varphi : S \to G$ een afbeelding.
Dan is er een <u>uniek</u> homomorfisme $\varphi^* : F(S) \to G$ dat φ uitbreidt.

Bew Aangezien $F(S)$ wordt voortgebracht door $S \subseteq F$ is er hoogstens één φ^* die φ uitbreidt, want een homomorfisme wordt vastgelegd door zijn waarden op de voortbrengers.

en $\varphi^*(s^{-1}) = \varphi(s)^{-1}$ voor $s \in S$

Existentie: definieer $\varphi^*(g) = \varphi(s_1^{\pm}) \cdot\cdot \varphi(s_k^{\pm}) \in G$
waarbij $g = s_1^{\pm} \cdot\cdot s_k^{\pm}$ als gereduceerd woord.
Ten eerste is deze definitie niet afhankelijk van een keuze van $s_1^{\pm} \cdot\cdot s_k^{\pm}$, want $s_1^{\pm} \cdot\cdot s_k^{\pm} \in [g]$ is uniek.

We moeten dus alleen aantonen dat dit inderdaad een homomorfisme geeft. Dit doen we als volgt:

$$\varphi^*(s)\varphi^*(s^{-1}) = \varphi(s)\varphi(s)^{-1} = e$$

Dus als $h = s_1^{\varepsilon} \cdot\cdot s_k^{\varepsilon}$, $g = t_1^{\varepsilon} \cdot\cdot t_\ell^{\varepsilon}$ als gereduceerde woorden en $hg = s_1^{\varepsilon} \cdots s_{k-r}^{\varepsilon} t_{r+1}^{\varepsilon} \cdot\cdot t_\ell^{\varepsilon}$ dan
$s_{k-r}^{\varepsilon} = t_1^{-\varepsilon} \ldots s_k^{\varepsilon} = t_r^{-\varepsilon}$ en dus

$$\varphi^*(hg) \overset{\text{def}}{=} \varphi(s_1)^{\varepsilon}\varphi(s_2)^{\varepsilon} \cdot\cdot \varphi(s_{k-r})^{\varepsilon}\varphi(t_{r+1})^{\varepsilon} \cdot\cdot \varphi(t_\ell)^{\varepsilon}$$
$$= \varphi(s_1) \cdot\cdot \varphi(s_{k-r})^{\varepsilon} e^r \varphi(t_{r+1})^{\varepsilon} \cdot\cdot \varphi(t_\ell)^{\varepsilon}$$

$$\ldots = \varphi(s_1)^\varepsilon \cdots \varphi(s_{k-r})^\varepsilon \varphi(s_{k-r+1})^\varepsilon \cdots \varphi(s_k)^\varepsilon \varphi(s_k)^{-\varepsilon} \cdots \varphi(s_{k-r+1})^\varepsilon \varphi(t_{r+1})^\varepsilon \cdots \varphi(t_\ell)^\varepsilon$$

$$= \underbrace{\varphi(s_1)^\varepsilon \cdots \varphi(s_{k-r})^\varepsilon \varphi(s_{k-r+1})^\varepsilon \cdots \varphi(s_k)^\varepsilon}\ \underbrace{\varphi(t_1)^\varepsilon \cdots \varphi(t_r)^\varepsilon \varphi(t_{r+1})^\varepsilon \varphi(t_\ell)^\varepsilon}$$

$$\overset{def}{=} \underbrace{\varphi^*(s_1^\varepsilon \cdots s_r^\varepsilon)}_{\text{want } s_1^\varepsilon \cdots s_r^\varepsilon \text{ is gereduceerd}} \cdot \underbrace{\varphi(t_1^\varepsilon \cdots t_\ell^\varepsilon)}_{\text{want } t_1^\varepsilon \cdots t_\ell^\varepsilon \text{ is gereduceerd}}$$

$\Rightarrow$ $\varphi^*(g)\varphi^*(h) = \varphi^*(gh)$ en dit voor alle $h, g \in F$ gereduceerd, en dat kunnen we zwa voor allemaal want elke $g \in F$ correspondeert met een unieke $\hat{g} \in F$ gereduceerd en dus

$$\varphi^*(gh) \overset{def}{=} \varphi^*(\hat{g}\hat{h}) \underset{\text{vanwege groepseig. } F}{=} \varphi^*(\hat{g}\hat{h}) \underset{\text{dit is boven bewezen}}{=} \varphi^*(\hat{g})\varphi^*(\hat{h}) \overset{def}{=} \varphi^*(g)\varphi^*(h)$$

$\square$

De omkering is interessant:

def De universele eigenschap van de vrije groep $F = F(S)$ is de hierboven beschreven / bewezen eigenschap.

def Een groep G heet vrij met basis $S \subseteq G$ als er voor elke groep G' en afb $\varphi : S \to G'$ een unieke uitbreiding $\varphi^* G \to G'$ is die een homomorfisme is.

2.9 St. Elke groep G die vrij met basis $S \subseteq G$ is, is isomorf met de vrije groep over S (als alfabet)

Bew: neem $\varphi : S \to F(S)$ als $s \mapsto s$, embedding. Dan is er een uniek homomorfisme $\varphi^* : G \to F(S)$ die φ uitbreidt. Nu is aan te tonen dat φ^* een bijectie is

– surjectiviteit: elke $f \in F$ kan op voortbrengers worden geschreven, dus volgt $f = s_1^\varepsilon \cdots s_k^\varepsilon = \varphi^*(s_1^\varepsilon \cdots s_k^\varepsilon)$ met $s_1^\varepsilon \cdots s_k^\varepsilon \in G$.

injectiviteit : zij $h \in \ker(\varphi^*)$ van minimale gereduceerde lengte $h = s_1^{\varepsilon} \cdots s_k^{\varepsilon}$ in G, schrijf h als minimaal woord van voortbrengers.

Dan $\varphi^*(h) = s_1^{\varepsilon} \cdots s_k^{\varepsilon} = e$ en omdat $s_1^{\varepsilon} \cdots s_k^{\varepsilon}$ minimaal product van voortbrengers is, is $s_1^{\varepsilon} \cdots s_k^{\varepsilon} \in F$ gereduceerd. Maar dan is $k=0$ want $s_1^{\varepsilon} \cdots s_k^{\varepsilon}$ kan alleen maar het lege woord zijn als het gelijk is aan e in F

$\Longrightarrow$ $h = e_G$ dus kern triviaal $\square$

φ^* is dus een isomorfisme.

2.10 Gevolg G is vrij van basis $S \subseteq G$ $\Longleftrightarrow$

1) $\langle S \rangle = G$
2) geen woord van lengte > 0 over $S^{\pm}$ is gelijk aan $e \in G$

Bew. $\Rightarrow$ Dit is de eigenschap dat $F(S)$ geen triviale relatoren heeft, dus $G \cong F(S)$ ook niet

$\Leftarrow$ neem $i : F \to G$ door $f \in G$ af te beelden op $s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ waar $f = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$ als gereduceerd woord in S^* in F is. Dan is i_F duidelijk surj.

want $\langle S \rangle = G$ en $\ker(i_F) = \{ s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} \in F \mid s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} = e \text{ in } G \}$
$= \{e\}$ want er zijn geen woorden over $S^{\pm}$ die in G e zijn.

dus $i_F : F \to G$ is een isomorfisme en dus is G te identificeren met vrije groep $F(S)$ en dan volgt met 2.7 dat G vrij is met basis S. $\square$

wat een equivalenties weer.

Diagram:

$$\begin{tikzcd} S \arrow[d, "id_S"] \arrow[dr, bend left, "\varphi"] & \\ F(S) \arrow[r, dashed, "\varphi^*"] & G \end{tikzcd}$$

$\exists! \, \varphi^* : \varphi = \varphi^* \circ id_S$, φ^* hom. $F \to G$

Gevolg 2.11 Zij G groep $G = \langle X \rangle$. Dan is G een quotiëntgroep van $F(X)$, i.e $G \cong F(X)/H$

Bew. neem $id_X : X \to G$ embedding. Dan is er de unieke uitbreiding $\varphi^* : F(X) \to G$ wegens 2.7. Met de eerste isomorfiestelling volgt $F(X)/Ker(\varphi^*) \cong \varphi^*(X)$ en $X \subseteq \varphi^*(X)$ dus $G = \langle X \rangle \leq \varphi^*(X)$ want $\varphi^*(X) \leq G$. Dus $F(X)/_{ker\,\varphi^*} \cong G$ $\square$

2.12 Zij G groep met voortbrengende verz S. Als $\Gamma(G,S)$ een boom is dan is G vrij met basis S.

Bew 1) S brengt G voort

2) te laten zien is dat voor φ^* de unieke uitbr. van $\varphi : S \to G$ door $s \mapsto s$, geldt dat deze injectief is.

Bewijs hiervan: laat $w = s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} \in ker\,\varphi^*$ een woord van minimale lengte zijn. (k minimaal, zd $k > 0$)

Het is dan gereduceerd, want anders $s_i = s_{i+1}^{-1}$ voor een i en we kunnen dan ook $s_1^{\varepsilon_1} \cdots s_{i-1}^{\varepsilon_{i-1}} s_{i+2}^{\varepsilon_{i+2}} \cdots s_k^{\varepsilon_k}$ schrijven. Verder $s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} = e$ in G

Dus, dit geeft een pad in $\Gamma(G,S)$ dat begint en eindigt in e.

Dat kan in een boom alleen als het een geodesic heen- en terug bewandelt.

dus het bevat een backtrack $s_i \overline{s_i}$

maar het heen en terugbewandelen van een . lijn correspondeert in $\Gamma(G, S)$ met het rechtsverm. met s, daarna met s^{-1}. $\Longrightarrow$ er is een deelwoord ss^{-1} in $s_1^{\varepsilon_1}\cdots s_k^{\varepsilon_k}$ $\Longrightarrow$ $s_1^{\varepsilon_1}\cdots s_k^{\varepsilon_k}$ is niet van minimumlengte want we kunnen dit deelwoord verwijderen:

$$\varphi^*(s_1^{\varepsilon_1}\cdots s_{i-1}^{\varepsilon_{i-1}} s_{i+2}^{\varepsilon_{i+2}}\cdots s_k^{\varepsilon_k}) = \varphi^*(s_1^{\varepsilon_1}\cdots s_{i-1}^{\varepsilon_{i-1}})\, e\, \varphi^*(s_{i+2}^{\varepsilon_{i+2}}\cdots s_k^{\varepsilon_k})$$
$$= \varphi^*(s_1^{\varepsilon_1}\cdots s_{i-1}^{\varepsilon_{i-1}} s_i^{\varepsilon} s_i^{-\varepsilon} s_{i+2}^{\varepsilon_{i+2}}\cdots s_k^{\varepsilon_k}) = e$$

dus er is een korter woord in de kern. Als dit niet-triviaal is, hebben we een tegenspraak.
[Als $w = s$ was, dat kan sowieso niet want dan $\varphi^*(s) = e$ en dus $s = e$ want $\varphi^*(s) = \varphi(s) = s$ maar $w \neq e$ per aanname]
Als het kortere woord e was, dan was $w = ss^{-1} = e$ ook tegenspraak. Dus $\ker(\varphi^*) = \{e\}$ $\Rightarrow$ $G \cong F(S)$ $\square$

— dit bewijst de omkering van 2.4 !

— we noemen $S \subseteq G$ zodat G vrij is met basis S, een basis. Dat lijkt een suggestie te zijn voor unieke kardinaliteit.. inderdaad het geval!

2.13 Als F vrij is, dan heeft elke basis voor F dezelfde kardinaliteit. Dit definiëren we de rang van F.

bew. Zij S basis voor F, dus voor S geldt de universele eigenschap.

Zij G de groep van Abelse functies $f: S \to \mathbb{Z}_2$ met eindige support, dus eindig veel $s \in S$ zodat $f(s) = 1$. [als S eindig is met $\#S = n$, dan kan men G identificeren met $\mathbb{Z}_2^n$]. Neem φ^* unieke uitbr. van φ op F. waarbij $\varphi: S \to G$,
$$\varphi: s \mapsto f_s, \quad f_s(s') = \begin{cases} 1 & \text{als } s = s' \\ 0 & \text{als } s \neq s' \end{cases}$$

Dan is $N = \ker \varphi^*$ de woorden over S waarin s en s^{-1} samen een even aantal keer voor komen voor elke $s \in S$.

De claim is dat N de groep $\square_F = \langle \{ w^2 \mid w \in F \} \rangle$ is gegenereerd door kwadraten van $w \in F$.

duidelijk is $w^2 \in N$ voor alle $F \ni w$ dus $\square_F \subseteq N$
Omgekeerd, $w \in \ker(\varphi^*)$, dan stel dat voor w' met $|w'| < |w|$ en $w' \in \ker(\varphi^*)$ al bewezen is dat $w' \in \square_F$
zij $s \in S^{\pm}$ de eerste letter van w
Omdat $w \in \ker \varphi^*$ volgt $w = sw's^{-1}v$ of $w = sw'sv$

- voor $w', v \in \ker(\varphi^*)$. $w = sw's^{-1}v$ geeft

$$w = sw's^{-1}v = s^2(s^{-1}w')^2 w'^{-1} v \Longrightarrow$$

$$s^{-2}(s^{-1}w')^{-2} w = w'^{-1}v \in \square_F \text{ per IH}$$

want $w'v \in \ker(\varphi^*)$ en $|w'v| < |w|$

dus $w \in \square_F$.

- Als $w = susv$ dan $w = (su)^2 u^{-1} v$, $u, v \in \ker(\varphi^*)$ en dus met $u^{-1}v \in \square_F$ wegens IH geeft dit $w \in \square_F$

Omdat φ^* surjectief is, immers elke $f : S \to \mathbb{Z}_2$ met eindige support wordt geraakt door het woord $w = s_1 \ldots s_k$ waarbij $\{s_1, \ldots s_k\}$ de support van f is, volgt dat $G \cong F/N = F/\square_F$

Hierbij is $F/\square_F$ een groep onafhankelijk van S.
Dus voor elke basis $S \subseteq F$ is de groep G van eindig gesupporte abelse fies $S \to \mathbb{Z}_2$ van dezelfde cardinaliteit (want er is een bijectie met $F/\square_F$)

$\Rightarrow$ voor oneindige S is $|S| = |G| = |F/\square_F|$
eindige S " " $|G| = 2^{|S|}$ ihb is $|F/\square_F|$ eindig en $2^{|S|}$

— gevolg: twee vrije groepen F, G zijn isomorf $\Longleftrightarrow$ ze hebben bases van gelijke kardinaliteit

Bew $\Leftarrow$ neem bijectie met inbedding $S_F \xrightarrow{\sim} S_G \hookrightarrow G$.
dan is de universele eigenschap: uitbreiding tot homom. $F \to G$. Dit is surjectief want $\langle S_G \rangle = G$ en $S_F \xrightarrow{\sim} S_G$ was surjectief. Ook injectief want als er een niet-triviale $s_1 \cdots s_k \in S_F^*$ is met $\varphi^*(s_1 \cdots s_k) = e_G$ dan zou $s_1' \cdots s_k' = e$ in G terwijl dit ook een gereduceerd woord is wegens isomorfie $\Rightarrow$ G is niet vrij, tegenspraak.

$\Rightarrow$ volgt met 2.13: zij S_F een basis voor F en S_G voor G. Zij $w = v^2$, $v \in F$. dan met ψ isomfisme $F \to G$ volgt $\psi(v^2) = \psi(v)^2$ dus we zien dat $\psi|_{\square_F} : \square_F \to \square_G$ kan en dit is nog steeds injectief, en evenzo surjectief (neem $w \in \square_G$, dan is w voortgebr. door $w_i^{\pm 2}$, $w_i \in G$, en $\psi : F \to G$ is surjectief dus er is een $v_i \in F$ met $\psi(v_i) = w_i$, dus $\psi(\prod_i v_i^{\pm 2}) = w$ wordt geraakt)

hieruit volgt $\square_F \cong \square_G$ dus met $F \cong G$ volgt $F/\square_F \cong G/\square_G$ en dit bepaalt dus $|F/\square_F| = |G/\square_G|$ dus bases S_F, S_G moeten wel gelijke kardinaliteit hebben.

$\boxtimes$