Algèbre 1 2008-09
Obligatorisk opgave (la tâche obligatoire)

Rasmus Sylvester Bryder

Le 22 mai 2009

1

Soit une permutation $\sigma \in S_8$. On sait que $\sigma^3 = (1\ 2\ 3\ 4\ 5)$ et $\sigma^5 = (6\ 7\ 8)$. Il faut trouver σ.

Comme la notation ci-dessus exclut les points fixes, on sait que σ se compose de deux cycles de longueur 5 et 3, qui se composent des éléments $\{1,2,3,4,5\}$ et $\{6,7,8\}$ respectivement ;

c'est pourquoi un cycle de longueur 5 est toujours un cycle de longueur 5 quand on l'élève au cube – comme 5 est un nombre premier – et le structure n'est que changé quand on l'élève aux multiples de 5 ; la même chose pour l'autre cycle. Les éléments dans les cycles sont conservés de cela. Comme la permutation mouve 8 éléments, il n'y a pas d'autres cycles, parce que σ est une permutation dans S_8 !

Alors il faut trouver les cycles γ_1 et γ_2 de $\sigma = \gamma_1\gamma_2$, tel que $\gamma_1^3 = (1\ 2\ 3\ 4\ 5)$ et $\gamma_2^5 = (6\ 7\ 8)$. C'est facile de comprendre que $\gamma_1 = (1\ 3\ 5\ 2\ 4)$, tel que chaque élément est mouvé trois places ; l'image dans γ_1^3 de 1 est 2, etc. On sait de cela aussi que $\gamma_2 = (6\ 8\ 7)$.

Donc $\sigma = (1\ 3\ 5\ 2\ 4)(6\ 8\ 7)$ [1]. C'est facile de voir que cette σ satisfait aux exigences originales.

Comme σ se compose de 2 orbites, $\{1,2,3,4,5\}$ et $\{6,7,8\}$, et le nombre des éléments qui σ permute est 8, la signature de σ égale $\operatorname{sign}\sigma = (-1)^{8-2} = 1$, GRP(2.18). Donc σ est paire, GRP(2.22).

Il faut trouver l'indice de $\langle\sigma\rangle$ dans A_8. Soient les permutations dans S_8 $\sigma_1 = (1\ 3\ 5\ 2\ 4)$ et $\sigma_2 = (6\ 8\ 7)$. Celles-ci ont les ordres 5 et 3. Comme $\sigma_1\sigma_2 = \sigma_2\sigma_1 = \sigma$, et 3 et 5 sont premiers entre eux, le produit σ de celles-ci a l'ordre $3\cdot 5 = 15$, GRP(3.17). L'ordre de σ égale l'ordre du sous-groupe $\langle\sigma\rangle$, GRP(3.5). Alors $|\langle\sigma\rangle| = 15$ dans S_8.

Comme σ est paire, on sait que $\langle\sigma\rangle \in A_8$, parce que les signatures de tous les produits possibles de les puissances de σ est 1 ; alors tous les éléments de $\langle\sigma\rangle$ existent dans A_8. Le nombre des éléments dans A_8 est $8!/2$, GRP(2.22).

Donc le théorème de Lagrange GRP(4.2) dit que l'indice de $\langle\sigma\rangle$, $|A_8 : \langle\sigma\rangle|$, égale

$$|A_8 : \langle\sigma\rangle| = |A_8|/|\langle\sigma\rangle| = 8!/(2\cdot 15) = 8\cdot 7\cdot 6\cdot 4 = 1344.$$

1. On peut comprendre aussi que $\sigma = \sigma^6\sigma^{-5} = (\sigma^3)^2(\sigma^5)^{-1} = (1\ 3\ 5\ 2\ 4)(6\ 8\ 7)$.

2

Dans un groupe abélien d'ordre 1000 G, il existe 4 éléments d'ordre 10. Il faut demonstrer que G est cyclique.

Comme $1000 = 2^3 \cdot 5^3$, on peut ulitiser le théorème fondamental des groupes abéliens finis, GRP(6.10)(3), qui dit qu'on peut choisir les ordres des groupes cycliques d'un produit direct $\mathrm{C}_{m_1} \times \cdots \times \mathrm{C}_{m_r}$ tel que chaque m_i est un puissance d'un nombre premier, et GRP(6.11) dit qu'il faut que chaque m_i doive être un puissance d'un nombre premier de la factorisation de 1000 en un produit de nombres premiers, tel que $m_1 \cdots m_r = 1000$.

Comme il y a 3 manières de diviser 2^3 en des puissances de 2, et la même chose pour 5^3 en des puissances de 5, il y a $3 \cdot 3 = 9$ groupes abeliéns d'ordre 1000 à un isomorphisme près. Pour trouver quel groupe de ces produits directs des groupes cycliques qui a 4 éléments d'ordre 10, on peut comprendre les exigences suivantes des éléments d'ordre 10 :

$$\begin{aligned}(g_1,\ldots,g_r)^{10} = (e_1,\ldots,e_r) \quad &\Leftrightarrow \quad (g_1^{10},\ldots,g_r^{10}) = (e_1,\ldots,e_r) \\ &\Leftrightarrow \quad g_1^{10} = e \wedge \ldots \wedge g_r^{10} = e.\end{aligned}$$

L'ordre de chaque element g_i, $i = 1,\ldots,r$ divise 10, GRP(3.6). Il y a quatre ordres possibles comme $10 = 5 \cdot 2$: ces ordres-ci sont 1, 2, 5 et 10, puisque ces entiers positifs divisent 10.

Notre méthode pour trouver le nombre des éléments d'ordre 10 est la suivante : d'abord on trouve toutes les éléments d'ordre 1, 2, 5 ou 10. Ici c'est important de comprendre qu'il n'y a pas d'éléments d'ordre 10 dans un groupe d'ordre m, le groupe cyclique C_m en particulier, où m est une puissance de 2 ou 5, comme $10 = 5 \cdot 2$ tel que $5 \cdot 2 \nmid 2^i$ et $5 \cdot 2 \nmid 5^i$ pour tout $i \in \mathbb{N}$, GRP(3.6).

Alors on cherche le nombre des éléments d'ordre 1, 2, 5 ou 10 dans chaque groupe cyclique dans le produit de ceux. De l'argument ci-dessus on peut abandonner la recherche d'éléments d'ordre 10 dans cettes groupes. Dans un groupe cyclique C_m où m est une puissance de 2, il y a 2 éléments d'ordre 1, 2 ou 5 : il n'y a pas d'éléments d'ordre 5 comme $5 \nmid 2^i$ pour tout i, seulement $\varphi(2) = 1$ élément d'ordre 2, et l'élément neutre, GRP(3.16). Dans un groupe cyclique C_n où n est une puissance de 5, il y a 5 éléments d'ordre 1, 2 ou 5 : il n'y a pas d'éléments d'ordre 2 comme $2 \nmid 5^i$ pour tout i, $\varphi(5) = 4$ éléments d'ordre 5, et aussi l'élément neutre, GRP(3.16).

Alors on multiplie les nombres trouvés de chaque groupe. Ce nouveau nombre p_f pour un groupe n'est naturellement pas le nombre qu'on cherche – il y a trop. On veut maintenant trouver le nombre des éléments d'ordre 1 ou 2 et d'ordre 1 ou 5 de tous les groupes ; on trouve ces nombres-ci à la même manière tel que vu avant. Alors on soustrait ces nouveaux nombres-ci de p_f et ajoute 1 parce qu'on a soustrait l'élément neutre deux fois. Ce vraiment nouveau nombre-ci est le nombre des éléments d'ordre 10 du groupe [2] !

Toutes les groupes abéliens d'ordre 1000 sont (soit $p_{\{a_1,\ldots,a_r\}}$ le nombre des éléments d'ordre $a_1, a_2, \ldots, a_{r-1}$ ou a_r) :

2. Si on n'en souvient pas, on risque qu'il y a des éléments d'ordre 2 contenu dans le premier nombre. On veut des combinations des ordres 1, 2 et 5, et rien d'autre !

Groupe abélien d'ordre 1000	$p_{\{1,2,5,10\}}$	$p_{\{1,5\}}$	$p_{\{1,2\}}$	$p_{\{10\}}$
$C_5 \times C_5 \times C_5 \times C_2 \times C_2 \times C_2$	$5^3 \cdot 2^3 = 1000$	$5^3 = 125$	$2^3 = 8$	868
$C_5 \times C_5 \times C_5 \times C_{2^2} \times C_2$	$5^3 \cdot 2^2 = 500$	$5^3 = 125$	$2^2 = 4$	372
$C_5 \times C_5 \times C_5 \times C_{2^3}$	$5^3 \cdot 2 = 250$	$5^3 = 125$	2	124
$C_{5^2} \times C_5 \times C_2 \times C_2 \times C_2$	$5^2 \cdot 2^3 = 200$	$5^2 = 25$	$2^3 = 8$	168
$C_{5^2} \times C_5 \times C_{2^2} \times C_2$	$5^2 \cdot 2^2 = 100$	$5^2 = 25$	$2^2 = 4$	72
$C_{5^2} \times C_5 \times C_{2^3}$	$5^2 \cdot 2 = 50$	$5^2 = 25$	2	24
$C_{5^3} \times C_2 \times C_2 \times C_2$	$5 \cdot 2^3 = 40$	5	$2^3 = 8$	28
$C_{5^3} \times C_{2^2} \times C_2$	$5 \cdot 2^2 = 20$	5	$2^2 = 4$	12
$C_{5^3} \times C_{2^3}$	$5 \cdot 2 = 10$	5	2	4

Alors le théorème des groupes abéliens finis GRP(6.11) dit que ces 9 groupes-ci sont uniques ! Alors, le groupe qu'on cherche est un de ces 9-groupes ci.

On voit que $C_{5^3} \times C_{2^3}$ est le seul groupe avec 4 éléments d'ordre 10. Comme les ordres de chaque groupe au produit direct 5^3 et 2^3 sont premiers entre eux, le produit direct $G = C_{125} \times C_8$ est cyclique, GRP(3.20). **CQFD.**

Il faut aussi indiquer un groupe abélien d'ordre 1000 qui contient 72 éléments d'ordre 10. Tel que visible au tableau, le groupe $H = C_{25} \times C_5 \times C_4 \times C_2$ est un groupe abélien qui satisfait à cettes exigences.

3

Il faut trouver le nombre des groupes abéliens d'ordre 6075 à un isomorphisme près.

On peut ulitiser le théorème fondamental des groupes abéliens finis, GRP(6.10). Il existe un isomorphisme entre un groupe abélien d'ordre 6075 et un produit direct des groupes cycliques $C_{m_1} \times \cdots \times C_{m_r}$, tel que $m_i > 1$ pour tout i.

GRP(6.10)(3) dit qu'on peut choisir les ordres des groupes cycliques tel que chaque m_i est un puissance d'un nombre premier, et GRP(6.11) dit qu'il faut que chaque m_i doive être un puissance d'un nombre premier de la factorisation de 6075 en un produit de nombres premiers, tel que $m_1 \cdots m_r = 6075$.

Comme $6075 = 3^5 \cdot 5^2$, il faut trouver toutes les manières possibles d'arranger les puissances de nombres premiers quand on les divise. Comme il y a 7 structures de cycles différents dans S_5 (vois GRP2, tâche n. 6, utilisé au cours "Dis1"), il y a 7 manières d'arranger les puissances de 3, une manière pour chaque structure de cycle (ex $(* \ * \ * \ *)(*)$ réalise $3^4 \cdot 3$ et $3 \cdot 3^4$). Il y a 2 types de cycles différents dans S_2, alors il y a 2 manières d'arranger les puissances de 5.

Si on compose les manières d'arranger les puissances des 3 et 5, il y a 7 manières d'arranger les puissances de 3 pour chaque manière d'arranger les puissances de 5. Alors, il y a $7 \cdot 2 = 14$ manières d'arranger les puissances de nombres premiers de 6075.

Comme il y a 14 manières de choisir des m_i pour le produit direct des groupes cycliques et chaque m_i est une puissance d'un nombre premier, toutes les 14 manières sont uniques, GRP(6.10). Alors, il y a 14 groupes abéliens d'ordre 6075 à un isomorphisme près, GRP(6.10).

4

Soient $\varphi : G \to G'$ un homomorphisme de groupes et G un groupe cyclique. Il faut demonstrer que le groupe des images $\mathrm{Im}\varphi = \varphi(G)$ est cyclique.

Étant donné que G est cyclique, il existe un élément $g \in G$ tel que $G = \langle g \rangle$, GRP(3.7) ; c'est-à-dire que tous les éléments dans G sont des puissances de l'élément g. On regarde $\varphi(\langle g \rangle)$, donc les images de tous les éléments dans G par φ :

$$\begin{aligned} \varphi(\langle g \rangle) &= \varphi(\{\ldots, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots\}) \\ &= \{\ldots, \varphi(g^{-2}), \varphi(g^{-1}), \varphi(e), \varphi(g), \varphi(g^2), \varphi(g^3), \ldots\}, \end{aligned}$$

puisqu'on trouve l'image de chaque élément dans $\langle g \rangle$. Comme φ est un homomorphisme, on trouve :

$$\begin{aligned} \varphi(\langle g \rangle) &= \{\ldots, \varphi(g^{-2}), \varphi(g^{-1}), \varphi(e), \varphi(g), \varphi(g^2), \varphi(g^3) \ldots\} \\ &= \{\ldots, \varphi(g^{-1} \cdot g^{-1}), \varphi(g^{-1}), \varphi(e), \varphi(g), \varphi(g \cdot g), \varphi(g \cdot g \cdot g), \ldots\} \\ &= \{\ldots, \varphi(g^{-1})\varphi(g^{-1}), \varphi(g^{-1}), \varphi(e), \varphi(g), \varphi(g)\varphi(g), \varphi(g)\varphi(g)\varphi(g), \ldots\} \\ &= \{\ldots, \varphi(g)^{-2}, \varphi(g)^{-1}, e', \varphi(g), \varphi(g)^2, \varphi(g)^3, \ldots\}, \end{aligned}$$

puisqu'on utilise GRP(3.2) au deuxième signe d'égalité et GRP(5.2) au avant-dernier. Donc on voit que tous les éléments ci-dessus sont différents : comme tous les éléments de $\langle g \rangle$ sont différents puisque les puissances sont différentes, les images de ces éléments-ci sont différents aussi :

Étant donné $g \in G$ et φ un homomorphisme, on peut comprendre si un groupe cyclique a un ordre fini n, que $g^i = g^j$ si et seulement si $i \equiv j \pmod{n}$, GRP(3.5). Alors $\varphi(g)^i = \varphi(g^i) = \varphi(g^j) = \varphi(g)^j$ si et seulement si $i \equiv j \pmod{n}$, comme φ est un homomorphisme. On voit équivalemment pour un groupe cyclique d'ordre infini que $\varphi(g)^i = \varphi(g)^j$ si et seulement si $i = j$. Donc tous les éléments dans

$$\{\ldots, \varphi(g)^{-2}, \varphi(g)^{-1}, e', \varphi(g), \varphi(g)^2, \varphi(g)^3, \ldots\}$$

sont différents précisement comme les éléments dans $\langle g \rangle$.

Comme on trouve que tous les éléments ci-dessus constituent toutes les puissances de $\varphi(g) \in G'$, on voit que $\varphi(\langle g \rangle) = \langle \varphi(g) \rangle$. Donc $\langle \varphi(g) \rangle$ se compose de toutes les éléments de $\varphi(G)$. Alors $\varphi(G) = \langle \varphi(g) \rangle$, et $\varphi(G)$ est cyclique, GRP(3.7).

5

Soient $\varphi : \mathrm{C}_{28} \to \mathrm{A}_5$ un homomorphisme non-trivial et d l'ordre de $\varphi(\mathrm{C}_{28})$.

Soit $N = \varphi^{-1}(\mathrm{id})$ le noyau du morphisme de groupes φ du groupe C_{28} vers le groupe A_5. À cause du théorème d'isomorphisme GRP(5.8), les deux groupes C_{28}/N et $\varphi(\mathrm{C}_{28})$ sont isomorphes. Ils ont le même ordre, GRP(5.10). Alors, on trouve que $|\mathrm{C}_{28}/N| = |\varphi(\mathrm{C}_{28})| = d$.

Le nombre des éléments de C_{28}/N égale $|\mathrm{C}_{28} : N|$, GRP(4.1). Le théorème de Lagrange GRP(4.2) dit que $|\mathrm{C}_{28}| = |\mathrm{C}_{28} : N| \cdot |N|$. Comme l'ordre de C_{28} égale 28, on voit que

$$d = |\mathrm{C}_{28}/N| = |\mathrm{C}_{28} : N| = |\mathrm{C}_{28}|/|N| = 28/|N| \Rightarrow d \cdot |N| = 28,$$

et comme $|N|$ est un entier positif, on déduit que $d \mid 28$, TAL(3.2). Alors, les ordres possibles de $\varphi(\mathrm{C}_{28})$ sont 1, 2, 4, 7, 14 et 28, comme ces entiers-ci divisent 28.

$\varphi(C_{28})$ est un sous-groupe de A_5, GRP(5.3). Alors, l'ordre de $\varphi(C_{28})$ d divise l'ordre de A_5, GRP(3.16). L'ordre de A_5 égale $5!/2 = 60$, GRP(2.22). Alors $d \mid 60$ et il existe un entier $k \in \mathbb{Z}$ tel que $60 = kd$. Comme $7 \mid d \Rightarrow 7 \mid kd$, on trouve que $kd = 60 \Rightarrow 7 \nmid kd$. La proposition contraposée donne que $7 \nmid kd \Rightarrow 7 \nmid d$. Alors $7 \nmid d$.

Comme C_{28} est un groupe cyclique, $\varphi(C_{28})$ est un groupe cyclique aussi, voir tâche n. 4. Alors, il existe un élément $g \in \varphi(C_{28})$ tel que $\langle g \rangle = \varphi(C_{28})$. Il faut demonstrer que l'ordre de $\varphi(C_{28})$ n'égale pas 4.

$\varphi(C_{28})$ ne peut qu'avoir l'ordre 4 si l'ordre maximal dans $\varphi(C_{28})$ égale 4 ; ça veut dire qu'il faut exister un élément d'ordre 4 dans $\varphi(C_{28})$. Comme $\varphi(C_{28})$ est un sous-groupe de A_5, GRP(5.3), on peut essayer de trouver un élément d'ordre 4 dans A_5.

Les seuls éléments d'ordre 4 dans S_5 sont les permutations qui sont des 4-cycles, GRP(3.14). Le signature d'un de ces 4-cycles-ci égale $(-1)^{5-2} = -1$, comme un 4-cycle dans S_5 se compose de deux orbites, le 4-cycle et un point fixe. Mais on voit que ce 4-cycle n'est pas paire, et alors, il n'y a pas des permutations qui sont des 4-cycles dans A_5, comme A_5 se compose des permutations paires dans S_5.

Alors, il n'y a pas d'éléments d'ordre 4 dans A_5, et donc $\varphi(C_{28}) \subseteq A_5$ ne contient pas un élément d'ordre 4. On déduit que l'ordre de $\varphi(C_{28})$ $d \neq 4$.

Maintenant on voit que d ne peut qu'être 1 ou 2. Comme φ est un homomorphisme non-trivial, il existe un element $h \in C_{28}$ tel que $\varphi(h) \neq \mathrm{id}$, $\mathrm{id} \in A_5$, GRP(5.5)(0). Alors $d \neq 1$, et on voit que $d = 2$ puisque c'est la seule possibilité.

Il faut demonstrer qu'il y a 15 homomorphismes non-triviaux $C_{28} \to A_5$.

On sait que les seuls éléments d'ordre 2 dans S_5 sont les transpositions et les permutations de structure du cycle $2^2 1^1$. Le premier type a 2 orbites, le dernier type a 3 orbites. Seulement le dernier type est paire, puisque les signatures de ceux sont $(-1)^{5-3} = 1$. Alors, les seuls éléments d'ordre 2 dans A_5 sont les permutations de structure du cycle $2^2 1^1$.

Il faut calculer le nombre des permutations de ce type. Il y a 5 possibilités pour choisir le point fixe. Alors on fixe un élément d'une des transpositions et décide quel élément qui est permuté avec celui-ci ; il y a 3 possibilités pour choisir cet élément. Alors quand on a choisi cet élément, l'autre transposition est donnée par les 2 éléments restants. Alors, il y a $5 \cdot 3 = 15$ permutations de structure du cycle $2^2 1^1$.

Alors si on veut construire un homomorphisme, il faut que l'image de l'élément neutre de C_{28} soit l'élément neutre de A_5, GRP(5.2). Comme l'ordre de $\varphi(C_{28})$ égale 2, il faut que l'autre élément de $\varphi(C_{28})$ soit une des permutations de structure du cycle $2^2 1^1$ comme trouvé avant. Alors on choit un élément (d'ordre 28) de C_{28} ξ. On sait que l'image de ξ n'est pas l'élément neutre de A_5 : sinon l'ordre de $\varphi(C_{28})$ est 1 ; donc l'homomorphisme est trivial, comme le seul élément dans $\varphi(C_{28})$ est l'élément neutre. Alors l'image de cet élément ξ doit être une des 15 permutations d'ordre 2, comme $\varphi(C_{28})$ est cyclique parce que C_{28} est cyclique, voir tâche n. 4.

Pour chaque des 15 possibilités de l'image, on définit que $\varphi(\xi^i) = \varphi(\xi)^i$; on voit que maintenant φ est un homomorphisme, GRP(5.1). C'est-à-dire : on construit un homomorphisme à cette manière pour chaque permutation de structure du cycle $2^2 1^1$ en définant que $\varphi(\xi^i) = \varphi(\xi)^i$ pour un élément ξ dans C_{28}. Alors on prend soin de le construire qu'il soit bien défini !

Il n'y a pas d'autres possibilités pour construire un homomorphisme : on a besoin d'un élément d'ordre 2 dans A_5. Comme il n'y a que 15 permutations dans A_5, et on construit un homomorphisme pour chaque de cettes permutations-ci, il y a 15 homomorphismes non-triviaux $C_{28} \to A_5$.

6

Soit $\sigma = (2\ 3\ 4\ 5\ 6)$ une permutation circulaire d'ordre 5 dans S_6. Il faut trouver le nombre des conjuguées de σ dans S_6.

Deux permutations du ensemble fini S_6 sont conjuguées si et seulement s'ils ont le même structure de cycle, GRP(7.18). Il faut trouver le nombre des 5-cycles dans S_6 ; des cycles du structure $1^1 5^1$.

Il y a 6 possibilités de choisir le point fixe. Pour le 5-cycle restant, on peut placer un des cinq nombres restants sur la première place (ex si on choit 1 comme le point fixe et 2 sur cette place) et alors il y a $4 \cdot 3 \cdot 2 \cdot 1$ manières d'arranger les quatre nombres restants dans le 5-cycle. Donc il y a $6 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 144$ cycles du structure $1^1 5^1$; il y a 144 conjuguées de σ dans S_6, GRP(7.18).

L'indice du centralisateur $C(\sigma)$ dans S_6, $|S_6 : C(\sigma)|$ égale le nombre des conjuguées de σ dans S_6, GRP(7.17). Donc le théorème de Lagrange GRP(4.2) dit que le nombre des éléments dans le centralisateur de σ dans S_6 égale

$$|C(\sigma)| = |S_6|/|S_6 : C(\sigma)| = 6!/144 = 5.$$

Il faut trouver les 5 permutations dans le centralisateur de σ dans S_6 ; les permutations γ qui satisfont que $\gamma\sigma = \sigma\gamma$. Soit $\gamma = \sigma^i$ une puissance de σ, on voit que $\sigma^i\sigma = \sigma^{i+1} = \sigma^{1+i} = \sigma\sigma^i$; donc ce γ satisfait l'équation. Comme σ est un 5-cycle, on sait que $\sigma^5 = \mathrm{id}$, GRP(3.14). Alors, $\sigma^i = \sigma^j$ si et seulement si $i \equiv j \pmod 5$, GRP(3.14). Ça veut dire qu'on n'a que besoin de mentionner 5 permutations qui satisfont l'équation : celles-ci donnés par les restes possibles en division d'un entier relatif par 5 (0, 1, 2, 3, 4) constituent $C(\sigma)$:

$$C(\sigma) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \sigma^4\}.$$

7

Der skal vises, at Klein's Vierer-gruppe V er isomorf med en undergruppe af diedergruppen D_n, hvis og kun hvis n er lige.

Bevis. Antag derfor først, at V er isomorf med en undergruppe $H \subseteq D_n$. Da gælder pr. GRP(5.10), at V og H har samme orden ; da ordenen for V er 4, gælder tilsvarende, at $|H| = 4$. Grundet Lagranges Indexsætning, GRP(4.3), gælder at $|D_n| = |D_n : H| \cdot |H|$, og da alle gruppeordener er heltallige, ser vi heraf, at $|H|$ går op i $|D_n|$ jf. TAL(3.2), og dermed, at 4 går op i $|D_n|$. Da ordenen for diedergruppen D_n er $2n$ jf. GRP(1.21), gælder altså pr. antagelsen at $4 \mid 2n$. Dette vil sige, at der findes et $q \in \mathbb{N}$, så $4q = 2n$, jf. TAL(3.2). Da $4q = 2n \Rightarrow n = 2q$, følger herpå, at n er lige. Hermed er implikationen "til venstre" vist.

Antag nu, at n er lige. Diedergruppen D_n består af $2n$ symmetrier af en regulær n-kant i planen, nemlig n drejninger og n spejlinger, GRP(1.21). Da antallet af drejninger n er antaget lige, findes da en halvdrejning $D^{n/2}$ i D_n – idet denne vil dreje kanterne $n/2$ gange, hvilket er et helt antal, da n er lige – samt en spejling S, en halvdrejning fulgt af en spejling $SD^{n/2}$ og naturligvis identiteten id.

Vi vil nu vise at delmængden $F = \{\mathrm{id}, D^{n/2}, S, SD^{n/2}\}$ udgør en undergruppe af D_n. Det er klart at se, at $\mathrm{id} \in F$ og at alle elementer i F er at finde i D_n.

Vi skal nu finde, at F er stabil. Kompositet af id og ethvert andet element i F findes selvfølgelig i F. Ifølge ligningerne s. 55 ses, at $D^{n/2}D^{n/2} = D^n = \mathrm{id}$, idet vi

her drejer punkterne to halve omgange, altså en hel omgang, som udgør ingen forskel (netop id), at $S^2 = \mathrm{id}$, idet vi spejler punkterne i en akse og spejler tilbage igen. Ligeledes findes $SD^{n/2}$ i F. Med ligningerne ses også, at $D^{n/2}S = SD^{-n/2} = SD^{n/2}$, idet en halvdrejning af punkterne den ene vej eller den anden gør ingen forskel, at $D^{n/2}SD^{n/2} = D^{n/2}D^{-n/2}S = S$ og at $SSD^{n/2} = S^2D^{n/2} = D^{n/2}$. Altså findes alle kompositer af elementer i F i F, og F er stabil.

Vi skal også finde, at alle elementer i F har inverser i F : det inverse element til halvdrejningen $D^{n/2}$ er $D^{n/2}$ idet $D^{n/2}D^{n/2} = \mathrm{id}$; tilsvarende er det inverse element til S også S, idet $S^2 = \mathrm{id}$. Idet vi benytter ligningerne s. 55, har vi, at $(SD^{n/2})(SD^{n/2}) = SD^{n/2}D^{-n/2}S = S^2 = \mathrm{id}$, da vi benytter at en halvdrejning frem og tilbage også giver identiteten. Altså er den inverse til elementet $SD^{n/2}$ netop $SD^{n/2}$, og derfor ligger alle inverser til elementer i F i F. Ved GRP(1.6) sluttes da, at F er en undergruppe af D_n.

Med ovenstående har vi da, at antallet af elementer i F er 4, hvorpå ordenen af F er 4, GRP(1.2). Vi ved, at id i F har orden 1, da denne er det neutrale element – de resterende elementer har orden 2, da de er deres egne inverse, som vi så ovenfor. Idet der op til isomorfi kun findes to grupper af orden 4, nemlig C_4 og $\mathrm{V} \simeq \mathrm{C}_2 \times \mathrm{C}_2$ jf. GRP(5.11), må F være isomorf med en af disse. Da C_4 har $\varphi(4) = \varphi(2^2) = 2$ elementer af orden 4 jf. GRP(3.16), kan F ikke være isomorf med C_4, idet F har ingen elementer af orden 4, jf. GRP(5.10). Men da må F nødvendigvis være isomorf med V, da der op til isomorfi kun findes de to førnævnte grupper af orden 4. Vi har altså ud fra antagelsen vist, at V er isomorf med en undergruppe af D_n. **QED.**

8

Vi har i opgaven givet 6 grupper, $G_k,\ k = 1,\ldots,6$, som vi skal undersøge om er isomorfe. Samtlige givne grupper er produkter af cykliske grupper, og det er let at indse, at grupperne alle har orden 2000. Da cykliske grupper er abelske, jf. GRP(3.7), er samtlige grupper i opgaven G_k abelske, idet vi kan betragte kompositet af vilkårlige r-sæt $g = (g_1,\ldots,g_r)$ og $h = (h_1,\ldots,h_r)$, hvor $g,h \in G_1 \times G_r$, hvor samtlige $G_i,\ i = 1,\ldots,r$:

$$\begin{aligned} gh &= (g_1,\ldots,g_r)(h_1,\ldots,h_r) \\ &= (g_1h_1,\ldots,g_rh_r) = (h_1g_1,\ldots,h_rg_r) = (h_1,\ldots,h_r)(g_1,\ldots,g_r) = hg, \end{aligned}$$

hvorpå vi slutter, at det direkte produkt af cykliske grupper er abelsk. Derpå kan vi benytte Struktursætningen på disse, GRP(6.10)(3), hvilket betyder, at grupperne G_k er isomorfe med et produkt af cykliske grupper, hvorom der gælder for ordenerne, at de er primtalspotenser.

Dette er imidlertid ikke gældende for alle ordener i de cykliske grupper i de givne produkter G_k (fx i G_1, hvor man ser C_{10} : 10 er ikke en primtalspotens). Vi kan dog benytte sætning GRP(3.20) : er en af de cykliske grupper i de givne produkter ikke af primtalspotensorden, kan vi primopløse ordenen af denne, $n = p_1^{a_1}\cdots p_r^{a_r}$ (fx kan man i fornævnte eksempel primopløse 10 til $2 \cdot 5$), hvor $p_i \neq p_j$ for $i \neq j$, og betragte de cykliske grupper af orden $p_1^{a_1}$ til $p_r^{a_r}$.

Da alle $p_1^{a_1},\ldots,p_r^{a_r}$ er parvis og indbyrdes primiske (da alle $p_i,\ i = 1,\ldots,r$ er forskellige primtal) gælder pr. GRP(3.20), at produktgruppen af de cykliske grupper af orden $p_1^{a_1}$ til $p_r^{a_r}$ er cyklisk, og specielt pr. GRP(3.20), at ordenen af denne er $n = p_1^{a_1}\cdots p_r^{a_r}$. Men da C_n er den eneste cykliske gruppe af orden n op til isomorfi jf. GRP(5.11), må der gælde, at $\mathrm{C}_n \simeq \mathrm{C}_{p_1^{a_1}} \times \cdots \times \mathrm{C}_{p_r^{a_r}}$.

Derfor kan vi omskrive og opløse de cykliske grupper i de givne produktgrupper G_k, så hver cyklisk gruppe i produktgruppen har en primtalspotensorden. Derpå vil gælde pr. GRP(6.10)(3), at denne fremstilling er entydig, og så vil det være enkelt at indse, hvilke af grupperne, der er isomorfe.

Vi har derfor, at

$$\begin{aligned}
G_1 &:= & \mathrm{C}_2 \times \mathrm{C}_{10} \times \mathrm{C}_{100} &\simeq & \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_5 \times \mathrm{C}_{2^2} \times \mathrm{C}_{5^2} \\
G_2 &:= & \mathrm{C}_4 \times \mathrm{C}_4 \times \mathrm{C}_{125} &\simeq & \mathrm{C}_{2^2} \times \mathrm{C}_{2^2} \times \mathrm{C}_{5^3} \\
G_3 &:= & \mathrm{C}_4 \times \mathrm{C}_5 \times \mathrm{C}_{100} &\simeq & \mathrm{C}_{2^2} \times \mathrm{C}_5 \times \mathrm{C}_{2^2} \times \mathrm{C}_{5^2} \\
G_4 &:= & \mathrm{C}_4 \times \mathrm{C}_{10} \times \mathrm{C}_{50} &\simeq & \mathrm{C}_{2^2} \times \mathrm{C}_2 \times \mathrm{C}_5 \times \mathrm{C}_2 \times \mathrm{C}_{5^2} \\
G_5 &:= & \mathrm{C}_4 \times \mathrm{C}_{20} \times \mathrm{C}_{25} &\simeq & \mathrm{C}_{2^2} \times \mathrm{C}_{2^2} \times \mathrm{C}_5 \times \mathrm{C}_{5^2} \\
G_6 &:= & \mathrm{C}_4 \times \mathrm{C}_{500} &\simeq & \mathrm{C}_{2^2} \times \mathrm{C}_{2^2} \times \mathrm{C}_{5^3},
\end{aligned}$$

og at disse fremstillinger er entydige. Er der altså ens fremstillinger (idet rækkefølgen i produktet af disse cykliske grupper er ligegyldig), kan vi være sikker på, at grupperne med disse ens fremstillinger er isomorfe. Her ser vi, at $G_1 \simeq G_4$, $G_2 \simeq G_6$ og $G_3 \simeq G_5$.

Altså er de i opgaven ønskede par givet ved $(1,4)$, $(2,6)$ og $(3,5)$.

9

Gruppen S_4 virker på talrummet $\mathbb{R}^4$ ved for vektorer $x = (x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ at permutere de 4 koordinater.

Isotropigruppen for vektoren $x = (0,1,0,1)$ skal bestemmes, altså mængden S_{4_x} af permutationer $\sigma \in \mathrm{S}_4$, så $\sigma.x = x$, dvs. de σ under hvilke x er invariant.

Da første- og tredjekoordinat i x er ens, samt anden- og fjerdekoordinat, må permutationerne i isotropigruppen for x være dem, som ombytter lige nøjagtig disse. Ombyttes fx første og anden koordinat i x, fås ikke x. Isotropigruppen består altså af permutationerne, som ombytter 1. og 3. koordinat, 2. og 4. koordinat eller både 1. og 3. samt 2. og 4. koordinat, samt selvfølgelig identiteten i S_4 :

$$S_{4_x} = \{\mathrm{id}, (1\ 3), (2\ 4), (1\ 3)(2\ 4)\}.$$

Banen gennem x skal ligeledes bestemmes. Her ville det selvfølgelig være smart først at bestemme antal elementer i banen, hvilket kan gøres ved hjælp af Baneformlen, GRP(7.15) ; idet antallet af elementer i isotropigruppen for x er 4, som fundet, og antal permutationer i S_4 er $4! = 24$, får vi ved Baneformlen og Lagranges Indexsætning, GRP(4.2), at $|S_4.x| = |S_4 : S_{4_x}| = |S_4|/|S_{4_x}| = 24/4 = 6$.

Vi skal, idet vi skal bestemme banen gennem x, bestemme virkningen af samtlige elementer i S_4 på x. Idet S_4 virker på $\mathbb{R}^4$ ved permutation af de 4 koordinater i 4-tuplet i $\mathbb{R}^4$, skal vi finde de vektorer i $\mathbb{R}^4$, som har samme antal af tallene 0 og 1 på de 4 koordinater i 4-tuplet, da vi til disse knytter en permutation i S_4 ; vi husker jo, at permutationer er bijektive afbildninger, jf. GRP(2.1), og derfor skal antallet af nuller og ettaller bevares i vektorerne. Altså er banen gennem x givet ved

$$S_4.x = \{(0,0,1,1), (0,1,0,1), (0,1,1,0), (1,0,0,1), (1,0,1,0), (1,1,0,0)\}.$$

Her ser vi også, at antallet af elementer i banen gennem x er $\binom{4}{2} = 6$, idet vi skal vælge 2 pladser ud af 4 pladser at placere ettaller (eller nuller) på.

Vi skal til sidst angive en vektor i $\mathbb{R}^4$, hvis isotropigruppe har orden 2. Betragt vektoren $y = (0,1,2,1) \in \mathbb{R}^4$. Vi skal finde de $\sigma \in \mathrm{S}_4$, så $\sigma.y = y$. Identiteten i S_4 opfylder

selvfølgelig dette. Den eneste anden permutation, som opfylder, at permutationen af koordinaterne i y stadig giver y, er tydeligt den, der ombytter 2. og 4. koordinat. Da er $S_{4_y} = \{\mathrm{id}, (2\ 4)\}$. Denne isotropigruppe har orden 2, idet den har 2 elementer (og naturligvis idet $(2\ 4)$ er af orden $2 : (2\ 4)^2 = (2\ 4)(2\ 4) = (2)(4) = \mathrm{id}$).

10

Der skal bestemmes antal perlekæder med 8 perler, når der er to farver perler at vælge imellem. Vi skal altså finde antallet af mulige mønstre med to farver, og til dette vil vi benytte Polyas formel, GRP(7.28).

Det er selvfølgelig klart, at to perlekæder er ens, hvis vi kan få den ene ved at spejle og dreje den anden. Vores symmetrigruppe skal have en masse drejninger og spejlinger som elementer, og her er D_8 selvfølgelig et oplagt bud. Lægger vi nemlig perlekæden i planen, kan vi dreje og spejle punkterne i denne ved virkning af D_8 og dermed forsøge at opnå "en anden" perlekæde, som essentielt er den samme som den første.

Vi definerer nu ved Polyas formel X til at være mængden af perlekæder, og F til at være mængden af farver, som kunne være $F = \{\mathrm{sort}, \mathrm{hvid}\}$. Vi betragter nu virkningen af D_8 på mængden $\mathscr{F} = X^F$ af perlekæder med 8 perler og 2 farver. Hvis to perlekæder ligger i samme bane $\mathrm{D}_8.\mathscr{F}$, er de essentielt ens, idet vi kan opnå den ene ved spejling og drejning i D_8 af den anden, så vi ønsker altså at finde antallet af baner $|\mathscr{F}/\mathrm{D}_8|$, idet dette jo nødvendigvis er antallet af forskellige perlekæder (når alle mulige drejninger og spejlinger af alle mulige perlekæder med 8 perler og 2 farver er medregnet). Polyas formel giver da, at

$$|\mathscr{F}/\mathrm{D}_8| = \frac{1}{|\mathrm{D}_8|} \sum_{g \in \mathrm{D}_8} |F|^{m(g_X)} = \frac{1}{16} \sum_{g \in \mathrm{D}_8} 2^{m(g_X)},$$

idet $|F| = 2$ (to farver) og ordenen af D_8 er $2 \cdot 8 = 16$, og hvor $m(g_X)$ er antallet af baner til den for g svarende permutation.

Vi har i D_8 forskellige permutationer, men nogle af dem har ens effekt. En $\frac{1}{8}$-drejning D til venstre medfører, at alle 8 punkter i planen som D_8 bliver flyttet i én og samme retning og cykeltypen for denne permutation er derfor en 8-cykel ; men samme type drejning til højre D^{-1} vil naturligvis udløse samme cykeltype. En $\frac{1}{4}$-drejning D^2 til venstre medfører at punkter med ét punkt imellem bliver flyttet rundt à 4, og vi opnår derfor to separate baner med hver sin 4-cykel ; samme for D^{-2} til højre. $\frac{3}{8}$-drejningen D^3 gør, at alle elementer bliver i samme bane med 8 elementer, idet vi skal dreje 8 gange for at ende i identiteten igen, så her får vi en 8-cykel igen (og samme for D^{-3}), og $\frac{1}{2}$-drejningen D^4 smækker et punkt over i punktet overfor, og tilbage igen ved endnu en drejning af denne type. Her er altså 4 transpositioner, og dermed 4 baner (da $D^{-4} = D^4$, tæller vi ikke denne to gange).

Spejlingerne er der to typer af : S_1 over aksen gennem midten af to modstående sider i den regulære 8-kant og S_2 over aksen gennem to modstående punkter i 8-kanten. Den første type S_1 ombytter alle modstående elementer to og to (idet vi blot skal spejle igen for at komme tilbage til udgangspunktet), så her er der tale om 4 transpositioner, og denne type spejlinger er der 4 af. Den anden type S_2 ombytter ikke de to elementer som aksen går igennem, men ellers ombyttes modstående elementer to og to som før. Cykelfremstillingen her består altså af 3 transpositioner og 2 fixpunkter, i alt 5 baner. Vi mangler selvfølgelig identiteten her, men denne har 8 baner, idet den blot fører punkterne over i sig selv.

Vi kan selvfølgelig opstille en tabel for at overskueliggøre situationen :

Element $g \in \mathrm{D}_8$	Cykelfremstilling	$m(g_X)$
id	$(*)(*)(*)(*)(*)(*)(*)(*)$	8
D, D^{-1}	$(* * * * * * * *)$	1
D^2, D^{-2}	$(* * * *)(* * * *)$	2
D^3, D^{-3}	$(* * * * * * * *)$	1
D^4	$(* *)(* *)(* *)(* *)$	4
$4 \times S_1$	$(* *)(* *)(* *)(* *)$	4
$4 \times S_2$	$(* *)(* *)(* *)(*)(*)$	5

Med Polyas formel får vi så, idet vi summerer over 16 forskellige led (et for hvert element i D_8), men hvor nogle af leddene er ens og kan sættes sammen ved et gangetegn som angivet ved tabellen ovenfor, at :

$$|\mathscr{F}/\mathrm{D}_8| = \frac{1}{16}\sum_{g\in \mathrm{D}_8} 2^{m(g_X)} = \frac{1}{16}\left(2^8 + 2\cdot 2^1 + 2\cdot 2^2 + 2\cdot 2^1 + 2^4 + 4\cdot 2^4 + 4\cdot 2^5\right)$$
$$= \frac{1}{16}\left(256 + 4 + 8 + 4 + 16 + 64 + 128\right) = 30.$$

Altså kan vi lave 30 forskellige perlekæder med 8 perler og 2 farver, hvor to forskellige perlekæder skal forstås som et par af perlekæder, hvor den ene ved drejning og spejling ikke vil kunne ligne den anden.

11

Der skal bestemmes antallet af karusseller med 8 træheste, når der er to farver træheste at vælge imellem (man kunne også bruge grise).

Situationen ligner den ovenfor. Imidlertid må vi erkende, at en karussel ikke just ser godt efter en spejling som den i D_8, idet hestene ville vende på hovedet, hvis de altså var så man kunne ride på dem før spejlingen – hestene ville da drejes over en akse, og billedet er fuldbyrdet. Her er det altså kun drejningerne, der duer til noget – to karruseller er ens, hvis den ene kan drejes så man får den anden.

Vi vil nu igen benytte Polyas formel, GRP(7.28). Den nye symmetrigruppe vi søger, som kun egner sig til drejninger, er C_8. Lægger vi karussellen i planen og nummererer hestene i rækkefølge, kan vi dreje denne ved C_8 ved at lægge enhedsrodseksponenten til numrene på hesten modulo 8. Da lader vi nu X være mængden af karruseller og F være mængden af farver, som kunne være $F = \{\text{gul}, \text{lilla}\}$.

Vi ser nu på virkningen af C_8 på mængden $\mathscr{F} = X^F$ af karusseller med 8 heste og 2 farver. Hvis to karusseller ligger i samme bane $\mathrm{C}_8.\mathscr{F}$, er de essentielt ens, idet vi kan opnå den ene ved drejning i C_8 af den anden, så vi ønsker altså at finde antallet af baner $|\mathscr{F}/\mathrm{C}_8|$. Polyas formel giver da, at

$$|\mathscr{F}/\mathrm{C}_8| = \frac{1}{|\mathrm{C}_8|}\sum_{g\in \mathrm{C}_8} |F|^{m(g_X)} = \frac{1}{8}\sum_{g\in \mathrm{C}_8} 2^{m(g_X)},$$

idet $|F| = 2$ (to farver) og ordenen af C_8 er 8, og hvor $m(g_X)$ er antallet af baner til den for g svarende permutation.

Her behøver vi ikke at gøre så stort postyr over så at finde antallene af baner. Hvis man nu fjerner spejlingerne fra D_8 i opgave 10, kan perlekæden kun drejes i planen.

Dette kan netop videreføres til vores karussel, som også er repræsenteret ved 8 punkter i planen, som perlekæden var. Banerne ved de mulige 7 drejninger og identiteten i C_8 vil derfor naturligvis være de samme for karusseller som for perlekæderne :

Element $g \in C_8$	Cykelfremstilling	$m(g_X)$
id	$(*)(*)(*)(*)(*)(*)(*)(*)$	8
D, D^{-1}	$(* * * * * * * *)$	1
D^2, D^{-2}	$(* * * *)(* * * *)$	2
D^3, D^{-3}	$(* * * * * * * *)$	1
D^4	$(* *)(* *)(* *)(* *)$	4

Altså giver Polyas formel, GRP(7.28), idet vi udregner i det formlen givne sumudtryk præcis som i opgave 10 (bare uden spejlinger) :

$$|\mathscr{F}/C_8| = \frac{1}{8}\sum_{g\in C_8} 2^{m(g_X)} = \frac{1}{8}\left(2^8 + 2\cdot 2^1 + 2\cdot 2^2 + 2\cdot 2^1 + 2^4\right)$$
$$= \frac{1}{8}(256+4+8+4+16) = 36.$$

Altså kan laves 36 forskellige karusseller med 8 heste og 2 farver til disse, hvor to forskellige karusseller skal forstås som et par af karusseller, hvor den ene ved drejning ikke vil kunne ligne den anden.

12

Der skal vises, at der kun findes én homomorfi $A_4 \to C_2$.

Bevis. I S_4 findes identiteten, transpositioner, dobbelttranspositioner, 3-cykler og 4-cykler. Her er de lige permutationer dem, der har et lige antal baner (idet differensen af antallet af elementer, som permuteres over, 4, og antallet af baner vil være lige, og dermed udløse fortegnet 1, så permutationen er lige, jf. GRP(2.22)), og disse er identiteten, dobbelttranspositioner og 3-cykler.

Vi definerer nu en gruppehomomorfi $\varphi : A_4 \to C_2$. For permutationer $\sigma, \gamma \in A_4$ gælder da, at $\varphi(\sigma\gamma) = \varphi(\sigma)\varphi(\gamma)$, da φ er en homomorfi, jf. GRP(5.1). For denne homomorfi må der nødvendigvis gælde, jf. GRP(5.2), at det neutrale element i S_4, identiteten, bliver sendt over i det neutrale element i C_2, nemlig 1. Vi har altså, at $\varphi(\mathrm{id}) = 1$. I det følgende husker vi, at kompositionen i C_2 er den multiplikative $\cdot$.

Betragt nu en vilkårlig 3-cykel $\sigma = (a\ b\ c)(d) \in A_4$. Opløfter vi denne i 3. potens, ser vi, at $\sigma^3 = (a)(b)(c)(d) = \mathrm{id}$. Altså må der nødvendigvis gælde for en vilkårlig 3-cykel σ, at $\varphi(\sigma^3) = \varphi(\mathrm{id}) = 1$. Idet $\varphi(\sigma^3) = \varphi(\sigma\sigma\sigma) = \varphi(\sigma)\varphi(\sigma)\varphi(\sigma) = \varphi(\sigma)^3$ jf. GRP(5.1), da φ er en homomorfi, får vi altså, at $\varphi(\sigma)^3 = 1$, hvorpå der nødvendigvis må gælde, at $\varphi(\sigma) = 1$ for en vilkårlig 3-cykel σ.

Vi vil nu finde billedet for en vilkårlig dobbelttransposition $\gamma = (a\ b)(c\ d) \in A_4$. Betragt nu de to 3-cykler i A_4, $\tau_1 = (a\ b\ c)$ og $\tau_2 = (b\ c\ d)$. Da er $\tau_1\tau_2 = (a\ b)(c\ d) = \gamma$. Der må altså gælde, at $\varphi(\tau_1\tau_2) = \varphi(\gamma)$. Men da φ er en homomorfi, får vi jf. GRP(5.1), at $\varphi(\gamma) = \varphi(\tau_1)\varphi(\tau_2) = 1\cdot 1 = 1$, da τ_1 og τ_2 var 3-cykler i A_4, hvorpå billedet af disse var 1, som fundet i sidste afsnit.

Det vil altså sige, at alle mulige tre typer elementer i A_4 nødvendigvis må have samme billede 1, det neutrale element, i C_2, hvis vi definerer homomorfien $\varphi : A_4 \to C_2$. Da er φ nødvendigvis defineret ved $\varphi(\sigma) = 1$ for alle $\sigma \in A_4$. Da dette er den *eneste* homomorfi vi kan danne mellem de to givne grupper, er den triviel, idet den trivielle

homomorfi altid er mulig at definere, idet alle grupper har et neutralt element. Der er altså kun én homomorfi $A_4 \to C_2$. **QED.**

13

Lad G være en endelig abelsk gruppe, og lad $\varphi : G \to G$ være en homomorfi. Der skal vises, at hvis G er cyklisk, så gælder, at $\varphi^{-1}(e) \simeq G/\varphi(G)$.

Bevis. Antag, at G er en endelig, abelsk og cyklisk gruppe. Isomorfisætningen, GRP(5.8) giver, idet φ er en homomorfi, en veldefineret isomorfi $G/N \to \varphi(G)$, hvor N er kernen for homomorfien, nemlig $N = \varphi^{-1}(e)$. Idet de to grupper $G/\varphi^{-1}(e)$ og $\varphi(G)$ da er isomorfe, må de jf. GRP(5.10) have samme orden, altså $|G/\varphi^{-1}(e)| = |\varphi(G)|$. Men da har vi, at antallet af elementer i $G/\varphi^{-1}(e)$ er lig index for kernen i G, og vi har ved Lagranges Indexsætning GRP(4.2), at $|G/\varphi^{-1}(e)| = |G : \varphi^{-1}(e)| = |G|/|\varphi^{-1}(e)|$. Altså har vi, at

$$|\varphi(G)| = |G|/|\varphi^{-1}(e)|.$$

Men da må gælde, idet vi ganger over kors, og dernæst går hele vejen baglæns, at

$$|\varphi^{-1}(e)| = |G|/|\varphi(G)| = |G : \varphi(G)| = |G/\varphi(G)|.$$

Altså har grupperne $\varphi^{-1}(e)$ og $G/\varphi(G)$ samme orden. Da vi husker ved GPR(5.3), at kernen $\varphi^{-1}(e)$ er en undergruppe af G, og ved GRP(3.16) er $\varphi^{-1}(e)$ cyklisk, da den er en undergruppe af G, som var antaget cyklisk. Vi skal nu blot vise, at gruppen $G/\varphi(G)$ er cyklisk ; da der ved GRP(5.11) kun er én cyklisk gruppe af orden $n = |\varphi^{-1}(e)|$ op til isomorfi, er grupperne $\varphi^{-1}(e)$ og $G/\varphi(G)$ nødvendigvis isomorfe, hvorpå vi har det ønskede.

Skal $G/\varphi(G)$ være cyklisk, skal der altså findes en frembringer h i $G/\varphi(G)$, så potenserne h^i vil ramme alle elementer i $G/\varphi(G)$; altså så $\langle h \rangle = G/\varphi(G)$, jf. GRP(3.7). Alle elementer i $G/\varphi(G)$ er sideklasser i G modulo $\varphi(G)$, altså på formen $g\varphi(G)$ for hvert element $g \in G$, GRP(4.1).

Lad os nu undersøge GRP(4.14), et lemma : hvis $\varphi(G)$ er en normal undergruppe i G, findes netop en komposition i mængden $G/\varphi(G)$ af sideklasser modulo $\varphi(G)$, så der for alle $g_1, g_2 \in G$ gælder, at $(g_1\varphi(G))(g_2\varphi(G)) = g_1g_2\varphi(G)$. Vi har nu pr. GRP(5.3), at billedmængden $\varphi(G)$ er en undergruppe af G, idet homomorfien φ afbilder elementer fra G over i G. Hvis et element h ligger i $\varphi(G)$, gælder da, at $h \in G$. Idet G er antaget abelsk (selvom cykliskheden også medfører kommutativitet), får vi for ethvert element $g \in G$ pr. GRP(4.1), at

$$g\varphi(G) = \{gh \,|\, h \in \varphi(G)\} = \{hg \,|\, h \in \varphi(G)\} = \varphi(G)g,$$

idet vi ved andet lighedstegn bruger, at G er abelsk. Da er $\varphi(G)$ en normal undergruppe i G jf. GRP(4.13). Nu skal vi forsøge at finde en frembringer for $G/\varphi(G)$ med den komposition, vi nu har jf. lemmaet GRP(4.14). Idet G er cyklisk, er alle elementer i G på formen g_0^i, hvor $i \in \mathbb{Z}$ og g_0 er en frembringer for G, jf. GRP(3.7). Da er alle elementer i $G/\varphi(G)$ nødvendigvis på formen $g_0^i\varphi(G)$. Vi får med kompositionen GRP(4.15), at

$$g_0^i\varphi(G) = \underbrace{g_0 \cdots g_0}_{i}\varphi(G) = \underbrace{(g_0\varphi(G)) \cdots (g_0\varphi(G))}_{i} = (g_0\varphi(G))^i,$$

idet kompositionen i $G/\varphi(G)$ er multiplikativ, jf. GRP(4.15). Men da ser vi, at $g_0\varphi(G)$ er en frembringer for gruppen $G/\varphi(G)$, idet g_0 var en frembringer for G : vi kan opløfte

den i i'te potens for at opnå en af sideklasserne i G modulo $\varphi(G)$, som er på formen $g_0^i\varphi(G)$, og *alle* sideklasser kan opnås herved, ved bare at tage et tilsvarende element på formen g_0^i og sætte det sammen med $\varphi(G)$.

Men da har $G/\varphi(G)$ en frembringer $h = g_0\varphi(G)$, og må derfor være cyklisk. Da er $G/\varphi(G)$ isomorf med $\varphi^{-1}(e)$ ifølge ovenstående, og det ønskede er vist. **QED.**

14

Lad $\varphi : \mathbb{Z}/2 \times \mathbb{Z}/8 \to \mathbb{Z}/4$ være en surjektiv gruppehomomorfi. Der skal vises, at kernen er isomorf med $\mathbb{Z}/4$ eller $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Idet φ er en homomorfi, og vi lader $N := \varphi^{-1}([0]_4)$ betegne kernen (da det neutrale element i $\mathbb{Z}/4$ er $[0]_4$), siger isomorfisætningen GRP(5.8), at der er en veldefineret isomorfi $(\mathbb{Z}/2 \times \mathbb{Z}/8)/N \to \varphi(\mathbb{Z}/2 \times \mathbb{Z}/8)$. Idet grupperne $(\mathbb{Z}/2 \times \mathbb{Z}/8)/N$ og $\varphi(\mathbb{Z}/2 \times \mathbb{Z}/8)$ er isomorfe, jf. GRP(5.10), har de specielt samme orden. Altså er $|(\mathbb{Z}/2 \times \mathbb{Z}/8)/N| = |\varphi(\mathbb{Z}/2 \times \mathbb{Z}/8)|$. Ved Lagranges Indexsætning GRP(4.2) får vi, da at

$$\frac{|\mathbb{Z}/2 \times \mathbb{Z}/8|}{|N|} = |(\mathbb{Z}/2 \times \mathbb{Z}/8)/N| = |\varphi(\mathbb{Z}/2 \times \mathbb{Z}/8)| \Rightarrow |N| = \frac{|\mathbb{Z}/2 \times \mathbb{Z}/8|}{|\varphi(\mathbb{Z}/2 \times \mathbb{Z}/8)|}$$

$$\Rightarrow |N| = \frac{|\mathbb{Z}/2||\mathbb{Z}/8|}{4} = \frac{2 \cdot 8}{4} = 4,$$

idet vi benytter at homomorfien var surjektiv i nævneren, så alle 4 elementer i $\mathbb{Z}/4$ bliver ramt, og GRP(6.1). Altså har kernen orden 4. Men der findes kun to grupper af orden 4, nemlig C_4, som er isomorf med $\mathbb{Z}/4$ jf. GRP(5.11), og V, som er isomorf med $C_2 \times C_2$ og dermed $\mathbb{Z}/2 \times \mathbb{Z}/2$ jf. GRP(5.11). Men da må kernen altså være isomorf med en af disse to grupper, hvilket var hvad skulle vises. (Yderligere kan nævnes, at begge disse grupper er kommutative, så kernen må altså være kommutativ.)

Der skal nu vises, at begge muligheder kan forekomme.

Lad $\varphi_1 : \mathbb{Z}/2 \times \mathbb{Z}/8 \to \mathbb{Z}/4$ være givet ved $([a]_2, [b]_8) \mapsto [b]_4$. Dette er en homomorfi jf. GRP(5.1), da vi får ved restklasseregning, at

$$\begin{aligned} \varphi_1(([a]_2, [b]_8) + ([c]_2, [d]_8)) &= \varphi_1(([a+c]_2, [b+d]_8)) = [b+d]_4 \\ &= [b]_4 + [d]_4 = \varphi_1(([a]_2, [b]_8)) + \varphi_1(([c]_2, [d]_8)). \end{aligned}$$

Denne homomorfi er surjektiv, da vi kan ramme alle elementer i $\mathbb{Z}/4$, da fx $\varphi_1([0]_2, [b]_8) = [b]_4$ for alle $[b]_4 \in \mathbb{Z}/4$. Vores $\ker\varphi_1$ er da $\varphi_1^{-1}([0]_4) = \{([0]_2, [0]_8), ([0]_2, [4]_8), ([1]_2, [0]_8), ([1]_2, [4]_8)\}$, idet $[0]_4 = [4]_4$, og vi blot kan kombinere 0 og 4 i $\mathbb{Z}/8$ med de to elementer 0 og 1 i $\mathbb{Z}/2$.

Da genstår at vise, at denne "kerne" er en undergruppe. Idet vi bruger koordinatvis komposition jf. GRP(3.19) og grupperne $\mathbb{Z}/n$ benytter additiv notation, får vi, at

$\varphi_1^{-1}([0]_4)$ (+)	$([0]_2, [0]_8)$	$([0]_2, [4]_8)$	$([1]_2, [0]_8)$	$([1]_2, [4]_8)$
$([0]_2, [0]_8)$	$([0]_2, [0]_8)$	$([0]_2, [4]_8)$	$([1]_2, [0]_8)$	$([1]_2, [4]_8)$
$([0]_2, [4]_8)$	$([0]_2, [4]_8)$	$([0]_2, [0]_8)$	$([1]_2, [4]_8)$	$([1]_2, [0]_8)$
$([1]_2, [0]_8)$	$([1]_2, [0]_8)$	$([1]_2, [4]_8)$	$([0]_2, [0]_8)$	$([0]_2, [4]_8)$
$([1]_2, [4]_8)$	$([1]_2, [4]_8)$	$([1]_2, [0]_8)$	$([0]_2, [4]_8)$	$([0]_2, [0]_8)$

Heraf ses, at "kernen" er stabil med det neutrale element og alle inverser liggende – da er den en undergruppe, og dermed en egentlig kerne ! Den må altså være isomorf med $\mathbb{Z}/4$ eller $\mathbb{Z}/2 \times \mathbb{Z}/2$ jf. foregående resultat. Men vi ser ved kompositionstavlen, at alle elementerne undtagen neutralelementet $([0]_2,[0]_8)$ er deres egne inverser og dermed er af orden 2 ; da kan kernen ikke være isomorf med $\mathbb{Z}/4$, idet der er to elementer af orden 4 i $\mathbb{Z}/4$, jf. GRP(5.10). Men da må altså $\ker\varphi_1$ være isomorf med den anden gruppe af orden 4, nemlig $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Senere rettelse. Denne anden homomorfi φ_2, som vi benytter nedenfor, er ikke veldefineret. I stedet fungerer $([a]_2,[b]_8) \mapsto [2a+b]_4$ til dette formål, idet vi har at den i den afleverede opgave brugte homomorfi ikke er repræsentantuafhængig – de små ting vi viser nedenfor for φ_2 forløber stort set på samme måde for denne.

Lad nu $\varphi_2 : \mathbb{Z}/2 \times \mathbb{Z}/8 \to \mathbb{Z}/4$ være givet ved $([a]_2,[b]_8) \mapsto [a+2b]_4$. Dette er en homomorfi jf. GRP(5.1), da

$$\begin{aligned} \varphi_2(([a]_2,[b]_8)+([c]_2,[d]_8)) &= \varphi_2(([a+c]_2,[b+d]_8)) = [(a+c)+2(b+d)]_4 \\ &= [a+2b+c+2d]_4 = [a+2b]_4+[c+2d]_4 \\ &= \varphi_2(([a]_2,[b]_8))+\varphi_2(([c]_2,[d]_8)). \end{aligned}$$

Denne homomorfi er surjektiv, da vi kan opnå de ulige restklasser i $\mathbb{Z}/4$ ved at vælge $a=1$ og derpå vælge b lig 0 eller 1, og de lige restklasser ved $a=0$ og samme b.

Vores $\ker\varphi_2$ er da $\varphi_2^{-1}([0]_4) = \{([0]_2,[0]_8),([0]_2,[2]_8),([0]_2,[4]_8),([0]_2,[6]_8)\}$, idet vi ikke kan have, at $a+2b$ er ulige, hvorpå vi vælger $a=0$, og derpå skal finde de tal som ganget med 2 er kongruente med 0 modulo 4, som er 0, 2, 4 og 6, som så er vores valg af b. Vi opstiller igen en kompositionstavle for vores "kerne", bare for at være sikre i vores sag :

$\varphi_2^{-1}([0]_4)$ (+)	$([0]_2,[0]_8)$	$([0]_2,[2]_8)$	$([0]_2,[4]_8)$	$([0]_2,[6]_8)$
$([0]_2,[0]_8)$	$([0]_2,[0]_8)$	$([0]_2,[2]_8)$	$([0]_2,[4]_8)$	$([0]_2,[6]_8)$
$([0]_2,[2]_8)$	$([0]_2,[2]_8)$	$([0]_2,[4]_8)$	$([0]_2,[6]_8)$	$([0]_2,[0]_8)$
$([0]_2,[4]_8)$	$([0]_2,[4]_8)$	$([0]_2,[6]_8)$	$([0]_2,[0]_8)$	$([0]_2,[2]_8)$
$([0]_2,[6]_8)$	$([0]_2,[6]_8)$	$([0]_2,[0]_8)$	$([0]_2,[2]_8)$	$([0]_2,[4]_8)$

Da er "kernen" stabil og har neutralt element og alle inverser indeholdt (og bla bla) – den er dermed en undergruppe af $\mathbb{Z}/2 \times \mathbb{Z}/8$, og en egentlig kerne. Kernen er isomorf med $\mathbb{Z}/4$ eller $\mathbb{Z}/2 \times \mathbb{Z}/2$. Men vi ser, at elementet $([0]_2,[2]_8)$ er en frembringer for kernen, idet vi kan opnå elementerne $([0]_2,[4]_8)$, $([0]_2,[6]_8)$ og $([0]_2,[0]_8)$ med at multiplicere vores såkaldte frembringer med hhv. 2, 3 og 4 (jf. GRP(3.9)). Altså er vores restklassepar $([0]_2,[2]_8)$ en frembringer for $\ker\varphi_2$, hvorpå $\ker\varphi_2$ er en cyklisk gruppe jf. GRP(3.7). Den er derfor isomorf med en gruppe af orden 4, der er cyklisk. Men da $\mathbb{Z}/2 \times \mathbb{Z}/2$ ikke er cyklisk, jf. GRP(3.21) og GRP(5.11), må den være isomorf med $\mathbb{Z}/4$, som er cyklisk, jf. GRP(3.9).

Altså kan begge isomorfimuligheder forekomme.

15

Antag, at $d \mid n$, altså at n er på formen $n=rd$, $r \in \mathbb{Z}$. Der skal nu vises, at $[a]_n \mapsto [a]_d$ er en veldefineret homomorfi $(\mathbb{Z}/n)^* \to (\mathbb{Z}/d)^*$; vi definerer afbildningen ξ herved. Denne er en homomorfi jf. GRP(5.1), idet vi får for alle $[a]_n,[b]_n \in (\mathbb{Z}/n)^*$, at

$$\xi([a]_n[b]_n) = \xi([ab]_n) = [ab]_d = [a]_d[b]_d = \xi([a]_d)\xi([b]_d),$$

ved regning med primiske restklasser. Nu genstår det blot at vise, at homomorfien er veldefineret. Lad derfor $a,b \in \mathbb{Z}$ være primiske med n. Da skal vises, at a og b er primiske med d. Hvis dette gælder, har vi så, at de to primiske restklasser $[a]_n$ og $[b]_n$, hvorom der gælder, at $a \equiv b \equiv 1 \pmod{n}$, vil føres over i primiske restklasser $[a]_d$ og $[b]_d$, hvorom der gælder, at $a \equiv b \equiv 1 \pmod{d}$, hvorpå homomorfien er veldefineret.

Men ved TAL(3.9) er $p,q \in \mathbb{Z}$ primiske hvis og kun hvis der findes hele tal x og y, så $1 = xp + yq$. Men da a og b er primiske med n, kan vi finde $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ således, at

$$1 = x_1 a + y_1 n = x_1 a + y_1 rd = x_1 a + (y_1 r)d$$
$$1 = x_2 b + y_2 n = x_2 a + y_2 rd = x_1 b + (y_2 r)d,$$

hvorpå vi ser, at a og b ifølge samme korollar er primiske med d. Da er homomorfien veldefineret ifølge ovenstående.

Det skal nu vises, at homomorfien er surjektiv, hvis n er en primtalspotens og hvis n er et naturligt tal. Men hvis n er en primtalspotens, er n følgelig også et naturligt tal, så det genstår selvfølgelig bare at vise det for et naturligt tal n.

Antag derfor, at $n \in \mathbb{N}$. Ved Aritmetikkens Fundamentalsætning TAL(3.17) kan vi da skrive n som en primopløsning $n = p_1^{n_1} \cdots p_k^{n_k}$, hvor $p_1, \ldots, p_k$ er forskellige primtal. Da gælder da naturligvis, at alle $p_i^{n_i}$ er indbyrdes primiske, og følgelig har vi pr. GRP(6.3.2), at $(\mathbb{Z}/n)^* \simeq (\mathbb{Z}/p_1^{n_1})^* \times \cdots \times (\mathbb{Z}/p_k^{n_k})^*$.

Da $d \mid n$, kan vi også opskrive d som en primopløsning $d = p_1^{m_1} \cdots p_k^{m_k}$, hvor $m_i \leq n_i$ for $i = 1, \ldots, k$. Derpå gælder på samme måde, at $(\mathbb{Z}/d)^* \simeq (\mathbb{Z}/p_1^{m_1})^* \times \cdots \times (\mathbb{Z}/p_k^{m_k})^*$.

Vi vil nu vise, at $\xi_i : (\mathbb{Z}/p_i^{n_i})^* \to (\mathbb{Z}/p_i^{m_i})^*$ givet ved $[a]_{p_i^{n_i}} \mapsto [a]_{p_i^{m_i}}$ for alle $i = 1, \ldots, k$ er surjektiv; da vil gælde, at afbildningen $\xi : (\mathbb{Z}/p_1^{n_1})^* \times \cdots \times (\mathbb{Z}/p_k^{n_k})^* \to (\mathbb{Z}/p_1^{m_1})^* \times \cdots \times (\mathbb{Z}/p_k^{m_k})^*$ også er surjektiv – da hver af grupperne i produktet er surjektiv med den "modstående" – og dermed med ovenstående isomorfier vil gælde, at $\xi : (\mathbb{Z}/n)^* \to (\mathbb{Z}/d)^*$ er surjektiv.

Lad derfor $[a]$ være en primisk restklasse modulo $p_i^{m_i}$. Da gælder ved TAL(3.9), at vi kan finde $x,y \in \mathbb{Z}$, så $1 = xa + yp_i^{m_i} = xa + (yp_i^{m_i - 1})p_i$, hvorpå vi ser, at a også er primisk med p_i. Vi har da ved TAL(3.10), at a er primisk med $p_i^{n_i}$, og derfor at $[a]$ er en primisk restklasse modulo $p_i^{n_i}$. Vi har derfor implikationen, at

$$[a] \in (\mathbb{Z}/p_i^{m_i})^* \Rightarrow [a] \in (\mathbb{Z}/p_i^{n_i})^*.$$

Idet $\xi_i([a]_{p_i^{n_i}}) = [a]_{p_i^{m_i}}$, har vi med ovenstående implikation, at vi blot kan vælge en eller anden primisk restklasse modulo $p_i^{m_i}$, hvorpå den nødvendigvis *vil* blive ramt af $[a]_{p_i^{n_i}}$. Men da er ξ_i surjektiv, og dermed er ξ surjektiv for et naturligt tal n og dermed også en primtalspotens.

Der skal til sidst (gudskelov) findes antallet af primiske restklasser $[a]_{2000}$ modulo 2000 opfylder, at $a \equiv 1 \pmod{5}$. Vi skal altså finde antallet af elementer $[a]_{2000}$ i $(\mathbb{Z}/2000)^*$, som er primiske med 5 (hvilket $a \equiv 1 \pmod{5}$ betyder, jf. TAL(6.11)); da $[1]_5$ er det neutrale element i $(\mathbb{Z}/5)^*$ (da kompositionen i disse grupper er multiplikativ), skal vi altså finde antallet af elementer $[a]_{2000}$ for hvilke der gælder, at $\xi([a]_{2000}) = [1]_5$, idet vi definerer $\xi : (\mathbb{Z}/2000)^* \to (\mathbb{Z}/5)^*$ ved $[a]_{2000} \mapsto [a]_5$, hvilket vi kan jf. foregående, da $5 \mid 2000$.

Hvis et element $[a]_{2000} \in (\mathbb{Z}/2000)^*$ skal opfylde dette, skal der altså gælde, at $[a]_{2000} \in \xi^{-1}([1]_5)$, som jo er kernen ! Altså skal vi bestemme $|\ker \xi|$.

Dette gøres ved isomorfisætningen GRP(5.8), idet vi ved, at $(\mathbb{Z}/2000)^*/\ker\xi \simeq \xi((\mathbb{Z}/2000)^*)$, hvorpå antallet af elementer i de isomorfe grupper er det samme. Da antallet af primiske restklasser modulo 2000 er $\varphi(2000)$ jf. TAL(6.11), er $|(\mathbb{Z}/2000)^*| = \varphi(2000)$. Da homomorfien ξ er vist surjektiv, bliver alle primiske restklasser i $(\mathbb{Z}/5)^*$ ramt af elementer fra $(\mathbb{Z}/2000)^*$, så billedet af $(\mathbb{Z}/2000)^*$ ved ξ er altså alle primiske restklasser i $(\mathbb{Z}/5)^*$, og antallet af disse er $\varphi(5)$. Da får vi ved Lagranges Indexsætning GRP(4.2), at

$$|(\mathbb{Z}/2000)^*/\ker\xi| = \frac{|(\mathbb{Z}/2000)^*|}{|\ker\xi|} = |\xi((\mathbb{Z}/2000)^*)|$$

$$\Rightarrow |\ker\xi| = \frac{|(\mathbb{Z}/2000)^*|}{|\xi((\mathbb{Z}/2000)^*)|} = \frac{\varphi(2000)}{\varphi(5)} = \frac{\varphi(2^4)\varphi(5^3)}{4} = \frac{2^3\cdot 5^2\cdot 4}{4} = 200.$$

Altså er der 200 primiske restklasser $[a]_{2000}$ modulo 2000, som opfylder, at $a \equiv 1 \pmod 5$.