Groups

By Jacob J. A. Koot

1. Definition

A group is a system $G(G, \varphi, e)$ consisting of: 0

G : a non-empty set	1
φ : a map $x,y \in G \rightarrow \varphi(x,y) \in G$, called composition. We write $xy \equiv \varphi(x,y)$	2
e : an element $e \in G$, called identity	3
such that:	
$\forall x \in G: ex = x$	4
$\forall x \in G: \exists x^{-1} \in G: x^{-1}x = e$; x^{-1} is called inverse of x	5
$\forall x,y,z \in G: x(yz) = (xy)z$; composition φ is associative. We write $x(yz) \equiv xyz \equiv (xy)z$	6

It will be shown that every group has one identity element only, that every element has one inverse only and that the identity and inversion are symmetrical, id est:

$\forall x \in G: ex = x = xe$	4a
$\forall x \in G: x^{-1}x = e = xx^{-1}$	5a

Because the composition is associative, parentheses can be omitted from the composition of every arbitrary number of group elements without causing ambiguity. A group is abelean if and only if its composition is commutative, id est, if $\forall x,y \in G: xy = yx$. There are both abelean and non-abelean groups. A group *G* is finite if its set G is finite. The number of elements of a finite group is called the order of that group. If G is not finite, the group and its order are called infinite. There are finite and both denumerable and non-denumerable infinite groups.

2. Simple examples of groups

The set of all integer, rational, real or complex numbers form groups with addition as composition, 0 as identity and –k as inverse of k. The sets of rational, real or complex numbers without 0 form groups with multiplication as composition, 1 as identity and 1/x as inverse of x.

A permutation is a bijection of a set onto itself. A finite set of n elements has n! distinct permutations that form a so called symmetric group S_n. Consider the permutations of the set {A,B,C}. It has 3! = 6 distinct permutations, say P_1, P_2 ... P_6 as in figure 1.

	$P_i(A)$	$P_i(B)$	$P_i(C)$		inverse
P_1	A	B	C	identity	P_1
P_2	A	C	B	exchange B and C	P_2
P_3	B	C	A	rotate ABC to the left	P_5
P_4	B	A	C	exchange A and B	P_4
P_5	C	A	B	rotate ABC to the right	P_3
P_6	C	B	A	exchange A and C	P_6

Figure 1

P_1 is the identity. P_3 and P_5 are inverses of each other. For i = 1, i = 2, i = 4 and i = 6, P_i is the inverse of itself. The permutations P_1, P_2 ... P_6 form a group. Each composition P_iP_j, id est the map $x \in \{A,B,C\} \rightarrow P_i(P_j(x))$, is a permutation too. For example: $P_2P_3 = P_6$:

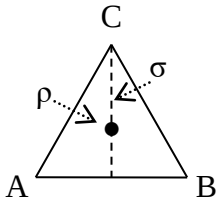
$P_2P_3(A) \equiv P_2(P_3(A)) = P_2(B) = C = P_6(A)$
$P_2P_3(B) \equiv P_2(P_3(B)) = P_2(C) = B = P_6(B)$
$P_2P_3(C) \equiv P_2(P_3(C)) = P_2(A) = A = P_6(C)$

Hence, $P_2P_3 = P_6$

Figure 2

The permutations of {A,B,C} are the same as what happens with the names of the vertices of an equilateral triangle ABC when applying its symmetry operations within its plane. See figure 3. The triangle has a rotation axis ρ through the centre, perpendicular to the plane of the triangle. It has a reflection σ in the perpendicular from vertex C onto side AB, which is the same as a mirror in the plane spanned by the axis of rotation and vertex C. By combining these two symmetry operations

and their results, all symmetry operations are found as shown in figure 4. The identity is regarded as a symmetry operation too, notwithstanding the fact that an object whose only symmetry is the identity usually is said to have no symmetries.



Equilateral triangle — Figure 3

ρ: rotation axis
σ: reflection

ε	P_1: ABC → ABC	Identity	Figure 4
ρ	P_3: ABC → BCA	Anti clockwise rotation about 120°	
ρ^2	P_5: ABC → CAB	Anti clockwise rotation about 240°, two times ρ	
σ	P_4: ABC → BAC	Reflection in perpendicular from C	
σρ	P_2: ABC → ACB	Reflection in perpendicular from A = ρ followed by σ	
$\sigma\rho^2$	P_6: ABC → CBA	Reflection in perpendicular from B = two times ρ followed by σ	

The symmetry operations shown in figure 4 form a group whose elements correspond to the permutations of the set {A,B,C}. Composition of two of the six symmetry operations always results in one of the six symmetry operations. For example:

$\rho\sigma(A) = \rho(\sigma(A)) = \rho(B) = C = \sigma\rho^2(A)$
$\rho\sigma(B) = \rho(\sigma(B)) = \rho(A) = B = \sigma\rho^2(B)$
$\rho\sigma(C) = \rho(\sigma(C)) = \rho(C) = A = \sigma\rho^2(C)$

Hence: $\rho\sigma = \sigma\rho^2$ — Figure 5

Figure 5 shows that the composition is not necessarily communicative. Figure 6 shows all compositions of the symmetry group, which is called C_{3v} and has the same structure as S_3. The similarity is called isomorphism and is indicated as $C_{3v} \sim S_3$. The name 'C_{3v}' contains the subscript '3' because it has a threefold axis of rotation. It contains the subscript 'v' because it has a plane of reflection containing the axis of rotation. The plane of the triangle is considered to be horizontal. Hence, the axis of rotation and the planes of reflections are considered to be vertical.

$C_{3v} \sim S_3$		**y →**						Figure 6
	xy	**ε**	**ρ**	**ρ^2**	**σ**	**σρ**	**$\sigma\rho^2$**	Corresponding permutation in S_3
x ↓	**ε**	ε	ρ	ρ^2	σ	σρ	$\sigma\rho^2$	P_1: ABC → ABC
	ρ	ρ	ρ^2	ε	$\sigma\rho^2$	σ	σρ	P_3: ABC → BCA
	ρ^2	ρ^2	ε	ρ	σρ	$\sigma\rho^2$	σ	P_5: ABC → CAB
	σ	σ	σρ	$\sigma\rho^2$	ε	ρ	ρ^2	P_4: ABC → BAC
	σρ	σρ	$\sigma\rho^2$	σ	ρ^2	ε	ρ	P_2: ABC → ACB
	$\sigma\rho^2$	$\sigma\rho^2$	σ	σρ	ρ	ρ^2	ε	P_6: ABC → CBA

A table of composition is usually simplified as follows. The rows and columns are labelled in the same order. The identity always is the first. Because ex = x = xe, the first row and first column show copies of the labels. Hence, the row and column with the labels can be omitted:

						Figure 7
ε	ρ	ρ^2	σ	σρ	$\sigma\rho^2$	
ρ	ρ^2	ε	$\sigma\rho^2$	σ	σρ	
ρ^2	ε	ρ	σρ	$\sigma\rho^2$	σ	
σ	σρ	$\sigma\rho^2$	ε	ρ	ρ^2	
σρ	$\sigma\rho^2$	σ	ρ^2	ε	ρ	
$\sigma\rho^2$	σ	σρ	ρ	ρ^2	ε	

In figure 7, the six symmetry operations are built starting from ε, ρ and σ. Because $\varepsilon = \rho^3 = \sigma^2$, only ρ and σ are required in order to form all operations. They form a minimal base for the group. There are more minimal bases {α,β} for this group:

base		examples of composing the group elements in base {α, β}						Figure 7a
α	β	ε	ρ	ρ^2	σ	σρ	$\sigma\rho^2$	
ρ	σ	β^2	α	α^2	β	βα	αβ	Rotation combined with a reflection.
ρ	σρ	β^2	α	α^2	αβ	β	βα	
ρ	$\sigma\rho^2$	β^2	α	α^2	βα	αβ	β	
ρ^2	σ	β^2	α^2	α	β	αβ	βα	
ρ^2	σρ	β^2	α^2	α	βα	β	αβ	
ρ^2	$\sigma\rho^2$	β^2	α^2	α	αβ	βα	β	
σ	σρ	β^2	αβ	βα	α	β	αβα	Two distinct reflections.
σρ	$\sigma\rho^2$	β^2	αβ	βα	αβα	α	β	
$\sigma\rho^2$	σ	β^2	αβ	βα	β	αβα	α	

In this case, a minimal base consists either of a rotation (ρ or ρ^2) and a reflection (σ, σρ or $\sigma\rho^2$) or of two distinct reflections. When placing the origin of an orthogonal system of coordinates (x,y) in the centre of the triangle and putting the x-axis parallel with side AB, we find:

		Figure 8
$\varepsilon(x, y) = (x, y)$	$\rho^2(x, y) = (-\frac{1}{2}x+\frac{1}{2}y\sqrt{3}, -\frac{1}{2}x\sqrt{3}-\frac{1}{2}y)$	
$\rho(x, y) = (-\frac{1}{2}x-\frac{1}{2}y\sqrt{3}, +\frac{1}{2}x\sqrt{3}-\frac{1}{2}y)$	$\sigma\rho(x, y) = (+\frac{1}{2}x+\frac{1}{2}y\sqrt{3}, +\frac{1}{2}x\sqrt{3}-\frac{1}{2}y)$	
$\sigma(x, y) = (-x, y)$	$\sigma\rho^2(x, y) = (+\frac{1}{2}x-\frac{1}{2}y\sqrt{3}, -\frac{1}{2}x\sqrt{3}-\frac{1}{2}y)$	

In matrix form: Figure 9

$$\varepsilon = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \rho = \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ +\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix} \text{ and } \sigma = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

The other symmetry operations can be computed as compositions of ρ and σ:

$$\rho^2 = \begin{pmatrix} -\frac{1}{2} & +\frac{1}{2}\sqrt{3} \\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix},\ \sigma\rho = \begin{pmatrix} \frac{1}{2} & \frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix} \text{ and } \sigma\rho^2 = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$$

The formulas of figure 8 and the matrices of figure 9 depend on the system of coordinates being used. Complex numbers form another system of coordinates. With coordinates as shown in figure 10 and writing complex numbers in polar coordinates as $re^{i\varphi}$, we find the formulas of figure 11.

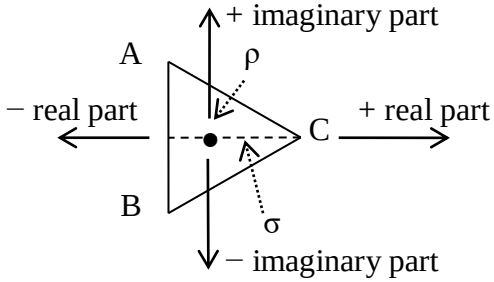


Figure 10

Equilateral triangle

ρ: rotation axis
σ: reflection

		Figure 11
$\varepsilon\left(re^{\varphi i}\right) = re^{\varphi i}$	$\sigma\left(re^{\varphi i}\right) = re^{-\varphi i}$	
$\rho\left(re^{\varphi i}\right) = re^{(\varphi+\frac{2}{3}\pi)i}$	$\sigma\rho\left(re^{\varphi i}\right) = re^{-(\varphi+\frac{2}{3}\pi)i}$	
$\rho^2\left(re^{\varphi i}\right) = re^{(\varphi+\frac{4}{3}\pi)i}$	$\sigma\rho^2\left(re^{\varphi i}\right) = re^{-(\varphi+\frac{4}{3}\pi)i}$	

In general, a contra clockwise rotation ρ_α within the complex plane around point 0 about angle α and a reflection σ_β in a line through point 0 making a contra clockwise angle β with the positive real axis can be described as:

$\rho_\alpha(re^{i\varphi}) = re^{i(\varphi+\alpha)}$	$\sigma_\beta(re^{i\varphi}) = re^{i(2\beta-\varphi)}$	Figure 12
Straightforward calculations show:		
$(\rho_\alpha)^{-1} = \rho_{-\alpha}$	$(\sigma_\beta)^{-1} = \sigma_\beta$	
$\sigma_\beta\rho_{2\alpha} = \sigma_{\beta-\alpha}$	$\sigma_\beta\rho_\alpha = \rho_{-\alpha}\sigma_\beta$	
$\sigma_{\beta'}\sigma_\beta = \rho_{2(\beta-\beta')}$	$\rho_{\alpha'}\rho_\alpha = \rho_{\alpha+\alpha'}$	

3. Elementary theorems

In the previous section some properties of groups have been used, for example those shown in 4a and 5a. In the present section, these and more properties are proven. In the following, x, y and z are arbitrary elements of some group $G(G, \varphi, e)$, id est, every line should be read as beginning with "$\forall x,y,z \in G$:". With this convention axioms 4, 5 and 6 are written as:

$ex = x$ 4b

$x^{-1}x = e$ 5b

$x(yz) = (xy)z \equiv xyz$ 6b

In the proofs, "$=^k$" refers to an axiom or to a previous theorem. "$=^h$" introduces a hypothesis of the current theorem or refers to it. In the proofs, parentheses are omitted as allowed by associativity.

Theorem **7**

$xy =^h xz \Leftrightarrow y = z$

Proof: $\Leftarrow$: obvious.

Proof: $\Rightarrow$: $y =^4 ey =^5 x^{-1}xy =^h x^{-1}xz =^5 ez =^4 z$. QED.

Theorem: symmetry of identity **8**

$xe = x$

Proof: $x^{-1}xe =^5 ee =^4 e =^5 x^{-1}x \Rightarrow^7 xe = x$. QED.

Combining 4 and 8 we have $xe = x = ex$.

Theorem: symmetry of inverse **9**

$xx^{-1} = e$

Proof: $x^{-1}xx^{-1} =^5 ex^{-1} =^4 x^{-1} =^8 x^{-1}e \Rightarrow^7 xx^{-1} = e$. QED

Combining 5 and 9 we have $x^{-1}x = e = xx^{-1}$.

Theorem **10**

$yx =^h zx \Leftrightarrow y = z$.

Proof: $\Leftarrow$: obvious.

Proof: $\Rightarrow$: $y =^8 ye =^9 yxx^{-1} =^h zxx^{-1} =^9 ze =^8 z$. QED.

Theorem: existence and uniqueness of root for y in equation xy = z **11**

$xy =^h z \Rightarrow x = zy^{-1}$

Proof: $y =^8 ye =^5 xyy^{-1} =^h zy^{-1}$. QED.

Theorem: existence and uniqueness of root for x in equation yx = z **12**

$yx =^h z \Rightarrow x = y^{-1}z$

Proof: $x =^4 ex =^5 y^{-1}yx =^h y^{-1}z$. QED.

Theorem **13**

$(xy)^{-1} = y^{-1}x^{-1}$

Proof: $(xy)^{-1}(xy) =^4 e =^5 y^{-1}y =^4 y^{-1}ey =^5 y^{-1}x^{-1}xy \Rightarrow^{10} (xy)^{-1} = y^{-1}x^{-1}$. QED.

In general: $(x_1 \ldots x_n)^{-1} = (x_n^{-1} \ldots x_1^{-1})$, easily proven by means of mathematical induction:
$(x_1 \ldots x_n)^{-1} = (x_n^{-1} \ldots x_1^{-1}) \Rightarrow$
$(x_1 \ldots x_n x_{n+1})^{-1} = ((x_1 \ldots x_n) x_{n+1})^{-1} =^{13} x_{n+1}^{-1}(x_1 \ldots x_n)^{-1} = x_{n+1}^{-1} x_n^{-1} \ldots x_1^{-1}$.

Theorem: uniqueness of identity **14**
$xy =^h y \Rightarrow x = e$
Proof: $ey =^4 y =^h xy \Rightarrow^{10} x=e$. QED.

Theorem: uniqueness of identity **15**
$xy =^h x \Rightarrow y = e$
Proof: $ey =^4 y =^h xy \Rightarrow^7 x=e$. QED.

Theorem: uniqueness of inverse **16**
$xy =^h e \Rightarrow x = y^{-1}$.
Proof: $xy =^h e =^5 y^{-1}y \Rightarrow^{10} x = y^{-1}$. QED.

Theorem: uniqueness of inverse **17**
$xy =^h e \Rightarrow y = x^{-1}$.
Proof: $xy =^h e =^9 xx^{-1} \Rightarrow^7 x^{-1} = y$. QED.

Notation **18**
In the following n is an integer number.

$x^0 \equiv e$
$x^{n+1} \equiv xx^n$
$x^{n-1} \equiv x^{-1}x^n$

This notation is consistent with the notation x^{-1} for the inverse of x.

Theorem **19**
$\forall i,j \in \mathbb{Z}$: $x^i x^j = x^{i+j}$, where $\mathbb{Z}$ is the set of all integer numbers.
Proof: The theorem holds for i = 0 with every integer value of j. If it holds for some integer value i = k and every integer value of j, then we have $x^{k+1}x^j \equiv^{18} xx^kx^j =^h xx^{k+j} \equiv^{18} x^{k+1+j}$ and $x^{k-1}x^j \equiv^{18} x^{-1}x^kx^j =^h x^{-1}x^{k+j} \equiv^{18} x^{k-1+j}$. By mathematical induction, the theorem holds for all integer numbers i and j. QED.

Theorem **20**
$\forall i,j \in \mathbb{Z}$: $(x^i)^j = x^{ij}$, where $\mathbb{Z}$ is the set of all integer numbers.
Proof: The theorem holds for j = 0 with every integer value of i. If it holds for some integer value j = k and every integer value of i, then we have: $x^{i(k+1)} = x^{ik+i} =^{19} x^ix^{ik} =^h x^i(x^i)^k \equiv^{18} (x^i)^{k+1}$ and $x^{i(k-1)} = x^{ik-i} =^{19} x^{-i}x^{ik} =^h (x^i)^{-1}(x^i)^k =^{18} (x^i)^{k-1}$. By mathematical induction, the theorem holds for all integer numbers i and j. QED.

Theorem
The above theorems also show that: $\forall x \in G$: $\{xy: y \in G\} = \{yx: y \in G\} = G$. This means that every row and every column of a table of compositions is a distinct rearrangement of the elements of G. Every row and every column contains every element of G exactly once.

4. Necessity of axioms 4, 5 and 6

Identity

	e	**e'**
e	e	e'
e'	e'	e'

It is essential that the identity in axiom 4 is the same one as in axiom 5. Consider an associative composition with two distinct elements e and e' such that $ex = x$ and $x^{-1}x = e'$. The figure shows such a composition, but contradicts theorems 7 and 10.

Axiom 4

	e	**a**
e	e	e
a	e	e

Axiom 4 cannot be omitted. The figure shows an associative composition that satisfies axiom 5 but does not satisfy axiom 4. It contradicts theorems 7 and 10.

Axiom 5

	e	**a**
e	e	a
a	a	a

Axiom 5 cannot be omitted. The figure shows an associative composition that satisfies axiom 4 but does not satisfy axiom 5. It contradicts theorems 7 and 10.

Associativity

	e	**a**
e	e	a
a	e	e

Axiom 6 (associativity) cannot be omitted, because the shown composition contradicts theorem 8, although it satisfies axioms 4 and 5. This composition is not associative, because in this case: $a(ea) = aa = e \neq a = ea = (ae)a$. Hence $a(ea) \neq (ae)a$.

Symmetry and uniqueness of identity and inverse

Although axioms 4 and 5 are not symmetric, the identity and inverse are symmetric as shown in theorems 8 and 9: $ex = x = xe$ and $x^{-1}x = e = xx^{-1}$. From the elementary theorems, we also learn that a group has one identity only and that every group element has one inverse only. In fact every equation $xy = z$ has exactly one root for x and exactly one root for y (theorems 11 and 12).

5. Order and period

Definition **21**

If for a group element x there is a positive natural number n such that $x^n = e$, then the smallest positive natural number n for which $x^n = e$ is called the order of x. The group elements x, x^2, x^n are called the period of x. This definition implies that $x^k = x^{k \bmod n}$, where n is the order of x and k an arbitrary integer number.

> Define $(k \bmod m)$ for integer numbers k and m, but m=0 excluded, as follows: $(k \bmod m) \equiv (k - m\lfloor k/m \rfloor)$, where $\lfloor k/m \rfloor$ is the floor of k/m, id est, the greatest integer number not greater than k/m. For positive values of m we have $0 \leq (k \bmod m) < m$. For example, $(2 \bmod 3) = 2$ and $(-2 \bmod 3) = 1$. Do not confuse the order of a group with the orders of its elements.

Theorem **22**

Every element of a finite group has a finite order that does not exceed the order of the group.

Proof: Let n be the order of a finite group *G*(G, φ, e). Consider an arbitrary group element x with the sequence $(x^1, x^2 \ldots x^{n+1})$. Because G contains n elements only, the sequence necessarily contains two group elements x^i and x^{i+k} such that $x^i = x^{i+k}$ and $0 < i \leq n$ and $0 < k \leq n-i+1$. Now $x^k = e$ with $0 < k \leq n$. QED.

Later we shall see that the order of an element of a finite group always is a divisor of the order of the group.

6. Homomorphism

Definition **23**

A group *G*'(G', φ', e') is called homomorphic with a group *G*(G, φ, e) if there is a map $\xi: G \rightarrow G'$ such that $\forall x,y \in G: \xi(xy) = (\xi x)(\xi y)$. ξ is called a homomorphism.

Theorem **24**

Using definition 23: let $\xi: G \rightarrow G'$ be a homomorphism. Then $\xi e = e'$.

Proof: $e'\xi(x) = \xi(x) = \xi(ex) = \xi(e)\xi(x) \Rightarrow \xi(e) = e'$. QED.

Theorem **25**

Using definition 23: let $\xi: G \rightarrow G'$ be a homomorphism. Then: $\xi(x^{-1}) = (\xi x)^{-1}$

Proof: $\xi(x^{-1})(\xi x) = \xi(x^{-1}x) = \xi(e) = e' = (\xi x)^{-1}(\xi x) \Rightarrow \xi(x^{-1}) = (\xi x)^{-1}$. QED.

7. Isomorphism

Definition **26**

A group *G*'(G', φ', e') is called isomorphic with a group *G*(G, φ, e) if there is bijective homomorphism ξ: G' ↔ G. ξ is called an isomorphism.

Theorem **27**

The inverse of an isomorphism is an isomorphism.

Proof: With definition 26, let x,y∈G, x' = ξx and y' = ξy. Because ξ is invertible, we have ξ^{-1}x' = x and ξ^{-1}y' = y. Now ξ^{-1}(x'y') = ξ^{-1}((ξx)(ξy)) = ξ^{-1}(ξ(xy)) = xy = (ξ^{-1}x')(ξ^{-1}y'). QED.

Theorem: equivalence of isomorphism **28**

Isomorphism is an equivalence relation.

Proof: Every group is isomorphic with itself with the map ξ: x ↔ x. If *G* is isomorphic with *G'*, then *G*' is isomorphic with *G* according to theorem 27. If ξ: G ↔ G' and ξ': G' ↔ G" are isomorphisms, then ξξ': G ↔ G" is an isomorphism as well. QED.

Non uniqueness of isomorphisms **29**

Let G and G' be two isomorphic groups. There can be more than one isomorphism between G and G, for example with G = {e, a, b, c} and the composition of figure 13:

e	a	b	c	Figure 13
a	e	c	b	
b	c	e	a	
c	b	a	e	

In this case, there are 6 distinct isomorphisms G ↔ G corresponding to the 6 distinct permutations of the group elements a, b and c.

x →	e	a	b	c	Figure 14
ξ_1(x)	e	a	b	c	
ξ_2(x)	e	a	c	b	
ξ_3(x)	e	b	c	a	
ξ_4(x)	e	b	a	c	
ξ_5(x)	e	c	a	b	
ξ_6(x)	e	c	b	a	

Another example is the group:

e	r	r^2	r^3	Figure 15
r	r^2	r^3	e	
r^2	r^3	e	r	
r^3	e	r	r^2	

In this case, there are two isomorphisms between {e, r, r^2, r^3} and itself:

x →	e	r	r^2	r^3	Figure 16
ξ_1(x)	e	r	r^2	r^3	
ξ_2(x)	e	r^3	r^2	r	

The isomorphisms of a group with itself form a group. For example for the group of figure 13 we find the group of the 6 permutations of a, b and c, leaving the identity e unaffected. For figure 16 the group is:

ξ_1	ξ_2	identity	Figure 16a
ξ_2	ξ_1	exchanges r with r^3, leaving e and r^2 unaffected	

Theorem: isomorphism of finite groups with groups of permutations **30**
Every finite group of order n is isomorphic with a subgroup of the n! permutations of a set of n elements.

Proof: Let G be a group with identity e. For every element x of G define ξ_x: y → xy. According to theorems 7, 10, 11 and 12, every ξ_x is a permutation of G. Take composition $\xi_x\xi_y = \xi_{xy}$. We have: $\xi_x\xi_y(z) = xyz = \xi_{xy}(z)$, $\xi_e\xi_y(z) = eyz = yz = \xi_y(z)$ and $\xi_{x-1}\xi_x(z) = x^{-1}xz = ez = \xi_e(z)$. QED

Corollary
We also may consider: ξ'_x: y → yx^{-1}. We have: $\xi'_x\xi'_y(z) = zy^{-1}x^{-1} = z(xy)^{-1} = \xi'_{xy}(z)$. Define φ'(x,y) = φ(y,x). *G*(G,e,φ) and *G*(G,e,φ') are isomorphic to each other with the map f: x → x^{-1} because φ'(f(x),(f(y)) = φ'(x^{-1},y^{-1}) = $y^{-1}x^{-1}$ = $(xy)^{-1}$ = f(xy).

8. Subgroups

Definition **31**
A group *H*(H, φ_h, e_h) is a subgroup of a group *G*(G, φ_g, e_g) if H⊆G and ∀x,y∈H: $\varphi_h(x,y) = \varphi_g(x,y)$. Loosely said, a subgroup is a subset of a group forming a group by itself with the same composition. Clearly:

$e_h = e_g$ 32
∀x∈H: x^{-1}∈H 33

The group shown in figure 7 has the following subgroups:

{ε, ρ, ρ^2, σ, ρσ, $\rho^2\sigma$}	Trivial	Figure 17
{ε}	Trivial	
{ε, ρ, ρ^2}	Rotations only	
{ε, σ}	One single reflection	
{ε, ρσ}	One single reflection	
{ε, $\rho^2\sigma$}	One single reflection	

Definition **34**
Let S be a subset of group G. For every element x∈G, the subset xS ≡ {xs, s∈S} is called a left coset of S and the subset Sx ≡ {sx, s∈S} a right coset. Notice that eS = S = Se. If S_1 and S_2 are subsets of a group G, then we write S_1S_2 ≡ {s_1s_2: s_1∈S_1 and s_2∈S_2}. Intermixed combinations of group elements and subsets are associative. For example, xSy ≡ {xsy, s∈S} = x(Sy) = (xS)y. Furthermore, if H is a subgroup of G, then HH = H.

Theorem **35**
All cosets of a finite subset S of a group G have the same number of elements as S.

Proof. This follows from theorems 7 and 10.

Theorem (Lagrange) **36**
The order of a subgroup H of a finite group G is a divisor of the order of group G.

Proof: Let xH and yH have an element in common. Then we have two elements h_1,h_2∈H such that $xh_1 = yh_2$. Now $xh = yh_2h_1^{-1}h$∈yH, because $h_2h_1^{-1}h$∈H. Likewise yh∈xH. This means that distinct cosets are disjoint. If H is finite, they all have the same number of elements (theorem 35). The junction of all cosets of H forms the whole group G (every coset xH and Hx contains x=xe=ex) Therefore, the order of a subgroup of a finite group is a divisor of the order of the latter.

The period of an element is a subgroup. This implies that the order of every group element is a divisor of the order of the whole group, provided the group is finite.

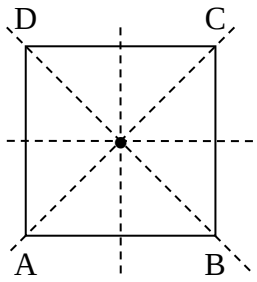
Definition **37**
A subgroup H of a group G is invariant if and only if ∀x∈G: x^{-1}Hx = H.

Definition: factor groups **38**

Let H be an invariant subgroup of group G. Consider the cosets of H with composition as in definition 34. For every element x of G we have xH = Hx, for $xH = xx^{-1}Hx = eHx = Hx$. Now:

$eHxH = xH$
$(x^{-1}H)(xH) = x^{-1}HxH =^{31} HH = H = eH$

Hence, with the composition of definition 34, the cosets of invariant subgroup H form a group, called a factor group and denoted as G/H. Example: consider the group of the planar symmetry operations of a square (figure 18) with rotation axis ρ and reflexion σ. ρ rotates anticlockwise about 90°. σ reflects in the vertical middle line.



Symmetries of a square.

The dotted lines are reflection lines. The rotation axis is perpendicular to the plane of the square and intersects the middle of the square, indicated by a dot.

Figure 18

Taking ρ for a rotation about 90° and σ for reflection in the vertical middle line, the group table is:

ε	ρ	ρ^2	ρ^3	σ	ρσ	$\rho^2\sigma$	$\rho^3\sigma$	Figure 19
ρ	ρ^2	ρ^3	ε	ρσ	$\rho^2\sigma$	$\rho^3\sigma$	σ	
ρ^2	ρ^3	ε	ρ	$\rho^2\sigma$	$\rho^3\sigma$	σ	ρσ	
ρ^3	ε	ρ	ρ^2	$\rho^3\sigma$	σ	ρσ	$\rho^2\sigma$	
σ	$\rho^3\sigma$	$\rho^2\sigma$	ρσ	ε	ρ^3	ρ^2	ρ	
ρσ	σ	ρσ	$\rho^2\sigma$	ρ	ε	ρ^3	ρ^2	
$\rho^2\sigma$	ρσ	σ	$\rho^3\sigma$	ρ^2	ρ	ε	ρ^3	
$\rho^3\sigma$	$\rho^2\sigma$	ρσ	σ	ρ^3	ρ^2	ρ	ε	

The subgroups of figure 19 are:

Subgroup	Invariant?
{ε, ρ, ρ^2, ρ^3, σ, ρσ, $\rho^2\sigma$, $\rho^3\sigma$}	Yes
{ε}	Yes
{ε, ρ, ρ^2, ρ^3}	Yes
{ε, σ, ρ^2, $\rho^2\sigma$}	Yes
{ε, ρσ, ρ^2, $\rho^3\sigma$}	Yes
{ε, ρ^2}	Yes
{ε, σ}	No
{ε, ρσ}	No
{ε, $\rho^2\sigma$}	No
{ε, $\rho^3\sigma$}	No
Figure 20	

9. Permutations

Definition **39**

A permutation is a bijection of a set onto the same set. Obviously, the permutations of a set form a group. Writing the permutations of {a,b,c} as (P(a),(P(b),(P(c)) we find:

(a,b,c), (b,c,a), (c,a,b), (c,b,a), (b,a,c) and (a,c,b)

A group of all permutations of a non-empty finite set of n elements is called a symmetric group and is denoted as S_n, which contains n! elements.

10. Cycle notation and transpositions

Let P be a permutation of a finite set S. Let n be the order of P. Its period is (P ... P^n), where P^n is the identity. An element $a \in S$ can be subjected to repeated applications of P such as to form a list of distinct elements (a, P(a), P^2(a) ... P^{m-1}(a)). This list is called a cycle, particularly the cycle of element a under permutation P. Clearly, m is a divisor of n. If m would not be a divisor of n, say n = jm+k with $0 \leq k < m$, then both P^{jm+k}(a) and P^m(a) and P^{jm}(a) would be equal to a, meaning that P^k(a) would be equal to a too, contrary to the assumption that all elements of the cycle of a under P are distinct. Every permutation of a finite set can be written as ((k_0 k_1 k ...) ...), where all cycles (k_0 k_1 k ...) are disjoint. Each individual cycle (k_0 k_1 k ...) represents a permutation and ((k_0 k_1 k ...) ...) the product of these permutations. Cycle (k_0 k_1 k ...) maps each element to its successor and the last element to the first one. Elements not present in (k_0 k_1 k ...) are mapped onto themselves. For example in the set {0, 1, 2, 3, 4} we have:

element	image under (0 2 3)	image under ((0 2 3) (1 4))
0	2	2
1	1	4
2	3	3
3	0	0
4	4	1

An empty cycle and every cycle consisting of one element only, represents the identity. In the permutation ((k_0 k_1 k ...) ...), the identities may be omitted. A cycle consisting of two elements is called a transposition. Every permutation of a finite set can be written as a product of disjoint cycles. Every permutation of a finite set can be written as a product of transpositions, because every cycle (k_0 k_1 ... k_n) can be written as ((k_0 k_1) (k_1 k_2) ... (k_{n-1} k_n)). For example ((a b c)) = ((a b) (b c)) and ((a b c d)) = ((a b) (b c) (c d)). There are other ways to decompose a permutation of a finite set into a product of transpositions, but for a given permutation, the decomposition has either always an even number of transpositions or always an odd number of transpositions. Hence, group elements have parity.

Proof: writing a permutation P as a product of disjoint cycles. Take any element a of the set on which P operates and write the cycle (a) if P(a) = a. Write (a P(a) P^2(a) … P^{m-1}(a)) if $P(a) \neq a$. Take the least m such that $P^m(a) = a$. Because the permutation P has a finite order, m exists. If (a P(a) P^2(a) … P^{m-1}(a)) does not contain all elements of the set, take any other element b and form the cycle (b P(b) P^2(b) … $P^{m'-1}$(b)). Repeat forming such cycles until all elements of the set have been accounted for. Now we have a product of disjoint and distinct cycles. Because they are disjoint, all cycles commute with each other. If none of the cycles has more than one element, we have the identity and can write the product as ( ). If there is at least one cycle of at least two elements, all cycles with less than two elements can be omitted, because they represent the identity. Modulo the order of the individual cycles, the choice of the first element of a cycle and the inclusion or exclusion of cycles of zero or one elements, each permutation P has only one way to write it as a product of disjoint cycles, for if a is in a cycle, then so are P^i(a) and those only, for i running from 0 up to but not including the order of P.

Proof of parity. As shown above, every permutation can be written as the product of disjoint cycles. Include all cycles of length 1. Because the cycles are disjoint, they commute and can be written in any order. If the set on which the permutations operate has n elements then the sum of the lengths of the cycles is n. Let k be the number of cycles. n−k is called the decrement of the permutation. Each cycle of length n_i can be written as a product of n_i-1 transpositions and $\Sigma n_i = n$. A cycle of one single element is written as a product of zero transpositions. Hence, the number of transpositions is the decrement n−k. Now consider taking a product with a transposition (a b): ((…) … (a b)) or ((a b) (…) …). There are two possibilities: either a and b occur in the same cycle of ((…) …) or in two disjoint ones.

Case 1a: a and b in the same cycle. 40
(a c … c' b d …d') (a b) = (b c … c') (a d … d') , which decreases the decrement by 1.

Case 1b: a and b in the same cycle. 41
(a b) (a c … c' b d …d') = (c … c' a) (d … d' b) , which decreases the decrement by 1.

Case 2a: a and b in two disjoint cycles. 42
(a c ... c') (b d ... d') (a b) = (b c ... c' a d ... y'), which increases the decrement by 1.

Case 2b: a and b in two disjoint cycles. 43
(a b) (a c ... c') (b d ... d') = (a c ... c' b d ... d'), which increases the decrement by 1.

Hence, the parity of the decrement is always equal to the parity of the number of transpositions into which a permutation is decomposed. QED.

The parity of the identity is even. The product of two permutations with the same parity is even. For two permutations with opposite parity, the product is odd. The parity of an inverse permutation x^{-1} equals the parity of permutation x, because when written as a product of transpositions, x^{-1} equals the product in reversed order, as each transposition is its own inverse. Hence, the subset of all even permutations forms a subgroup. This is not true for the set of odd permutations, for it does not include the identity and the product of two odd permutations is even, not odd. A group containing at least one odd element has as many odd elements as even ones.{xz: z even} has as many elements as {z: z even} and contains all odd elements, for let y be another odd element, then $y = xx^{-1}y$ in which $x^{-1}y$ is even.

11. Conjugation classes

Definition **44**

Two group elements x and y are conjugate to each other and we write $x \approx y$, if there is a group element z such that $x = z^{-1}yz$.

Theorem **45**

Conjugation is an equivalence relation.
Proof:

Reflectivity: $x = e^{-1}xe \Rightarrow x \approx x$
Symmetry: $x \approx y \Rightarrow \exists z: z^{-1}xz = y \Rightarrow zyz^{-1} = x \Rightarrow y \approx x$
Transitivity: $x \approx y \wedge y \approx z \Rightarrow \exists p,q: x = p^{-1}yp \wedge y = q^{-1}zq \Rightarrow x = p^{-1}q^{-1}zqp = (qp)^{-1}z(qp)$

Hence, conjugate group elements form disjoint classes, called conjugation classes. Examples:

Classes of S_3:	even	( )
	even	((0 1 2)) and ((0 2 1))
	odd	((0 1)), ((0 2)) and ((1 2))
Classes of C_{4v}:	even	( )
	odd	((1 3)) and ((0 2))
	even	((0 2) (1 3))
	even	((0 1) (2 3)) and ((0 3) (1 2))
	odd	((0 1 2 3)) and ((0 3 2 1))

Theorem **46**

All elements of the same conjugation class of a finite group of permutations have the same cycle structure when written as a product of disjoint cycles.

Proof: Consider y and $z^{-1}yz$. Write z as a product of transpositions and z^{-1} as the same product in reversed order. The transpositions are not necessarily elements of the group. First consider the case that z is a single transposition. Then yz may have another cycle-structure than y, but 40, 41, 42 and 43 show that z^{-1} in $z^{-1}yz$ undoes the changes made by z and restores the cycle structure of y. When

z is a product of two or more transpositions, say $z_1 \ldots z_n$, then in $z_n \ldots z_1 y z_1 \ldots z_n$, each transposition z_i at the left undoes the effect of the same transposition z_i at the right. QED.

Theorem **47**

For a symmetric group S_n, two elements have the same cycle structure if and only if they belong to the same conjugation class.

Proof: Theorem 46 already states that all conjugate permutations have the same cycle structure. In the symmetric group S_n, all permutations of the n elements of the set on which the permutations operate, are part of the group. Consider two permutations x and y with the same cycle structure. They only differ in the names of the elements in their cycles. Renaming the elements of y before applying y and undoing the renaming afterwards yields the same effect as x. Of course, the renaming afterwards must be the inverse of the renaming before applying y. Hence, in S_n all permutations with the same cycle structure are conjugates of each other. QED.

Theorem 47 does not apply to all proper subgroups of S_n. For example:

e	(0 1)	(2 3)	(0 1) (2 3)	figure 21
(0 1)	e	(0 1) (2 3)	(2 3)	
(2 3)	(0 1) (2 3)	e	(0 1)	
(0 1) (2 3)	(2 3)	(0 1)	e	

As the group of figure 21 is abelean, every permutation is conjugate with itself only.

12. Group structure

The above material provides tools to construct all non-isomorphic groups modulo isomorphism of a specified finite number of group elements.

Groups of prime order

A group containing an element x such that the set of the powers of x form the whole group is called cyclic. It is denoted as C_n and is abelean. If the order of the group is a prime number, it is necessarily cyclic, because the order of a group element always is a divisor of the order of the group.

Groups of order 4

Now let us examine the possible structures for groups of 4 elements. The simplest one is the abelean group C_4 with a group element of order 4. The other one is the so-called four-group V. It is abelean too, but has no group element of order 4.

e	x	x^2	x^3
x	x^2	x^3	e
x^2	x^3	e	x
x^3	e	x	x^2

← C_4 V →

e	x	y	z
x	e	z	y
y	z	e	x
z	y	x	e

Figure 22 Figure 23

These are all groups of order 4 (modulo isomorphism) This is easily understood as follows. If the group is not cyclic, its elements, the identity excepted, must have order 2 because this is the only divisor of 4 greater than 1 and no group element, the identity excepted, can have order 1. Therefore, we start with the green cells of the table. Because a row or column cannot contain the same group element twice, there is only one choice for each white cell. Finally, we may check that the table is associative. The minimal bases of C_4 are {x} and $\{x^3\}$, those of V are all combinations of two elements out of x, y and z.

Groups of order 6

Now let us examine all possible structures of a group of order 6. The first one is the abelean group C_6. The largest divisor of 6 less than 6 is 3. Therefore we try a period $x^3 = e$ and add an element y Suppose y commutes with x. Then we get:

e	x	x^2	y	yx	yx^2
x	x^2	e	yx	yx^2	y
x^2	e	x	yx^2	y	xy
y	yx	yx^2	e	x	x^2
yx	yx^2	y	x	x^2	e
yx^2	y	xy	x^2	e	x

Figure 24.

This is isomorphic with the group C_{3h}, having of a three fold rotation axis x and a plane of symmetry y perpendicular to the axis of rotation. C_{3h} is also isomorphic with C_6 because the period of yx is (yx, x^2, y, x, yx^2, e).

Whether or not y commutes with x, not both can have periods of order 3 within a group of order 6, for this would lead to:

e	x	x^2	y	y^2	z
x	x^2	e	z		
x^2	e	x			
y			y^2	e	
y^2			e	y	
z					
Figure 25					

Because each row and each column must contain each element of the group, there is only one option for the green cell. However, no group element is left to put into the red cell. Hence, y is of order 2. The case that y commutes with x has already been investigated. Hence we try the case that y does not commute with x. This leads to:

e	x	x^2	y	yx	yx^2
x	x^2	e	yx^2		
x^2	e	x			
y	yx	yx^2	e		
yx	yx^2	y			
yx^2	y	yx			

Figure 26.

The green cell of figure 26 cannot contain yx, because x and y are supposed not to commute with each other. The only other group element not yet in the same row and column is yx^2. With the knowledge that $xy = yx^2$, the remaining products are easily found, for example:

$(yx)y = y(xy) = y(yx^2) = (yy)x^2 = ex^2 = x^2$

e	x	x^2	y	yx	yx^2
x	x^2	e	yx^2	y	yx
x^2	e	x	yx	yx^2	y
y	yx	yx^2	e	x	x^2
yx	yx^2	y	x^2	e	x
yx^2	y	yx	x	x^2	e

Figure 27.

Figure 27 is isomorphic with the group C_{3v}. One other possibility remains to be investigated, namely that all group elements have order 2, the identity excepted. The table becomes:

e	x	y	xy	z	xz
x	e	xy	y	xz	z
y		e			
xy		x	e		
z		xz	x	e	
xz		z		x	e

Figure 28

The yellow cell of figure 28 can contain xz only. Now only one choice remains for the two blue cells. However, no group element remains to be put in the red cell. Hence there is no group of order 6 with all elements, the identity excepted, having order 2.

Now we have exhausted all structures of groups of order 6. All groups of order 6 are isomorphic with one of the following ones: C_6~C_{3h} or C_{3v}~S_3.

Groups of order 8

In the same way, all structures of groups of order 8 can be found. There is C_8, which is isomorphic with the group consisting of the natural numbers 0 up to and including 7, with 0 for its identity and addition modulo 8 for its composition. There is no group of order 8, without an element of order 8 and with 2 elements with disjoint cycles of order 4. The reason is the same as for which there is no group of order 6 with two elements with disjoint cycles of order 3. Now let x be of order 4 and y an arbitrary other group element that is not a power of x. We start from the following table:

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y							
xy							
x^2y							
x^3y							

Figure 29.

If x and y commute, we get:

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y	xy	x^2y	x^3y				
xy	x^2y	x^3y	y				
x^2y	x^3y	y	xy				
x^3y	x^3y	y	xy				

Figure 30.

What to put in the yellow cell? Options are e, x, x^2 and x^3. The results are:

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y	xy	x^2y	x^3y	e	x	x^2	x^3
xy	x^2y	x^3y	y	x	x^2	x^3	e
x^2y	x^3y	y	xy	x^2	x^3	e	x
x^3y	x^3y	y	xy	x^3	e	x	x^2

Figure 31.

In figure 31 y^2=e, x and y commute. This is isomorphic with C_{4h} formed by a four fold axis x of rotations and a plane of reflection y perpendicular on axis x.

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y	xy	x^2y	x^3y	x	x^2	x^3	e
xy	x^2y	x^3y	y	x^2	x^3	e	x
x^2y	x^3y	y	xy	x^3	e	x	x^2
x^3y	x^3y	y	xy	e	x	x^2	x

Figure 22. y^2=x, x and y commute. Isomorphic with C_8: (y, x, xy, x^2, x^2y, x^3, x^3y, e)

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y	xy	x^2y	x^3y	x^2	x^3	e	x
xy	x^2y	x^3y	y	x^3	e	x	x^2
x^2y	x^3y	y	xy	e	x	x^2	x^3
x^3y	x^3y	y	xy	x	x^2	x	e

Figure 23. $y^2=x^2$, x and y commute. This is isomorphic with C_{4h} formed by a four fold axis x of rotations and a plane of reflection x^3y perpendicular on axis x. This group is isomorphic with that of figure 22.

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y	xy	x^2y	x^3y	x^3	e	x	x^2
xy	x^2y	x^3y	y	e	x	x^2	x^3
x^2y	x^3y	y	xy	x	x^2	x	e
x^3y	x^3y	y	xy	x^2	x	e	x

Figure 24. $y^2=x^3$, x and y commute. Isomorphic with C_8. (y, x^3, x^3y, x^2, x^2y, x, xy, e)

Now suppose x and y do not commute. We get:

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y							
xy							
x^2y							
x^3y							

Figure 25.

The options for the yellow cell are x^2y and x^3y. Group element xy is excluded because x and y are not supposed to commute. However, $yx=x^2y$ must be excluded as well, because it would imply $yx^2 = (yx)x = (x^2y)x = x^2(yx) = x^2x^2y = y$, which would imply x^2=e. Therefore the only option left is $yx=x^3y$.

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y	x^3y	x^2y	xy				
xy	y	x^3y	x^2y				
x^2y	xy	y	x^3y				
x^3y	x^2y	xy	y				

Figure 26. The options for the yellow cell are e, x, x^2 and x^3. However, $y^2=x$ combined with $yx=x^3y$ would imply $yyx=yx^3x=y$, from which $yx=e$. For the same reason $y^2=x^3$ must be excluded.

Now two options are left: $y^2=e$ and $y^2=x^2$.

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y	x^3y	x^2y	xy	e	x^3	x^2	x
xy	y	x^3y	x^2y	x	e	x^3	x^2
x^2y	xy	y	x^3y	x^2	x^3	e	x
x^3y	x^2y	xy	y	x^3	x^2	x	e

Figure 27. $y^2=e$. x and y do not commute. This is isomorphic with the group C_{4v} consisting of a four fold axis of rotation r=x and a plane of reflection s=y containing the axis of rotation.

e	x	x^2	x^3	y	xy	x^2y	x^3y
x	x^2	x^3	e	xy	x^2y	x^3y	y
x^2	x^3	e	x	x^2y	x^3y	y	xy
x^3	e	x	x^2	x^3y	y	xy	x^2y
y	x^3y	x^2y	xy	x^2	x	e	x^3
xy	y	x^3y	x^2y	x^3	x^2	x	e
x^2y	xy	y	x^3y	e	x^3	x^2	x
x^3y	x^2y	xy	y	x	e	x^3	x^2

Figure 28. $y^2=x^2$. x and y do not commute. This is isomorphic with the quaternion group shown in figure 29. Rename e=1, x=i, $x^2=-1$, $x^3=-i$, y=j, xy=k, $yx^2=-k$ and $yx^3=-j$.

1	−1	i	−i	j	−j	k	−k
−1	1	−i	i	−k	k	−j	j
i	−i	−1	1	k	j	−k	−j
−i	i	1	−1	−j	−k	j	k
j	−k	−j	k	−1	−i	i	1
−j	k	−k	j	i	−1	1	−i
k	−j	j	−k	−i	1	−1	i
−k	j	k	−j	1	i	−i	−1

Figure 29: quaternion group

This group can be constructed from base {i , j} with the following equations: $i^2=j^2=k^2=-1$, ij=k, jk=i and ki=j. Notice: $ji=-i^2ji=-iki=-ij$. Likewise kj=−i and ik=−j.

Now one case remains, a group of order 8 with no elements of order greater than 2. There is only one solution, which is abelean:

e	x	y	z	xy	xz	yz	xyz
x	e	xy	xz	y	z	xyz	yz
y	xy	e	yz	x	xyz	z	xy
z	xz	yz	e	xyz	x	y	xy
xy	y	x	xyz	e	yz	xz	z
xz	z	xyz	x	yz	e	xy	x
yz	xyz	z	y	xz	xy	e	x
xyz	yz	xz	xy	z	y	x	e

Figure 30. This is isomorphic with the abelean group D_{2h}, which is formed by a two fold rotation axes $c_2=x$ and two planes of reflection $s_h=y$ and $s_v=z$ Notice that every group element is its own inverse.

This completes the search for all groups of 8 elements. Summary:

name	abelean?	Rotations	Reflections
C_8	yes	1 of order 8	none
C_{4h}	yes	1 of order 4	horizontal
D_{2h}	yes	1 of order 2	horizontal and vertical
C_{4v}	no	1 of order 4	vertical
Q	no	na	na

The quaternion group is isomorphic with the group formed from the base (in cycle notation): (0 1 2 3) (4 5 6 7)) and ((0 4 2 6) (1 7 3 5)).

13. Groups of order 9

There are two groups of order 9. First, there is C_9. All group elements of the only other possible structure, the identity excepted, have order 3. This is the direct product of C_3 with itself, which is the set $C_3 \times C_3$ with the composition (x,x')(y,y')=(xx',yy'). The group is abelean. Figure 33:

ee'	ea'	ea'^{2}	ae'	aa'	aa'^{2}	a^{2}e'	a^2'a	a^{2}a'^{2}	figure 33
ea'	ea'^{2}	ee'	aa'	aa'^{2}	ae'	a^{2}a'	a^2'a^2	a^{2}e'	
ea'^{2}	ee'	ea'	aa'^{2}	ae'	aa'	a^{2}a'^{2}	a^2'e	a^{2}a'	
ae'	aa'	aa'^{2}	a^{2}e'	a^{2}a'	a^{2}a'^{2}	ee'	e'a	ea'^{2}	
aa'	aa'^{2}	ae'	a^{2}a'	a^{2}a'^{2}	a^{2}e'	ea'	ea'^{2}	ee'	
aa'^{2}	ae'	aa'	a^{2}a'^{2}	a^{2}e'	a^{2}a'	ea'^{2}	ee'	ea'	
a^{2}e'	a^{2}a'	a^{2}a'^{2}	ee'	ea'	ea'^{2}	ae'	aa'	aa'^{2}	
a^{2}a'	a^{2}a'^{2}	a^{2}e'	ea'	ea'^{2}	ee'	aa'	aa'^{2}	ae'	
a^{2}a'^{2}	a^{2}e'	a^{2}a'	ea'^{2}	ee'	ea'	aa'^{2}	ae'	aa'	

14. Group structure and isomorphism

In this section, an investigation is made how well data about the structure of a group do identify that group. Of course, a group is fully determined by its table of compositions. However, two tables of a group may seem much different when the group elements have different names and are put in a different order. Isomorphism of two finite groups can be decided by brute force. First, the groups must have the same order, of course, say n. There are n! different bijections between the sets of the two groups. If the groups are isomorphic, then at least one of the bijections is an isomorphism. However, the number of bijections that have to be tried can be reduced. Group elements with the same property such as their order and their size of the conjugation class must be mapped on group elements with the same properties. For each group element, the following data can easily be retrieved from the table of compositions.

1 The length of the cycle of the group element.
2 Is this cycle an invariant subgroup?
3 With how many group elements does the group element commute?
4 How many elements of the group contain the group element in their cycle?
5 Size of the conjugate class of the group element.

For the group as a whole we have furthermore:

6 The order of the group
7 The number and sizes of the conjugation classes.
8 The number and sizes of disjoint cycles.
9 The number and orders of the subgroups.

If two groups differ in at least one of these data, they certainly are not isomorphic. What if all data match? In that case, we can eliminate many of the n! bijections between them. Group elements with the same properties must be mapped onto group elements with the same property. As an example, consider group C_{4v}.

group element	commutes	cycle	order	invariant	conjugation class	size	nr of cycles
ε	8	ε	1	yes	$\{\varepsilon\}$	1	8
ρ	4	$\rho, \rho^2, \rho^3, \varepsilon$	4	yes	$\{\rho, \rho^3\}$	2	2
ρ^2	8	ρ^2, ε	2	yes	$\{\rho^2\}$	1	3
ρ^3	4	$\rho^3, \rho^2, \rho, \varepsilon,$	4	yes	$\{\rho, \rho^3\}$	2	2
σ	4	σ, ε	2	no	$\{\sigma, \rho^2\sigma\}$	2	1
$\rho\sigma$	4	$\rho\sigma, \varepsilon$	2	no	$\{\rho\sigma, \rho^3\sigma\}$	2	1
$\rho^2\sigma$	4	$\rho^2\sigma, \varepsilon$	2	no	$\{\sigma, \rho^2\sigma\}$	2	1
$\rho^3\sigma$	4	$\rho^3\sigma, \varepsilon$	2	no	$\{\rho\sigma, \rho^3\sigma\}$	2	1

Figure 34

Column ‘commutes’ of figure 34 shows the number of group elements the group element commutes with. Column invariant shows whether the cycle of the group element forms an invariant subgroup. Column ‘size’ shows the number of group elements of the conjugation class of the group element. Column ‘nr of cycles’ shows how many group elements include the group element in their cycles. We can distinguish families of group elements according to these properties.

family	size of family	commutes	order	invariant	size	nr of cycles
ε	1	8	1	yes	1	8
ρ^2	1	8	2	yes	1	3
ρ, ρ^3	2	4	4	yes	2	2
$\sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma$	4	4	2	no	2	1

Figure 35

If two groups do not show the same blue part of the table (after sorting the tables), then the two groups certainly are not isomorphic. If the tables match, then only those bijections need to be inspected which map group elements to group elements of the same family. Hence the number of bijections to be investigated can be reduced to 1!×1!×2!×4! = 48, which is considerably less than 8! = 40320.

The families of C_{6v} are:

family	size of family	commutes	order	invariant	size	nr of cycles
ε	1	12	1	yes	1	12
ρ, ρ^5	2	6	6	yes	2	2
ρ^3	1	12	2	yes	1	3
ρ^2, ρ^4	2	6	3	yes	2	4
$\sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma, \rho^4\sigma, \rho^5\sigma$	6	4	2	no	3	1

Figure 36

For C_{6v}, the number of bijections to be tried is 1!×2!×1!×2!×6! = 2880, whereas the group has 12 elements and 12! = 479,001,600. Twelve of the bijections are isomorphisms. C_{6v} can be mapped isomorphically onto itself in the following 12 ways:

	Auto-isomorphisms of C_{6v}	
	pure rotations	reflection-rotations
1	$\rho^n \to \rho^n$	$\rho^n\sigma \to \rho^n\sigma$
2	$\rho^n \to \rho^n$	$\rho^n\sigma \to \rho^{n+1}\sigma$
3	$\rho^n \to \rho^n$	$\rho^n\sigma \to \rho^{n+2}\sigma$
4	$\rho^n \to \rho^n$	$\rho^n\sigma \to \rho^{n+3}\sigma$
5	$\rho^n \to \rho^n$	$\rho^n\sigma \to \rho^{n+4}\sigma$
6	$\rho^n \to \rho^n$	$\rho^n\sigma \to \rho^{n+5}\sigma$
7	$\rho^n \to \rho^{-n}$	$\rho^n\sigma \to \rho^n\sigma$
8	$\rho^n \to \rho^{-n}$	$\rho^n\sigma \to \rho^{n+1}\sigma$
9	$\rho^n \to \rho^{-n}$	$\rho^n\sigma \to \rho^{n+2}\sigma$
10	$\rho^n \to \rho^{-n}$	$\rho^n\sigma \to \rho^{n+3}\sigma$
11	$\rho^n \to \rho^{-n}$	$\rho^n\sigma \to \rho^{n+4}\sigma$
12	$\rho^n \to \rho^{-n}$	$\rho^n\sigma \to \rho^{n+5}\sigma$

Figure 37

We see that ρ^n can be mapped onto ρ^n or ρ^{-n}. Independently, $\rho^n\sigma$ can be mapped onto $\rho^n\sigma$, $\rho^{n+1}\sigma$, $\rho^{n+2}\sigma$, $\rho^{n+3}\sigma$, $\rho^{n+4}\sigma$ or $\rho^{n+5}\sigma$. Each auto-isomorphism corresponds to a base of a pure rotation and a rotation reflection. C_{6v} can be built from a base of two group elements consisting of ρ or ρ^{-1} combined with any of the 6 reflection-rotations. Mapping ρ^n or ρ^{-n} corresponds to reversal of the direction of rotation. The reflection σ can be chosen in arbitrary position of the 6 rotations.

How can we further delimit the number bijections to be investigated? One might look for all minimal bases of the two groups whose isomorphism is to be decided. For C_{4v} there are 12 minimal bases. If the list of bases of the groups have different structure, then the two groups are not isomorphic. If the two lists agree, then form a map by taking one minimal base of the first group and looking for a minimal base of the second group with the same structure. The minimal bases of C_{4v} are:

	base		orders	
1	ρ	σ	4	2
2	ρ	$\rho\sigma$	4	2
3	ρ	$\rho^2\sigma$	4	2
4	ρ	$\rho^3\sigma$	4	2
5	ρ^3	σ	4	2
6	ρ^3	$\rho\sigma$	4	2
7	ρ^3	$\rho^2\sigma$	4	2
8	ρ^3	$\rho^3\sigma$	4	2
9	σ	$\rho\sigma$	2	2
10	σ	$\rho^2\sigma$	2	2
11	σ	$\rho^3\sigma$	2	2
12	$\rho\sigma$	$\rho^2\sigma$	2	2
13	$\rho\sigma$	$\rho^3\sigma$	2	2
14	$\rho^2\sigma$	$\rho^3\sigma$	2	2

There are 8 bases with orders 4 and 2 and 6 bases with orders 2 and 2. Each blue base can be mapped onto each blue base. Likewise, each yellow base can be mapped onto a yellow base.

The easiest way to find an isomorphism between a group G_1 and a group G_2 is by taking a minimal base of G_1 and looking for a minimal base of G_2 with the same and consistent structure.

The end