Mathematical Faculty
University of Belgrade

Rowaida Shaban Elmarghni

The symmetric group

Master thesis

Supervisor

Prof. Aleksandar Lipovski, PhD.

Belgrade, 2011

Table of Contents

Introduction

In abstract algebra, as in the case of most twentieth-century developments, the basic concepts and goals were fixed in the nineteenth century. The fact that algebra can deal with collections of objects that are not necessarily real or complex numbers was demonstrated in a dozen nineteenth-century creations. Vectors, quaternions, matrices, forms such as $ax^2 + bxy + cy^2$, hyper numbers of various sorts, transformations. and substitutions or permutations are examples of objects that were combined under operations and laws of operation peculiar to the respective collections, liven the work on algebraic numbers, though it dealt with classes of complex numbers, brought to the lore the variety of algebras because it demonstrated that only some properties are applicable to these classes as opposed to the entire complex number system.

These various classes of objects were distinguished in accordance with the properties that the operations in them possessed; and we have seen that such notions as group, ring, ideal, and field, and subordinate notions such as subgroup, invariant subgroup, and extension field were introduced to identify the sets of properties. However, nearly all the nineteenth-century work on these various types of algebra dealt with the concrete systems mentioned above. It was only in the last decades of the nineteenth century that the mathematicians appreciated that they could move up to a new level of efficiency; by integrating many separate algebras through abstraction of their common content. Thus permutation groups, the groups of classes of forms treated by Gauss, hyper numbers under addition, and transformation groups could all be treated in one swoop by speaking of a set of elements or things subject to an operation whose nature is specified only by certain abstract properties, the foremost of these being that the operation elements of the set produces a third element of the set. The same advantages could be achieved for the various collections that formed rings and fields. Though the idea of working with abstract collections preceded the axiomatics of Pasch, Peano, and Hilbert, the latter development undoubtedly accelerated the acceptance of the abstract approach to algebras.

Thus arose abstract algebra as the conscious study of entire classes of algebras, which individually were not only concrete but which served purposes in specific areas as substitution groups did in the theory of equations. The advantage of obtaining results that might be useful in many specific areas by considering abstract vectors was soon lost sight of, and the study of abstract structure and the derivation of their properties became an end in itself

Abstract algebra has been one of the fevered fields of the twentieth century and is now a vast area.

It is a fevered activity of historians, now that abstract theory is in existence, to trace how many of the abstarct ideas were foreshadowed by the concrete works of Gauss, Abel, Galois, Cauchy, Sylow and dozens of other men.

In mathematics and abstract algebra, **group theory** studies the algebraic structures known as groups. The concept of a group is central to abstract algebra: other well-known algebraic structures, such as rings, fields, and vector spaces can all be seen as groups endowed with additional operations and axioms. Groups recur throughout mathematics, and the methods of group theory have strongly influenced many parts of algebra. Linear algebraic groups and Lie groups are two branches of group theory that have experienced tremendous advances and have become subject areas in their own right.

Various physical systems, such as crystals and the hydrogen atom, can be modeled by symmetry groups. Thus group theory and the closely related representation theory have many applications in physics and chemistry.

One of the most important mathematical achievements of the 20th century was the collaborative effort, taking up more than 10,000 journal pages and mostly published between 1960 and 1980, that culminated in a complete classification of finite simple groups.

Group theory can be considered the study of symmetry; the collection of symmetries of some object preserving some of this structure from a group, in some sense all groups arise this way. Formally a group is a set G on which there is a multiplication (*) defined satisfying associative law, in addition, there is to be element (1) in G with $1*g = g*1 = g$ for every $g \in G$ and every element g in G must have an inverse h satisfying $g*h = h*g = 1$.

A particularly important class of groups is the set of permutation groups, those in which the elements are permutation of some set and the group operation is simply composition, for example the symmetric group on objects is the set of all N! rearrangements of the N elements.
The symmetric group on n letters is generated by the transposition
S_i = (i, i+1), i=1, . . n-1). These generators satisfy the well known relations $S_i^2 = 1$, $S_iS_j=S_jS_i$ ($|i-j| \geq 2$) and $S_iS_{i+1} + S_i = S_{i+1}S_iS_{i+1}$
Moreover, the abstract group defined by the S_i with the given relations is a Coxeter group , isomorphic to S_n .
This set $\{S_i\}$ can be presented by a graph on the vertices 1, . . . , n where S_i is the edge connecting i and i+1. More generally, one can use any connected graph T on n vertices to define a Coxeter group C (T), from which there is a natural projection onto the corresponding symmetric group.

1. History of symmetric group

The history of group theory, a mathematical domain studying groups in their various forms, has evolved in various parallel threads. There are three historical roots of group theory: the theory of algebraic equations, number theory and geometry. Lagrange, Abel and Galois were early researchers in the field of group theory.

- Early 19th century
- Development of permutation groups
- Groups related to geometry
- Appearance of groups in number theory
- Convergence
- Late 19th century
- Early 20th century
- Mid 20th century
- Later 20th century
- Late 20th century
- Today

1.1. Early 19th century

The earliest study of groups as such probably goes back to the work of Lagrange in the late 18th century. However, this work was somewhat isolated, and 1846 publications of Cauchy and Galois are more commonly referred to as the beginning of group theory. The theory did not develop in a vacuum, and so 3 important threads in its pre-history are developed here.

1.2. Development of permutation groups

One foundational root of group theory was the quest of solutions of polynomial equations of degree higher than 4.
An early source occurs in the problem of forming an equation of degree m having as its roots m of the roots of a given equation of degree $n > m$. For simple cases the problem goes back to Hudde (1659). Saunderson (1740) noted that the determination of the quadratic factors of a biquadratic expression necessarily leads to a sextic equation, and Le Sœur (1748) and Waring (1762 to 1782) still further elaborated the idea.
A common foundation for the theory of equations on the basis of the group of permutations was found by mathematician Lagrange (1770, 1771), and on this was built the theory of substitutions. He discovered that the roots of all resolvents (*résolvantes, réduites*) which he examined are rational functions of the roots of the respective equations. To study the properties of these functions he invented a *Calcul des Combinaisons*. The contemporary work of Vandermonde (1770) also foreshadowed the coming theory.
Ruffini (1799) attempted a proof of the impossibility of solving the quintic and higher equations. Ruffini distinguished what are now called intransitive and transitive, and imprimitive and primitive groups, and (1801) uses the group of an equation under the name *l'assieme delle permutazioni*. He also published a letter from Abbati to himself, in which the group idea is prominent.

Galois found that if r_1, r_2, ... r_n are the n roots of an equation, there is always a group of permutations of the r's such that every function of the roots invariable by the substitutions of the group is rationally known, and conversely, every rationally determinable function of the roots is invariant under the substitutions of the group.

In modern terms, the solvability of the Galois group attached to the equation determines the solvability of the equation with radicals. Galois also contributed to the theory of modular equations and to that of elliptic functions. His first publication on group theory was made at the age of eighteen (1829), but his contributions attracted little attention until the publication of his collected papers in 1846 (Liouville, Vol. XI). Galois is honored as the first mathematician linking group theory and field theory, with the theory that is now called Galois theory.

Groups similar to Galois groups are (today) called permutation groups, a concept investigated in particular by Cauchy. A number of important theorems in early group theory is due to Cauchy. Cayley's *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$ (1854) gives the first abstract definition of finite groups.

1.3. Groups related to geometry

Secondly, the systematic uses of groups in geometry, mainly in the guise of symmetry groups, were initiated by Klein's 1872. The study of what are now called Lie groups started systematically in 1884 with Sophus Lie, followed by work of Killing, Study, Schur, Maurer, and Cartan. The discontinuous (discrete group) theory was built up by Felix Klein, Lie, Poincaré, and Charles Émile Picard, in connection in particular with modular forms and monodromy.

1.4. Appearance of groups in number theory

The third root of group theory was number theory. Certain abelian group structures had been implicitly used in number-theoretical work by Gauss, and more explicitly by Kronecker. Early attempts to prove Fermat's last theorem were led to a climax by Kummer by introducing groups describing factorization into prime numbers.

1.5. Convergence

Group theory as an increasingly independent subject was popularized by Serret, who devoted section IV of his algebra to the theory; by Camille Jordan, whose *Traité des substitutions et des équations algébriques* (1870) is a classic; and to Eugen Netto (1882), whose *Theory of Substitutions and its Applications to Algebra* was translated into English by Cole (1892). Other group theorists of the nineteenth

century were Bertrand, Charles Hermite, Frobenius, Leopold Kronecker, and Émile Mathieu; as well as Burnside, Dickson, Hölder, Moore, Sylow, and Weber.

The convergence of the above three sources into a uniform theory started with Jordan's *Traité* and von Dyck (1882) who first defined a group in the full modern sense. The textbooks of Weber and Burnside helped establish group theory as a discipline. The abstract group formulation did not apply to a large portion of 19th century group theory, and an alternative formalism was given in terms of Lie algebras.

1.6. Late 19th century

Groups in the 1870-1900 period were described as the continuous groups of Lie, the discontinuous groups, finite groups of substitutions of roots (gradually being called permutations), and finite groups of linear substitutions (usually of finite fields). During the 1880-1920 period, groups described by presentations came into a life of their own through the work of Arthur Cayley, Walther von Dyck, Dehn, Nielsen, Schreier, and continued in the 1920-1940 period with the work of Coxeter, Magnus, and others to form the field of combinatorial group theory.

Finite groups in the 1870-1900 period saw such highlights as the Sylow theorems, Hölder's classification of groups of square-free order, and the early beginnings of the character theory of Frobenius. Already by 1860, the groups of automorphisms of the finite projective planes had been studied (by Mathieu), and in the 1870s Felix Klein's group-theoretic vision of geometry was being realized in his Erlangen program. The automorphism groups of higher dimensional projective spaces were studied by Jordan in his *Traité* and included composition series for most of the so called classical groups, though he avoided non-prime fields and omitted the unitary groups. The study was continued by Moore and Burnside, and brought into comprehensive textbook form by Leonard Dickson in 1901. The role of simple groups was emphasized by Jordan, and criteria for non-simplicity were developed by Hölder until he was able to classify the simple groups of order less than 200. The study was continued by F. N. Cole (up to 660) and Burnside (up to 1902), and finally in an early "millennium project", up to 2001 by Miller and Ling in 1900.

Continuous groups in the 1870-1900 period developed rapidly. Killing and Lie's foundational papers were published, Hilbert's theorem in invariant theory 1882, etc.

1.7. Early 20th century

In the period 1900-1940, infinite "discontinuous" (now called discrete groups) groups gained life of their own. Burnside's famous problem ushered in the study of arbitrary subgroups of finite dimensional linear groups over arbitrary fields, and indeed arbitrary groups. Fundamental groups and reflection groups encouraged the developments of J. A. Todd and Coxeter, such as the Todd–Coxeter algorithm in combinatorial group theory. Algebraic groups, defined as solutions of polynomial equations (rather than acting on them, as in the earlier century), benefited heavily from the continuous theory of Lie. Neumann and Neumann produced their study of varieties of groups, groups defined by group theoretic equations rather than polynomial ones.

Continuous groups also had explosive growth in the 1900-1940 period. Topological groups began to be studied as such. There were many great achievements in continuous groups: Cartan's classification of semisimple Lie algebras, Weyl's theory of representations of compact groups, Haar's work in the locally compact case.

Finite groups in the 1900-1940 grew immensely. This period witnessed the birth of character theory by Frobenius, Burnside, and Schur which helped answer many of the 19th century questions in permutation groups, and opened the way to entirely new techniques in abstract finite groups. This period saw the work of Hall: on a generalization of Sylow's theorem to arbitrary sets of primes which revolutionized the study of finite soluble groups, and on the power-commutator structure of p-groups, including the ideas of regular p-groups and isoclinism of groups, which revolutionized the study of p-groups and was the first major result in this area since Sylow. This period saw Zassenhaus's famous Schur-Zassenhaus theorem on the existence of complements to Hall's generalization of Sylow subgroups, as well as his progress on Frobenius groups, and a near classification of Zassenhaus groups.

1.8. Mid 20th century

Both depth, breadth and also the impact of group theory subsequently grew. The domain started branching out into areas such as algebraic groups, group extensions, and representation theory. Starting in the 1950s, in a huge collaborative effort, group theorists succeeded to classify all finite simple groups in 1982. Completing and simplifying the proof of the classification are areas of active research.

Anatoly Maltsev also made important contributions to group theory during this time; his early work was in logic in the 1930s, but in the 1940s he proved important embedding properties of semi groups into groups, studied the isomorphism problem of group rings, established the Malçev correspondence for polycyclic groups, and in the 1960s return to logic proving various theories within the study of groups to be undecidable. Earlier, Alfred Tarski proved elementary group theory undecidable.

1.9. Later 20th century

The period of 1960-1980 was one of excitement in many areas of group theory. In finite groups, there were many independent milestones. One had the discovery of 22 new sporadic groups, and the completion of the first generation of the classification of finite simple groups. One had the influential idea of the Carter subgroup, and the subsequent creation of formation theory and the theory of classes of groups. One had the remarkable extensions of Clifford theory by Green to the indecomposable modules of group algebras. During this era, the field of computational group theory became a recognized field of study, due in part to its tremendous success during the first generation classification.

In discrete groups, the geometric methods of Tits and the availability the surjectivity of Lang's map allowed a revolution in algebraic groups. The Burnside problem had tremendous progress, with better counterexamples constructed in the 60s and early 80s, but the finishing touches "for all but finitely many" were not completed until the 90s. The work on the Burnside problem increased interest in Lie algebras in exponent p, and the methods of Lazard began to see a wider impact, especially in the study of p-groups.

Continuous groups broadened considerably, with *p*-adic analytic questions becoming important. Many conjectures were made during this time, including the coclass conjectures.

1.10. Late 20th century

The last twenty years of the twentieth century enjoyed the successes of over one hundred years of study in group theory.
In finite groups, post classification results included the O'Nan–Scott theorem, the Aschbacher classification, the classification of multiply transitive finite groups, the determination of the maximal subgroups of the simple groups and the corresponding classifications of primitive groups. In finite geometry and combinatorics, many problems could now be settled. The modular representation theory entered a new era as the techniques of the classification was axiomatized, including fusion systems, Puig's theory of pairs and nilpotent blocks. The theory of finite soluble groups was likewise transformed by the influential book of Doerk–Hawkes which brought the theory of projectors and injectors to a wider audience.
In discrete groups, several areas of geometry came together to produce exciting new fields. Work on knot theory, orbifolds, hyperbolic manifolds, and groups acting on trees (the Bass–Serre theory), much enlivened the study of hyperbolic groups, automatic groups. Questions such as Thurston's 1982 geometrization conjecture, inspired entirely new techniques in geometric group theory and low dimensional topology, and were involved in the solution of one of the Millennium Prize Problems, the Poincaré conjecture.
Continuous groups saw the solution of the problem of hearing the shape of a drum in 1992 using symmetry groups of the laplacian operator. Continuous techniques were applied to many aspects of group theory using function spaces and quantum groups. Many 18th and 19th century problems are now revisited in this more general setting, and many questions in the theory of the representations of groups have answers.

1.11. Today

Group theory continues to be an intensely studied matter. Its importance to contemporary mathematics as a whole may be seen from the 2008 Abel Prize, awarded to John Griggs Thompson and Jacques Tits for their contributions to group theory.

2. Definitions and Properties

- Definition 1.
- Definition 2.
- Definition 3.
- Definition 4.
- Definition 5
- Definition 6
- Definition 7
- Definition 8
- Properties :
- Definition 9.
- Defination10.
- Theorem 1.
- Theorem 2.
- Theorem 3.
- Lemma 1.
- Theorem 4.
- Corollary 1.
- Proposition 1.
- Definition 11.
- Proposition 2.
- Proposition 3.
- Lemma 2.
- Lemma 3.
- Lemma 4.
- Defination 12.
- Theorem 5.
- Defination 13.
- Theorem 6.
- Theorem 7.
- Corollary 2.

2.1. Definition 1.

A group is a set *G* with an operation (called the *group product*) witch associates to each ordered pair (*a, b*) of elements of *G* an element *ab* of *G* in such a way that:

(1) For any element a, b, c ∈ *G*, (ab)c = a(bc);
(2) There is unique element e ∈ *G* such that *ea* = *a* = *ae* for any element a ∈ *G*
Thus (1) and (2) are the conditions for G to be a semi group with identity ;
(3) For each a ∈ *G* there is $a^{-1} \in G$ such that $a^{-1}a = e = a\,a^{-1}$.

2.2. Example 1.

The additive group of integers (Z, +)

(1) a + 0 = a = 0 + a for every a ∈ *Z*. thus (Z, +) has an identity element
(2) If a, b, c are integers, (a + b) + c = a + (b + c)
i.e. (Z, +) is a semi group
(3) If a ∈ *Z*, then – a in *Z* has the property a + (- a) = 0 = (- a) + a
i.e. –a is an inverse of a in (*Z*, +)
(*Z*, +) is a group

2.3. Example 2.

The set A = {-3, -2, -1, 0, 1, 2, 3} is not a group with respect to addition on *I* although 0 is the identity element, each element of A has an inverse, and addition is associative . The reason in, of course, that addition is not a binary operation on A, that is, the set A is not closed with respect to addition.

2.4. Definition 2.

A sub group of a group G is a nonempty subset H such that

(1) a, b ∈ *H* implies ab ∈ *H*
(2) a ∈ *H* implies $a^{-1} \in H$.

2.5. Example 3.

Is *Z* – {0} a subgroup of $(Q^*, \cdot)$, the multiplicative group of nonzero rational numbers?

1 is the identity. $3 \in Z - \{0\}$, but 3 has no inverse in $z - \{0\}$. There for $z - \{0\}$ is not a subgroup of $(Q^*, \cdot)$.

2.6. Example 4.

A proper subgroup of the multiplicative group $G = \{1, -1, i, -i\}$ is $H = \{1, -1\}$

2.7. Definition 3.
Let X denotes a finite set. A permutations of X is a one-to-one onto mapping from X to X.

The set A(x) of all permutation of X is a group in a natural way:
if $S,T \in A(x)$, then $ST \in A(x)$ is the composite mapping given by $(ST)(x)=S(T(x))$ for $x \in X$, the inverse of $S \in A(x)$ is just the inverse mapping S^{-1}, A sub group of A(x) will be called a group of permutations of X.

A permutation group is a special kind of transformation group.

If *G* is a group of permutations of the finite set X, then the action of *G on X* is given by $g * x = g(x)$. This action satisfies:

(1) $g*(h*x) = (gh)*x$ for all $g, h \in G$ and all $x \in X$;
(2) $e * x = x$ for all $x \in X$;
(3) If $g * x = x$ for all $x \in X$, then $g = e$.

Only conditions (1) and (2) are required for transformation groups in general.
An action of G on X witch satisfies (3) is called effective, or alternatively, G is said to act effectively. It's clearly that we could have made the definition:
a permutation group is a group which acts effectively on a finite set.

2.8. Example 5.
There are exactly n! permutation of on n-element set.

Proof

For an n-element set $S= \{x,\ldots\ldots,x_n\}$ we can construct a permutation action σ on S as follows.

Assign one of the n elements of S to $\sigma(x_1)$

Assign one of the n-1 elements of S-{σ (x_1)} to σ(x_2)

.

.

.

n assign the 1 remaining element to σ (x_n).

This method can generate (n (n-1) …… 1=n!) different permutations of S.

Furthermore it should be reasonably clear that these permutations are distinct, and that any permutation can be generated in this way and thus we know that there are exactly n! permutations of an n -elements set. □

2.9. Definition 4.

A group G acts on a set X (as a group of transformations) if to each pair (g, x) ∈ G x *X* there is associated an element g*x ∈ *X* in such a way that

g* (h * x) = (gh) * x for all g, h ∈ G and all x ∈ *X*;

e * x = x for all x ∈ *X*. (e is the identity element of G.)

We note that each g ∈ G determines a one-to-one correspondence g: *X* →*X*, given by g(x) = g * x, whose inverse is g^{-1}: *X* →*X*. (These one-to-one correspondences are sometimes called transformations of X.)
As examples of transformation groups we note that every group G acts on itself by the rule g * h = gh for all g, h ∈ G, and more generally, if H is a subgroup of G, then G acts on the left coset space X = G/H by the rule g*(g'H) = (gg')H.

2.10. Example 6.

To make G act on itself by *left multiplication*, we let X = G and g · x (for g ∈ G and x ∈ G) be the usual product of g and x. This example was used already in the proof of Cayley's theorem, and the definition of a group action is satisfied by the axioms for multiplication in *G*.
Note that right multiplication of G on itself, given by r_g(x) = xg for g and x in G, is

not an action since the order of composition gets reversed: r_{g1} **o** $r_{g2} = r_{g2g1}$. But if we set r_g (x) = xg^{-1} then we do get an action. This could be called the action by right-inverse multiplication (non-standard terminology).

2.11. Example 7.

To make G act on itself by *conjugation*, take X = G and let g · x = gxg^{-1}.
Here g∈G and x ∈ G. Since e · x = exe^{-1} = x and

$$\begin{aligned} g_1 \cdot (g_2 \cdot x) &= g_1 \cdot (g_2 x g_2^{-1}) \\ &= g_1 (g_2 x g_2^{-1}) g_1^{-1} \\ &= (g_1 g_2) x (g_1 g_2)^{-1} \\ &= g_1 g_2) \cdot x, \end{aligned}$$

conjugation is a group action.

Note: we use this application of this action to proof Sylow's theorem.

2.12. Definition 5

Orbits: Let G be a group acting on the set X. e define an equivalence relation ~ on X by setting x ~ y if and only if y = g * x for some g ∈ G. An equivalence class under ~ is called an *orbit*. The orbit of x ∈ X is simply the set :

$$G * x = \{y \in \boldsymbol{X} / \ \boldsymbol{y = g * x, for\ some\ g} \in \boldsymbol{G}\}$$

The quotient set X/~ is called *the set of orbits of X under the action of G*.

2.13. Definition 6

Let S be any subset of a group G, and let a be any element of G. The set

$$S^a = \{x \in G \mid axa^{-1} \in S\}$$

Is called the *Conjugate* of S by a. we note that $(S^a)^b = S^{ab}$ and that $S^e = S$.

2.14. Definition 7

Coxeter group:

Let M = $(m_{ij})_{1 \le i, j \le n}$ be a symmetric *n* x *n* matrix with entries from N ∪{∞} such that m_{ij} = 1 for all i ∈ [n] and m_{ij} > 1 whenever i ≠ j. The Coxeter group of type M is the group

$$W(M) = \langle \{(s_1, \ldots, s_n) \,|\{s_i s_j\}^{m_{ij}} = 1 \,/ i, j \in [n], m_{ij} < \infty\}\rangle$$

We often write S instead of $\{s_1, \ldots, s_n\}$ and, if no confusion is imminent, W instead of W(M). The pair (W, S) is called the *Coxeter system* of type M.

2.15. Definition 8
Topological group:

G is a topological space and group such that the group operation of product:

$G \times G \rightarrow G: (x, y) \mapsto xy$

And taking inverses $G \rightarrow G: x \mapsto x^{-1}$
are continues function here, $G \times G$ is viewed as a topological space by using the product topology.

2.16. Properties:
Let $a_1, a_2, \ldots a_k \in N_n$ be distinct integers we shall denote by $(a_1, \ldots a_k)$

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_k & \ldots i & \ldots \\ a_2 & a_3 & \ldots & a_1 & \ldots i & \ldots \end{pmatrix}$$

Which carries a_1 to a_2 , a_2 to a_3 , , , , , and a_k to a_i leaving all the other elements of N_i fixed. We call (a_1 , a_2 , , , , , a_n) a cyclic permutation of order K or a K-cycle, this notation is almost too efficient.
(a_1, a_2, , , , a_k) can denote an element of any one the groups S_n for which $n \geq k$.

A cycle permutation of order 2, (a_1 , a_2) simply interchanges a_1 and a_2 is called transposition . Two cyclic permutation (a_1 , a_2 , , , , a_k) and (b_1 , , , , , , b_t) are disjoint if they have no entries in common. Disjoint cyclic permutations commute that is (a_1, a_2 , , , , , , a_k) (b_1 , b_2 , , ,. b_t) = (b_1, b_2 , , , , b_t) (a_1 , a_2 , , , a_k) however the group S_n is not abelian for n >2 .

2.17. Definition 9
Group homomorphism
Let G and G_1 be groups and let $\varphi: G \rightarrow G_1$ be a mapping from G in to G_1.
If $\varphi(ab) = (\varphi a).(\varphi b)$ for all $ab \in G$, the φ called a group homomorphism

Example:
let G be any group. And let a be any element of G. Define $\varphi: Z \rightarrow G$ by $\varphi(n) = a^n$ for all n in Z this is a group homomorphism from Z to G.

Example 2
On homomorphism is very well known to the reader. It's the logarithm function $\log: R^+ \rightarrow R$
from the group R^+ of positive real numbers (under multiplication) into the group R of all real numbers (under addition). The homomorphism property of the logarithm function is the well known identity
$\log ab = \log a + \log b$ that holds for all $a, b \in R^+$.

2.18. Definition 10
Group isomorphism
Let G and G_1 be groups and let $\varphi: G \rightarrow G_1$ be a group isomorphism. Then φ is a group isomorphism if φ is bijection and we use the notation $G \cong G_1$.

2.19. Example 8.
If $|S| = n$ then perm $(S) \cong S_n$

Proof:

Since S has n elements .we can index them $S = \{ x_1, \ldots, x_n \}$

Then our isomorphism $\varphi: S_n \rightarrow$ perm (S) operates simply as $\varphi(\sigma)(x_i) = x_{\sigma}(i)$ which is clearly a homomorphism and clearly bijective .

2.20. Theorem 1. (Cayley)
Every finite group G *can be embedded in a symmetric group.*
Proof
To each $g \in G$, define the left multiplication function $\ell_g: G \rightarrow G$, where $\ell_g(x) = gx$ for $x \in G$. Each ℓ_g is a permutation of G as a set, with inverse ℓ_g^{-1}. So ℓ_g belongs to Sym (G). Since $\ell_{g_1} \; o \; \ell_{g_2} = \ell_{g_1 g_2}$ (that is, $g_1(g_2x) = (g_1g_2)x$ for all $x \in G$), associating g to ℓ_g gives a homomorphism of groups, $G \rightarrow$ Sym(G). This homomorphism is one-to-one since ℓ_g determines g (after all, $\ell_g(e) = g$). Therefore the correspondence $g \rightarrow \ell_g$ is an embedding of G as a subgroup of Sym (G).

□

Allowing an abstract group to behave like a group of permutations, as happened in the proof of Cayley's theorem, is a useful tool.

□

2.21. Theorem 2.

Let G *act on* X. *If* $x \in X$, $g \in G$, *and* $y = g \cdot x$, *then* $x = g^{-1} \cdot y$.

If $x \neq x'$ *then* $gx \neq gx'$.

Proof:

From $y = g \cdot x$ we get $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$. To show $x = x' \Rightarrow gx = gx'$, we show the contrapositive: if $gx = gx'$ then applying g^{-1} to both sides gives $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot x')$, so $(g^{-1}g) \cdot x = (g^{-1} g) \cdot x'$, so $x = x'$. □

2.22. Theorem 3.

Actions of the group G *on the set* X *are the same as group homomorphisms from* G *to* Sym(X), *the group of permutations of* X.

Proof.

Suppose we have an action of G on X. We view $g \cdot x$ as a function of x (with g fixed). That is, for each $g \in G$ we have a function π_g: X — X by $\pi_g(x) = g \cdot x$. The axiom $e \cdot x = x$ says π_e is the identity function on X. The axiom

$g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$

says π_{g_1} **o** $\pi_{g_2} = \pi_{g_1 g_2}$, so composition of functions on X corresponds to multiplication in G. Moreover, π_g is an invertible function since $\pi_{g^{-1}}$ is an inverse: the composite of π_g and $\pi_{g^{-1}}$ is π_e, which is the identity function on X. Therefore $\pi_g \in$ Sym(X) and $g \rightarrow \pi_g$ is a homomorphism G → Sym(X).

Conversely, suppose we have a homomorphism *f*: G → Sym(X). For each $g \in G$, we have a permutation f (g) on X, and $f(g_1 g_2) = f(g_1)$ **o** $f(g_2)$. Think about the effect of the permutation f (g) on $x \in X$ as an action: $g \cdot x = f(g)(x)$. This defines a group action of G on X, since the homomorphism properties of f yield the defining properties of a group action.

□

From this viewpoint, the set of $g \in G$ which acts trivially ($g \cdot x = x$ for all $x \in X$) is simply the kernel of the homomorphism $G \rightarrow Sym(X)$ associated to the action. Therefore those g which act trivially on X are said to lie in the *kernel* of the action.

2.23. Lemma 1.
Disjoint permutations commute.
Proof:
Let σ and τ be disjoint. If x is not in the support of σ or τ, then στx = xτσ x. If x is in the support of σ, then so is σ x, since σ x ≠ x implies σσx ≠ σ x;
then στx = σ x = τσ x, since σ and τ are disjoint. Similarly, if x is in the support of τ, then στx = τ x = τσ x.

□

2.24. Theorem 4.
Every permutation on n letters is the product of disjoint cyclic permutation in exactly one way (except for the order of the factors).
Proof:
Let $\pi \in S_n$. We shall donate by H the cyclic subgroup of S_n generated by π. H acts on the set $N_n = \{1, 2, 3, \ldots, n\}$ dividing it into disjoint orbits, $X_1, X_2, \ldots, X_r$. In other words, tow elements I and j of N_n belong to the same orbit if and only if $j=\pi^k(i)$ for some power π^k of π. In any orbit X_k we may list elements in order $a_{k1}, a_{k2}, \ldots, a_{ks_k}$,

So that $a_{k\,i+1} = \pi(a_{ki})$ and $a_{k1} = \pi a_{ks_k}$. We let a_k denote the cyclic permutation $(a_{k1}, a_{k2}, \ldots, a_{ks_k})$. We claim that $\pi = a_1, a_2, \ldots, a_r$.

To prove this we need to only show that π and $a_1, a_2, \ldots, a_r$ have the same effect on every element $x \in N_n$. If $x \in X_k$, then $a_i(x) = x$ for $i \neq k$ and $a_k(x) = \pi(x)$. Therefore, $(a_1, a_2, \ldots, a_r)(x) = a_k(x) = \pi(x)$.
Finally, the expression $\pi = a_1, a_2, \ldots, a_r$ is clearly unique except for the order of the $a_i's$.
Note that we may include or exclude factors of the form $a_k = (m)$ since every 1-cyclic is the identity.

in practice it is a simple matter to express a permutation as the product of disjoint cyclic permutation. For example $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 1 & 7 & 3 & 2 & 4 \end{pmatrix} = (1,5,3)(2,6)(4,7).$

2.25. Corollary 1.

If $\alpha_1, \alpha_2, \ldots, \alpha_s \in S_n$ are disjoint cyclic permutations then the order of $\alpha_1, \alpha_2, \ldots, \alpha_s$ is the least common multiple of the orders of factors ;

Proof:

Let k_i denote the order of α_i, and let k be the least common multiple of the k_i .

Since the α_i's commute we have $(\alpha_1, \alpha_2, \ldots, \alpha_s)^k = \alpha_1^k, \alpha_2^k, \ldots, \alpha_s^k = e$ so that $o(, \alpha_2, \ldots, \alpha_s)$ = divides k since the α_i, are disjoint it follows that $(\alpha_1, \alpha_2, \ldots, \alpha_s)^i = e$ implies $\alpha_i^i = e$ for each i, then k_i/L for each i , and thus k/L particular k/ $o(\alpha_1, \alpha_2, \ldots, \alpha_s)$ and therefore $o(\alpha_1, \alpha_2, \ldots, \alpha_s) = k$

□

2.26. Proposition 1.

Every permutation is a product of transpositions.

Proof:

By induction on n. Proposition 1 is vacuous if n = 1. Let n > 1 and $\sigma \in S_n$.

If $\sigma n = n$, then, by the induction hypothesis, the restriction of σ to {1, 2, . . ., n −1} is a product of transpositions; therefore σ is a product of transpositions.

If $\sigma n = j \neq n$, then (n j) σ n = n , (n j) σ is a product of transpositions

(n j) $\sigma = \tau_1 \tau_2 \ldots \tau_r$, and so is $\sigma = (n\ j)\ \tau_1 \tau_2 \ldots \tau_r$. \

Example:- write $= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 1 & 3 & 5 & 7 & 9 & 11 & 13 \end{pmatrix}$ as the product of disjoint cycles Solution :

1 α = 2 , 2 α = 4, 4 α = 8, 8 α = 1, 3 α = 6, 6 α = 12, 12 α = 9, 9 α = 3.

5 α = 10, 10 α = 5. 7 α = 14, 14 α = 13, 13 α = 11, 11 α = 7. Hence

α = (1,2,4,8)(3,6,12,9)(5,10)(7,14,13,11)

□

Even and odd permutations :

We are interested in special subgroup of S_n the alternating group of degree n. usually denoted by A_n. This sub group A_n is obtained from S_n by singling out certain elements.

To begin with consider S_3 let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Then

$$\frac{\sigma(2)-\sigma(1)}{2-1} * \frac{\sigma(3)-\sigma(1)}{3-1} * \frac{\sigma(3)-\sigma(2)}{3-2} = \frac{3-2}{2-1} * \frac{1-2}{3-1} * \frac{1-3}{3-2} = 1$$

If $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ then

$$\frac{\tau(2)-\tau(1)}{2-1} * \frac{\tau(3)-\tau(1)}{3-1} * \frac{\tau(3)-\tau(2)}{3-2} = \frac{2-3}{2-1} * \frac{1-3}{3-1} * \frac{1-2}{3-2} = -1$$

We say σ is even and τ is odd

More generally, let us call $\sigma \in S_n$ even (or an even permutation) if

$$\frac{\sigma(2)-\sigma(1)}{2-1} * \frac{\sigma(3)-\sigma(1)}{3-1} * \frac{\sigma(3)-\sigma(2)}{3-2} *,,,* \frac{\sigma(n)-\sigma(1)}{n-1} * \frac{\sigma(n)-\sigma(2)}{n-2} * \frac{\sigma(n)-\sigma(n-1)}{n-(n-1)} = 1$$

On the other hand, we call $\sigma \in S_n$ odd (or an odd permutation) if

$$\frac{\sigma(2)-\sigma(1)}{2-1} * \frac{\sigma(3)-\sigma(1)}{3-1} * \frac{\sigma(3)-\sigma(2)}{3-2} *,,,* \frac{\sigma(n)-\sigma(1)}{n-1} * \frac{\sigma(n)-\sigma(2)}{n-2} * \frac{\sigma(n)-\sigma(n-1)}{n-(n-1)} = -1$$

The definition of even or odd is written more briefly as

σ is even if

$$\prod_{i<k} \frac{\sigma(k)-\sigma(i)}{k-i} = 1$$

σ is odd if

$$\prod_{i<k} \frac{\sigma(k)-\sigma(i)}{k-i} = -1$$

- We shell show that an element is in S_n is ether even or odd, i.e.
- $\prod_{i<k} \frac{\sigma k-\sigma i}{k-i} = \pm 1$

It follows the set of even permutations is a subgroup of S_n called the alternating groups on n letters and customarily denoted A_n. We may regard sgn:$S_n \rightarrow K_2$ as homomorphism from S_n to $K_2 = \{\pm 1\}$, the group of square roots. This shows that A_n is normal subgroup of S_n and the quotient group S'_n/A_n is isomorphic to $'K_2$

2.27. Definition 11.

$$\text{Sgn } \sigma = \prod_{i<k} \frac{\sigma(k) - \sigma(i)}{k - i}$$

2.28. Proposition 2.

The function sgn: $S_n \rightarrow (+1, -1)$ satisfies sgn $(\tau\sigma)$ = sgn(τ) sgn(σ) $(\tau, \sigma \in S_n)$

Proof:

$$\text{Sgn } \tau\sigma = \prod_{i<k} \frac{\tau\sigma(k) - \tau\sigma(i)}{k - i}$$

$$= \prod_{i<k} \frac{\tau(\sigma(k)) - \tau(\sigma(i))}{k - i} * \frac{\sigma(k) - \sigma(i)}{\sigma(k) - \sigma(i)}$$

$$= \prod_{i<k} \frac{\tau(\sigma(k)) - \tau(\sigma(i))}{\sigma(k) - \sigma(i)} * \prod_{i<k} \frac{\sigma(k) - \sigma(i)}{k - i}$$

$$\text{Sgn } \sigma$$

Since

$$\prod_{i<k} \frac{\sigma(k) - \sigma(i)}{k - i} = \text{Sgn } \sigma \qquad (1)$$

σ: {1, …, n}→{1, …, n}

$T = \{i, j\} | \{i < j\}$ Indices in the product

$\bar{\sigma}: T \to T$

$$\bar{\sigma}(i,j) = \begin{cases} (\sigma(i), & \sigma(j)) & \sigma(i) < \sigma(j) \\ (\sigma(j), & \sigma(i)) & \sigma(j) < \sigma(i) \end{cases}$$

By Lemma: $\bar{\sigma}$ is a bijection of T

$$\prod_{i<k} \frac{\tau(\sigma(k)) - \tau(\sigma(i))}{\sigma(k) - \sigma(i)} = \prod_{i<k} \frac{\tau(k) - \tau(i)}{k - i} = \text{sgn } \tau. \quad (2)$$

$$(\sigma(k), \sigma(i))$$

From (1) and (2) we get sgn (τσ) = sgn(τ) sgn(σ).

□

2.29. Proposition 3.

A_n is generated by all 3-cycles.

Proof:

First, (a b c) = (a b)(c b) for all distinct a, b, c , so that 3-cycles are even and A_n contains all 3-cycles. Now we show that every even permutation is a product of 3-cycles. It is enough to show that every product (a b)(c d) of two transpositions is a product of 3-cycles.

Let a ≠ b, c ≠ d. If {a, b} = {c, d}, then (a b)(c d) = 1. If {a, b} ∩ {c, d} has just one element, then we may assume that b = d, a ≠ c, and then

(a b)(c d) = (a b)(c b) = (a b c).

If {a, b} ∩ {c, d} = Ø, then (a b)(c d) = (a b)(c b)(b c)(d c) = (a b c)(b c d).

□

2.30. Lemma 2.

In S_n (n≥2) ,the number of even permutation equals The number of odd permutation, and equals $n!/2$.

Proof:

$A_n \equiv$ the Set of even permutation.
$B_n \equiv$ The Set of odd permutation.

We define a map $\varphi_i : A_n \rightarrow B_n$ by

$\varphi(\sigma) = \sigma(\mu)$ where $N(1,2) \forall \sigma \in A_n$

if $\varphi(\sigma) = \varphi(\rho)$

$\Rightarrow \sigma \mu = \rho \mu$

$\Rightarrow (\sigma\mu)\mu = (\rho\mu)\mu$

$\Rightarrow \sigma\mu^2 = \rho\mu^2$

$\Rightarrow \sigma\rho_0 = \rho\rho_0$

$\Rightarrow \sigma = \rho$

$\Rightarrow \varphi = 1\text{-}1$

For any $\rho \in B_n$, there exist :

$\rho\mu \in A_n$

$\varphi(\rho\mu) = (\rho\mu)\mu$

$= \rho\mu^2$

$= \rho\rho_0$

ρ^2

φ is onto

S_n is finite

$|A_n| = |B_n|$.

□

2.31. Lemma 3.

The product of:

two even permutations is even

two odd permutations is even

an odd permutation and an even permutation is odd

An even permutation and an odd permutation is odd.

2.32. Lemma 4.

$A_n \subseteq S_n$, $(n \geq 2)$,the subset of even permutations is a subgroup.

$A_n \neq \varphi$ (since $\rho_o \in A_n$),

let $\rho, \sigma \in A_n$

$\rho = \mu'_1, \mu'_2, \ldots, \mu'_{2r}$, $\sigma = \mu_1, \mu_2, \ldots, \mu_{2k}$

$\rho\,\sigma^{-1} = (\mu'_1, \mu'_2, \ldots, \mu'_{2r})*(\mu_1, \mu_2, \ldots, \mu_{2k})^{-1}$

$= (\mu'_1, \mu'_2, \ldots, \mu'_{2r})*(\mu^{-1}_{2k}, \ldots, \mu^{-1}_2, \mu^{-1}_1)$

$= \mu'_1\,\mu'_2, \ldots, \mu'_{2r}\,\mu_{2k}, \ldots, \mu_2\mu_1$

$\rho\,\sigma^{-1}$ is a product of even number of transposition

$\rho\,\sigma^{-1} \in A_n$

$\Rightarrow A_n \subseteq S_n$

□

2.33. Definition 12
Normal subgroup:

A subgroup, N, of a group, G, is called normal subgroup if it is invariant under conjugation that is for each element n in N each g in G the element gng^{-1} is still in N. we write $N \triangle G \Leftrightarrow \forall\, n \in N, \forall\, g \in G, gng^{-1} \in N$.

Simple group:

A simple group is a nontrivial group whose only normal subgroups are the trivial group and the group itself.

2.34. Theorem 5.
The alternating group A_n is simple except for $n = 4$

Proof :
Recall that a group is simple of it has only itself and the trivial group as normal subgroups . For $n < 4$ the order of an is either 1 or 3, and A_n is obviously simple. The major part of the proof is the case $n > 4$.

Let N be a nontrivial normal subgroup of A_n for $n > 4$. We must show that $N = A_n$. The first step is to see that N contains a 3-cycle.

Let $\alpha \neq e$ be an element of N which leaves fixed as many element of N_n as possible. A_s guaranteed by Theorem 4, let

$$\alpha = \alpha_1\alpha_2 \ldots \alpha_s$$

Where the α_1 are disjoint cycles, which we may assume are given in order of decreasing length. Renumbering if necessary, we may assume that

$$\alpha_1 = (1,2,\ldots..k)$$

and, when s > 1, that

$$\alpha_2 = (k + 1, k + 2,\ldots..,L) .$$

we distinguish several cases .

Case 1. α moves each of the numbers 1, 2, 3, 4, 5. (This occurs when s > 2, when s = 2 and $\alpha = (1, 2,\ldots..k) (k + 1 , k + 2,\ldots L)$ with L > 4, or when s = 1 and $\alpha = \alpha_1 = (1, 2,\ldots..k)$ for k > 4) Setting $\beta = (3, 4 , 5)$, the element $\beta^{-1}\alpha^{-1}\beta$ belongs to the normal subgroup N, and thus $\beta^{-1}\alpha^{-1}\beta\alpha \in N$. How- ever it is easily checked that permeation $\beta^{-1}\alpha^{-1}\beta\alpha$ leaves the number 1 fixed in addition to leaving fixed all the elements fixed by α This contradicts the choice of α, and case l is impossible .

Case2. α moves the numbers 1,2,3,4 and no others (This occurs only when $\alpha = (1,2) (3,4)$, since (1,2,3,4) is an odd permutation) Again we set $\beta = (3,4,5)$ and argue that the element $\beta^{-1}\alpha^{-1}\beta\alpha$ belongs to N . However,

Direct computation shows that $\beta^{-1}\alpha^{-1}\beta\alpha = (3, 4, 5) = \beta$ Thus, $\beta \in N$ and β moves fewer elements than α . This contradiction eliminates case 2.

Case 3. Moves the numbers 1,2,3 and no others. (This occurs only when α = (1,2, 3) there are no other cases now that the first and second are eliminated. Thus, we have shown that N contains a 3-cycle, which we may assume to be (1, 2, 3).

It remains to show that *N* contains every 3-cycle. Choose an even permutation.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots \\ i & j & k & \ldots \end{pmatrix};$$

Then, $\sigma(1,2,3)\sigma^{-1} = (i,j,k)$ belongs to the normal subgroup N. Varying i, j, and k, we obtain all 3-cycles . Thus, *N* contains every 3-cycle, and in view of proposition 3, $N = A_n$, and we are finished.

2.35. Definition 13
Solvable Group:

A group G witch have subgroups G_0, G_1, . . ., G_n where $G_0 = G$, G_n = the identity element alone, and each G_i is a normal subgroup of G_{i-1} witch the quotient group G_{i-1}/G_i abelian.

2.36. Theorem 6.
For n > 4, *the symmetric group S_n is not solvable*.
Proof:
Since the groups $K_2 \approx S_n/A_n$ and A_n (for n > 4) are simple, the normal series

$$\{e\} \subset A_n \subset S_n$$

Is a composition series for S When n > 4. However, A_n is not abelian for n > 3. (For example (1, 2, 3)(2, 3, 4) = (1, 2)(3, 4) while (2, 3, 4)(1, 2, 3) = (1, 3)(2, 4).) Consequently, A_n is not cyclic for n > 3. As a result S_n is not solvable for n > 4.

□

2.37. Theorem 7.
If H is a subgroup of finite group G and H contains no nontrivial normal subgroup of G, then G is isomorphic to a subgroup of sym(G/H), the group of permutations of the set G/H.
Proof:
Define a homomorphism ϕ:G→ sym(G/H) by setting $\Phi(g)(xH) = (gx)H$ all x ∈ G. Ker Φ is a normal subgroup of G. An element g belongs to Ker Φ if and only if $(gx)H = xH$ for all x ∈ G, or what is the same thing, $x^{-1}gx \in H$ for all x ∈ G. In other words, Ker $\Phi \subset H$ and by hypothesis Ker Φ must be trivial. It follows that $G \approx$ Im Φ.

2.38. Corollary2.
For n >4 A_n is the only proper subgroup of index less the n in S_n .

Proof:

If fllows that for n>4, A_n Is the only proper, nontrivial, normal subgroup of S_n. Supose that H is subgroup of S_n and $[S_n:H]<n$. If $[S_n:H]= 2$, then H is normal and $H=A_n$. On the other hand $[S_n:H] >2$ implies $A_n \not\subset H$. Thus, the hypothesis of the theorem is satisfied, and S_n is isometric to subgroup of $sym(S_n /H)$. However,

$$o(A(S_n /H)) = [S_n : H]! < n! = o(S_n),$$

Which is contradiction.

3. Applications and Problems

- Problem 1.
- Problem 2.
- Problem 3.
- Problem 4.
- Problem 5.
- Problem 6.
- Problem7.
- Application 1.
- Problem8.
- Application 2.
- Problem 9.

•

3.1. Problem 1.

A = {1, 2, 3} find the elements of S_3 and show that (S_3, 0) is a group but not abelian.

Solution:

elements of S_3 i.e. $|S_3| = 3! = 6$

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

We must compute the products. A_S an example we calculate $\sigma_1\tau_1$

$$\tau_1\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ \tau(k_1) & 2\tau_1(\sigma_1) & 3\tau_1(\sigma_1) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \tau_1(2) & \tau_1(3) & \tau_1(1) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$= \tau_2$

The multiplication table for S_3 is

	i	σ_1	σ_2	τ_1	τ_2	τ_3
i	i	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	i	τ_2	τ_3	τ_1
σ_2	σ_2	i	σ_1	τ_3	τ_1	τ_2
τ_1	τ_1	τ_3	τ_2	i	σ_2	σ_1
τ_2	τ_2	τ_1	τ_3	σ_1	i	σ_2
τ_3	τ_3	τ_2	τ_1	σ_2	σ_2	i

Note that $\sigma_1\tau_1 = \tau_2$ and $\tau_1\sigma_1 = \tau_3$, so that $\sigma_1\tau_1 \neq \tau_1\sigma_1$

Hence S_3 is not commutative .

3.2Problem2 :- Determine whether (a1,…am), so (a1,…am) is the product of m – 1 transpositions .

$(a_1,\ldots,a_m) = (a_1,a_2)(a_1,a_3) \ldots (a_1,a_m)$, so $(a_1,\ldots a_m)$ is the product of m – 1 transpositions .

Thus $(a_1,\ldots a_m)$ is even or odd according as m is odd or even.

3.3. Problem 3.
Decompose

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 7 \end{pmatrix} \in S_5$$

into a product of transpositions.
Solution:
We have:

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

Some alternative decomposition are:

$$\sigma = (2\ 1)(2\ 4)(2\ 5) = (5\ 2)(5\ 1)(5\ 4)$$

□

3.4. Problem 4.
In the group S_n the cyclic permutation $(i_1\ i_2 \ldots i_r)$ of length r has order:

$$|(i_1 i_2 \ldots i_r)| = r$$

Solution:
Setting $\sigma = (i_1\ i_2 \ldots i_r)$, we have

$$\sigma^k(1) = \begin{cases} i_{k+1} & \text{if } k < r, \\ i_1 & \text{if } k = r, \end{cases}$$

hence $|\sigma| \leq r$. As $i_k \neq 1$ for $1 < k \leq r$, r is the smallest such power which is l, hence $|\sigma| = r$.

□

3.5. Problem 5.

Calculate $\alpha\beta$ $\beta\alpha$, α^{-1}, β^{-1}, $(\alpha\beta)^{-1}$ and $(\beta\alpha)^{-1}$.

If $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 5 & 4 & 1 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 6 & 2 & 4 \end{pmatrix}$

Solution:

$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 6 & 1 \end{pmatrix}$, $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 1 & 3 & 5 \end{pmatrix}$

To find α^{-1} we note that x $(\alpha\alpha^{-1})$ = x and hence α^{-1} must carry x_α to x, now we determine which x is taken into 1, $6\alpha = 1$

So we must have $1\alpha^{-1} = 6$ next since $1\alpha = 2$, $2\alpha^{-1} = 1$ proceeding in this way we obtain

$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix}$

An easy method of calculating the answer mechanically follows take

$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 5 & 4 & 1 \end{pmatrix}$

Interchange the rows

$\begin{pmatrix} 2 & 3 & 6 & 5 & 4 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$

Rearrange the columns so that the top row reads 1 2 3 4 5 6.

$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix}$

This method is conceptually the same as the first. To find β^{-1} integrating the rows to obtain

$$\begin{pmatrix} 1 & 3 & 5 & 6 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

And $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 3 & 4 \end{pmatrix}$, $(\alpha\beta)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 3 & 2 & 5 \end{pmatrix}$

$(\beta\alpha)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 3 & 6 & 2 \end{pmatrix}$

3.6. Problem 6.

Verify that $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ where

$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$

Solution:

$(\alpha\beta)\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$

$\alpha(\beta\gamma) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$

3.7. Problem 7.

Is the subset R = $\{i, \sigma_1, \sigma_2\}$ a subgroup of S_3.

$R \neq \emptyset$ from application 1of S_3 the product of any two elements in R is again in R, since $\sigma^{-1}{}_1 = \sigma_2$ and $\sigma^{-1}{}_2 = \sigma_1$ it follow that (R is subgroup $\Leftrightarrow \forall$ x, y $\in$ R, $xy^{-1} \in$ R) for any x, y $\in$ R. Hence R is subgroup of S_3

3.8. Application 1.

S_4 = { (1) , (12), (13), (14), (23), (24), (34), α = (123) , α^2 = (132), β= (124), β^2 = (142), γ = (134), γ^2 = (143), δ = (234), δ^2 = (243),

ρ = (1234), ρ^2 = (13) (24), ρ^3 = (1432), σ = (1243), σ^2 = (14)(23), σ^3 = (1342), τ= (1324), τ^2 = (12) (34) , τ^3 = (1423) }.

The subgroup of S_4 (i) {(1) , (1 2) } (ii) { (1) , α , α^2 } (iii) = { (1) , (1 2) , (3 4) , (1 2) (3 4) } and (iv) A_4 = { (1) , α , α^2 , β , β^2 γ ,γ^2 , δ , δ^2 , σ2 , ρ_2 , τ^2 } are examples of permutation groups on 4 symbols. A_4 consist of all even permutation in S_4 and is known as the *alternating group* on 4 symbols. A_4

The sub set {u =(1), ρ, ρ^2, ρ^3, σ^2, τ^2, b= (13), e = (24)} of S_4 is a group (see the operation tale below), called the *octic group of a square* or the *general dihedral group* D_4.

We shall now show how this permutation group may be obtained using properties of symmetry of a square.

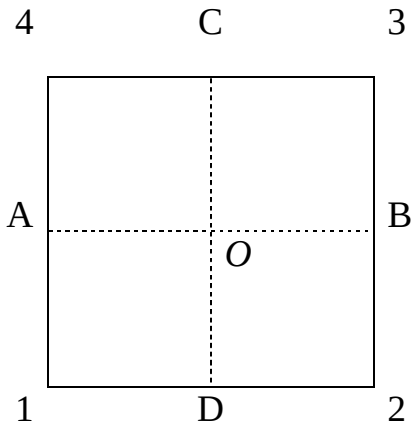

Figure 1

Consider the square (figure 1) with vertices denoted by 1, 2, 3, 4; locate its center *O* the bisectors A*O*B and C*O*D of its parallel sides, and the diagonals 1*O*3 and 2*O*4. We shall be concerned with all rigid motions (rotations in the plane about *O* and in space about bisectors and diagonals) such that the square will look the same after the motion as before.

Denote by ρ the counterclockwise rotation of the square about *O* through 90º. Its effect is to carry 1 into 2. 2 into 3, 2 into 4, and 4 into 1; thus, ρ = (1234).
Now ρ^2 = ρ $^o\rho$ = (13) (24) is a rotation about *O* of 180º ρ^3 = (1432) is a rotation of

270º and $\rho^4 = (1) = u$ is rotation about O of 360º or 0º. The rotation of 180º about bisectors AOB and COD give rise respectively to $\sigma^2 = (14)\,(23)$ and $\tau^2 = (12)\,(34)$ while the rotation through 180º about the diagonals 1O3 and 2O4 give rise to $e = (24)$ and $b = (13)$.

The operation table for this group is

	u	ρ	ρ^2	ρ^3	σ^2	τ^2	b	e
u	u	ρ	ρ^2	ρ^3	σ^2	τ^2	b	e
ρ	ρ	ρ^2	ρ^3	u	b	e	τ^2	σ^2
ρ^2	ρ^2	ρ^3	u	ρ	τ^2	σ^2	e	b
ρ^3	ρ^3	u	ρ	ρ^2	e	b	σ^2	τ^2
σ^2	σ^2	e	τ^2	b	u	ρ^2	ρ^3	ρ
τ^2	τ^2	b	σ^2	e	ρ^2	u	ρ	ρ^3
b	b	σ^2	e	τ^2	ρ	ρ^3	u	ρ^2
e	e	τ^2	b	σ^2	ρ^3	ρ	ρ^2	u

3.9. Problem 8.

Write out a multiplication table for (i) A_1, (ii) A_2, (iii) A_3,

Solution:

There is only one element in S_1, namely $i = \binom{1}{1}$, and it's an even permutation. Hence a multiplication table A_1 is $\begin{array}{c|c} & i \\ \hline i & \boxed{i} \end{array}$. Notec A_1 is the same as S_1.

$S_2 = \left\{\binom{1\ \ 2}{1\ \ 2}, \binom{1\ \ 2}{2\ \ 1}\right\}$. $\binom{1\ \ 2}{1\ \ 2}$ is an even permutation and $\binom{1\ \ 2}{2\ \ 1}$ is an odd permutation there for $A_2 = \left\{\binom{1\ \ 2}{1\ \ 2}\right\}$ and $\begin{array}{c|c} & i \\ \hline i & \boxed{i} \end{array}$ where

$i = \binom{1\ \ 2}{1\ \ 2}$ is a multiplication table for A_2

S_3 contains six elements. The elements i, σ_1 and σ_2 are the even permutations, and a multiplication table for A_3 is

	i	σ_1	σ_2
i	i	σ_1	σ_2
σ_1	σ_1	σ_2	i
σ_2	σ_2	i	σ_1

3.9. Application 2.

S_n acts on X = {1, 2,..., n} in the usual way. Here $\pi_\sigma(i) = \sigma(i)$ in the usual notation.

3.11. Problem 9.

Prove $A_n = S_n$ implies n = 1.

Solution:

If n>1, S_n must contain a permutation witch interchange 1 and 2 and leaves everything else fixed, i.e. 1r=2, 2r=1 and $ir = i$ (i= 3, . . ., n). $r \notin A_n$, since r is an

odd permutation, and therefore $A_n \neq S_n$. by problem 6 (i), $A_1 = S_1$. Hence $A_n = S_n$ implies n = 1.

3.12. Problem 10.

Definition derived group :

The commuter subgroup (also called a derived group) of group G is the subgroup generated by the commentators of its elements, and is commonly denoted $G^{\backslash}$ or [G, G]. it is the smallest normal subgroup of G such that $G/G^{\backslash}$ is abilian.

Prove that if $G = A_n$, $n \geq 5$, then the derived group $G^{\backslash}$ of G is a G.

Solution:

We know that $G^{\backslash} \triangle G$. Hence $G^{\backslash} = G$ or else $G^{\backslash} = \{i\}$ as a G is simple by theorem.

If $G^{\backslash} = \{i\}$ is abilian. But A_n is not abilian for $n \geq 5$ For example

$$(1,2,3)(3,4,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \cdots & n \\ 2 & 4 & 1 & 5 & 3 & 6 & \cdots & n \end{pmatrix}$$

But

$$(3,4,5)(1,2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \cdots & n \\ 2 & 3 & 4 & 5 & 1 & 6 & \cdots & n \end{pmatrix}$$

Therefore $G^{\backslash} = G$.

References

1. Israel Kleiner "A history of abstract algebra", Springer, 2007
2. Morris Kline "Mathematical thought from ancient Io modem limes. 1990, Volume 3"
3. G. A. Miller "A proof of Sylow's theorem"
4. M. Suzuki: Group Theory I, Springer-Verlag (Berlin, 1982) [English translation of Gunron, lwanami Sholen (Tokyo, 1977)]
5. V.Pannone: A rounded proof of Sylows Theorem, seminar notes typewritten hy P. Sanlaniello (2000).
6. R. Gow, Sylow's proof of SyIoWs theorem, Irish Math. Soc. Hull. 1994.
7. W. C Walerhouse. The early proofs of Sylow's theorem. Arch. Hist. Hcl Sci-21. 1979/80.
8. Helmut Wieland and Bertam Huppert, Arithmetic and normal structure of finite groups, Proc. Sympos . Pure Math., Vol . VI, Year 1962, Page 17-38.
9. Ronald M-Solomon, A brief history of the classification of the finite simple groups. Bulletin of the American Mathematical Society. Volume 38, Year 2001.
10. Daniel Gorenstein, Finite Groups, American Mathematical Society,
11. Walter fate and John J. Thompson, Solvability of groups of odd order, Pacific journals of mathematics, Volume 13, Year 1963.
12. Finite simple groups, edited by Graham Hangman and Marten B. Paul Academic Press.
13. A. Baker, Algebra & Number Theory, 2003.
14. Allan Clark, Elements of Abstract Algebra,1984.
15. BENJAMIN BAUMSLAG, Ph.D. and BRUCE CHANDLER, Ph.D. SCHAUM'S OUTLINE OF THEORY AND PROBLEMS OF GROUP THEORY, 1968.
1. History of group theory URL http://en.wikipedia.org/wiki/History_of_group_theory.