

The Genesis Of The Concept
Of Group Presentation
As Seen In Papers
Of Cayley, Kronecker and Dyck

by

Gilmar Rodríguez-Pierluissi

B.S., Kansas State University, 1983

A THESIS

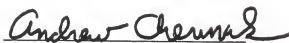
submitted in partial fulfillment of the
requirements for the degree

MASTER OF SCIENCE

College of Arts and Sciences
Department of Mathematics
Kansas State University
Manhattan, KS

1988

Approved by:



Major Professor

LD
21608
.T4
MATH
1988
R63
C. 2

A11208 231795

ACKNOWLEDGEMENTS:

I want to express my deep gratitude to my family in Jayuya and Ponce, and above all, to my wife Liliam, for their constant spiritual and material support during these critical years. I am also deeply indebted to the following people:

- 1) Dr. Alberto Delgado for suggesting the central theme for this project and for his translations of Kronecker's and Dyck's papers from German to English.
- 2) Dr. Robert Burckel for his translation of *Auseinandersetzung einiger Eigenschaften der Klassenanzahl idealer komplexer zahlen*.
- 3) Dr. David Miller for providing the computer programs that made possible the diagrams on pages 26 and 27 illustrating the free group \mathcal{F} .
- 4) Dr. Willard Parker and Dr. Todd Cochrane for their valuable corrections and suggestions on how to improve the content of this project.
- 5) Miss Reta McDermott for making available her magnificent secretarial skills in the typing of this thesis.

Finally I want to thank my advisor Dr. Andrew Chermak for his strong guidance in the completion of this project, his friendship and great patience.

Thank you all!

INTRODUCTION:

In "The History of Combinatorial Group Theory: A Case Study in the History of Ideas", Chandler and Magnus; [5, p. 5], say: "The definition of a group G by a presentation, that is, by a system of generators and defining relations, is a particular aspect of the abstract definition of a group". Hence, in studying the Genesis of the Concept of Group Presentation as seen in the papers of Cayley, Kronecker and Dyck, we are focusing on one particular aspect of the genesis of the abstract group concept.

Chapter I deals with Cayley's 1854 paper entitled *On the Theory of Groups, as depending on the Symbolic Equation $\theta^n = 1$* . Here we find Cayley's definition of a group which we recognize as a monoid using modern terminology. The concept of a group multiplication table is discussed, which we recognize as a basic first step to present a group.

Chapter II deals with Cayley's 1878 paper *The Theory of Groups*. Here, Cayley recognizes the generality of the group concept by identifying "substitutions" as representative of a more general variety of "functional symbols" which he already has identified as a group. He also shows some examples of groups found in other areas of mathematics. We also find "Cayley's Dictum" where Cayley attempts to put in a nutshell, what he considers to be the essence of a group, that is "the laws of combination of its symbols". As we shall see this notion described in the Dictum is not well defined.

Cayley attempts to classify all distinct groups of a given order n . He makes a mistake for the case $n = 6$ due to the ambiguity found in his Dictum. He realizes that this problem is identical to that of constructing all permutation groups of order n . He states and proves his famous theorem that every finite group can be represented as a group of permutations. Here we find another way to present a group and hence another step in the genesis of this concept.

Chapter III deals with Kronecker's 1870 paper entitled *Auseinandersetzung einiger Eigenschaften der Klassenanzahl idealer complexer zahlen*. Here he introduces the notion of an abstract finite abelian group. He states and proves the "existence part" of the Fundamental Theorem of Finite Abelian Groups. Every finite abelian group has a presentation of the form described in this theorem. He anticipates Cayley, since this theorem defines abelian groups in terms of simple and specific "laws of combinations of its symbols".

Chapter IV gives some general background needed to unravel the ideas found in Dyck's 1882 paper, entitled *Gruppentheoretische Studien*. Chapter IV is divided into four sections. Section I deals basically with the effects that the mapping $(z)T = w + \frac{r^2}{\bar{z}-\bar{w}}$ has on a circle C of radius r and center w . We also explore the effects that this mapping has on a circle D orthogonal to C . Section II outlines a geometric construction of a group \mathcal{F} whose elements are forms by even numbers of compositions of mappings of the form described in Section I. Section III establishes the group properties of \mathcal{F} and its relation with the group \mathcal{M} of Möbius Transformations. Section IV establishes the fact that \mathcal{F} is a free group.

In particular Chapter IV fills in the details left out by Dyck in his paper.

Chapter V deals directly with Dyck's 1882 paper. Here in a vague way we find the idea that any group G can be presented as a homomorphic image of a free group. Let $g_1, \dots, g_n \in G$ and let \mathcal{F} be the free group on n generators $S_1, \dots, S_n \in \mathcal{F}$. Then G is a homomorphic image of \mathcal{F} via a homomorphism ϕ defined by $(S_i)\phi = g_i, 1 = 1, \dots, n$. Let K be the kernel of this homomorphism. Then, by the First Isomorphism Theorem $\frac{\mathcal{F}}{K} \cong G$, and $S_{i_1} \dots S_{i_n} \in K \Leftrightarrow g_{i_1} \dots g_{i_n} = I_G$. Thus K can be regarded as a list of "relations" concerning the generators g_1, \dots, g_n . Thus we have a presentation of G in terms of g_1, \dots, g_n . This we recognize as a final step toward the Genesis of the concept of group presentation.

CHAPTER I: CAYLEY'S 1854 PAPER

In the year 1854, Arthur Cayley published a paper in two parts, entitled *On the Theory of Groups, as depending on the Symbolic Equation $\theta^n = 1$* ; see [3]. In the first part of the paper Cayley:

1. introduces a general symbol θ such that $\theta(x, y, \dots) = (x', y', \dots)$ for some system of quantities x, y, \dots and x', y', \dots what makes θ "general" is that x', y', \dots can be:
 - (a) arbitrary functions of x, y, \dots
 - (b) a permutation of x, y, \dots . In this case θ is called a "substitution".
2. shows that substitutions can be iterated and composed, that these operations are associative and that there is an element that acts as the identity. (Here we are using modern terminology.)
3. defines the concept of a group table.
4. show some examples of groups.

In the second part of the paper, Cayley introduces the concept of a "symmetric holder" which is equivalent to that of a coset in modern terminology. Here we will be concerned with the first part of his paper; that which has the most relevance to this project.

Having introduced the general symbol θ in the manner described above, Cayley adds that if the operand is a single quantity x , then the symbol θ is an "ordinary function symbol" $\theta(x) = x'$.

The symbol 1 "will naturally denote the operation which leaves the operand unaltered", and $\theta\Phi$ denotes the "compound operation". He notes that the symbols θ are not in general commutative, but are associative. Next he defines his notion of a group:

"A set of symbols $1, \alpha, \beta, \dots$ all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself belongs to the set, is said to be a group."

Cayley's group is a non-empty set with a binary operation defined on it in which the associative law holds and in which there exists a two-sided identity element. Using modern terminology, we can say that Cayley's "group" is a monoid. The concept of the inverse is absent in these papers.

Cayley also introduces the notion of a group table. He notices that multiplying the entire group by each of its symbols has the effect of reproducing the group. The set of multiplications can be recorded in a square array: the multiplication table. He says:

“It follows that if the entire group is multiplied by anyone of the symbols, either as further or as nearer factor, the effect is simply to reproduce the group; or what is the same thing, that if the symbols of the group are multiplied together so as to form a table, thus:

		FURTHER FACTORS			
		1	α	β	...
NEARER FACTORS	1	1	α	β	
	α	α	α^2	$\alpha\beta$	
	β	β	$\beta\alpha$	β^2	
	\vdots				

that as well each line as each column of the square will contain all the symbols $1, \alpha, \beta, \dots$ ”

As we shall see in our examination of a latter paper, Cayley uses this group-table concept in proving his famous theorem, which says that every finite group can be represented as a group of permutations. Cayley recognized the presence of his concept of “group” in other areas of the mathematics of his day. His paper contains specific examples from the theories of permutations, elliptic functions, quadratic forms, the theory of matrices and the theory of quaternions. Here he illustrates the generality of his group concept.

CHAPTER II: CAYLEY'S 1878 PAPER

According to Wussing [10, p. 232], Cayley's return to group theory in 1878 was due to the rapidly growing recognition of the importance of the group concept. In *The Theory of Groups* published in 1878; see [4], Cayley:

1. gives a more abstract definition of a group in terms of "function symbols".
2. attempts to classify all finite groups of a given order n .
3. states and proves his famous theorem asserting that every finite group can be represented as a group of permutations.
4. discusses some graphical representations of groups.

Cayley starts by considering "functional symbols" α, β, \dots "each operating upon one and the same number of letters, and producing as its result the same number of functions of these letters". Here, he is working with mappings of a finite set onto itself. These operations can be iterated and composed, are associative and include an identity.

Looking back for a moment into the 1854 paper we find that Cayley defines a substitution θ there via $\theta(x, y, \dots) = (x', y', \dots)$ where x', y', \dots represent a permutation of x, y, \dots . Now in his 1878 paper he identifies substitutions as another variety of these "functional symbols" that he is working with. He explains:

"The functional symbols may be substitutions ..."

Altogether, Cayley has a set of functional symbols that can be iterated and composed, are associative and include an identity. He knows that substitutions are among these functional symbols and he is also acquainted with a few "groups of substitutions" from his 1854 paper. Putting these ideas together, he makes the following definition:

"A set of symbols $\alpha, \beta, \gamma, \dots$, such that the product $\alpha\beta$ of each of them (in each order, $\alpha\beta$ or $\beta\alpha$), is a symbol of the set is a group."

This makes a conceptual generalization of the notion of "permutation group".

We have seen in both the 1854 and 1878 papers, that the axioms of closure, associativity and identity are implicit in Cayley's definition of a group. The concept of the inverse of an element is again absent, so that he is still dealing with monoids.

We next find the following statement that we call "Cayley's Dictum" for future reference:

"A group is defined by means of the laws of combination of its symbols."

By this statement he meant that a group can be defined without making reference to the specific concrete nature of its elements, and that the essential structure of a group depends solely on the way in which the binary operation is prescribed on pairs of elements. Further on he adds:

“For the statement of these [laws] we may either:

- (1) by the introduction of powers and products, diminish as much as may be the number of independent functional symbols, or else:
- (2) using distinct letters for the several terms of the group employ a square diagram ...”

Cayley gives an example to illustrate what he has in mind for (1) and (2) above. In this example he introduces what he calls a “first mode” and “second mode” of a group. He explains:

“Thus in the first mode, a group is

$$1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2 (\alpha^2 = 1, \beta^3 = 1, \alpha\beta = \beta^2\alpha);$$

we observe that these conditions imply also $\alpha\beta^2 = \beta\alpha$.

Or, in the second mode, calling the same group

$$(1, \alpha, \beta, \gamma, \delta, \epsilon),$$

the laws of combinations are given by the square diagram

	1	α	β	γ	δ	ϵ
1	1	α	β	γ	δ	ϵ
α	α	1	γ	β	ϵ	δ
β	β	ϵ	δ	α	1	γ
γ	γ	δ	ϵ	1	α	β
δ	δ	γ	1	ϵ	β	α
ϵ	ϵ	β	α	δ	γ	1

for the symbols $(1, \alpha, \beta, \gamma, \delta, \epsilon)$ are in fact $= (1, \alpha, \beta, \alpha\beta, \beta^2, \alpha\beta^2)$.”

As we shall see, this notion of “first mode” is not well-defined by the author and leads him into error. The error appears in his attempt to classify all distinct groups of a given order n . For the case $n = 2$, Cayley correctly identifies the group: $1, \alpha$ ($\alpha^2 = 1$) as the only group of order two. (Today we would add that only up to isomorphism, is this true).

Next, for the case $n = 4$, he correctly identifies the groups $1, \alpha, \alpha^2, \alpha^3$ ($\alpha^4 = 1$) and $1, \alpha, \beta, \alpha\beta$ ($\alpha^2 = 1, \beta^2 = 1, \alpha\beta = \beta\alpha$) as the only groups of order four. Here we recognize Z_4 and $Z_2 \oplus Z_2$ as we know them today.

Finally, when $n = 6$, Cayley incorrectly presents three different groups of order six. These are:

$$1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 \quad (\alpha^6 = 1)$$

$$1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2 \quad (\alpha^2 = 1, \beta^3 = 1)$$

and

$$1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2 \quad (\alpha^2 = 1, \beta^3 = 1, \alpha\beta = \beta^2\alpha, \alpha\beta^2 = \beta\alpha).$$

Here we recognize Z_6 , $Z_2 \times Z_3$ and D_3 (the dihedral group of order 6) respectively. The problem is that he is presenting

$$1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 \quad (\alpha^3 = 1)$$

and

$$1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2 \quad (\alpha^2 = 1, \beta^3 = 1)$$

as different groups when in fact they should be accounted as one and the same group: $Z_6 \cong Z_2 \times Z_3$, by his own criterion. The question is, why does he make this error?

To answer this question, notice that “both” groups are expressed in first mode. We now compare both modes to realize that the author does not provide a criterion to determine whether these modes represent the same group or are modes corresponding to different groups. We conclude that the statement:

“A group is defined by means of the laws of combination of its symbols” is open to ambiguity.

Cayley realized that the problem of constructing all groups of a given order n is identical to the problem of constructing all permutation groups of order n . He says:

“But although the theory as above stated is a general one, including as a particular case the theory of substitutions, yet the general problem of finding all the groups of a given order n , is really identical with the apparently less general problem of finding all the groups of the same order n , which can be formed with the substitution upon n letters.”

This is the content of Cayley’s theorem as we know it today that asserts that every finite group can be represented as a group of permutations. To prove this theorem Cayley takes the group

$$1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2 \quad (\alpha^2 = 1, \beta^3 = 1, \alpha\beta = \beta^2\alpha)$$

in its “second mode” $(1, \alpha, \beta, \gamma, \delta, \epsilon)$, with its laws of combinations given by the square diagram, and shows that this group

“May be regarded as substitutions performed upon the six letters $1, \alpha, \beta, \gamma, \delta, \epsilon \dots$ which changes $1\alpha\beta\gamma\delta\epsilon$ into $\alpha 1\gamma\beta\epsilon\delta$, and so on [for the “nearer factors”] $\beta, \gamma, \delta, \epsilon$.”

The fact that this method of group table can be used to represent any finite group as a group of permutations is implicit, but it is not actually mentioned by Cayley in his paper. His proof is not rigorous in the modern sense.

CHAPTER III: KRONECKER'S 1870 PAPER

In 1870, Leopold Kronecker published a paper entitled *Auseinandersetzung einiger Eigenschaften der Klassenanzahl idealer complexer zahlen* or "Explanation of some properties of the class-number of ideal complex numbers"; see [8]. In this paper, Kronecker introduces the notion of an abstract finite abelian group. He considers a finite number of elements θ', θ'', \dots such that from any two of them, a third element $f(\theta', \theta'')$ is defined according to a fixed rule. He assumes the associative and commutative laws: $f(\theta', f(\theta'', \theta''')) = f(f(\theta', \theta''), \theta''')$ and $f(\theta', \theta'') = f(\theta'', \theta')$. Later on he uses the simpler notation $\theta' \cdot \theta''$ instead of $f(\theta', \theta'')$.

Next, Kronecker sets out to prove the following results in finite group theory:

Theorem (i) *If θ is any "element" of the set under discussion, then $\theta^k = 1$ for some positive integer k . If k is the smallest such positive integer then θ is said to "belong to k ". If θ belongs to k and $\theta^m = 1$ then k divides m .*

Theorem (ii) *If an element θ belongs to k , then every divisor of k has an element belonging to it.*

Theorem (iii) *If θ and θ' belong to k and k' respectively, and k and k' are relatively prime, then $\theta\theta'$ belongs to kk' .*

Theorem (iv) *There exists a "fundamental system" of elements $\theta_1, \theta_2, \theta_3, \dots, \theta_m$ such that the expression $\theta_1^{a_1} \theta_2^{a_2} \theta_3^{a_3} \dots \theta_m^{a_m}$ ($a_i = 1, 2, 3, \dots, e_i$) represents each element of the given set of elements exactly once. The numbers $e_1, e_2, e_3, \dots, e_m$ to which respectively, $\theta_1, \theta_2, \theta_3, \dots, \theta_m$ belong, are such that each is divisible by its successor; the product $e_1 e_2 e_3 \dots e_m$ is equal to the totality of elements of the set. (This is the "existence part" of the Fundamental Theorem of Finite Abelian Groups.)*

We now proceed to translate each of the above theorems into current-day mathematical language. We also feel the necessity of proving them, because Kronecker's proofs are extremely hard to read. Kronecker has a tendency to imply that he has somewhere proved a theorem, without being at all specific about it.

Theorem (i) *If $|\theta| = k$ and $\theta^m = 1$ then $k|m$.*

Proof: Write $m = qk + r$ where $0 \leq r < k$. Then $\theta^m = 1$ becomes $\theta^{qk+r} = 1$ which implies that $(\theta^k)^q \theta^r = 1$. But, $\theta^k = 1$ and so our previous equation becomes $\theta^r = 1$. By hypothesis we know that k is the smallest integer such that $\theta^k = 1$. Now, r is smaller than k , so $\theta^r = 1$ is impossible unless $r = 0$. Thus $m = qk + 0$, so that $k|m$.

Theorem (ii) Let $|\theta| = k$. Let d be a divisor of k . Then there exists $\theta' \in G$ such that $|\theta'| = d$.

Proof: Let $\theta' = \theta^{k/d}$. Suppose that $0 < c < d$. Then $(\theta')^c = \theta^{k \cdot c/d} = 1$, but $\frac{kc}{d} < k$ contradicting $|\theta| = k$.

Theorem (iii) If $|\theta| = k$ and $|\theta'| = k'$ with $(k, k') = 1$, then $|\theta\theta'| = kk'$.

Proof: Given G abelian, we have that

$$(\theta\theta')^{kk'} = \theta^{kk'}(\theta')^{kk'} = (\theta^k)^{k'}(\theta'^{k'})^k = 1.$$

Hence, $|\theta\theta'|$ divides kk' by Theorem (i). Next, if $(\theta\theta')^m = 1$, i.e. $\theta^m(\theta')^m = 1$, then $\theta^m = (\theta')^{-m}$ and $1 = (\theta^m)^k = (\theta')^{-mk}$. Since $|\theta'| = k'$ we have $k'| -mk$ by Theorem (i). Since $(k, k') = 1$ we have $k'|m$. Similarly $k|m$. Now, $k'|m$ and $k|m$ imply $kk'|m$. Finally, let $m = |\theta\theta'|$. Then $|\theta\theta'| | kk'$ and $kk' | m$, so $|\theta\theta'| = kk'$ as desired.

The fourth result above is what is known today as The Fundamental Theorem of Finite Abelian Groups. We will restate and prove this theorem following Kronecker's reasoning, but using some modern terminology. First we state and prove three lemmas needed to establish Theorem (iv).

Lemma (1) Let $|\theta|_G$ denote the order of an arbitrary element θ in G . There exists $\theta_1 \in G$ such that $|\theta_1|_G = \ell \text{cm}\{|\theta| : \theta \in G\}$.

Proof: Let $\ell cm\{|\theta| : \theta \in G\} = m = p_1^{e_1} \cdots p_s^{e_s}$. Then there exists $\bar{\theta}_i \in G$ such that $p_i^{e_i}$ divides $|\theta_i|$, $1 \leq i \leq s$. Put $\theta_i = (\bar{\theta}_i)^{n_i p_i^{-e_i}}$ where $n_i = |\bar{\theta}_i|$. Then $\theta_i^{p_i^{e_i}} = 1$. Assume $0 < c < p_i^{e_i}$. Then $(\theta_i)^c = (\bar{\theta}_i)^{n_i c p_i^{-e_i}} = 1$, but $0 < n_i c p_i^{-e_i} < n_i$ contradicting $|\bar{\theta}_i| = n_i$. Thus $|\theta_i| = p_i^{e_i}$. Put $\theta = \theta_1 \cdots \theta_s$. Then $|\theta| = m$ by Theorem (iii) above.

Lemma (2) *Let G be a finite abelian group, N a subgroup of G and $\theta \in G$. Then the order of θN as an element of $\frac{G}{N}$ divides the order of θ .*

Remark: This result is true for G non-abelian taking N normal in G .

Proof: Let N be a subgroup of G . Let $|\theta N| = m$. Then $\theta^m = 1_G$, so $\theta^m N = N = 1_{G/N}$. By Theorem (i) applied to $\frac{G}{N}$ we have that $m|n$.

We now introduce the following notation:

Let $\langle \theta \rangle$ denote the group generated by an arbitrary element θ in G .

Let $\frac{G}{\langle \theta \rangle}$ be the group of cosets of $\langle \theta \rangle$ in G .

Let $|\theta_{11}\langle \theta_1 \rangle|_{G/\langle \theta_1 \rangle}$ denote the order of the coset $\theta_{11}\langle \theta_1 \rangle$ in $\frac{G}{\langle \theta_1 \rangle}$.

Let $\exp(G) = \ell cm\{|\theta|_G : \theta \in G\}$.

Lemma (3) *Let G be a finite abelian group, and let $\theta_1 \in G$ such that $|\theta_1|_G = \exp(G)$. Then every coset $\theta_{11}\langle \theta_1 \rangle$ of $\langle \theta_1 \rangle$ in G contains a representative θ_2 such that $|\theta_2|_G = |\theta_{11}\langle \theta_1 \rangle|_{G/\langle \theta_1 \rangle}$.*

Proof: Let G be a finite abelian group. Let $\theta_1 \in G$ such that $e_1 = \exp(G) = |\theta_1|$. Let $\theta_{11}\langle \theta_1 \rangle \in \frac{G}{\langle \theta_1 \rangle}$ and put $e_2 = |\theta_{11}\langle \theta_1 \rangle|_{G/\langle \theta_1 \rangle}$. Then $\theta_{11}^{e_2} \in \langle \theta_1 \rangle$ so $\theta_{11}^{e_2} = \theta_1^k$ for some integer k . Put $m = \frac{k}{e_2}$. Then $m \in \mathcal{Q}$, but we will eventually see that $m \in N$. Then $m e_1 = \frac{k}{e_2} e_1 = k \frac{e_1}{e_2}$. Now, $e_2 | e_1$ by Lemma (2), so $m e_1$ is an integer

and $\theta_1^{q e_1} = \theta_1^{k e_1/e_2} = \theta_1^{e_1} = 1$. As $\theta_1^k e_1/e_2 = 1$, we have $k \geq e_2$. Write $k = q e_2 + r$ with $0 \leq r < e_2$. So, $1 = \theta_1^k e_1/e_2 = \theta_1^{q e_2} \theta_1^r e_1/e_2 = \theta_1^r e_1/e_2$. As $r < e_2$, we conclude that $r = 0$. That is, $e_2 | k$ and m is an integer. Next define θ_2 by $\theta_2 \theta_1^m = \theta_{11}$ and observe that then $\theta_2 \langle \theta_1 \rangle = \theta_{11} \langle \theta_1 \rangle$. Also, we have $\theta_1^k = \theta_1^{e_2} = (\theta_2 \theta_1^m)^{e_2} = \theta_2^{e_2} \theta_1^{m e_2} = \theta_2^{e_2} \theta_1^k$, so $1 = \theta_2^{e_2}$. Therefore $|\theta_2| = e_2 = |\theta_{11} \langle \theta_1 \rangle|_{\frac{G}{\langle \theta_1 \rangle}}$ so that θ_2 is the desired representative of $\theta_{11} \langle \theta_1 \rangle$.

Theorem (iv) *Let G be a finite abelian group. Then there exist $\theta_1, \dots, \theta_m \in G$ and positive integers e_1, \dots, e_m such that:*

- (1) $|\theta_i|_G = e_i$.
- (2) $e_m | e_{m-1} | \dots | e_1$.
- (3) Every element of G can be written in a unique way in the form $\theta_1^{a_1} \theta_2^{a_2} \dots \theta_m^{a_m}$ with $0 \leq a_i < e_i$, $1 \leq i \leq m$.

Proof: (Following Kronecker)

Let $e_2 = \exp\left(\frac{G}{\langle \theta_1 \rangle}\right)$. By Lemma (1), there exist $\theta_{11} \langle \theta_1 \rangle \in \frac{G}{\langle \theta_1 \rangle}$ such that $|\theta_{11} \langle \theta_1 \rangle| = e_2$. By Lemma (3), there exist $\theta_2 \in \theta_{11} \langle \theta_1 \rangle$ with $|\theta_2| = e_2$ in G .

Next, put $e_3 = \exp\left(\frac{G}{\langle \theta_1, \theta_2 \rangle}\right)$. Then there exists $\theta_{111} \langle \theta_1, \theta_2 \rangle$ of order e_3 in $\frac{G}{\langle \theta_1, \theta_2 \rangle}$. We can identify $\langle \theta_1, \theta_2 \rangle$ with a cyclic subgroup of $\frac{G}{\langle \theta_1 \rangle}$ by observing that $\langle \theta_1, \theta_2 \rangle = \theta_2 \langle \theta_1 \rangle \cup \theta_2^2 \langle \theta_1 \rangle \cup \dots \cup \theta_2^{e_2} \langle \theta_1 \rangle$. That is (in modern terminology)

$$\frac{\langle \theta_1, \theta_2 \rangle}{\langle \theta_1 \rangle} = \{ \theta_2 \langle \theta_1 \rangle, \theta_2^2 \langle \theta_1 \rangle, \dots \}$$

is a cyclic subgroup of order e_2 in $\frac{G}{\langle \theta_1 \rangle}$ where $e_2 = \exp\left(\frac{G}{\langle \theta_1 \rangle}\right)$.

By Lemma (1), there exists $\frac{\theta_{111} \langle \theta_1, \theta_2 \rangle}{\langle \theta_1 \rangle} \in \frac{G}{\langle \theta_1 \rangle} / \frac{\langle \theta_1, \theta_2 \rangle}{\langle \theta_1 \rangle}$ of order $e_3 = \exp\left(\frac{G}{\langle \theta_1 \rangle} / \frac{\langle \theta_1, \theta_2 \rangle}{\langle \theta_1 \rangle}\right)$. Conclude from Lemma (3) that $\frac{\theta_{111} \langle \theta_1, \theta_2 \rangle}{\langle \theta_1 \rangle}$, regarded as a coset of $\frac{\langle \theta_1, \theta_2 \rangle}{\langle \theta_1 \rangle}$ in $\frac{G}{\langle \theta_1 \rangle}$ contains an element $\theta_{111} \langle \theta_1 \rangle$ of order e_3 in $\frac{G}{\langle \theta_1 \rangle}$. Apply Lemma (3) again to G to conclude that $\theta_{111} \langle \theta_1 \rangle$ contains an element θ_3 of order e_3 in G .

Proceed in this way until one produces $\theta_1, \theta_2, \dots, \theta_m$ which generate G , with $|\theta_i| = e_i = \exp\left(\frac{G}{\langle \theta_1, \dots, \theta_{i-1} \rangle}\right)$. Then $e_m | e_{m-1} | \dots | e_1$ by Lemma (2). Every element of G can be written in at least one way in the form $\theta_1^{a_1} \theta_2^{a_2} \dots \theta_m^{a_m}$, $0 \leq a_i < e_i$ since $\{\theta_1, \dots, \theta_m\}$ generates G . Suppose $\theta_1^{a_1} \theta_2^{a_2} \dots \theta_m^{a_m} = \theta_1^{b_1} \theta_2^{b_2} \dots \theta_m^{b_m}$, $0 \leq b_i < e_i$. Then $\theta_m^{b_m - a_m} \in \langle \theta_1, \dots, \theta_{m-1} \rangle$, so $e_m | b_m - a_m$ by Theorem (i) and then $b_m = a_m$ since $|b_m - a_m| < e_m$. Argue by repetition and obtain $b_{m-1} = a_{m-1}, \dots, b_1 = a_1$. This proves the theorem.

Returning now to our discussion; Kronecker's theorem implies that two abelian groups G_1 and G_2 having the same factors e_i must be isomorphic. Notice that if Cayley had known this, perhaps he would have been more successful in his attempt to classify all non-isomorphic groups of order 6. Namely, the error about Z_6 being nonisomorphic to $Z_2 \oplus Z_3$ would have been eliminated from his 1878 paper.

Kronecker's theorem predicts that there will be at most two isomorphism classes of abelian groups of order 12, namely those corresponding to the two sets of factors $\{2, 6\}$ and $\{12\}$. Why can't $\{2, 6\}$ and $\{12\}$ be factors for isomorphic groups? Kronecker does not address this issue.

The factors e_i are called "invariants". The uniqueness of these factors was later proved by Frobenius and Stickelberger in their 1879 paper entitled *Ueber Gruppen von vertauschbaren Elementen*; see [10, p. 234].

In his 1878 paper, Cayley tells us that "A group is defined by means of the law of combination of its symbols". Thus, we see that Kronecker had anticipated this fact (for finite abelian groups) in 1870, since his theorem defines abelian groups in terms of simple and specific "laws of combinations of its symbols".

Kronecker tells us that every finite abelian group has a presentation of the form described in his theorem. In fact, Kronecker gives us the most efficient possible set of generators and relations for a finite abelian group. By "most efficient" we mean that the number of generators is as small as possible and the number of relations is as small as possible. Here $G = \langle \theta_1, \dots, \theta_m \mid [\theta_i, \theta_j] = \theta_i^{e_i} = 1 \rangle$ where $[\theta_i, \theta_j] = \theta_i^{-1} \theta_j^{-1} \theta_i \theta_j$. As we will see, it was Dyck's achievement to successfully formalize the notion that every group admits such a description in terms of generators and relations.

Thus, while Cayley was able to observe that the multiplication table of a group G "presents" G in terms of laws of combination of symbols, Kronecker improves this (in the case of abelian groups) by showing that it suffices to consider combinations of generators, and Dyck shows that this same principle extends to arbitrary groups.

CHAPTER IV: PRELUDE TO DYCK'S *Gruppentheoretische Studien*

SECTION I: SOME PROPERTIES OF THE MAPPING $(z)T = w + \frac{r^2}{\bar{z} - \bar{w}}$.

Let \mathcal{C} be a circle in the complex plane \mathbb{C} with radius $r > 0$ and center w . Denote the interior and exterior of \mathcal{C} by $\text{Int}(\mathcal{C})$ and $\text{Ext}(\mathcal{C})$ respectively. Let $\dot{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ be the extended complex plane. Define a mapping $T : \dot{\mathbb{C}} \rightarrow \dot{\mathbb{C}}$ by $(z)T = w + \frac{r^2}{\bar{z} - \bar{w}}$ where \bar{z} and \bar{w} denote the complex conjugates of z and w .

Proposition 1:

- (a) T takes w to ∞ and ∞ to w .
- (b) T is invertible and $T^{-1} = T$.
- (c) \mathcal{C} is pointwise invariant under T .
- (d) T takes $\text{Int}(\mathcal{C})$ to $\text{Ext}(\mathcal{C})$ and $\text{Ext}(\mathcal{C})$ to $\text{Int}(\mathcal{C})$.
- (e) For $z \notin \{w, \infty\}$, $(z)T$ lies on the ray joining w , z and ∞ . Also $|(z)T - w| |\bar{z} - \bar{w}| = r^2$.

Proof:

- (a) $(w)T = w + \frac{r^2}{\bar{w} - \bar{w}} = \infty$ and $(\infty)T = w + \frac{r^2}{\infty - \bar{w}} = w$.
- (b) Let I denote the identity mapping $(z)I = z$. Let T^2 denote the composition $((z)T)T$. Then $(z)T^2 = w + \frac{r^2}{(z)T - \bar{w}} = w + \frac{r^2}{\left\{ \bar{w} + \frac{r^2}{z - w} \right\} - \bar{w}} = w + (z - w) = z$. Hence $T^2 = I$, i.e. $T = T^{-1}$ and therefore T is invertible.
- (c) Let $z \in \mathcal{C}$. Then $|z - w| = r$. Now

$$(z)T = w + \frac{r^2}{\bar{z} - \bar{w}} \frac{z - w}{z - w} = w + \frac{r^2(z - w)}{|z - w|^2} = w + \frac{r^2(z - w)}{r^2} = z.$$

(d) Let $z \in \text{Int}(\mathcal{C})$. Then $|z - w| < r$. Now

$$\begin{aligned} |(z)T - w| &= \left| w + \frac{r^2}{\bar{z} - \bar{w}} - w \right| = \left| \frac{r^2}{(z - \bar{w})} \frac{(z - w)}{(z - \bar{w})} \right| \\ &= \frac{r^2 |z - w|}{|z - w|^2} = \frac{r^2}{|z - w|} > \frac{r^2}{r} = r. \end{aligned}$$

Hence $(z)T \in \text{Ext}(\mathcal{C})$. Similarly, let $z \in \text{Ext}(\mathcal{C})$. Then $|z - w| > r$ so that $|(z)T - w| < r$. Therefore $(z)T \in \text{Int}(\mathcal{C})$.

(e) $(z)T = w + \frac{r^2}{\bar{z} - \bar{w}} \frac{z - w}{z - w} = w + \frac{r^2}{|z - w|^2} (z - w)$. Put $\alpha = \frac{r^2}{|z - w|^2}$. Notice that $\alpha > 0$. Then $(z)T = w + \alpha(z - w)$, i.e. $(z)T$ lies on the ray $\{w + \alpha(z - w) : 0 < \alpha < \infty\}$ from w through z . Also

$$\begin{aligned} (z)T &= w + \frac{r^2}{\bar{z} - \bar{w}} \Leftrightarrow (z)T - w = \frac{r^2}{\bar{z} - \bar{w}} \Leftrightarrow |(z)T - w| \\ &= \frac{r^2}{|\bar{z} - \bar{w}|} \Leftrightarrow |(z)T - w| |\bar{z} - \bar{w}| = r^2. \end{aligned}$$

Remark 1: The image of a line through the center w under T is the same line. This line is not pointwise invariant under T because, except for those points on \mathcal{C} we have $(z)T \neq z$ with w , z and $(z)T$ collinear.

Remark 2: For any points $z, z' \in \dot{\mathcal{C}}$ with $z' = (z)T$ we have that $|z' - w| = \frac{r^2}{|z - w|}$. The mapping T is usually called a “circular inversion” from the fact that as z becomes a variable point, the distances $|z - w|$ and $|z' - w|$ are inversely proportional.

Proposition 2: *The image under T of a line ℓ not passing through w is a circle passing through w .*

Proof: Let P be a point on ℓ such that the ray \overrightarrow{wP} emanating from w and passing through P is perpendicular to ℓ . Let Q be another point on ℓ . Let

$P', Q' \in \mathbb{C}$ such that $P' = (P)T$ and $Q' = (Q)T$. Then by Proposition 1(e) $|P' - w||P - w| = r^2$ and $|Q' - w||Q - w| = r^2$ so that $|P' - w||P - w| = |Q' - w||Q - w|$. Hence $\frac{|P - w|}{|Q - w|} = \frac{|P' - w|}{|Q' - w|}$. This last result implies that ΔwPQ is similar to $\Delta wQ'P'$ since they share the same angle. Thus $\Delta wQ'P'$ is also a right triangle with right angle at the Q' vertex.

Now let Q become a variable point on \overline{PQ} . Then Q' becomes a variable vertex of the right angle in $\Delta wQ'P'$ and thus traces a circle. Since $(\infty)T = w$ then this circle passes through w and has diameter $\overline{P'w}$.

Proposition 3: *The image under T of a circle D not passing through w is a circle not passing through w .*

Proof:

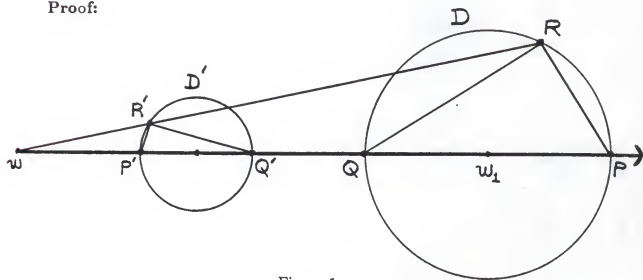


Figure 1

Refer to the figure above. Let w_1 be the center of D . Let the line from w through w_1 intersect D in Q and P . Then \overline{QP} is the diameter of D . Let $P', Q' \in \mathbb{C}$ such that $P' = (P)T$ and $Q' = (Q)T$. Consider a third point R in D and a point $R' \in \mathbb{C}$ such that $R' = (R)T$. Now by Proposition 1(e) the points w, P', Q', Q, w_1 and P are collinear and the points w, R' and R are collinear. Consider the line segments $\overline{wR'}$, $\overline{P'R'}$, $\overline{R'Q'}$, \overline{QR} and \overline{RP} . Now by Proposition 1(e) we have

$$|w - P||w - P'| = |w - Q||w - Q'| = |w - R||w - R'| \quad (= r^2).$$

Hence $\frac{|w-P|}{|w-R|} = \frac{|w-R'|}{|w-P'|}$ and thus ΔwRP is similar to $\Delta wP'R'$, with $\angle wRP = \angle wP'R'$. Also $\frac{|w-Q|}{|w-R|} = \frac{|w-R'|}{|w-Q'|}$ and thus ΔwQR is similar to $\Delta wQ'R'$ with $\angle wRQ = \angle wQ'R'$. Subtracting angles we get $\angle wRP - \angle wRQ = \angle wP'R' - \angle wQ'R'$.

Let R be a variable point following the contour of D . Now the line segments \overline{QR} and \overline{RQ} have variable length. Notice that $\angle QRP$ maintains a constant measure of $\frac{\pi}{2}$ because \overline{PQ} is the diameter of D .

Now notice that $\angle QRP = \angle wRP - \angle wRQ$ is a right triangle. Hence $\angle wP'R' - \angle wQ'R'$ is a right triangle. Next, since the sum of the angles of $\Delta P'R'Q'$ equals π we have

$$\begin{aligned} \angle P'R'Q' &= \pi - (\angle R'P'Q' + \angle wQ'R') \\ &= \pi - (\pi - \angle wP'R') - \angle wQ'R' \\ &= \angle wP'R' - \angle wQ'R' \\ &= \frac{\pi}{2}. \end{aligned}$$

Let D' be the image of D under T . Since T is a continuous function in \mathring{C} , it is clear that D' is symmetric with respect to the line $\overline{wQ'P}$. In particular, since D' passes through P' and Q' in $\overline{wQ'P}$ then D' is symmetric with respect to the line segment $\overline{P'Q'}$. As R varies along D , the variable vertex R' in right angle $\angle P'R'Q'$ traces a circle D' with diameter $P'Q'$. Therefore the image under T of a circle D not passing through w is a circle not passing through w .

Proposition 4: *The measure of the angle between two intersecting smooth curves is an invariant under T , but its direction is reversed.*

PRELIMINARY REMARK:

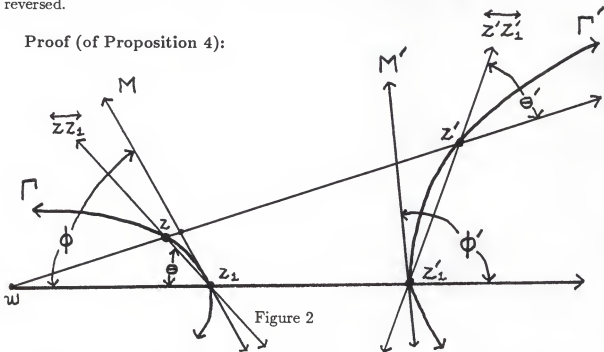
Let Γ be a smooth curve with image Γ' under T . Let $\overline{wz_1z'_1}$ be a ray emanating from w and intersecting Γ and Γ' at the points z_1 and z'_1 respectively. The angle between a curve and a ray is defined to be the angle between the tangent line to the curve (at some point in it) and the ray. Let ϕ and ϕ' be the angles that Γ and Γ' make respectively relative to $\overline{wz_1z'_1}$. We will show that $\phi = \phi'$ but their directions are reversed relative to $\overline{z_1z'_1}$. That is, if we measure ϕ counter-clockwise relative to $\overline{z_1z'_1}$ then ϕ' must be measured clockwise relative to this ray.

Let Λ be another smooth curve passing through z_1 with its image under T , Λ' passing through z'_1 . Let ψ and ψ' be the angles that Λ and Λ' make respectively relative to $\overline{wz_1z'_1}$. Then by the above result we will have $\psi = \psi'$ with their

directions reversed.

The angle between two curves is defined to be the angle between their tangents at their point of intersection. We will show that the angles $\phi - \psi$ and $\phi' - \psi'$ between Γ and Λ and Γ' and Λ' respectively are the same with their directions reversed.

Proof (of Proposition 4):



Refer to the figure. Let Γ , Γ' and wz_1z_1' be defined as in the remark. Let wz_1z' be another ray emanating from w and intersecting Γ and Γ' at the points z and z' respectively. Let $\overline{zz_1}$ and $\overline{z'z_1'}$ be lines secant to Γ and Γ' respectively. Let $\overline{zz_1}$ and $\overline{z'z_1'}$ subtend angles θ and θ' respectively relative to wz_1z_1' . Let M and M' be the tangent lines to Γ and Γ' respectively at the points z_1 and z_1' . Here M and M' subtend angles ϕ and ϕ' respectively relative to wz_1z_1' .

Now since z, z' and w are collinear and z_1, z_1' and w are collinear we have $|z - w||z' - w| = |z_1 - w||z_1' - w| (= r^2)$. Thus $\frac{|z - w|}{|z_1 - w|} = \frac{|z_1' - w|}{|z' - w|}$. Since Δwz_1z shares an angle with $\Delta wz_1'z'$ we conclude that these triangles are similar. Here $\angle wz_1z = \angle wz_1'z'$, i.e. $\theta = \theta'$.

Next let z become a variable point, following the path Γ toward z_1 . Then secant $\overline{zz_1}$ approaches the tangent M . Simultaneously, z' becomes a variable point, following the path Γ' toward z_1' . Then secant $\overline{z'z_1'}$ approaches the tangent M' . Angle θ' approaches ϕ' as angle θ approaches ϕ . At the limit positions where z and z_1 coincide and z' and z_1' coincide we have angle $\theta =$ angle $\phi =$ angle $\phi' =$ angle θ' .

As stated in Remark 2, for any point v in Γ and $v' = (v)T$ in Γ' collinear with w , the distances $|v - w|$ and $|v' - w|$ are inversely proportional. For this reason,

although the measure of the angles ϕ and ϕ' are the same, their directions are reversed.

Now consider a new smooth curve Λ intersecting Γ at z_1 with image Λ' under T intersecting Γ' at z'_1 . Let ψ and ψ' be the angles between Λ and $wz_1z'_1$ and Λ' and the same ray respectively. Then by the above $\psi = \psi'$ with their directions reversed.

Finally let the angles between Γ and Λ and Γ' and Λ' be $\phi - \psi$ and $\phi' - \psi'$ respectively. Then $\phi - \psi = \phi' - \psi'$, but their directions are reversed. This concludes the proof of Proposition 4.

Proposition 5: *A circle D is orthogonal to C if and only if for any two points z and z' on D collinear with w we have $(z)T = z'$.*

Proof: Let P be one of the points of intersection of C and D . Construct the line segments wz, wP, Pz' and Pz . Now compare the triangles ΔwPz and $\Delta wPz'$. Notice that these are similar triangles with congruent angles $\angle Pwz \cong \angle Pwz', \angle zPw \cong \angle z'Pw, \angle Pz'w \cong \angle Pzw$ and congruent sides $|P - z| \cong |z' - P|, |z - P| \cong |P - w|$ and $|P - w| \cong |z' - w|$. We now consider the ratio

$$\frac{|z - w|}{|P - w|} = \frac{|P - w|}{|z' - w|}.$$

Since $|P - w| = r$ then $|z - w||z' - w| = r^2$. Hence $z' = (z)T$ by Proposition 1(e).

Conversely, if any two points z and z' on D collinear with w are such that $z' = (z)T$ then D is orthogonal to C . The proof consists in reversing the above steps.

Proposition 6: *Let D be a circle orthogonal to C . Then D is setwise invariant under T .*

Proof: Let D' denote the image of D under T . Then D' is a circle (by Proposition 3) orthogonal to C (by Proposition 4). We now show that $D' = D$. For any ray emanating from w and joining two points z and z' on D we have $z' = (z)T \in D'$. Hence $D \subseteq D'$. Conversely since D' is a circle orthogonal to C then for $u \in D'$ there exists $u' \in D'$ collinear with u and w such that $u = (u')T$ by Proposition 5. But $u' = (v)T$ for some $v \in D$. Hence $u = (u')T = ((v)T)T = v \in D$. Hence $D' \subseteq D$ and thus $D' = D$. Therefore D is setwise invariant under T .

SECTION II. FIRST STEP IN A GEOMETRIC CONSTRUCTION OF A FREE GROUP.

PRELIMINARY REMARK:

The purpose of the following construction is to present a geometrical model of a free group following the approaches of Dyck [7] and Burnside [2]. Let $\dot{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ be the extended complex plane. Then the free group under consideration is a subgroup of the group of Möbius Transformations

$$\mathcal{M} = \left\{ (z)S = \frac{az + b}{cz + d} : ad - bd = 1, \quad a, b, c, d, z \in \dot{\mathbb{C}} \right\}; \text{ see [6].}$$

One starts with a domain denoted by [I] in \mathbb{C} bounded by arcs of circles $\mathcal{C}_1, \dots, \mathcal{C}_n$ mutually tangent, and orthogonal to the unit circle \mathcal{C} . The "circle" \mathcal{C}_n is taken to be as the imaginary axis. Each of these circles have radii and centers denoted by r_j and w_j respectively, where $1 \leq j \leq n-1$. These radii and centers will be computed in the discussion.

The polygon [I] (shaded for latter convenience) will be inverted through the boundaries of the above circles via the mappings $T_j : \dot{\mathbb{C}} \rightarrow \dot{\mathbb{C}}$ defined by $(z)T_j = w_j + \frac{r_j^2}{\bar{z} - \bar{w}_j}$, $1 \leq j \leq n-1$ and the mapping $T_n : \dot{\mathbb{C}} \rightarrow \dot{\mathbb{C}}$ defined by $(z)T_n = -\bar{z}$. These so called "inversion through the boundary of a circle \mathcal{C}_j " will produce a set of unshaded polygons surrounding [I]. Mappings of the form $S_j : \dot{\mathbb{C}} \rightarrow \dot{\mathbb{C}}$ defined in terms of our previous mappings T_j and specified as follows: $(z)S_1 = (z)T_n T_1$, $(z)S_2 = (z)T_1 T_2, \dots, (z)S_n = (z)T_{n-1} T_n$ will produce a set of shaded polygons surrounding [I], and called a "first level of tessellation".

An even and odd number of compositions of mappings T_j will produce more shaded and unshaded polygons respectively. The pattern of shaded and unshaded polygons so produced covers the interior of \mathcal{C} without overlapping, producing a so called "tessellation" of \mathcal{C} .

The free group that we are referring to is denoted by \mathcal{F} and is the group generated by the mappings S_1, S_2, \dots, S_n above. The group \mathcal{F} will be studied in more detail in the next section. The "free" nature of \mathcal{F} is also captured by our model but the details of this will be left for Section IV of this chapter.

CONSTRUCTION:

The following steps offer an outline of the construction:

- (1) Divide the complex plane \mathbb{C} into four quadrants in the usual way with a real and imaginary axis meeting orthogonally at the origin. Consider a unit circle centered at the origin and denoted by \mathcal{C} .
- (2) If $n = 2j + 1$ let the points A_j , $1 \leq j \leq n$ subtend counter-clockwise angles

relative to the positive real axis:

$$\phi_n = \frac{\pi}{2}, \phi_{n-1} = \frac{(j+1)\pi}{2j}, \phi_{n-2} = \frac{(j+2)\pi}{2j}, \dots, \phi_1 = \frac{(j+k)\pi}{2j}$$

where $k = 1, 2, \dots, 2j$ and j depends on n . If $n = 2j$ let these angles be instead:

$$\phi_n = \frac{\pi}{2}, \phi_{n-1} = \frac{(2j+1)\pi}{2(2j-1)}, \phi_{n-2} = \frac{(2j+3)\pi}{2(2j-1)}, \dots, \phi_1 = \frac{(2j+[2k+1])\pi}{2(2j-1)}$$

where $k = 0, 1, 2, \dots, 2(j-1)$ and j depends on n . Denote the points A_j by "vertices".

(3) Consider a family of circles C_j , $1 \leq j \leq n$ such that:

(a) The "circle" C_n is identified as the imaginary axis.

(b) C_j is orthogonal to C .

(c) $C \cap C_{j-1} = \{A_{j-1}, A_j\}$, $2 \leq j \leq n$ with $C \cap C_n = \{A_1, A_n\}$.

(d) C_{j-1} is tangent to C_j at A_j for $2 \leq j \leq n$ with C_n tangent to C_1 at A_1 .

(4) Consider the arcs formed by the portions of the circles $C_{n-1}, C_{n-2}, \dots, C_1$ found inside C and bounded by the vertices A_n and $A_{n-1}A_{n-1}$ and A_{n-2}, \dots, A_2A_1 and A_1 respectively. Denote these arcs by $A_{n-1}A_n, A_{n-1}A_{n-2}, \dots, A_2A_1$. Denote the "arc" formed by the portion of the "circle" C_n inside C and bounded by A_n and A_1 by A_1A_n .

(5) Let the region bounded by the arcs $A_{n-1}A_n, A_{n-2}A_{n-1}, \dots, A_2A_1$ and A_1A_n be denoted by $[I]$.

(6) Denote the centers of the circles $C_{n-1}, C_{n-2}, \dots, C$, by $w_{n-1}, w_{n-2}, \dots, w_1$. Denote the radii of these circles by $r_{n-1}, r_{n-2}, \dots, r_1$. Here $r_{n-1} = r_{n-2} = \dots = r_1$.

(7) Let $n = 2j + 1$. The centers $w_{n-1}, w_{n-2}, \dots, w_1$ subtain counter-clockwise angles relative to the positive real axis

$$\theta_{n-1} = \frac{(2j+1)\pi}{4j}, \theta_{n-2} = \frac{(2j+3)\pi}{4j}, \dots, \theta_1 = \frac{[2j+(2k-1)]\pi}{4j}$$

where $k = 1, 2, \dots, 2j$ and j depends on n . Let d_{n-1} denote the distance between w_{n-1} and the origin. Let $\psi_{n-1} = \frac{\pi}{4j}$ be the counter-clockwise angle subtended by w_{n-1} relative to the imaginary axis. Then

$$\begin{aligned} w_{n-1} &= d_{n-1} \{ \cos(\theta_{n-1}) + i \sin(\theta_{n-1}) \} \\ &= \frac{1}{\cos\left(\frac{\pi}{4j}\right)} \left\{ \cos\left[\frac{(2j+1)\pi}{4j}\right] + i \sin\left[\frac{(2j+1)\pi}{4j}\right] \right\}. \end{aligned}$$

Since

$$\frac{\sin\left[\frac{(2j+1)\pi}{4j}\right]}{\cos\left(\frac{\pi}{4j}\right)} = 1$$

we have

$$w_{n-1} = \frac{\cos\left[\frac{(2j+1)\pi}{4j}\right]}{\cos\left(\frac{\pi}{4j}\right)} + i.$$

Next

$$r_{n-1} = |w_{n-1} - A_n| = |w_{n-1} - (0, i)| = \frac{\left|\cos\left[\frac{(2j+1)\pi}{4j}\right]\right|}{\cos\left(\frac{\pi}{4j}\right)}.$$

Since $r_{n-1} = r_{n-2} = \dots = r_1$, the formula for the radii of the circles $C_{n-1}, C_{n-2}, \dots, C_1$ when n is odd is given by:

$$r_{\text{odd}} = \frac{\left|\cos\left[\frac{(2j+1)\pi}{4j}\right]\right|}{\cos\left(\frac{\pi}{4j}\right)}, \quad n = 2j + 1.$$

- (8) Let $n = 2j$. Here the centers subtain counter-clockwise angles relative to the positive real axis

$$\theta_{n-1} = \frac{j\pi}{2j-1}, \theta_{n-2} = \frac{(j+1)\pi}{2j-1}, \dots, \theta_1 = \frac{(j+k)\pi}{2j-1}$$

where $k = 0, 1, \dots, 2(j-1)$ and j depends on n . Similar calculations as those in (7) with $\psi_{n-1} = \frac{\pi}{2(2j-1)}$ give :

$$w_{n-1} = \frac{1}{\cos\left(\frac{\pi}{2(2j-1)}\right)} \left\{ \cos\left(\frac{j\pi}{2j-1}\right) + i \sin\left(\frac{j\pi}{2j-1}\right) \right\}.$$

But $\frac{\sin\left(\frac{j\pi}{2j-1}\right)}{\cos\left(\frac{\pi}{2(2j-1)}\right)} = 1$ so that $w_{n-1} = \frac{\cos\left(\frac{j\pi}{2j-1}\right)}{\cos\left(\frac{\pi}{2(2j-1)}\right)} + i$. Now

$$r_{n-1} = |w_{n-1} - A_n| = \frac{\left|\cos\left(\frac{j\pi}{2j-1}\right)\right|}{\cos\left(\frac{\pi}{2(2j-1)}\right)}.$$

Since $r_{n-1} = r_{n-2} = \dots = r_1$ the formulas for the radii of the circles $C_{n-1}, C_{n-2}, \dots, C_1$ is given by

$$r_{\text{even}} = \frac{\left|\cos\left(\frac{j\pi}{2j-1}\right)\right|}{\cos\left(\frac{\pi}{2(2j-1)}\right)}, \quad n = 2j.$$

- (9) A rough picture [Figure 3] showing some of the features described in items (1) to (8) is as follows:

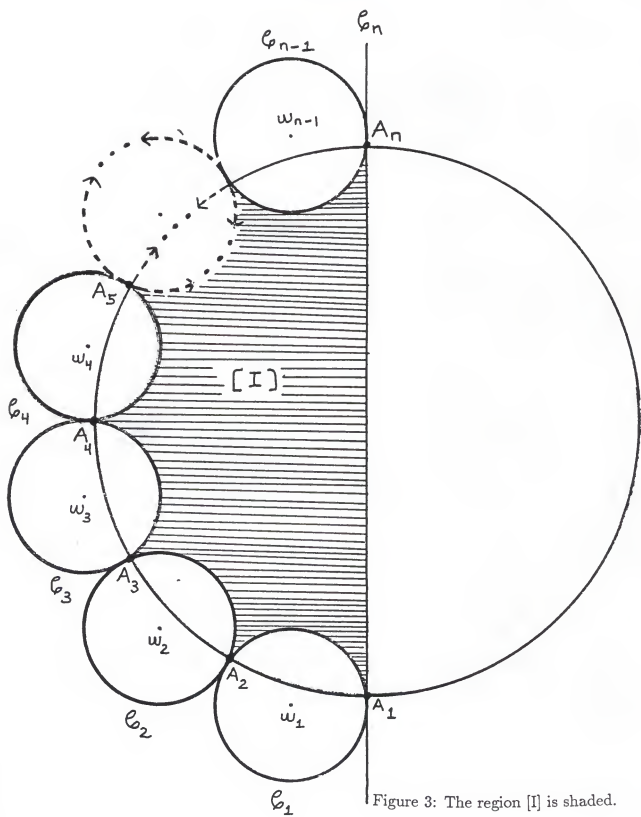


Figure 3: The region [I] is shaded.

- (10) Define "inversion through the boundary of a circle C_j " to be the mapping $T_j: \dot{C} \rightarrow \dot{C}$ defined by $(z)T_j = w_j + \frac{r_j^2}{\bar{z} - \bar{w}_j}$ where $1 \leq j \leq n-1$. Let "inversion through the boundary of the "circle" C_n " be the mapping $T_n: \dot{C} \rightarrow \dot{C}$ defined by $T_n(z) = -\bar{z}$. Define the mappings $S_i: \dot{C} \rightarrow \dot{C}$, $1 \leq i \leq n$ as follows:

$$\begin{aligned}(z)S_1 &= (z)T_n T_1 = ((z)T_n) T_1 \\(z)S_2 &= (z)T_1 T_2 = ((z)T_1) T_2 \\&\vdots \\(z)S_n &= (z)T_{n-1} T_n = ((z)T_{n-1}) T_n.\end{aligned}$$

Denote the images of [I] via S_1, S_2, \dots, S_n by $[S_1], [S_2], \dots, [S_n]$.

- (11) If we now shade the regions $[S_1], [S_2], \dots, [S_n]$, a pattern of shaded and unshaded polygons is produced. The unshaded regions correspond to the applications of the mappings T_j to the region [I]. We could denote these unshaded regions by $[T_1], [T_2], \dots, [T_n]$ but prefer not to do it. Observe that the composition of an even number of mappings T_j applied to [I] produces shaded regions. Similarly the composition of an odd number of mappings T_j applied to [I] produces unshaded regions. The pattern of shaded and unshaded polygons so produced covers the interior of the circle C without overlapping thus producing a so-called "tessellation" of C .

In general if σ is a product $T_{i_1} \dots T_{i_k}$ with k even, we denote the image of [I] under σ by $[\sigma]$. The regions $[\sigma]$ will often be referred to as "tiles".

- (12) The images of the vertices A_1, A_2, \dots, A_n under the mappings S_j , $1 \leq j \leq n$ (including composition of these mappings) are labeled again by A_1, A_2, \dots, A_n accordingly instead of $(A_i)S_j$.
- (13) The following figures are diagrams for the case $n = 3$. In Figure 4 we refer to the set of polygons $[S_3^{-1}], [S_2], [S_2^{-1}], [S_1], [S_1^{-1}]$ and $[S_3]$ depicted as a "first level of tessellation". In Figure 5 we illustrate a "second level of tessellation". The exterior of C is omitted for simplicity. Some additional properties of \mathcal{F} for the case $n = 3$ can be found in the Appendix.

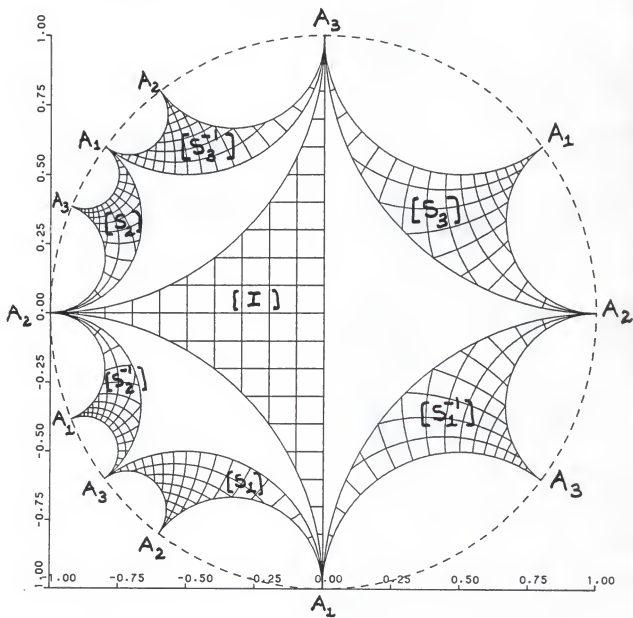


Figure 4

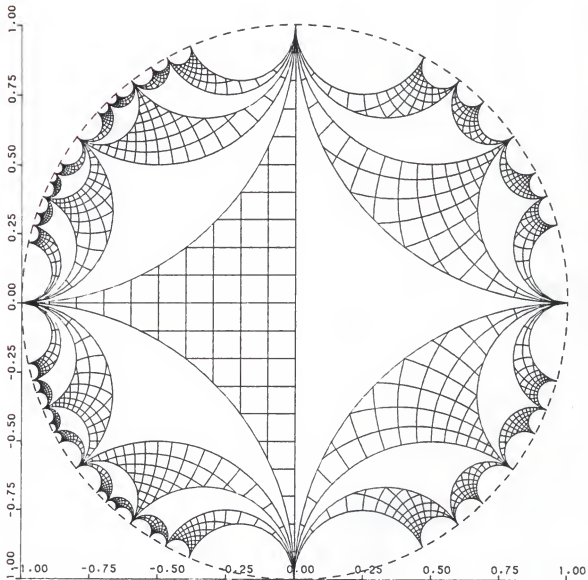


Figure 5

SECTION III. GROUP STRUCTURE OF THE SETS $\langle T_1, T_2, \dots, T_n \rangle$, $\langle S_1, S_2, \dots, S_n \rangle$ AND THEIR RELATION TO THE GROUP OF MÖBIUS TRANSFORMATIONS.

Having defined the mappings T_j and S_j , $1 \leq j \leq n$ in the previous section, we now form the following group with function composition as binary operation:

$$\begin{aligned} \mathcal{F} &= \text{Group generated by the mappings } S_1, S_2, \dots, S_n \\ &= \langle S_1, S_2, \dots, S_n \rangle. \end{aligned}$$

We also form the set $T_n \mathcal{F} = T_n \langle S_1, S_2, \dots, S_n \rangle$. Define

$$\dot{\mathcal{F}} = \mathcal{F} \cup T_n \mathcal{F}$$

Let

$$\begin{aligned} \mathcal{M} &= \text{Group of Möbius Transformations; see [6]} \\ &= \left\{ (z)S = \frac{az+b}{cz+d} : a, b, c, d, z \in \mathbb{C} \cup \{\infty\} \text{ and } ad - bc = 1 \right\}. \end{aligned}$$

Let $\overline{\mathcal{M}} =$ Set of conjugates of Möbius Transformations. (By definition, a conjugate of Möbius Transformation is a mapping $T : \dot{\mathbb{C}} \rightarrow \dot{\mathbb{C}}$ of the form

$$(z)T = \frac{a\bar{z}+b}{c\bar{z}+d}, \quad ad - bc = 1.)$$

Define $\dot{\mathcal{M}} = \mathcal{M} \cup \overline{\mathcal{M}}$. Let $\dot{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. We will see that $\dot{\mathcal{M}}$ is a group (a subgroup of the group $S_{\dot{\mathbb{C}}}$ of permutations in $\dot{\mathbb{C}}$.) Fix the mapping $\dot{T} \in \overline{\mathcal{M}}$ given by $(z)\dot{T} = -\bar{z}$. Define the set $\dot{T}\mathcal{M} = \left\{ \dot{T}S : S \in \mathcal{M} \right\}$.

In this section we develop some of the elementary properties of \mathcal{F} , $\dot{\mathcal{F}}$, and $\dot{\mathcal{M}}$. We will establish next, the following theorems:

Theorem 1: $\dot{\mathcal{M}}$ is a group and \mathcal{M} is a group of index 2 in $\dot{\mathcal{M}}$, i.e. $|\dot{\mathcal{M}} : \mathcal{M}| = 2$.

Theorem 2: $\dot{\mathcal{F}}$ is a group and \mathcal{F} is a group of index 2 in $\dot{\mathcal{F}}$, i.e. $|\dot{\mathcal{F}} : \mathcal{F}| = 2$.

Theorem 3: $\mathcal{F} = \dot{\mathcal{F}} \cap \mathcal{M}$.

Theorem 1 will be proved by showing the following lemmas:

Lemma 1: $\overline{\mathcal{M}} = \dot{T} \mathcal{M}$.

Lemma 2: $\mathcal{M} \neq \overline{\mathcal{M}}$.

Theorem 2 will be proved by showing the following lemmas:

Lemma 3: $\mathcal{F} = \{ \text{All words of even length in } T_1, T_2, \dots, T_n \}$ and $\mathcal{F} \subseteq \mathcal{M}$.

Lemma 4: $T_n \mathcal{F} = \{ \text{All words of odd length in } T_1, T_2, \dots, T_n \}$ and $T_n \mathcal{F} \subseteq \dot{T} \mathcal{M}$.

Once we establish the above, then we will be able to say that

$$\begin{aligned} \dot{\mathcal{F}} &= \text{Group generated by } T_1, T_2, \dots, T_n \\ &= \langle T_1, T_2, \dots, T_n \rangle \end{aligned}$$

Finally, the proof of Theorem 3 will follow using Set Theory.

Lemma 1: $\overline{\mathcal{M}} = \dot{T} \mathcal{M}$.

Proof: Let $(z)\overline{S} = \frac{a\overline{z} + b}{c\overline{z} + d} \in \overline{\mathcal{M}}$. Then $\exists (z)S' = \frac{-az + b}{-cz + d} \in \mathcal{M}$ such that $(z)\overline{S} = \frac{a\overline{z} + b}{c\overline{z} + d} = \frac{-a(-\overline{z}) + b}{-c(-\overline{z}) + d} = (-\overline{z})S' = \left((z)\dot{T} \right) S' = (z)\dot{T} S' \in \dot{T} \mathcal{M}$. Hence $\overline{\mathcal{M}} \subseteq \dot{T} \mathcal{M}$. On the other hand, let $\dot{T} S \in \dot{T} \mathcal{M}$. Then $(z)\dot{T} S = \left((z)\dot{T} \right) S = (-\overline{z})S' = \frac{-a\overline{z} + b}{-c\overline{z} + d} \in \overline{\mathcal{M}}$. Hence $\dot{T} \mathcal{M} \subseteq \overline{\mathcal{M}}$.

Lemma 2: $\mathcal{M} \neq \overline{\mathcal{M}}$.

Proof: Any Möbius Transformation is analytic everywhere in $\dot{\mathbb{C}}$ (except at its pole $z = -\frac{d}{c}$). On the other hand, the function $(z) \overset{\cdot}{T} = -\bar{z}$ is not analytic at any point in $\dot{\mathbb{C}}$.

Theorem 1: $|\overset{\cdot}{\mathcal{M}}: \mathcal{M}| = 2$.

Proof: By direct computation, $\overset{\cdot}{\mathcal{M}}$ is closed under composition and the taking of inverses. Hence, $\overset{\cdot}{\mathcal{M}}$ is a group (subgroup of the group $S_{\dot{\mathbb{C}}}$ of permutations in $\dot{\mathbb{C}}$.) Clearly, \mathcal{M} is a subgroup of $\overset{\cdot}{\mathcal{M}}$. We also have $\overline{\overset{\cdot}{\mathcal{M}}} = \overset{\cdot}{T} \mathcal{M} \subseteq \overset{\cdot}{\mathcal{M}}$ with $\mathcal{M} \neq \overset{\cdot}{T} \mathcal{M}$. Therefore $|\overset{\cdot}{\mathcal{M}}: \mathcal{M}| = 2$.

Lemma 3: $\mathcal{F} = \text{Set of all words of even length in } T_1, T_2, \dots, T_n \text{ and } \mathcal{F} \subseteq \mathcal{M}$.

Proof: First we show that $\{\text{words of even length in } T_1, T_2, \dots, T_n\} \subseteq \mathcal{F}$. Let w be an arbitrary non-trivial word in T_1, T_2, \dots, T_n . Let ℓ denote the length of w with respect to T_1, T_2, \dots, T_n . We have two cases to consider; namely $\ell = 2$ and $\ell > 2$.

Let $\ell = 2$ and consider $w = T_i T_j \in \overset{\cdot}{F}$ where $1 \leq i \leq n$, and $1 \leq j \leq n$. If $i = j$ then $w = (T_i)^2 = I$ and so $w \in \mathcal{F}$. If $i < j$ then

$$\begin{aligned} w &= T_i(T_{i+1}T_{i+1})(T_{i+2}T_{i+2}) \cdots (T_{j-1}T_{j-1})T_j \\ &= (T_i T_{i+1})(T_{i+1}T_{i+2}) \cdots (T_{j-1}T_j) \\ &= S_{i+1}S_{i+2} \cdots S_j \in \mathcal{F}. \end{aligned}$$

If $i > j$ then

$$\begin{aligned} w &= T_i(T_{i-1}T_{i-1})(T_{i-2}T_{i-2}) \cdots (T_{j+1}T_{j+1})T_j \\ &= (T_i T_{i-1})(T_{i-1}T_{i-2}) \cdots (T_{j+1}T_j) \\ &= S_{i-1}^{-1}S_{i-2}^{-1} \cdots S_{j+1}^{-1} \in \mathcal{F}. \end{aligned}$$

This concludes the proof of our first case.

Now let $\ell > 2$ and consider $w = T_{i_1}T_{i_2}T_{i_3}T_{i_4} \cdots T_{i_{2k-1}}T_{i_{2k}}$ with $i_1, i_2, \dots, i_{2k-1}, i_{2k} \in$

$\{1, 2, \dots, n\}$. Then we can associate the first k -pairs of w as follows:

$$w = (T_{i_1} T_{i_2})(T_{i_3} T_{i_4}) \cdots (T_{i_{2k-1}} T_{i_{2k}}).$$

From the previous case, we know that each pair above belongs to \mathcal{F} . Hence the product of the k -pairs is also in \mathcal{F} . Therefore $w \in \mathcal{F}$. This concludes the proof of our second case.

We now show that $\mathcal{F} \subseteq \{\text{words of even length in } T_1, T_2, \dots, T_n\}$. Since each S_i is a word of even length in T_1, T_2, \dots, T_n then it is clear that the product of n of these words is also a word of even length.

Finally we want to show that $\mathcal{F} \subseteq \mathcal{M}$. We are dealing with mappings $(z)T_j = w_j + \frac{r^2}{\bar{z} - \bar{w}_j}$, $1 \leq j \leq n-1$, $(z)T_n = -\bar{z}$. Our mappings S_j defined in terms of these T_j 's in section II can always be put in the form $(z)S = \frac{az+b}{cz+d}$ and can be identified as Möbius Transformations. Pick $x \in \mathcal{F}$. Then $x = \text{word of even length in } T_1, T_2, \dots, T_n$ i.e. x is formed by composing functions of the form $(z)T_j$ an even number of times. Hence x is of the form $(z)S = \frac{az+b}{cz+d} \in \mathcal{M}$. Therefore $\mathcal{F} \subseteq \mathcal{M}$. This concludes the proof of Lemma 3.

Lemma 4: $T_n \mathcal{F} = \text{Set of all words of odd length in } T_1, T_2, \dots, T_n \text{ and } T_n \mathcal{F} \subseteq \bar{T} \mathcal{M}$.

Proof: We first show that $\{\text{words of odd length in } T_1, T_2, \dots, T_n\} \subseteq T_n \mathcal{F}$. Let w be an arbitrary, non-trivial word in T_1, T_2, \dots, T_n and let ℓ denote the length of w with respect to T_1, T_2, \dots, T_n . We have two cases to consider; namely $\ell = 1$ and $\ell > 1$.

Let $\ell = 1$ and consider $w = T_i \in \bar{\mathcal{F}}$ with $1 \leq i \leq n$. Now notice that:

$$\begin{aligned} T_1 &= (T_n T_n)(T_{n-1} T_{n-1}) \cdots (T_2 T_2) T_1 \\ &= T_n (T_n T_{n-1}) \cdots (T_2 T_1) \\ &= T_n S_n^{-1} \cdots S_1^{-1} \end{aligned}$$

$$\begin{aligned} T_2 &= (T_n T_n)(T_{n-1} T_{n-1}) \cdots (T_3 T_3) T_2 \\ &= T_n (T_n T_{n-1}) \cdots (T_3 T_2) \\ &= T_n S_n^{-1} \cdots S_2^{-1} \end{aligned}$$

\vdots

$$\begin{aligned} T_{n-1} &= (T_n T_n) T_{n-1} = T_n (T_n T_{n-1}) = T_n S_n^{-1} \\ T_n &= T_n I. \end{aligned}$$

In this way we have managed to recognize each element T_i in $\bar{\mathcal{F}}$ as some element in $T_n \mathcal{F}$.

Now let $\ell > 1$ and consider $w = T_{i_1} T_{i_2} T_{i_4} \dots T_{i_{2k}} T_{i_{2k+1}}$ where $i_1, i_2, \dots, i_{2k}, i_{2k+1} \in \{1, 2, \dots, n\}$. Now associate the first k pairs leaving the term T_{2k+1} disassociated. By Lemma 3 we know that the product of the k pairs belong to \mathcal{F} . Also by the previous case above, we know that $T_{i_{2k+1}} = T_n S_n^{-1} \dots S_{2k+1}^{-1}$ belongs to $T_n \mathcal{F}$. Therefore $w \in T_n \mathcal{F}$. This concludes the proof of our second case.

We now show that $T_n \mathcal{F} \subseteq \overset{\cdot}{T} \mathcal{M}$. Pick $x = T_n Y$ with $Y \in \mathcal{F}$. Now $Y \in \mathcal{M}$ by Lemma 3 and $\overset{\cdot}{T} = T_n = -\bar{z}$. Hence $x \in \overset{\cdot}{T} \mathcal{M}$. Therefore $T_n \mathcal{F} \subseteq \overset{\cdot}{T} \mathcal{M}$. This concludes the proof of Lemma 4.

Theorem 2: $|\overset{\cdot}{F}: F| = 2$.

Proof: $\overset{\cdot}{F}$ is a group generated by T_1, T_2, \dots, T_n . \mathcal{F} is a subgroup of $\overset{\cdot}{F}$ because it is generated by words in T_1, T_2, \dots, T_n of even length. We also have $T_n \mathcal{F}$ in $\overset{\cdot}{F}$ with $\mathcal{F} \neq T_n \mathcal{F}$ by Lemmas 3 and 4. Therefore $|\overset{\cdot}{F}: \mathcal{F}| = 2$.

Theorem 3: $\mathcal{F} = \overset{\cdot}{F} \cap \mathcal{M}$.

Proof: We have defined $\overset{\cdot}{F} = \mathcal{F} \cup T_n \mathcal{F}$. Now $\overset{\cdot}{F} \cap \mathcal{M} = (\mathcal{F} \cup T_n \mathcal{F}) \cap \mathcal{M} = (\mathcal{F} \cap \mathcal{M}) \cup (T_n \mathcal{F} \cap \mathcal{M})$. Next since $\mathcal{F} \subseteq \mathcal{M}$ we have $\mathcal{F} \cap \mathcal{M} = \mathcal{F}$. Similarly, since $T_n \mathcal{F} \subseteq \overline{\mathcal{M}}$ and $\mathcal{M} \cap \overline{\mathcal{M}} = \phi$ we have that $T_n \mathcal{F} \cap \mathcal{M} = \phi$. Therefore $\overset{\cdot}{F} \cap \mathcal{M} = \mathcal{F} \cup \phi = \mathcal{F}$.

Remark : $\mathcal{F} \neq \mathcal{M}$.

Proof: $\mathcal{F} = \{S_1\} \cup \{S_1, S_2\} \cup \{S_1, S_2, S_3\} \cup \dots$ is a countable union of countable sets and therefore itself a countable set. On the other hand, \mathcal{M} is uncountable since we can form the subset $\{(z)S|(z)S = r + z, r \in \mathbb{R}\}$ which is uncountable. Therefore $\mathcal{F} \neq \mathcal{M}$.

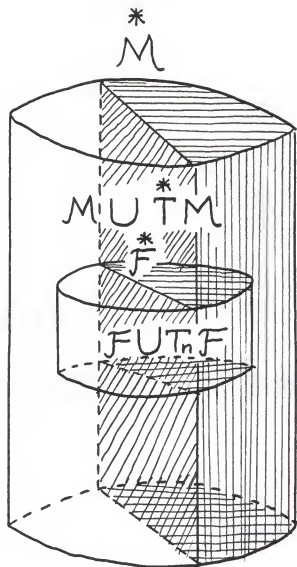


Figure 6: \bar{M}

SECTION IV. MORE PROPERTIES OF THE GROUP \mathcal{F} , WITH $n = 3$.

Remark : We continue the notation of the preceding sections, specializing to the case where $n = 3$. Thus, we are in the situation indicated by figures 4 and 5, on pages 26 and 27.

Definition: Let \mathcal{D} be a circle in $\dot{\mathcal{C}}$. Then $\dot{\mathcal{C}} - \mathcal{D}$ consists of two connected components, namely $\text{Ext}\mathcal{D}$ and $\text{Int}\mathcal{D}$. Let X be a subset of $\dot{\mathcal{C}}$ and let $\Sigma \in \mathcal{F}$. We say that Σ carries X across \mathcal{D} if X lies in one connected component of $\dot{\mathcal{C}} - \mathcal{D}$ and $\Sigma^{-1}X\Sigma$ lies in the other.

Lemma 1: *Let $\Sigma \in \mathcal{F}$ and let \mathcal{D} be a circle in $\dot{\mathcal{C}}$. Then $\dot{\mathcal{C}} - \mathcal{D}$ has precisely two connected components X_1 and X_2 and $\dot{\mathcal{C}} - (\mathcal{D})\Sigma$ has precisely two connected components $Y_1 = (X_1)\Sigma$ and $Y_2 = (X_2)\Sigma$.*

Proof: Notice that $\dot{\mathcal{C}} - \mathcal{D}$ has precisely two connected components, namely $X_1 = \text{Int}(\mathcal{D})$ and $X_2 = \text{Ext}(\mathcal{D})$. Let $Y_1 = (X_1)\Sigma$ and $Y_2 = (X_2)\Sigma$ denote the images of X_1 and X_2 respectively under the mapping Σ . Let $A, B \in X_2$ and let γ be a path joining these points in X_2 . Assume $(B)\Sigma \in Y_1$ and $(A)\Sigma \in Y_2$. Since Σ is a continuous mapping, there exists a path $(\gamma)\Sigma$ joining the points $(A)\Sigma$ and $(B)\Sigma$ in $(\gamma)\Sigma$. Notice that $(\gamma)\Sigma$ passes through a point $Q \in (\mathcal{D})\Sigma$. Now since Σ is a bijection, there exists a point $P \in \mathcal{D}$, $P \in \gamma$ such that $Q = (P)\Sigma$. But, $\gamma \cap \mathcal{D} = \emptyset$. This contradicts our assumption that $(B)\Sigma \in Y_1$ and $(A)\Sigma \in Y_2$. Hence either $(A)\Sigma, (B)\Sigma \in Y_1$ or $(A)\Sigma, (B)\Sigma \in Y_2$. Therefore $\dot{\mathcal{C}} - (\mathcal{D})\Sigma$ has precisely two connected components $Y_1 = (X_1)\Sigma$ and $Y_2 = (X_2)\Sigma$.

Lemma 2: *Let $\Sigma \in \mathcal{F}$. Then $(\Sigma)^{-1}S_i\Sigma$, $i \in \{1, 2, 3\}$ carries $[\Sigma]$ across a circle on the boundary of $[\Sigma]$.*

Proof: First, apply Σ^{-1} to $[\Sigma]$ to carry $[\Sigma]$ to $[I]$. Second, apply S_i , $i \in \{1, 2, 3\}$ to $[I]$ to carry $[I]$ across a circle C_i , $i \in \{1, 2, 3\}$ on the boundary of $[I]$. Notice that $[I]$ and $[I]S_i = [S_i]$ lie in different connected components of $\dot{\mathcal{C}} - C_i$. Third, apply Σ to $[I]$ and $[I]S_i$. Using Lemma 2 with C_i in the role of \mathcal{D} ,

we conclude that $[I]\Sigma = [\Sigma]$ and $([I]S_i)\Sigma = [\Sigma](\Sigma^{-1}S_i\Sigma)$ lie in two different connected components of $\dot{\mathbf{C}} - (C_i)\Sigma$. That is, $(\Sigma)^{-1}S_i\Sigma$ carries $[\Sigma]$ across the circle $(C_i)\Sigma$ on the boundary of $[\Sigma]$.

Theorem 1: *Let $\Sigma \in \mathcal{F}$, let \mathcal{D} be one of the three circles on the boundary of $[\Sigma]$ and let $(S_{i_1}, \dots, S_{i_n})$ be a reduced word in $\{S_1, S_2, S_3\}$. Then $\Sigma^{-1}S_{i_1} \dots S_{i_n}\Sigma$ carries $[\Sigma]$ across \mathcal{D} if and only if $\Sigma^{-1}S_{i_n}\Sigma$ does.*

Proof: (By induction on n .) Refer to the picture on page 36.

The theorem is trivially true if $n = 1$, so assume the theorem is true for all k , $1 \leq k \leq n - 1$. We must show that this assumption implies the statement of the theorem for $k = n$. First consider the case where $\Sigma = I$. Now, S_{i_n} carries $[I]$ across a circle \mathcal{D} on the boundary of $[I]$ to the tile $[S_{i_n}]$. Let $g = S_{i_1} \dots S_{i_n}$. Notice that

$$\begin{aligned} g &= (S_{i_n}S_{i_n}^{-1})S_{i_1} \dots S_{i_n} \\ &= S_{i_n}S_{i_n}^{-1}(S_{i_1} \dots S_{i_{n-1}})S_{i_n}. \end{aligned}$$

Put $\Sigma' = S_{i_n}$ and $g' = S_{i_1} \dots S_{i_{n-1}}$. Thus $g = S_{i_n}(\Sigma')^{-1}g'\Sigma'$. Now $[S_{i_n}] = [\Sigma']$ has three bounding circles. We next show that $(\Sigma')^{-1}g'\Sigma'$ carries $[\Sigma']$ across one of these circles.

By Lemma 2 $(\Sigma')^{-1}S_{i_{n-1}}\Sigma'$ carries $[\Sigma']$ across one of these circles, say \mathcal{D}' . By our inductive hypothesis $(\Sigma')^{-1}S_{i_1} \dots S_{i_{n-1}}\Sigma'$ carries $[\Sigma']$ across \mathcal{D}' provided that $(\Sigma')^{-1}S_{i_{n-1}}\Sigma'$ does. Hence by induction we conclude that $(\Sigma')^{-1}g'\Sigma'$ carries $[\Sigma']$ across \mathcal{D}' .

We next observe that two of the choices for \mathcal{D}' entail carrying $[\Sigma']$ into $\text{Int}(\mathcal{D}')$ with the remaining choice carrying $[\Sigma']$ into $\text{Ext}(\mathcal{D}')$. In detail, if “carrying $[\Sigma']$ across \mathcal{D}^m ” means that $[\Sigma']$ is carried into $\text{Int}(\mathcal{D}')$, i.e. $(\Sigma')^{-1}g'\Sigma'$ carries $[\Sigma']$ into $\text{Int}(\mathcal{D}') \subset \text{Int}(\mathcal{D})$ then we are done since $g = \Sigma'(\Sigma')^{-1}g'\Sigma'$ subsequently carries $[I]$ into $\text{Int}(\mathcal{D})$. If “carrying $[\Sigma']$ across \mathcal{D}^m ” means instead that $[\Sigma']$ is carried into $\text{Ext}(\mathcal{D}')$ then g carries $[I]$ into $\text{Ext}(\mathcal{D}')$. Moreover, this uniquely determines \mathcal{D}' .

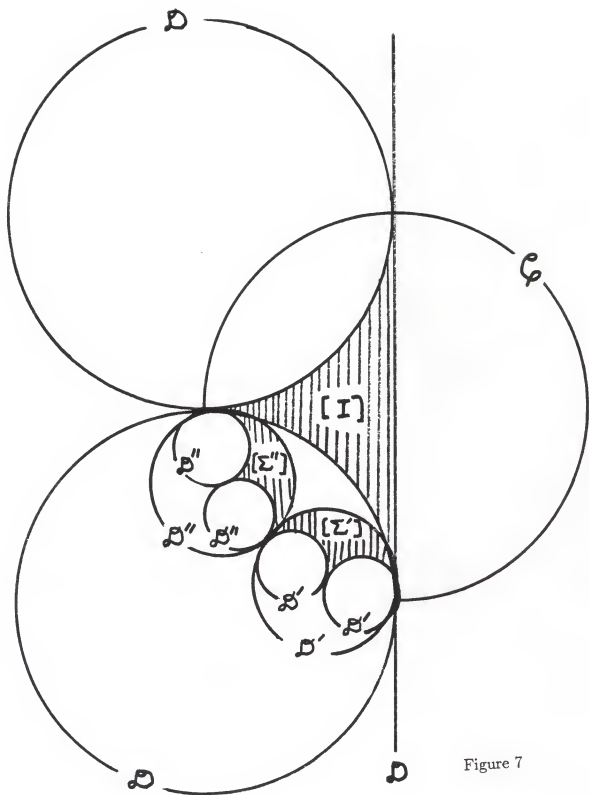


Figure 7

Next notice that $S_{i_n}^{-1}S_{i_{n-1}}S_{i_n}$ carries $[S_{i_n}]$ to the tile $[S_{i_{n-1}}S_{i_n}]$. Let $g = S_{i_{n-1}}S_{i_n}(S_{i_{n-1}}S_{i_n})^{-1}(S_{i_1}\dots S_{i_{n-2}})S_{i_{n-1}}S_{i_n}$. Put $\Sigma'' = S_{i_{n-1}}S_{i_n}$ and $g'' = S_{i_1}\dots S_{i_{n-2}}$. Thus $g = S_{i_{n-1}}S_{i_n}(\Sigma'')^{-1}g''\Sigma''$. Now $[S_{i_{n-1}}S_{i_n}] = [\Sigma'']$ has three bounding circles. By Lemma 2, $(\Sigma'')^{-1}S_{i_{n-2}}\Sigma''$ carries $[\Sigma'']$ across one of these circles, say \mathcal{D}'' .

As in the preceding case, we use our inductive hypothesis to add that $(\Sigma'')^{-1}g''\Sigma''$ carries $[\Sigma'']$ across \mathcal{D}'' . Two of these choices for \mathcal{D}'' entail carrying $[\Sigma'']$ into $\text{Int}(\mathcal{D}'') \subset \text{Int}(\mathcal{D})$ and $g = \Sigma''((\Sigma'')^{-1}g''\Sigma'')$ subsequently carries $[I]$ into $\text{Int}(\mathcal{D})$. On the other hand, if “carrying $[\Sigma'']$ across \mathcal{D}'' means that $[\Sigma'']$ is carried into $\text{Ext}(\mathcal{D}'')$ then a glance at the picture should convince the reader that $[\Sigma'']$ is thereby carried into $[I]$.

The case $\Sigma \neq I$ is similar. Conjugation transfers the situation discussed in the previous case, to some other region of our geometric model, and once there we follow a similar argument.

Corollary 1: Let $\Sigma \in \mathcal{F}$. Then there is a unique sequence of tiles $[I] = [X_0]$, $[X_1], \dots, [X_n] = [\Sigma]$ where $X_j \in \mathcal{F}$, $(0 \leq j \leq n)$ and such that for all j , $(0 \leq j \leq n-1)$ we have $[X_{j+1}] = [X_j]X_{j+1}^{-1}S_{i_{n-j}}X_j = [S_{i_{n-j}}X_j]$ for some reduced word $(S_{i_1}, \dots, S_{i_n})$ in $\{S_1, S_2, S_3\}$.

Proof: Consider the sequence of tiles

$$[X_0] = [I]$$

$$[X_1] = [S_{j_n}]$$

$$[X_2] = [S_{j_{n-1}}S_{j_n}]$$

$$\vdots$$

$$[X_n] = [S_{j_1}\dots S_{j_{n-1}}S_{j_n}].$$

Put $X_0 = I$ and $X_k = S_{j_{n-k+1}}\dots S_{j_n}$, $(k = 1, \dots, n)$. Then the above sequence of tiles can be described in an iterative way as follows:

$$[X_0] = [I]$$

$$[X_{k+1}] = [X_k]X_k^{-1}S_{j_{n-k}}X_k = [S_{i_{n-k}}X_k], (k = 0, \dots, n-1).$$

Hence, the existence of the sequence as in the statement of the corollary is established.

To show that this sequence is unique, let $[I] = [X'_0], \dots, [X'_m] = [\Sigma]$ be another such sequence, with associated reduced word $(S'_{j'_1}, \dots, S'_{j'_m})$ for Σ . Suppose that there exists $k \leq n$ such that $[X_{k+1}] \neq [X'_{k+1}]$. Let k be the first such index. Then $X_k = X'_k$ and $[X_k]X_k^{-1}S_{i_{n-k}}X_k \neq [X_k]X_k^{-1}S'_{j'_{m-k}}X_k$ since

$S_{i_{n-k}} = X_{k+1}X_k^{-1}$ and $S'_{j_{m-k}} = X'_{k+1}(X'_k)^{-1}$. This means that $X_k^{-1}S_{i_{n-k}}X_k$ carries $[X_k]$ across a circle \mathcal{D} on the boundary of $[X_k]$ while $X_k^{-1}S'_{j_{m-k}}X_k$ carries $[X_k]$ across a different circle \mathcal{D}' on the boundary of $[X_k]$. Theorem 1 then says that $X_k^{-1}(S_{i_1} \dots S_{i_{n-k}})X_k$ carries $[X_k]$ across \mathcal{D} while $X_k^{-1}(S'_{j_1} \dots S'_{j_{m-k}})X_k$ carries $[X_k]$ across \mathcal{D}' . Then $[X_k]X_k^{-1}S_{i_1} \dots S_{i_{n-k}}X_k \neq [X_k]X_k^{-1}S'_{j_1} \dots S'_{j_{m-k}}X_k$ implying that $[S_{i_1} \dots S_{i_{n-k}}X_k] \neq [S'_{j_1} \dots S'_{j_{m-k}}X_k]$, that is $[\Sigma] \neq [\Sigma']$ which is false. Thus $[X_{k+1}] = [X'_{k+1}]$ and we conclude that $X_k = X'_k$ for all k , $k \leq n$.

We now show that $n = m$. Now,

$$\begin{aligned} [\Sigma] = [X'_n] &= X'_n^{-1}(S'_{j_1} \dots S'_{j_{m-n}})X'_n \\ &= [S'_{j_1} \dots S'_{j_{m-n}}X'_n] \\ &= [S'_{j_1} \dots S'_{j_{m-n}}S'_{j_{m-n+1}} \dots S'_{j_m}] \\ &= [S'_{j_1} \dots S'_{j_m}]. \end{aligned}$$

This contradicts Theorem 1 if $m \neq n$. Therefore the uniqueness of the sequence is established.

Corollary 2: Let $\Sigma \in \mathcal{F}$. Then there exists a unique reduced word in $\{S_1, S_2, S_3\}$ such that $\Sigma = S_{i_1} \dots S_{i_n}$.

Proof: Let $(S_{i_1}, \dots, S_{i_n})$ be a reduced word in $\{S_1, S_2, S_3\}$ such that $\Sigma = S_{i_1} \dots S_{i_n}$. Suppose $(S'_{j_1}, \dots, S'_{j_m})$ is a reduced word in $\{S_1, S_2, S_3\}$ such that $\Sigma = S_{j_1} \dots S_{j_m}$. Put $Y_k = S'_{j_{m-k+1}} \dots S'_{j_m}$, ($k = 1, \dots, m$) and $Y_0 = I$. Then

$$[Y_{k+1}] = [Y_k]Y_k^{-1}S'_{i_{n-k}}Y_k = [S'_{j_{m-k}}Y_k].$$

By Corollary 1, $m = n$ and $X_i = Y_i$ for all i . Thus $S_{i_{n-k}} = X_{k+1}X_k^{-1} = Y_{k+1}Y_k^{-1} = S'_{j_{m-k}}$. Therefore $(S_{i_1} \dots S_{i_n}) = (S'_{j_1} \dots S'_{j_m})$.

Lemma 4: Let $S = (S_{i_1}, \dots, S_{i_n})$ be a word in S_1, S_2, S_3 (reduced or otherwise). Let $\Sigma = S_{i_1} \dots S_{i_n}$. Then $(\Sigma)\phi = X_{i_1} \dots X_{i_n}$.

Proof: (By induction on n).

Assume that S is not reduced. Then $S = (S_{i_1}, \dots, S_{i_{k-1}}, S_{i_k}, S_{i_{k+1}}, \dots, S_{i_n})$ where $S_{i_{k-1}}S_{i_k}S_{i_{k+1}} = I_{\mathcal{F}}$. Consider the shorter word S_0 obtained by deleting $S_{i_{k-1}}, S_{i_k}, S_{i_{k+1}}$ in S , that is $S_0 = (S_{i_1}, \dots, S_{i_{k-2}}, S_{i_{k+2}}, \dots, S_{i_n})$. Observe that $\Sigma = S_{i_1} \dots S_{i_{k-2}}S_{i_{k+2}} \dots S_{i_n}$. By induction on n $(\Sigma)\phi = X_{i_1} \dots X_{i_{k-2}}X_{i_{k+2}} \dots X_{i_n}$. But also

$$\begin{aligned} I_G &= X_{i_{k-2}} X_{i_k} X_{i_{k+1}}, \text{ so } (\Sigma) \phi = (X_{i_1} \dots X_{i_{k-1}}) I_G (X_{i_{k+2}} \dots X_{i_n}) \\ &= X_{i_1} \dots X_{i_n}. \end{aligned}$$

Next, the lemma is clearly true if \mathcal{S} is reduced.

We will now show that \mathcal{F} is a free group on $\{S_1, S_2\}$ in the modern sense.

Definition: Let F be a group and let X be a subset of F . We say that F is free on X if, whenever $\phi : X \mapsto G$ is a mapping of X into a group G , there exists a unique homomorphism $\Phi : F \mapsto G$ such that $\Phi|_X = \phi$.

Theorem 2: Let G be a group and let $X_1, X_2 \in G$. Then there exists a unique homomorphism $\phi : \mathcal{F} \rightarrow G$ such that $(S_i)\phi = X_i$, $i = 1, 2$. (That is \mathcal{F} is a "free group on two generators".)

Proof: Let $\Sigma \in \mathcal{F}$ and let $(S_{i_1}, \dots, S_{i_n})$ be the unique reduced word such that $\Sigma = S_{i_1} \dots S_{i_n}$. Define $(\Sigma)\phi = X_{i_1} \dots X_{i_n}$ where $X_3 = X_2^{-1} X_1^{-1}$. We now show that ϕ is a homomorphism. Let $(S_{i_1}, \dots, S_{i_n})$ and $(S_{j_1}, \dots, S_{j_m})$ be words in the generators S_1, S_2, S_3 for Σ and Σ' , respectively. Now $\Sigma \Sigma' = (S_{i_1}, \dots, S_{i_n}, S_{j_1}, \dots, S_{j_m})$ and this word might be reduced or otherwise. Next $(\Sigma \Sigma')\phi = X_{i_1} \dots X_{i_n} X_{j_1} \dots X_{j_m}$ by Lemma 4 and $(\Sigma)\phi(\Sigma')\phi = X_{i_1} \dots X_{i_n} X_{j_1} \dots X_{j_m}$ by definition of ϕ . Hence ϕ is a homomorphism.

Now to show that ϕ is unique, let $\psi : \mathcal{F} \rightarrow G$ be another homomorphism such that $(S_i)\psi = X_i$, $i = 1, 2$. Since $(I_{\mathcal{F}})\psi = (S_1 S_2 S_3)\psi = I_G$ then $(S_3)\psi = (S_2^{-1} S_1^{-1})\psi = X_2^{-1} X_1^{-1} = X_3$. Then also $(S_{i_1} \dots S_{i_n})\psi = X_{i_1} \dots X_{i_n}$, that is $\psi = \phi$.

Remark : With some extra effort one can get the same result for n number of generators.

Definition: A presentation is a description of a group in terms of elements that generate the group and relations satisfied by these generators.

Relation with Cayley's Dictum:

Let G be a group generated by elements X_1, \dots, X_n . Let \mathcal{F} be a free group on n generators S_1, \dots, S_n . Define $X_1 \dots X_{n+1} = I_G$ and $S_1 \dots S_{n+1} = I_{\mathcal{F}}$. We know that G is a homomorphic image of \mathcal{F} via $(S_i)\phi = X_i, i = 1, \dots, n$. Let K be the kernel of this homomorphism. Then K can be regarded as a list of "relations" concerning the generators X_1, \dots, X_n . Namely

$$S_{i_1} \dots S_{i_m} \in K \Leftrightarrow X_{i_1} \dots X_{i_m} = I_G.$$

Since $\frac{\mathcal{F}}{K} \cong G$ by the First Isomorphism Theorem we therefore have a "presentation" of G in terms of "rules of combinations of symbols" X_1, \dots, X_n in Cayley's sense.

CHAPTER V: DYCK'S 1882 PAPER

In the years of 1882 and 1883, Walter Dyck published a paper in two parts entitled *Gruppentheoretische Studien* (1882); see [7], and *Gruppentheoretische Studien II* (1883). According to Chandler and Magnus [5, p. 7] "Dyck's papers [1882 and 1883] contain ... the foundation of the theory of group presentations." They add

"But, the most noteworthy effect of Dyck's paper of 1882 is probably that from then on, the definition of a group through a presentation becomes a common feature in the literature."

Dyck's 1882 paper is divided into eight sections of which only three are relevant to this project, namely sections 1, 2 and 4.

In the first section, Dyck defines among other things the concept of a most general group G with m generating operations. This concept corresponds to that of a free group on m generators A_1, \dots, A_m (using modern terminology). As we shall see, his definition is not rigorous enough by today's standards and is open to ambiguity.

In the second section, Dyck attempts to construct a geometric model of the most general group. We have updated this construction in Chapter IV, sections II and IV and this concludes our consideration of this section.

The fourth section deals with the relationship between the most general group G with generators A_1, A_2, \dots, A_m and an arbitrary group \bar{G} with generators $\bar{A}_1, \bar{A}_2, \dots, \bar{A}_m$. Here, in a vague way, Dyck arrives at the foundations of the theory of group presentations.

We now consider sections 1 and 4 in detail.

The first section of Dyck's 1882 paper is entitled "Definition einer Gruppe G als Ausgangspunkt der Betrachtung", that is "Definition of a Group G as the Starting Point of the Investigation." We now quote a translation of this definition found in [5, p. 5-6]:

"Let $A_1, A_2, A_3, \dots, A_m$ be m operations of any kind which can be applied to an object J (identity) which, subsequently, will always be denoted by 2. Then these A_i may always be considered as the generating operations of a group which will be obtained by applying all operations on our object J in iteration and combinations.

The most general group with m generating operations will be obtained if we assume that the A_i do not have any periods and, in addition, are not connected mutually by any relation. We shall also consider the opposite operations of the A_i which we shall denote by A_i^{-1} . Then we obtain the infinitely many substitutions which belong to our group G if we apply to the thus resulting substitutions the same operations, and so on. Since we had assumed no relation between the generating operations, the substitutions thus produced are all distinct from

each other and each of them can be obtained only by one completely determined process from the generating substitutions. This is expressed by the formula

$$A_1^{\mu_1} A_2^{\mu_2} \dots A_1^{\nu_1} A_2^{\nu_2} \dots "$$

Here is to be understood that the exponents are not zero and that the identity is the only element that is not written in this fashion. The term "relation" is never defined precisely. Presumably what is meant by a "relation" is any combination of substitutions resulting in the identity element.

Dyck claims certain properties for this most general group. He claims that every nonidentity element can be written in a unique way in the form $A_1^{\mu_1} A_2^{\mu_2} \dots A_1^{\nu_1} A_2^{\nu_2} \dots$. It is difficult for the reader to justify this claim. One would like to say that the claim is an obvious consequence of G having no relations. The trouble is that there are relations as soon as the inverses are introduced.

The uniqueness question for representation of elements of G will be a source of trouble throughout the paper. There are various hints given that Dyck himself was not satisfied by his treatment of this question. The first indication of this dissatisfaction appears when he introduces the following artifice for avoiding the use of negative exponents. Here he introduces an additional generator A_n (with $n = m + 1$) and postulates that

$$A_1 A_2 A_3 \dots A_m A_n = 1. \quad (i)$$

Multiplying (i) from the left by A_1^{-1} gives:

$$A_2 A_3 \dots A_n = A_1^{-1}. \quad (ii)$$

Multiplying (ii) from the right by A_1 gives:

$$A_2 A_3 \dots A_n A_1 = 1. \quad (iii)$$

Multiplying (iii) from the left by A_2^{-1} gives:

$$A_3 A_4 \dots A_n A_1 = A_2^{-1}. \quad (iv)$$

Multiplying (iv) from the right by A_2 gives:

$$A_3 A_4 \dots A_n A_1 A_2 = 1.$$

In general, for $A_1, A_2, \dots, A_m, A_n$ with $A_1 A_2 A_3 \dots A_m A_n = 1$ we have

$$A_r^{-1} = A_{r+1} A_{r+2} \dots A_n A_1 A_2 \dots A_{r-1}$$

where $r = 1, 2, \dots, n$. This artifice does not solve the problem of uniqueness of expressions for elements. For example, suppose that we take two generators A_1, A_2 and then we introduce a third generator A_3 , so that $A_1 A_2 A_3 = 1$. Then we have many expressions for A_1 , namely $A_1 = (A_1 A_2 A_3) A_1 = A_1 (A_1 A_2 A_3) = \dots$, etcetera. Nevertheless, this method of removing negative exponents will play an important role in Dyck's geometric "construction" of the most general group.

In order to avoid the redundancy of expressions like $A_1 = (A_1A_2A_3)A_1 = A_1(A_1A_2A_3) = \dots$ we need some kind of notation of "reduced words". A modern treatment that seems closest to Dyck's original is given in [1]. We now proceed to sketch this treatment.

For any subgroup G and a non-empty subset X of G , a certain subgroup of G (denoted by $gp(X)$) is defined as follows:

$$gp(X) = \{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} | x_i \in X, \epsilon_i = \pm 1\}.$$

To avoid the situation where two different products of the form $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ give rise to the same element of G , the concept of a reduced product is introduced. A product $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$, where $\epsilon_i = \pm 1$ and $x_i \in X$ is said to be a reduced X -product if $x_i = x_{i+1}$ implies that $\epsilon_i \neq -\epsilon_{i+1}$.

Next, a lemma is stated and proved in [1, p. 245-246] showing that $gp(X)$ is the set of all products of the form $w = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$, $x_i \in X$, $\epsilon_i = \pm 1$, such that w is either equal to 1 or a reduced product in X ; that is:

Lemma : $gp(X) = \{w | w = 1 \text{ or } w = a \text{ reduced product in } X\}$.

The uniqueness of reduced words is built into their definition of a "group freely generated by a set" as follows:

Definition: A group G is said to be freely generated by the set $X \subseteq G$ if $X \neq \emptyset$ and

- (i) $gp(X) = G$
- (ii) two different reduced X -products define two different nonunit elements of G .

The above definition is in turn used to prove the following lemma:

Lemma : *A group F is freely generated by a set $X \neq \emptyset$, if and only if:*

- (a) $gp(X) = F$ and
- (b) no reduced X -product is equal to the identity element.

This concludes our consideration of the first section of the paper and now we move on to the fourth section.

The fourth section of Dyck's paper deals with the relationship between the most general group G , with generators A_1, A_2, \dots, A_m and an arbitrary group \bar{G} , with generators $\bar{A}_1, \bar{A}_2, \dots, \bar{A}_m$. This relationship is given by a theorem that we now quote in translation:

"The group G and \bar{G} can be seen to be isomorphic to each other."

This theorem can be stated more precisely using modern terminology as follows:

Given $\bar{A}_1, \dots, \bar{A}_m \in \bar{G}$, there exists a unique homomorphism $\phi : G \rightarrow \bar{G}$ such that $A_i \phi = \bar{A}_i$ for all $i \in N$. Dyck's "proof" of the theorem is understated, to say the least. For example, the mapping needed to establish the desired isomorphism between G and \bar{G} can be inferred to be $S(A_i) \mapsto S(\bar{A}_i)$ where $S(A_i)$ is an arbitrary combination of the elements A_i and their inverses. Dyck correctly asserts that this mapping is well-defined. However, his explanation of this fact is confusing and once again points to Dyck's discomfort with the assertion, made in the first part of his paper, that every element of G has a unique reduced expression. All what Dyck does, by way of proving well-definedness, is to say that if one expression $S(A_i)$ is mapped to two distinct elements $S(A_i), S'(A_i)$ of \bar{G} , then in fact $S(A_i) = S'(A_i)$ which "contradicts our general assumption about the operations A_i ." The meaning of this is unclear. If Dyck truly believed his earlier remark about the most general group G , he would have no difficulties in proving well-definedness. Namely, he could define a mapping $G \mapsto \bar{G}$ by considering the effect of this mapping only on reduced expressions.

Another related source of ambiguity is whether the given mapping is a homomorphism. Dyck says nothing about this, other than to assert it. It is not difficult to show that we have a homomorphism if one knows that the given mapping $G \mapsto \bar{G}$ has the effect $S(A_i) \mapsto S(\bar{A}_i)$ for any expression $S(A_i)$, and not just for the reduced expressions. It seems that Dyck wished to define $G \rightarrow \bar{G}$ in this way, but this leads to the confusion discussed above.

A modern treatment of what Dyck is attempting to do at this stage is given in [1, p. 250]. Here we find the following theorem:

Theorem : *Let F be freely generated by a set X , let H be any group, and let θ be a mapping of X into H . Then there exists a homomorphism $\hat{\theta}$ of F into H such that $\hat{\theta}$ agrees with θ on X . $\hat{\theta}$ is called an extension of θ .*

In proving the above theorem, Baumslag and Chadler first recall that part of the definition of a group freely generated by x_1, \dots, x_n given in [1, p. 248]; namely:

"Any nonunit element of F is uniquely expressible as a reduced X -product $f = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$, where $x_i \in X$, $\epsilon_i = \pm 1$ and $x_i = x_{i+1}$ implies $\epsilon_i \neq -\epsilon_{i+1}$."

Next, they define a mapping $\hat{\theta} : F \rightarrow H$ by $f\hat{\theta} = (x_1\theta)^{\epsilon_1} \dots (x_n\theta)^{\epsilon_n}$ with $1_F\hat{\theta} = 1_H$. Here θ is such that $\theta|_H = \theta$. To conclude their proof, they show that $\hat{\theta}$ is a homomorphism, adding that

"To do this, we shall show that if $f = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ where $x_i \in X$ and $\epsilon_i = \pm 1$, then $f\hat{\theta} = (x_1\theta)^{\epsilon_1} \dots (x_n\theta)^{\epsilon_n}$ whether or not $x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ is a reduced product."

This is done by induction on n .

Thus, the treatment in [1] avoids the difficulties encountered in Dyck's paper, essentially by defining them away. The real difficulties will appear later in establishing the existence of free groups. The discussion concerning the relationship between the most general group and an arbitrary group \overline{G} now continues. Dyck makes the following two assertions which we label by A and B:

Assertion A: Given an element $S(\overline{A}_i)$ of \overline{G} then either

- (1) only one element of G maps to $S(A_i)$, or
- (2) infinitely many elements of G map to $S(A_i)$.

Assertion B: If (1) above holds, then G and \overline{G} are for all practical purposes identical. Suppose that (1) does not always hold. Then (1) does not hold in the particular case that $S(\overline{A}_i) = 1_{\overline{G}}$.

No proofs for these assertions are given by Dyck. We now supply a proof of Assertion A:

Suppose $\overline{g} \in \overline{G}$ and suppose $g, h \in G$ with $g \neq h$ and with $\overline{h} \neq \overline{g}$. Then $(hg^{-1}) = \overline{h}(\overline{g})^{-1} = \overline{1}$. Thus 1 and hg^{-1} are two distinct elements of G which map to $\overline{1}$. Then one can produce infinitely many elements of G that map to \overline{K} (e.g. the powers of hg^{-1}). Then also infinitely many elements of G map to \overline{K} for any element \overline{K} of \overline{G} , since $K, Khg^{-1}, K(hg^{-1})^2, \dots$, all map to \overline{K} .

Instead of proving assertions A and B directly, Dyck retreats and consider the preimage of 1. If $g \mapsto 1_{\overline{G}}$ then also $h^{-1}gh \mapsto 1_{\overline{G}}$ for any $h \in G$ and any combination (word) in the various elements $h^{-1}gh$, $h \in G$ maps to $1_{\overline{G}}$. This shows that if some non-identity elements of G maps to $1_{\overline{G}}$, then infinitely many elements of G map to $1_{\overline{G}}$. Moreover, Dyck indicates that the set of elements of G which map to $1_{\overline{G}}$ forms

"a group H , and as one can see from its definition this group H is permutable or commutable with each operation S , or to use the notation of Herr Lie, the group H is said to be a distinguished subgroup."

In other words, the kernel of our homomorphism is a normal subgroup of G .

There is some further discussion of the structure of H , which is somewhat tangential to the main argument. Then, Dyck begins to consider the pre-image in G of an arbitrary element of \overline{G} . He goes as far as to say that if $\overline{g} \in \overline{G}$ then all elements of the coset gH will be mapped to \overline{g} . However, Dyck never clearly states that gH is equal to the preimage of \overline{g} in G .

Dyck now comes to the main point of his whole paper. He states (using modern terminology) that $G = H \cdot C$ where C is a complete set of coset representatives of H in G . He also states that C is in one-to-one correspondence with \overline{G} . There is more: In a very vague way he states (straining at the limitations of his language) that $\frac{G}{H} \cong \overline{G}$.

To finish our consideration of Dyck's 1882 paper we now establish a connection between:

- (1) Dyck's most general group and the results in section 4 of his paper.
- (2) Cayley's Dictum encountered in Chapter II.
- (3) The concept of group presentation.

Let \overline{G} be a group generated by A'_1, \dots, A'_n . Let G be a free group on n generators A_1, \dots, A_n . Define $A'_1 \dots A'_{n+1} = I_{\overline{G}}$ and $A_1 \dots A_{n+1} = I_G$. We now know that \overline{G} is a homomorphic image of G via $\phi(A_i) = A'_i, i = 1, \dots, n$. Let H be the kernel of this homomorphism. Then H can be regarded as a list of "relations" concerning the generators A'_1, \dots, A'_n . Namely, $A_{i_1} \dots A_{i_m} \in H \Leftrightarrow A'_{i_1} \dots A'_{i_m} = I_{\overline{G}}$. Since $\frac{G}{H} \cong \overline{G}$ by the First Isomorphism Theorem, we therefore have a "presentation" of \overline{G} in terms of "rules of combinations of symbols" A'_1, \dots, A'_n in Cayley's sense.

APPENDIX

Proposition 1: *The sequence of tiles $[S_j^k]$, $j \in \{1, 2, 3\}$ converges to the A_j -vertex as $k \rightarrow \infty$.*

Proof: Let $j = 1$. Put $(z)S_1 = \frac{(-1-i)z+1}{z+(-1+i)}$ in matrix form, i.e. $S_1 = \begin{bmatrix} -1-i & 1 \\ 1 & -1+i \end{bmatrix}$. Compute $S_1^2 = \begin{bmatrix} 1+2i & -2 \\ -2 & 1-2i \end{bmatrix}$, $S_1^3 = \begin{bmatrix} -1-3i & 3 \\ 3 & -1+3i \end{bmatrix}$,
 \dots , $S_1^{2k-1} = \begin{bmatrix} -1-(2k-1)i & 2k-1 \\ 2k-1 & -1+(2k-1)i \end{bmatrix}$, $S_1^{2k} = \begin{bmatrix} 1+2ki & -2k \\ -2k & 1-3ki \end{bmatrix}$
 $(1 \leq k < \infty)$. Now put S_1^{2k-1} in Möbius form and observe that $(z)S_1^{2k-1} = \frac{[-1-(2k-1)i]z+(2k-1)}{(2k-1)z+[-1+(2k-1)i]} = \frac{\left[\frac{-1}{2k-1}-i\right]z+1}{z+\left[\frac{-1}{2k-1}+i\right]}$ so that $(z)S_1^{2k-1} \mapsto \frac{-iz+1}{z+i}$ as $k \mapsto \infty$. Similarly, $(z)S_1^{2k} \mapsto \frac{-iz+1}{z+i}$ as $k \mapsto \infty$.

Next consider the following family of circles:

$$\begin{aligned} \mathcal{D}_1^2 : \left| z + \left(\frac{1}{2} + i \right) \right| &= \frac{1}{2} \\ \mathcal{D}_1^4 : \left| z + \left(\frac{1}{4} + i \right) \right| &= \frac{1}{4} \\ \mathcal{D}_1^6 : \left| z + \left(\frac{1}{6} + i \right) \right| &= \frac{1}{6} \\ &\vdots \\ \mathcal{D}_1^{2k} : \left| z + \left(\frac{1}{2k} + i \right) \right| &= \frac{1}{2k}. \end{aligned}$$

Notice that these circles converge to the point $A_1 = -i$ as $k \mapsto \infty$ since $\mathcal{D}_1^{2k} : |z+i|=0 \Rightarrow D_1^{2k} = \{-i\}$ as $k \mapsto \infty$. Also observe that A_1 belongs to each of these circles and that $(-i)S_1^{2k} = A_1$ for each k , $1 \leq k < \infty$. Moreover we have:

$$\begin{aligned} (i)S_1 &= \frac{-4}{5} - \frac{3}{5}i \in \mathcal{D}_1^2 \cap \mathcal{C} \\ (i)S_1^2 &= \frac{-8}{17} - \frac{15}{17}i \in \mathcal{D}_1^4 \cap \mathcal{C} \\ (i)S_1^3 &= \frac{-12}{17} - \frac{35}{37}i \in \mathcal{D}_1^6 \cap \mathcal{C} \\ &\vdots \end{aligned}$$

$$({}^i)S_1^k = \frac{-4k - (2k-1)(2k+1)}{(2k-1)(2k+1)+2} \in \mathcal{D}_1^{2k} \cap \mathcal{C} \text{ with } ({}^i)S_1^k \mapsto -i \text{ as } k \mapsto \infty.$$

Now consider the following family of circles:

$$\mathcal{D}_1^3 : \left| z + \left(\frac{1}{3} + i \right) \right| = \frac{1}{3}$$

$$\mathcal{D}_1^5 : \left| z + \left(\frac{1}{5} + i \right) \right| = \frac{1}{5}$$

$$\mathcal{D}_1^7 : \left| z + \left(\frac{1}{7} + i \right) \right| = \frac{1}{7}$$

⋮

$$\mathcal{D}_1^{2k+1} : \left| z + \left(\frac{1}{2k+1} + i \right) \right| = \frac{1}{2k+1}.$$

Observe that these circles also converge to A_1 and that A_1 belongs to each one of them with $(-i)S_1^{2k+1} = A_1$ for each k , $1 \leq k < \infty$. Moreover:

$$(-1)S_1 = \frac{-3}{5} - \frac{4}{5}i \in \mathcal{D}_1^3 \cap \mathcal{C}$$

$$(-1)S_1^2 = \frac{-5}{13} - \frac{12}{13}i \in \mathcal{D}_1^5 \cap \mathcal{C}$$

$$(-1)S_1^3 = \frac{-7}{25} - \frac{24}{25}i \in \mathcal{D}_1^7 \cap \mathcal{C}$$

⋮

$$(-1)S_1^k = \frac{-(2k+1) - 2k(k+1)i}{k^2 + (k+1)^2} \in \mathcal{D}_1^{2k+1} \cap \mathcal{C} \text{ with } (-1)S_1^k \mapsto -i \text{ as } k \rightarrow \infty.$$

Finally, observe that each tile $[S_1^k]$ is bounded above and below by the circles \mathcal{D}_1^{2k} and \mathcal{D}_1^{2k+1} respectively. Hence, the sequence of tiles $[S_1^k]$ converge to the A_1 -vertex.

The remaining cases $j = 2$ and $j = 3$ involve similar considerations and we omit their proof.

Remark : Clearly, the sequence of tiles $[S_j^{-k}]$, $j \in \{1, 2, 3\}$ also converges to the A_j -vertex as $k \rightarrow \infty$.

BIBLIOGRAPHY

- [1] B. Baumslag and B. Chandler, *Schaum's Outline of Theory and Problems of Group Theory*, McGraw-Hill, Inc., New York, (1968), p. 245-251.
- [2] W. Burnside, *Theory of Groups of Finite Order*, Cambridge, London, (1897), p. 262-266.
- [3] A. Cayley, *On the Theory of Groups, as Depending on the Symbolic Equation $\theta^n = 1$* , Philosophical Magazine and Journal of Science, Vol. 7, Cambridge, London, (1854), p. 40-47.
- [4] A. Cayley, *The Theory of Groups*, The Collected Mathematical Papers, Vol. 10, Cambridge, London, (1878), p. 401-403.
- [5] B. Chandler and M. Magnus, *The History of Combinatorial Group Theory: A Case Study in the History of Ideas*, Springer-Verlag, New York, (1982), p. 5-8.
- [6] J.B. Conway, *Function of One Complex Variable*, Springer-Verlag, New York, (1984), p. 47-54.
- [7] W. Dyck, *Gruppentheoretische Studien*, Mathematische Annalen, Vol. 20, (1882), p. 1-21.
- [8] L. Kronecker, *Auseinandersetzung einiger Eigenschaften der Klassenanzahl idealer komplexer Zahlen*, Mathematische werke Kronecker, Vol. 1, (1870), p. 271-282.
- [9] B.L. Van der Waerden, *A History of Algebra*, Springer-Verlag, New York, (1985), p. 149-153.
- [10] H. Wussing, *The Genesis of the Abstract Group Concept*, The MIT Press, Massachussets, (1984), p. 63-67, p. 230-243.

The Genesis Of The Concept
Of Group Presentation
As Seen In Papers
Of Cayley, Kronecker and Dyck

by

Gilmar Rodríguez-Pierluissi

B.S., Kansas State University, 1983

AN ABSTRACT OF A THESIS

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

College of Arts and Sciences
Department of Mathematics
Kansas State University
Manhattan, KS

1988

ABSTRACT

The idea behind the concept of a “group presentation” is to form a group by giving a set of “generators” for the group, and certain equations (called “relations”) that the generators should satisfy. It is desirable that the group is as free as possible of relations and generators subject to these relations.

As suggested by its title *The Genesis of the Concept of Group Presentations as seen in papers of Cayley, Kronecker and Dyck*; the purpose of this thesis is to investigate the genesis of the concept of group presentation. This genesis took place in some of the works of the alluded mathematicians between the years of 1854 and 1882, in England and Germany.

The thesis is divided into five chapters. The content of each of these chapters is summarized in our Introduction, on page 2.

In studying the genesis of the concept of group presentation, we are focusing on one particular aspect of the genesis of the abstract group concept.