THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

SCHOOL OF SCIENCE

FAITHFUL BLOCKINGS OF FINITE GROUPS AND PEDAGOGICAL APPLICATIONS

MARK EDWARD MEDWID II
Spring 2012

A thesis
submitted in partial fulfillment
of the requirements
for baccalaureate degrees
in Mathematics and Secondary Education
with honors in Mathematics

Reviewed and approved* by the following:

Paul Becker
Associate Professor of Mathematics
Thesis Supervisor

Joseph Previte
Associate Professor of Mathematics
Honors Adviser

*Signatures are on file in the Schreyer Honors College.
ABSTRACT

The thesis research project was in two areas: abstract algebra and pedagogy. Specifically, we explored which groups can be represented by blocked permutation matrices (called faithful blockings); we then used these representations to enhance teaching in abstract algebra and related courses. These faithful blockings offer a concrete picture of an abstract subject. The main pedagogical focus was the development of computer lab supplements for upper-level mathematics courses at Behrend. Our project had the following results: a new algebra theorem – every symmetric group admits a faithful blocking by non-normal subgroups; a new definition, “relatively normal” subgroups; some new results that brought about new examples of matrix representations for groups, and the development of the above mentioned computer labs. These results were presented by Dr. Becker at an AMS special session on Undergraduate Education: A Vision for the 21st Century (Notre Dame University, Nov. 2010).
# TABLE OF CONTENTS

Acknowledgements..............................................iii

Chapter 1. INTRODUCTION........................................1

Chapter 2. FAITHFUL BLOCKINGS.................................4

Chapter 3. GENERALIZING FAITHFUL BLOCKINGS..............8

Chapter 4. PEDAGOGICAL APPLICATIONS......................18

Chapter 5. CONCLUSION...........................................22

Appendix A: Maple Labs........................................23
   A. Introduction to Groups Lab............................23
   B. Group Example: *
      Dic
     _3 Lab............................................30
   C. Introduction to Homomorphisms Lab..................33
   D. Introduction to Isomorphisms Lab....................41
   E. Matrix Multiplication................................48

Appendix B – Summary of Groups of Order 12...............52
   A. \( \mathbb{Z}_{12} \)........................................52
   B. \( \mathbb{Z}_6 \times \mathbb{Z}_2 \)................................54
   C. \( Dic_3 \).............................................56
   D. \( D_6 \)..............................................58
   E. \( A_4 \)...............................................60

Bibliography....................................................62
ACKNOWLEDGEMENTS

I would like to thank Dr. Paul Becker for many things: introducing me to abstract algebra and other high-level mathematics; helping me get started with the process of original mathematical research; supervising my thesis; being a valuable mentor over the course of my study at Penn State Behrend. Additionally, I thank Dr. Joseph Previte for working with me on planning my schedules every semester – without this help, I don’t believe I ever could have sorted out the requirements for my majors and minor and certainly would not have graduated with honors. Finally, I thank my close friends and family, whose support kept me afloat during my entire university education.
Chapter 1. INTRODUCTION

This thesis research project began first as an honors option supplement to the MATH435—Introduction to Abstract Algebra course. That honors option was an extension of an earlier article published by Dr. Paul Becker in 2005 entitled “Do Normal Subgroups Have Straight Tails?” Then, the project began some important mathematical research the following summer. Then, the final bits of research came together during the fall 2011 semester.

In typical university abstract algebra courses, one of the most important concepts is that of a “group” and the role of groups in mathematics. When entering this course, students have a practical working definition of what they consider “real-world” groups. We use groups every day to categorize, organize, and increase efficiency either between people or between objects. Teachers can break students into groups in order to cooperate and gain better understandings. Likewise, we have groups that unite under common causes or interests (such as the NAACP or church youth groups). We have even given the word “group” a verbal form that is used every day to show the act of creating a group or placing things into a group.

Then, the concept of a mathematical group is introduced, which is highly abstract, and students can find this strange concept of a “group” to be at odds with their own definitions or ideas. Unfortunately, the abstract group concept is foundational. In order to understand all the important ideas and applications of abstract algebra such as normal subgroups, direct products, rings, fields, ideals and homomorphisms, it is necessary for the student to first understand groups.

A group of order $n$ is a set with $n$ elements, $G$, together with a binary operation, $*$, that fulfills certain axiomatic conditions. A binary operation takes two elements of a set and combines them in some way. To form a group, the operation must be associative (for elements $x, y, z$ in a set, $(x * y) * z = x * (y * z) = x * y * z$). Next, the elements of the said group must have closure under the operation (meaning that no matter which two elements are used in the operation, the result is...
still an element of the set). Next, there must exist a unique identity element (an element that behaves like 1 under multiplication). Finally, every element must have a unique inverse.

The purpose of this research project was twofold. The first objective of the research was to extend and generalize Dr. Becker’s previous results about representing small groups as matrices rather than abstract objects. The next phase of research involved pedagogical applications of these results, developing teaching labs for use with the Maple computer program.

The idea of “matrix representations” is crucial to understanding the research project. Each element in a group can be represented as a matrix. The function which matches group elements to the matrices representing them is formally called the group representation. Sometimes the process is intuitive for very small groups; a simple guess-and-check method will suffice in such a situation. However, for even slightly larger groups, such a method becomes a nightmare. There is a sure-fire way to represent elements as matrices without any guessing, and this method will be detailed later on. First, however, an example of a group represented as matrices: the group $K_4$, which is called the “Klein-four group.” It has the following typical presentation:

$$K_4 = < a, b, c | a^2 = b^2 = c^2 = e >$$

This is to say that each element in the group is its own inverse (with $e$ being the identity element). Presentations of this type are common in abstract algebra, but not helpful or informative to students who are new to the subject. We can instead choose to represent the Klein-four group as a group of matrices. We define:

$$f: K_4 \to a \text{ particular set of matrices}$$

$$\left\{ f(a) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, f(b) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, f(c) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, f(e) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \right\}$$

The operation can be defined as matrix multiplication. With this presentation, it is more readily evident how the elements interact with one another. For example, if we multiply $a$ and $b$ we get $c$; if we multiply $a$ by itself, we can confirm that $a^2 = e$. Also, we see that $a \cdot e = a$. As students
in MATH435 have completed the linear algebra (MATH220) course, which deals with matrix multiplication, they have some familiarity with this approach.
Chapter 2: FAITHFUL BLOCKINGS

Cayley’s Theorem states that every group of with \( n \) elements is isomorphic to a group of permutations on \( n \) objects. These permutations can be easily represented as binary matrices. However, as the groups increase in size, difficulty in computation also increases. If we consider a group of size 30, for example, the left regular representation is a matrix of size \( 30 \times 30 \). This “regular representation” is the usual, literal interpretation of Cayley's Theorem – these analogous permutations can be represented easily as binary permutation matrices. However, computations with such large matrices are a nightmare.

Dr. Becker (2005) describes a much better method of creating smaller, more manageable matrix representations. This is a generalization of Cayley's Theorem, and through this method, using matrix representations becomes a more feasible teaching tool. The method involves “factoring” large groups into products of smaller subgroups. Then, the matrix representation will be as large as the sum of orders of its factors.

A group factorization is defined as follows: a group \( G \) can be factored as \( G = N \cdot H \) if every \( g \in G \) can be expressed as \( n \cdot h \) for some \( n \in N \) and \( h \in H \). Additionally, \( N \) and \( H \) must be subgroups of \( G \). Another subject which is vital to understanding the remainder of the paper is that of normal subgroups. A standard definition is: A subgroup \( H \) of \( G \) is normal in \( G \) if and only if \( xHx^{-1} \subseteq H \) for all \( x \) in \( G \) (Gallian 2010).

Another idea crucial to the understanding of the research product is that of direct and semidirect products. If we consider the group \( G \) factored as \( NH \), with both \( N \) and \( H \) normal in \( G \), then \( NH \) is called a “direct product” and is denoted \( N \times H \). On the other hand, if \( N \) is a normal subgroup of \( G \) and \( H \) is not a normal subgroup of \( G \), then \( NH \) is called a “semidirect product” and is denoted \( N \rtimes H \). This idea of normality in group products plays heavily into matrix representations.

Consider our earlier example of a group with 30 elements (order 30). Let us call this group \( G \). If we factor \( G \) into two separate subgroups \( N \) and \( H \) with orders 5 and 6 respectively, then we can
decrease the matrix representation from 30x30 to (5+6)x(5+6) or 11x11. To do this, we make the “typical” matrix representations of N and H and arrange those matrices as blocks on the diagonal of a larger matrix. Dr. Becker describes exactly this in his article (2005): “Let \( \alpha \) and \( \beta \) denote the regular representations of N and H, respectively. If \( g = nh \) with \( n \) in N and \( h \) in H, then \( \alpha(n) \) is an \(|N|\times|N|\) permutation matrix, while \( \beta(h) \) is an \(|H|\times|H|\) permutation matrix. Our substitute for the regular representation of G is the \textit{blocked representation} \( \Phi \):

\[
\Phi(g) = \begin{bmatrix} \alpha(n) & 0 \\ 0 & \beta(h) \end{bmatrix}.
\]

Essentially, to make a large group manageable, we can assemble two small matrix representations. If the representation retains all the information about the group, we call the representation a “faithful blocking.”

In his article, Dr. Becker introduced some terminology which will be used throughout the remainder of the paper. He uses “blocks” and “tails” to describe the nonzero parts of the blocked representation matrix. If we are talking about \( n \) in N, the “block” of \( n \) is \( \alpha(n) \) while the “tail” of \( n \) is \( \beta(n) \). Similarly, an element \( h \) in H has block \( \beta(h) \) and tail \( \alpha(h) \). If the tail of an element is an identity matrix, then its tail is said to be \textit{straight}. If the tail is not straight, then it is \textit{twisted}. In his article, Dr. Becker also proved that normal subgroups have a straight tail representation, while non-normal subgroups have a twisted tail.

The method for creating these smaller blocked representations involves the action of a group element on its associated group of cosets (or quotient group). If we list, for example, the quotient group \( G/N \) with cosets in specific order \( \{c_1N, c_2N, \ldots, c_{|H|}N\} \) then the group action of \( x \) on \( G/N \) is \( \{xc_1N, xc_2N, \ldots, xc_{|H|}N\} \). This is the same list of cosets; the only difference is the possibility that its elements have been shuffled around. So the action of \( x \) is exactly equivalent to a permutation on \(|G/N|\) elements.

\textit{Example}: \( D_6 \)
The dihedral group of degree six has the following presentation:

\[ < x, y | x^6 = y^2 = e; yxy^{-1} = x^{-1} > \]

It can be factored as \(< x > \times < y >\), or equivalently, \( C_6 \rtimes C_2 \) (\(< x > = C_6, < y > = C_2\)). The name \( C_n \) represents a cyclic group of order \( n \). Further, \( C_6 \rtimes C_2 \) states that \( C_6 \) is a normal subgroup of \( D_6 \) while \( C_2 \) is not. Consider the following quotient groups:

\[ D_6/C_6 = \{C_6, yC_6\} \]
\[ D_6/C_2 = \{C_2, xC_2, x^2C_2, x^3C_2, x^4C_2, x^5C_2\} \]

We can then examine the action of the generators on said quotient groups. The action of \( x \), for example:

\[ x: \{C_6, yC_6\} \rightarrow \{xC_6, xyC_6\} = \{C_6, yC_6\} \]

\[ x \sim (1)(2) \]

The element \( x \) can be represented by a corresponding permutation matrix of \( \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \) or, more compactly in cycle notation \((1)(2)\). We see here that \( x \) does not affect the quotient group of \( D_6/C_6 \). So, the action of \( x \) on \( D_6/C_6 \) is the identity permutation on 2 elements. The action of \( x \) on \( D_6/C_2 \), however, looks like this:

\[ x: \{C_2, xC_2, x^2C_2, x^3C_2, x^4C_2, x^5C_2\} \rightarrow \{xC_2, x^2C_2, x^3C_2, x^4C_2, x^5C_2\} \]

\[ x \sim (1,2,3,4,5,6) \]

Here \( x \) shuffles the order of \( D_6/C_2 \), acting as the permutation \((1,2,3,4,5,6)\). With these two group actions, we get the following blocked representation of \( x \):

\[
\Phi(x) = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]
Because $x$ is a member of $C_6$, its block is the 6x6 matrix, and its tail is the 2x2 matrix. Its tail is straight, which is the predicted result, as $C_6$ is normal in $D_6$. Following the same method with $y$, the other generator of $D_6$, we obtain the following matrix representation:

$$
\Phi(y) = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
$$

In this case, as $y$ is an element of $C_2$, its block is the associated 2x2 matrix and its tail is the 6x6 matrix. Notice that in this case, the tail is not straight; this is expected, as $C_2$ is a non-normal subgroup of $D_6$.

Groups of order 12 serve as great introductory group examples – they are large enough to be interesting but small enough as to not overwhelm a beginner in group theory. There are a total of five groups of order 12; their faithful blockings are summarized as an appendix to this paper.
Dr. Becker proved straight tails always occur for normal subgroups in semidirect products, but his article makes no promise for a product in which neither subgroup is normal. As direct products and semidirect products are very common methods to generating groups, finding an example of a product in which neither group is normal can be quite difficult.

In my honors option part of the MATH435 course, I discovered an example of a group factorization in which neither subgroup was normal; this was the symmetric group $S_4$ factored as $S_3 \cdot C_4$. So, the first part of the summer research project was spent working with other examples and seeing how Dr. Becker’s method of creating smaller blocked representations generalized further.

I came up with my second example going a step further and came up with a factorization of $S_5 = S_4 \cdot C_5$. Again, neither factor was a normal subgroup. Continuing this line of thinking we obtain the following theorem:

*Theorem:* The symmetric group on $n+1$ elements can be factored in the following way:

$$S_{n+1} = S_n \cdot C_{n+1}$$

Further, $S_n$ and $C_{n+1}$ are non-normal subgroups of $S_{n+1}$.

*Proof:*

**Claim 1:** $S_{n+1} = S_n \cdot C_{n+1}$ as sets.

We express $C_{n+1}$ as a permutation on $n+1$ elements. Therefore, $|C_{n+1}| \leq |S_{n+1}|$. Also, we define multiplication in the product in terms of permutation multiplication; that is, we assume $S_n \cdot C_{n+1}$ is a subgroup of $S_{n+1}$. Note that $S_n \cap C_{n+1} = \{e\}$, as $e$ is the only element of $C_{n+1}$ that fixes $n+1$.

Now, assume that

$$ab = xy \text{ with } a, x \in S_n; b, y \in C_{n+1}.$$
Because $S_{n+1}$ is a group, we can right multiply by $b^{-1}$:

$$a = xyb^{-1}$$

By closure of a group, $(yb^{-1}) = w$ for some $w \in C_{n+1}$. So,

$$a = x \cdot w$$

We know $a$ is an element of $S_n$, as is $x$. The element $w$, then, must be the identity permutation, as it is in $S_n \cap C_{n+1}$. But $w$ as the identity forces $a = x$ and $b = y$. So every element of $S_{n+1}$ produced by these multiplications is unique. Thus $|S_{n+1}| = |S_n \cdot C_{n+1}|$, and the entire group $S_{n+1}$ has been represented. So,

$$S_{n+1} = S_n \cdot C_{n+1}.$$ 

**Claim 2:** $S_n$ is nonnormal in $S_{n+1}$.

Suppose $S_n$ was normal in $S_{n+1}$. Then for any $x \in S_{n+1}$ and $y \in S_n$, $yxy^{-1} \in S_n$. Consider the following counterexample:

$y = (n - 1, n)$ and $x = (1, n + 1, n, n - 1, ..., 2)$.

We then conjugate $y$:

$$xyx^{-1} = (1, n + 1, n, n - 1, 2)(n - 1, n)(1, 2, ..., n + 1)$$

This is another two-cycle. Every element is taken to itself (working from left to right) but $n$. In $x$, $n$ is taken to $n - 1$, which is taken back to $n$, and then to $n + 1$. Our result is the two-cycle $(n, n + 1) \notin S_n$. So $S_n$ is nonnormal in $S_{n+1}$.

**Claim 3:** $C_{n+1}$ is nonnormal in $S_{n+1}$.
Suppose that $C_{n+1}$ is normal in $S_{n+1}$. Then for any $x \in S_{n+1}$ and $y \in C_{n+1}$, $\gamma x y^{-1} \in C_{n+1}$. Consider the following counterexample:

$y = (1, 2, 3, \ldots, n, n + 1)$ and $x = (n - 1, n)$. Again, we conjugate $y$ by $x$:

$\gamma x y^{-1} = (n - 1, n)(1, 2, 3, \ldots, n, n + 1)(n - 1, n)$

This multiplication results in another $n + 1$-cycle. No matter the $n$ used, this cycle will not be an element of $C_{n+1}$. The subgroup $C_{n+1}$ is not closed under conjugation and thus is nonnormal in $S_{n+1}$.

QED

The theorem shows that it is possible to easily come up with a factorization of a common group with two non-normal subgroups, making an otherwise "exotic" idea relatively easy to access.

Another important result was the generalization of faithful blockings for any finite product. I was able to come up with some examples in which a group represented as a repeated direct product also admitted a faithful blocking. This logic led to the following theorem:

**Theorem:** A group $G$ factored as a finite direct product, $G = A_1 \times A_2 \times \cdots \times A_n$ admits a faithful blocking with $n$ blocks, with $\sum_{i=1}^{n} |A_i|$ rows and $\sum_{i=1}^{n} |A_i|$ columns.

**Proof:**

First, we define a blocked representation of $G$ in the following way: if $G = A_1 \times A_2 \times \cdots \times A_n$, then

$$
\Phi(g) = \begin{bmatrix}
\alpha_1(a_1) & 0 & \cdots & 0 & 0 \\
0 & \alpha_2(a_2) & 0 & \cdots & 0 \\
0 & 0 & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & \alpha_{n-1}(a_{n-1}) & 0 \\
0 & 0 & \cdots & 0 & \alpha_n(a_n)
\end{bmatrix}
$$

Where $\alpha_i$ is a faithful representation of $A_i$ and $g = a_1 \cdot a_2 \cdot \cdots \cdot a_n$.

We wish to show for any group factored as a finite direct product, there exists a faithful blocking structure. So, we suppose a group $G$ exists and can be factored as a finite direct product. We construct a blocked representation of $G$ as above. This blocked representation consists of blocks
\( \alpha_1, \alpha_2, \ldots, \alpha_n \) on the main diagonal of the \( \Phi \) matrix. Let \( g \) be any element of \( G \). Then, \( \alpha_i(g) \) is obtained through the left-action of \( g \) on the quotient group \( G/P_i \), where \( P_i \) is the product group of \( A \)'s with \( A_i \) excluded. For example, \( P_1 = A_2 \times A_3 \times \ldots \times A_n \), \( P_2 = A_1 \times A_3 \times A_4 \times \ldots \times A_n \), etc. The left action of \( g \) on \( G/P_i \) acts as a permutation to the list of cosets of \( P_i \) in \( G \). This permutation is then converted to a permutation matrix, and this resulting permutation matrix is \( \alpha_i(g) \). After obtaining \( \alpha_1, \alpha_2, \ldots, \alpha_n \), we arrange them in blocks on the main diagonal of another matrix. The entries are 0 elsewhere in this new matrix.

**Claim:** The \( \Phi \) blocking is also faithful.

We consider a blocked representation to be faithful if no loss of information occurs, i.e. the \( \Phi \) function is injective. We proceed here by contradiction, assuming that \( \Phi \) is NOT one-to-one. Assume \( x, y \in G \). Write \( x = \prod x_i, y = \prod y_i \). Then, by assumption, \( \Phi(x) = \Phi(y) \). As \( \Phi \) has a blocked structure, this implies that \( \alpha_i(x_i) = \alpha_i(y_i) \). These \( \alpha \) representations are faithful, so \( x_i = y_i \); their products are equal. In other words, \( x = y \). So, \( \Phi \) must be one-to-one.

\( \text{QED} \)

The concept of "blocks" and "tails" becomes complicated when a group is factored as a product of multiple (> 2) groups. How does one predict which tails are straight and which are crooked? Further, the definitions of blocks and tails become further complicated in such cases.

In the case of two-block matrices, this prediction is trivial – all tails will be straight in the case that the subgroup is a normal subgroup of the original group. However, describing semidirect no longer makes practical sense when three factors are involved. Depending on the group's presentation and the factoring, some of the factor groups may be normal but end up with twisted tails.

The above conjecture makes a promise of a faithful blocking in the case that all of the factors are a direct product with one another – in other words, every factor is a normal subgroup of \( G \).
such a case the representations are much like with two blocks – the block shows an element’s action, and all tails will be straight.

Consider the above factorization of a group \( G = A_1 \times A_2 \times \ldots \times A_n \). In its faithful representation function \( \Phi(g) \), we can further refine our sense of blocks and tails. If we wanted to examine \( \Phi(a_1) \), for example, then its block would be the result of the action of \( a_1 \) on \( G/P_1 \). Then the action of \( a_1 \) on all other \( G/P_i \) would generate the tail representations – all of which would be straight.

What of the cases where the factorization is not composed of direct products? In such a case, it becomes sensible to talk about factors being normal \textit{relative} to one another. In a factorization such as \( G = A_1 \cdot A_2 \cdot \ldots \cdot A_n \) interactions between groups can become complex. We propose that straight tails are contingent on the \textit{relative normality} of a subgroup, and a tentative definition of is as follows:

\textit{Assume} \( N, H \) and \( N \cdot H \) \textit{are subgroups of a group} \( G \). \textit{We say} \( N \) \textit{is normal relative to} \( H \) \textit{if} \( N \) \textit{is a normal subgroup of} \( N \cdot H \).

We have not found a standard definition for this concept. We have seen some non-official use of the term to describe similar ideas. We can then use this idea of relative normality to predict which tails will be straight or twisted in a group with a finite number of factor groups. In a faithful blocking representation, each block is a representation of one of the subgroups of the original group. So, if we examine \( \Phi(a_1) \), for example, then the straight tails would occur in blocks representing all the factor groups normal relative to \( A_1 \). Any nonnormal tails will be twisted. This conjecture still requires formal proof, but is consistent with a variety of examples we have considered.

As it stands, computations involving even three factors can become complicated. However, it is possible to write computer programs to both check the relative normality of the groups \textit{and} to derive their permutation/matrix representations. We plan to fully develop an implementation of this in the language GAP (Groups, Algorithms and Programming). We plan to produce a list of
blocked representations for the groups listed in GAP’s small groups library. Below are examples of faithfully blocked representations of groups with three factors.

**Example 1:** \( G = \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \)

This product group has the following usual presentation:

\[
\langle a, b, c | a^3 = b^2 = c^2 = e; ab = ba; bc = cb; ac = ca \rangle
\]

We then consider the following subgroups of \( G \):

\[
M = \langle a, b \rangle \\
N = \langle b, c \rangle \\
P = \langle a, c \rangle
\]

Then, the following quotient groups result:

\[
G/M = \{M, cM\} \\
G/N = \{N, aN, a^2N\} \\
G/P = \{P, bP\}
\]

Then, as before, we consider the group action of any element upon these cosets in the form of left-multiplication. For example, we can examine \( a \)'s action upon the quotient groups:

\[
a : \{M, cM\} \to \{aM, acM\} = \{M, cM\} \\
a \sim (1)(2)
\]

The element \( a \in \mathbb{Z}_3 \) does not affect the first quotient group because \( a \in M \). So, it acts as the identity permutation. This happens again with \( G/P \). However, with \( G/N \), we get the following:

\[
a : \{N, aN, a^2N\} \to \{aN, a^2N, N\} \\
a \sim (1,2,3)
\]
So we can again give the faithful blocked representation for this element (or any other elements in that group):

$$\Phi(a) = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{bmatrix}$$

Here, the middle component serves as the block of $a$. Notice that $G$ is a direct product. Hence, its two tails (the smaller 2x2 matrices) are straight.

Here is a more exotic example, which is not a direct product. It has 30 elements.

*Example 2: $G = X \cdot Y \cdot Z$

GAP ID: G[30, 2]

This group has the following presentation:

$$G = \langle x, y, z; x^3 = y^2 = z^5 = e; xy = yx; xz = zx; yz = z^{-1}y \rangle$$

We factor $G$ as $X \cdot Y \cdot Z$. Notice that the presentation above states that $X$ is normal relative to both $Y$ and $Z$, $Y$ is normal relative to $X$ but nonnormal relative to $Z$, and $Z$ is normal relative to both $X$ and $Y$. A reasonable prediction would state that elements of $X$ will have two straight tails, $Y$ will have one straight and one twisted tail, and $Z$ will have two straight tails. We then construct blocked representations of $x$, $y$ and $z$. Here we have three quotient groups:

$$\{G/P_X, xG/P_X, x^2G/P_X\}$$

$$\{G/P_Y, yG/P_Y\}$$

$$\{G/P_Z, zG/P_Z, z^2G/P_Z, z^3G/P_Z, z^4G/P_Z\}$$
Where \( P_X = Y \cdot Z, P_Y = X \cdot Z, P_Z = X \cdot Y \). As usual, we proceed by observing the action of \( x \) on these quotient groups:

\[
x: \{G/P_X, xG/P_X, x^2G/P_X\} \to \{xG/P_X, x^2G/P_X, G/P_X\}
\]
\[
x \sim (1, 2, 3)
\]

\[
x: \{G/P_Y, yG/P_Y\} \to \{xG/P_Y, xyG/P_Y\} = \{G/P_Y, yxG/P_Y\} = \{G/P_Y, yG/P_Y\}
\]
\[
x \sim (1)(2)
\]

\[
x: \{G/P_Z, zG/P_Z, z^2G/P_Z, z^3G/P_Z, z^4G/P_Z\} \to \{xG/P_Z, xzG/P_Z, xz^2G/P_Z, xz^3G/P_Z, xz^4G/P_Z\}
\]
\[
= \{G/P_Z, zxG/P_Z, z^2xG/P_Z, z^3xG/P_Z, z^4xG/P_Z\} = \{G/P_Z, zG/P_Z, z^2G/P_Z, z^3G/P_Z, z^4G/P_Z\}
\]
\[
x \sim (1)(2)(3)(4)(5)
\]

So, the final blocked representation of \( x \) is:

\[
\Phi(x) = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

Notice the agreement of the straight tails and predictions. As \( X \) is normal relative to \( Y \) and also normal relative to \( Z \), we expect that the \( Y \)-tail (second in the diagonal) and \( Z \)-tail (third in the diagonal) to be straight, and they are. Now, we examine \( y \), which we predict to have one straight and one twisted tail (as \( Y \) is nonnormal relative to \( Z \)).

\[
y: \{G/P_X, xG/P_X, x^2G/P_X\} \to \{yG/P_X, yxG/P_X, yx^2G/P_X\} = \{G/P_X, xyG/P_X, x^2yG/P_X\}
\]
\[
= \{G/P_X, xG/P_X, x^2G/P_X\}
\]
\[
y \sim (1)(2)(3)
\]
\[ y: \{ G/P_Y, yG/P_Y \} \rightarrow \{ yG/P_Y, G/P_Y \} \]
\[ y \sim (1, 2) \]

\[ y: \{ G/P_Z, zG/P_Z, z^2G/P_Z, z^3G/P_Z, z^4G/P_Z \} \rightarrow \{ yG/P_Z, yzG/P_Z, yz^2G/P_Z, yz^3G/P_Z, yz^4G/P_Z \} \]
\[ = \{ G/P_Z, z^4yG/P_Z, z^3yG/P_Z, z^2yG/P_Z, zyG/P_Z \} \]
\[ = \{ G/P_Z, z^4G/P_Z, z^3G/P_Z, z^2G/P_Z, zG/P_Z \} \]
\[ y \sim (1)(2, 5)(3, 4) \]

The faithfully blocked representation of \( y \), then, is:

\[
\Phi(y) = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0
\end{bmatrix}
\]

Again, the prediction holds. The \( X \)-tail is straight, while the \( Z \)-tail is twisted. We can now examine
the last generator of the group, \( z \).

\[ z: \{ G/P_X, xG/P_X, x^2G/P_X \} \rightarrow \{ zG/P_X, zxG/P_X, zx^2G/P_X \} = \{ G/P_X, xzG/P_X, x^2zG/P_X \} \]
\[ = \{ G/P_X, xG/P_X, x^2G/P_X \} \]
\[ z \sim (1)(2)(3) \]

\[ z: \{ G/P_Y, yG/P_Y \} \rightarrow \{ zG/P_Y, zyG/P_Y \} = \{ G/P_Y, yz^4G/P_Y \} = \{ G/P_Y, yG/P_Y \} \]
\[ z \sim (1)(2) \]
\[z: \{G/P_Z, zG/P_Z, z^2G/P_Z, z^3G/P_Z, z^4G/P_Z\} \rightarrow \{zG/P_Z, z^2G/P_Z, z^3G/P_Z, z^4G/P_Z, zG/P_Z\}\]

\[z \sim (1, 2, 3, 4, 5)\]

Then, the blocked representation of \(z\) is:

\[\Phi(z) = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}\]

The element \(z\) is shown to have both the X and Y tails as straight. It shows as, once again, consistent with the predictions based upon \(Z\)'s relative normality. In examples 1 and 2, we can make successful predictions on the straightness of the tails. By no means do these two examples constitute as formal proof, but they do illustrate the mentioned properties and serve as interesting objects of study in their own right. In particular, these and other examples illustrate that the concept of relative normality is consistent and may be useful.

We have only made such predictions based on the generators of the groups, and though this is an inefficient method of computing multiplication within a particular group, it does serve to illustrate and highlight which elements of which subgroups interact and how.
Applications of this work may not appear obvious. Dr. Becker’s research in this area found a use of blocked representations in information theory. Its most important application, however, may be to the art of teaching. Faithful blockings of small groups can create clever and powerful visual representations to aid in the basic concepts of group theory and other advanced undergraduate subjects. These blocked matrix structures provide concrete pictures/structures to represent more abstract ones.

The pedagogical question of the remainder of the project was, “is a computer lab-based course or component in abstract algebra feasible and effective?” Dr. Becker and I concluded that the answer to the above question is a resounding yes. The lab portions were developed with Maple in mind (preferably a newer edition), as Maple has a nice graphical interface. These labs take an inquiry-based approach to introducing abstract algebra concepts.

One of the great advantages of applying faithful blockings in abstract algebra is that the biggest ideas of group theory can be introduced first. We proposed the following flow of topics to introduce within the first few weeks of the class:

- Definition of a group
- Examples of small, finite groups (order 12)
- Functions and homomorphisms
- Isomorphisms

Anyone who has taught an introductory group theory class will recognize this as an unorthodox approach to the classroom flow. Usually such classes begin with the definition of a group, and then examples of permutation groups. Mappings, homomorphisms and isomorphisms are pushed to the middle of the course. They usually are pushed back further as confusion develops and the interesting applications of group theory take a back seat until a second course.
Our proposed introduction to group theory is ambitious but allows enough slack for explanatory lecture components in between the days spent in computer labs. The topics above are presented at a basic and introductory level. However, these labs still present a notion of mathematical rigor as the labs require several proofs on the students’ own time. Students will pick up notation on the way as well as the basic “grasp” of the subject. Later the subjects are re-visited and students build upon what they already know. This is an example of scaffolding, one of the tried and true methods of education.

As an illustration of the use of these particular labs, we can examine the lab introducing group homomorphisms (located in Appendix A of the paper). Group homomorphisms lie at the crux of introductory abstract algebra study and group theory. Essentially, we are preparing students to think about preservation of different operations when a function maps one group to another. This concept is a necessity for understanding isomorphisms, as isomorphisms are bijective homomorphisms.

One developed lab intended for a linear algebra class was used in an actual classroom. The response from both the professor and students was generally positive – students were engaging the material in a new light. The linear algebra lab focused on matrix multiplication and some of the properties of the operation, such as associativity. The grand conclusion at the end of the lab is that matrix multiplication constitutes an appropriate binary operation for group theory, and asks the students to define a group formally.

Several labs have already been written and are available for perusal in the appendices. This computer lab method has been tested for the elementary concepts. However, one of the concepts that the labs could be applied to is the actual construction of faithful blockings. This requires an understanding of the basic definitions, along with concepts of cosets, subgroups, quotient groups, and group actions. To be sure, the labs are in their rough stages and there is an inherent time cost
associated with developing. We hope that any professors interested in our methods will be able to use our labs as a springboard, cutting off some of the time cost.

In the lab, an example homomorphism presented is from $\mathbb{Z}_{12}$ to $\mathbb{Z}_3$. The group $(\mathbb{Z}_{12}, +)$ is presented as a faithfully blocked matrix based upon the factorization $\mathbb{Z}_{12} = \mathbb{Z}_3 \times \mathbb{Z}_4$. In a blocked representation, multiplication of matrices means that only corresponding blocks even interact. So, as $\mathbb{Z}_{12}$ is factored as $\mathbb{Z}_3 \times \mathbb{Z}_4$, we can easily visualize this homomorphism by ignoring the $\mathbb{Z}_4$ block. By multiplying a $\mathbb{Z}_{12}$ matrix by certain near-identity matrices, we can effectively “shave off” all but the $\mathbb{Z}_3$ block. The matrices are as follows:

$$\text{Id1} := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$\text{Id2} := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The formal function as used in Maple is a conjugation by these two matrices:

```plaintext
> f: Z_12 -> Z_3
> f := X -> Id1.X.Id2
```

Then, students can plug in different group elements and see what their resulting elements are in $\mathbb{Z}_3$. It becomes readily apparent that multiple elements of $\mathbb{Z}_{12}$ map to the same elements of $\mathbb{Z}_3$; in other words, the function has a non-trivial kernel. Discussion about the kernels from these homomorphisms seems more intuitive in this setting, as students can simply use the predefined functions in Maple to experiment.

Another homomorphism presented leaves only the $\mathbb{Z}_4$ block. Another function is given which takes a “chunk” out of the very middle of the matrix – part of it being the $\mathbb{Z}_3$ block and part of
it being the \( \mathbb{Z}_4 \)-- students are to explain, by counterexample, why such a function is not a homomorphism.

The approach of using faithfully blocked matrices in teaching homomorphisms truly shows the underlying and interacting of subgroups. The kernel of these homomorphisms is included toward the end of the lab, serving as a transition into discussions of normal subgroups, and hints at an important algebraic theorem -- that a normal subgroup of a particular group is the kernel of some group homomorphism. This is what is called the First Isomorphism Theorem:

If \( \phi \) is a group homomorphism, from \( G \) to a group, then \( G/\ker \phi \cong \phi(G) \). (Gallian 207)

The First Isomorphism Theorem is a fundamental theorem of elementary group theory study. The sooner it is introduced in class, the better. The above lab shows a direct connection to normal subgroups – from the homomorphism introduced in the computer lab, its kernel is readily apparent. This could later be useful in a question such as “Prove \( \mathbb{Z}_4 \) is a normal subgroup of \( \mathbb{Z}_{12} \).” Instead of conjugating elements of \( \mathbb{Z}_4 \), one can simply reference the previous homomorphism.

Normality of subgroups is an even more abstract subjects than groups themselves -- however, our research in representing groups as blocked matrices (again) provides a more concrete picture of the idea.
Chapter 5: CONCLUSION

In closing, my research project involved group representations as faithfully blocked matrices. Though the computations in converting groups to these blocked matrices can become complicated and inefficient, they can produce final matrices that are easy to work with and much smaller in size than their traditional matrix representation guaranteed via Cayley’s Theorem.

There is still room for quite a bit more work in the areas of faithful blockings involving 3 or more factors, and there are still yet questions left unanswered. These questions could pave the way to more possible undergraduate research projects. Though some questions are unanswered, the research project is far from unsuccessful – in fact, it was quite the opposite.

As a result of the research done over the past couple of years, there are a few nearly ready-to-use Maple labs which can be incorporated into undergraduate abstract algebra courses. Additionally, this work could find its way into making labs for other branches of mathematics – such as introducing the concept of a function to students or basic linear algebra.

Dr. Becker presented a summary of some of my work at an American Mathematical Society meeting (Notre Dame Univ., November 2010). The lab in linear algebra was presented at the MAA national meeting in Boston in January of 2012. Additionally, this work holds the potential to perhaps be published in a math education or even undergraduate research journal.
Basics of Groups

Linear Algebra Inclusion

with(LinearAlgebra)

In this lab, we will experiment with a small set of matrices and multiplication of matrices. Our goal is to develop the definition of a "group" of matrices.

Consider the following set, G:
G = {A, B, C, E}

Where A, B, C and E are the following matrices:

\[
A := \begin{bmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]

\[
B := \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]

\[
C := \begin{bmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]
With our matrices, we will be performing matrix multiplication. Matrix multiplication is an example of a **binary operation**. A binary operation takes two items from a given set and produces an output (hence, it is binary).

In MAPLE, to multiply two matrices together, we use a period (.) operator. So, A multiplied with B will be written as A.B.

Example:

\[
A.B = \begin{bmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]

Now, we can examine different properties groups can have.

**Associativity**

One of the first properties a group must satisfy is that the operation is associative. We can check this quickly and easily. Remember that associativity means we can change around where we put our parentheses and the expression's overall value remains unchanged. For example:

\[
A.(B.C) = (A.B).C
\]

\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0
\end{bmatrix} \times \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
0 & 0 & 1
\end{bmatrix} = \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
0 & 0 & 1
\end{bmatrix} \times \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
0 & 0 & 1
\end{bmatrix}
\]

\[
Equal(A.(B.C), (A.B).C)
\]
Now, verify this for $A^*(C^*E)$ and $(A^*C)^*E$. Then, though it is intuitively obvious whether or not the relation is true, use MAPLE's "Equal" function to see whether it's true or false. An example is above; you write Equal(LHS, RHS) where LHS is the left-hand side of your equation, and RHS is the right-hand side (don't forget to make sure the 'E' in Equal is capitalized!).

Our operation is associative. This is one of the more basic properties that a group must satisfy.

**Commutativity**

Consider the set of all integers under addition. We know (from experience) that all the integers under addition commute with one another. For example, $1 + 3 = 4 = 3 + 1$. Groups that have this property are called **abelian**.

In general, matrix multiplication is not commutative. For example:

$$M := \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$N := \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$M.N \quad \begin{bmatrix} 0 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 2 & 0 \end{bmatrix}$$

$$N.M$$
So, we can see here that MN yields a different matrix than NM. But what of our set, G?

**Question 1**
Using MAPLE, check to see if G is a commutative group. Carry out the multiplications listed on your worksheet, and use the space below to do so. Fill in the answers on your worksheet. The first multiplication is done for you.

**Closure**
When we work with groups, we need to make sure that we get some sort of predictable outcome when performing our operation, or doing any sort of computation becomes a nightmare. For example, what if you were to add two numbers together, and get the following:

\[ 3 + 7 = \text{fish} \]

You've added two numbers, but gotten a fish as a result. Suddenly all of mathematics falls apart!

With our set and operation, we need to make sure that the operation between any two elements yields another element in the set. This property is called **closure** under the operation.

For example:

\[ A.B \]
This matrix should look familiar. This is one of the matrix C in our set G.

\[
\begin{bmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]

Question 2
From the above results, examine the product matrices. Are these products in G? If so, identify them by name. Fill in the answers on your worksheet. You may use the additional space below if necessary.

Identity

From our past experiences, we can all think of examples where an element of a set never changes the other elements under the operation. For example, if we consider the set of integers under addition, this privilege belongs to 0. A few quick checks will verify this:

\[
\begin{align*}
1 + 0 & = 1 \\
3 + 0 & = 3 \\
120934582 + 0 & = 120934582 \\
-999999999999999 + 0 & = -999999999999999
\end{align*}
\]

So, we can say that 0 is the additive identity, as it changes no elements under addition. Do any other numbers have this property?

\[
\begin{align*}
1 + 5 & = 6 \\
3 + 5 & = 8 \\
120934582 + 5 & = 120934587 \\
-999999999999999 + 5 & = -999999999999999
\end{align*}
\]
Try as you might, you won't find any other number under addition that behaves like 0 does.

*Question:* What is the multiplicative identity of the integers?

Identities, as stated above, change no elements under the operation. More formally, an identity $e$ in a set $S$ satisfies the following:

$$e \cdot x = x \cdot e = x \quad \text{for every } x \in S.$$  

*Question 3*

Does our set of matrices have an identity? If so, what is it?

Prove this by writing its interaction with every element of the group, including itself. You may use the space below if necessary, but write all answers on your worksheet.

**Inverses**

Within a group, we perform operations. However, we must have some way to "un-do" an operation, or else computation again becomes a nightmare (imagine a world without subtraction, only addition!).

Again, think back to the integers and addition. Say you add "1" to a number; how would you get back to your original number? You would have to "subtract" 1, which is literally adding the number -1. -1 is the **inverse** of 1 under addition, because adding -1 and 1 yields 0, the identity. So, formally, the inverse of an element $x$ in S (noted as $x^{-1}$) satisfies the following:

$$x \cdot x^{-1} = x^{-1} \cdot x = e \quad \text{where } e \text{ is the identity element of } S.$$  

*Question 4*

For each matrix $X$ in our set $G$, find its specific inverse matrix in $G$. Verify that $X \cdot X^{-1} = I$ where $I$ is the identity matrix. You may use the space below; write all answers in your worksheet.

Is there any matrix in $G$ that does not have an inverse? If so, which one(s)?

**Conclusions**

With the numbers, we can solve simple linear equations. For example, in an equation such as

$$x + 5 = 36$$

$$x + 5 = 36$$
We can solve by simply adding -5 to both sides to get an answer. Try this with MAPLE below; simply right-click on the blue answer and click "solve for variable - x":

\[
\begin{align*}
832957698 + x &= 184917835809210938 \\
832957698 + x &= 184917835809210938
\end{align*}
\]

In our set, G, we can also solve equations similar to this.

**Question 5**

Solve the equations listed on your worksheet with the space below.

(Think back to basic algebra and the above examples; you can solve these with the same process)

**Question 6**

Out of the above mentioned properties, which are absolutely necessary to solve the equations in question 5? Explain.

(For example, would it be possible to solve the equation without an identity element? Why or why not?)

As you may have guessed by now, our set G with matrix multiplication forms what is called a "group." It is a well-known example called \( \mathbb{K}_4 \), the "Klein-four" group.

**Question 7**

If the point of a "group" is to solve equations within a given set (like in question 5), then state what defines a group specifically.

A *group* is a ____________, \( G \), together with a _________________, \( * \), that satisfies the following:

- \(* \) is associative
- 
- 
-
A New Group: The Di-cyclic Group of Degree Three

LinearAlgebra Inclusion

Recall that we’ve previously seen four other groups. They are (in order introduced):

\[ \mathbb{Z}_{12} \], the group of integers under addition, mod 12;
\[ \mathbb{Z}_6 \times \mathbb{Z}_2 \], the group of integers mod 6 together with integers mod 2;
\[ \text{D}_6 \], the group of symmetries of a regular hexagon;
\[ A_4 \], the alternating group of permutations on 4 items.

Today, we’re going to be examining a fifth unique group.

**Question 1**

a.) Thinking back to the previous groups we’ve looked at, list the common group properties that the groups all satisfy (as many as possible). Write this list on your worksheet.

b.) How do the groups differ? In other words, how do we know all the groups we’ve examined previously are not all the same? (For example: explain why \( \text{D}_6 \) is not the same as \( \mathbb{Z}_{12} \), etc)

Our new group, called \( \text{Dic}_3 \) (the di-cyclic group of degree three), is defined to be \( \{A^x B^y : x, y \in \mathbb{Z}\} \); we call A and B **generators** of \( \text{Dic}_3 \). A and B are as follows:

\[
A := \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0
\end{bmatrix}
\]

\[
B := \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0
\end{bmatrix}
\]
Now, based on those two matrices, we can generate the entire group, which is question 2 on your worksheet (use the following space to do so).

**Question 2**

a.) Predict the order (size) of the new group. Explain, based on the properties of the matrices, your reasoning.

b.) Using MAPLE, write out all the matrices of the elements on your worksheet.

c.) Generate the remaining unique elements of the group. Write them as a product $A^rB^s$.

Now that we have the entire group, we can look at its properties.

**Properties and Subgroups**

One of the first things we must examine about $\text{Dic}_3$ is the properties it satisfies. We know from its definition that the set $\text{Dic}_3$ forms a group. Assuming this,

a.) What is its order?

b.) What is its identity?

c.) What is the inverse of $A$?

d.) What is the inverse of $B$?

e.) What is the inverse of $A^rB^s$?

What about another important property? Is $\text{Dic}_3$ abelian? As a refresher, two elements $x$ and $y$ in a group $G$ satisfy the following:
\[ x \cdot y = y \cdot x \] for every \( x, y \) in \( G \)

In other words, the operation is commutative for every element of the set.

It turns out that our new group doesn't have this property. The proof of this is question 3 on your worksheet, which you can use the space below to solve.

**Question 3**
Prove that \( G \) is non-abelian by solving the following equation for \( X \) (show all work):

\[
AB = BX
\]

Another important group property is what its subgroups look like. We talk about subgroups being generated by an element or elements. The subgroup "generated by \( A \)" is the set \( <A> \) \( = \{A^k : k \in \mathbb{Z} \} \), or all powers of the generating element. It must be a subgroup of \( Dic_3 \).

**Question 4**

a.) List the elements of the more obvious subgroups of \( G \), namely \( <A> \) and \( <B> \).

b.) Now experiment with matrix multiplication to obtain the subgroups listed on your worksheet.

c.) Explain why \( <A> = <A^2> \) but \( <B> \neq <B^2> \).

**Uniqueness**

How are we sure that this new group is unique? For starters, as mentioned in the above section, \( Dic_3 \) is a non-abelian group. Because of this, it is automatically different from the two other groups that are abelian (\( Z_{12} \) and \( Z_6 \times Z_2 \)).

**Question 5**

Explain why \( Dic_3 \) is not isomorphic to \( A_4 \) or \( D_6 \). In other words, prove it is unique in relation to all the other groups previously discussed.

*Hint: Look at the subgroups and elements!*

In summary, we have five total groups introduced so far. Rest assured that we will be seeing all of them again! All of these groups are great examples of different ideas in group theory and abstract algebra.

Also, you may (or may not) be wondering why \( Dic_3 \) is called a dicyclic group. This will be addressed at a later time.
Group Homomorphisms

Linear Algebra Inclusion

As you may have guessed by this point in the course, groups are an important idea. We can use groups to classify and predict behaviors of not only numbers, but also more abstract ideas as well.

However, without some way to make sense of these more abstract ideas, the study of groups becomes utterly pointless. To do this, we need to be able to relate the groups that behave in similar ways.

For example, we can relate integers with addition to real numbers with multiplication. How?

This can be done with the exponential function: for all \( x \in \mathbb{Z} \), \( h(x) = e^x \).

\[
h := x \mapsto \exp(x)
\]

\[
x \mapsto e^x
\]

We know from experience that numbers usually behave differently under addition and multiplication. However, because of the rules of exponents, the domain and image behave in a very similar fashion. For example:

\[
5 + 6 = 11
\]

Now, if we look at their functional values and how those interact under multiplication:

\[
h(5) \cdot h(6) = e^5 \cdot e^6 = e^{11}
\]

This is the same as the functional value of 5 and 6 added together. Multiplication and addition are certainly different operations, however, with our exponential function, we can add the same way we do with the integers by multiplying. In this way, we can say that the exponential function preserves the operation of addition.

**Question 1**

Explain why \( h(5 + 6) = h(5) \cdot h(6) \). Give at least three other examples showing that the exponential function preserves the operation.

Actually, \((\mathbb{Z}, +)\) and \((\mathbb{R}, \cdot)\) form groups. What we have is a function between groups.
We can now apply this idea to another group we've seen before: \( \mathbb{Z}_{12} \). Recall that we can generate it with these two specific matrices:

\[
A := \begin{bmatrix}
 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 \\
\end{bmatrix}
\]

\[
B := \begin{bmatrix}
 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\]

Say that we wanted to relate this group to another group, \( \mathbb{Z}_3 \). We would first need a function or mapping from our first group to the smaller group. So, consider a function that keeps only the first 3x3 "block" of our matrix and chops off the rest of the matrix. We can do this with identity matrices of varying sizes:

\[
IdI := \begin{bmatrix}
 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 \\
\end{bmatrix}
\]
Our function, then, is going to be
\[ f : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_3 \]
\[ f := X \rightarrow \text{Id}_1 \cdot X \cdot \text{Id}_2 \]

where \( X \) is any matrix in our group. For example, let's look at \( A \):

\[ A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \]

Now we only have the first 3x3 "chunk" of \( A \).

**Question 2**

There are only three matrices in \( \mathbb{Z}_3 \). List them. Then, next to each, write which matrix(es) from \( \mathbb{Z}_{12} \) map(s) to it. This means to perform our function on each matrix of \( \mathbb{Z}_{12} \). You may use the space below if necessary for calculations.

How many matrices in \( \mathbb{Z}_{12} \) go to each matrix in \( \mathbb{Z}_3 \)?

In other words, \( f \) is a _________-to-one function.

By contrast, the exponential function is a _________-to-one function.
Now, state the homomorphism with the integer notation (a function from \{0, 1, 2,\ldots, 11\} to \{0, 1, 2\})

Notice that we can do the exact same kinds of multiplication we do in $\mathbb{Z}_3$ that we do in $\mathbb{Z}_{12}$! For example...

$$B.B$$

\[
[ 0 0 1 0 0 0 \\
 1 0 0 0 0 0 \\
 0 1 0 0 0 0 \\
 0 0 0 1 0 0 \\
 0 0 0 0 1 0 \\
 0 0 0 0 0 1 ]
\]

\[ f(B.B) \]

\[
[ 0 0 1 \\
 1 0 0 \\
 0 1 0 ]
\]

\[ f(B).f(B) \]

\[
[ 0 0 1 \\
 1 0 0 \\
 0 1 0 ]
\]

Like with the exponential function, it doesn't matter when we apply the function while performing our operation, our answer is still the same!

**Question 3**

Verify that $f(X).f(Y) = f(X.Y)$ for the matrix products listed on your worksheet. Use the space below if necessary. Show the work on your worksheet.

As it turns out, functions like $f$ and the exponential function are part of a very important class of functions called **homomorphisms**. Homomorphisms have the special property of preserving the operation, that is, while performing an operation in one group, we can apply a homomorphism either before or after the operation and the end result does not change. Formally, a homomorphism $\theta$ from a group $G$ to another group $G'$ satisfies:

$$\theta(a)*\theta(b) = \theta(a*b)$$

for all $a, b$ in $G$.

Homomorphisms are perhaps the most important idea in this course! However, they can be confusing. The important thing to remember with homomorphisms is that the operation in both groups behave very similarly, and when we map one group to another, we can do the exact same operation with results we'd expect.
Notice that we lose some information from \( f \) (we can't tell what's happening with the other "block" of the matrices). So we can define a similar function which chops off the upper 3x3 block and leaves only the 4x4 block. In this case, it will be a function from \( \mathbb{Z}_{12} \) to \( \mathbb{Z}_4 \). The identity matrices we will use have to be a bit different:

\[
\begin{bmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
\end{bmatrix}
\]

So, our new function is

\[ g := X \rightarrow \text{Id3} \cdot X \cdot \text{Id4} \]

\[ X \rightarrow \text{Typesetting}:-\text{delayDotProduct} \ (\text{Typesetting}:-\text{delayDotProduct} \ (\text{Id3}, X), \text{Id4}) \]

This function shaves off the upper block of our matrix, leaving only the bottom 4x4 matrix. For example:

\[ g(A) \]

\[
\begin{bmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
\end{bmatrix}
\]
**Question 4**

Is \( g \) a homomorphism? If so, show how \( g(X) \cdot g(Y) = g(X \cdot Y) \) for the \( X \) and \( Y \) on your worksheet.

**Question 5**

Now consider the following function that takes "chunks" out of the middle of the matrices, rather than the upper or lower blocks.

\[
\begin{align*}
\text{Id}_5 &:= \\
&= \begin{bmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}
\end{align*}
\]

\[
\begin{bmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

\[
\begin{align*}
\text{Id}_6 &:= \\
&= \begin{bmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\end{align*}
\]

\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\]

\( p := X \mapsto \text{Id}_5 \cdot X \cdot \text{Id}_6 \)

Prove, by counterexample, why this is NOT a homomorphism.

**The Kernel of a Function**

Consider an element of \( \mathbb{Z}_{12} \):
Question 6
Compute \( f(AB) \). Explain why, even though neither \( A \) or \( B \) are the identity, that our answer ends up the way it does.

The element "A" belongs to an important part of the function \( f \). As we are aware by now, the identity is a special element in a group. So, when establishing a function between two groups, we also need to take special consideration of what elements get mapped to the identity. The set of all elements getting mapped to the identity in the codomain is called the kernel of the function. In other words, more formally, for a function \( \theta \) from \( G \) to \( G' \),

\[
\ker(\theta) = \theta^{-1}(\epsilon), \text{ where } \epsilon \text{ is the identity element of } G'.
\]

***NOTE***
\( \theta^{-1}(\epsilon) \) means the complete inverse image of \( \epsilon \); in other words \( \{g \in G \mid \theta(g) = \epsilon\} \).

Question 7
List the kernels of each function we've looked at so far. (write out on worksheet)

Exponential function: _________________

\( f : \) _________________

\( g : \) _________________

This is another very important idea in abstract algebra. Kernels of homomorphisms are particularly important; this will be covered in more detail later on.
Conclusions

**Question 8**
Write out the formal definition of a group homomorphism. Then, using your own words, explain what this definition means.

**Question 9**
There are other examples of homomorphisms for $\mathbb{Z}_{12}$ as well. However, they are slightly more complicated than simply cutting out part of a matrix. Find a homomorphism from $\mathbb{Z}_{12}$ to $\mathbb{Z}_6$ (integer notation), and prove that it is a homomorphism.
(Note: To do this means you need to formally define the function! You don't necessarily need Maple to do complete the question.)

If we consider "1" in $\mathbb{Z}_6$ to be the matrix

$$
\begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
$$

state the above homomorphism for the matrix notation.
Group Isomorphisms
LinearAlgebra Inclusion

In this course we have thrown around the word "isomorphism" as a vague way of saying that two groups are essentially the same. The goal of this lab is to "clear up" and formally define this idea of an isomorphism.

First, an example of something we've previously stated as an isomorphism: matrix and integer notation for $\mathbb{Z}_{12}$. Recall our two generating matrices:

\[
A := \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
\end{bmatrix}
\]

\[
B := \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
\end{bmatrix}
\]
Sometimes we refer to the notation \( \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \) with addition (mod 12) as \( \mathbb{Z}_{12} \), also. We can think of this as another version of the group \( \mathbb{Z}_{12} \).

Two groups are **isomorphic** if and only if there exists an isomorphism between them. So, we need to come up with the function between the matrix notation and integer notation. Try out the following function:

\[
f : x \mapsto (A \cdot B)^x
\]

### Question 0

What is the domain of \( f \)?

What is the range of \( f \)?

### Question 1

We are trying to define a notion that two groups are essentially equal to each other. In that case, our operations must be able to correspond in some way. If \( f \) truly is an isomorphism (as is claimed), then it must be a special homomorphism. Prove \( f \) is a homomorphism. You may use the space below for calculations.

(Hint: What is \( f(3 + 4) \)? What is \( f(3) \)? \( f(4) \)?)

Not surprisingly, isomorphisms have some correspondence between operations. Let's look at a different isomorphism. Recall the group \( \mathbb{Z}_6 \times \mathbb{Z}_2 \) generated by these matrices:

\[
C := \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 \\
\end{bmatrix}
\]
We want to again match these matrices with integers.

**Question 2**

Explain why we cannot simply use the integers \( \{0, 1, 2, \ldots, 11\} \) even though there are exactly 12 elements in \( \mathbb{Z}_6 \times \mathbb{Z}_2 \). Prove that the same function as above won't work with a counterexample.

\[
g := x \mapsto (C, E)^x
\]

Since we can represent \( \mathbb{Z}_{12} \) as \( \{0, 1, 2, \ldots, 11\} \), what if we were to try to represent \( \mathbb{Z}_6 \times \mathbb{Z}_2 \) as a Cartesian product of \( \{0, 1, 2, \ldots, 5\} \) and \( \{0, 1\} \)? So let's look at the following function:

\[
h := (a, b) \mapsto C^a, E^b
\]

If we wanted the identity matrix, then, we can see that it matches with \((0,0)\):

\[
h(0, 0)
\]
Question 3

What is the domain of \( h \)? What is the range of \( h \)? Is \( \text{dom}(h) \) a group? Prove that \( \text{range}(h) \) is a group.

Question 4

Prove that \( h \) is a homomorphism, as we claim it is an isomorphism.

However, not ALL homomorphisms are isomorphisms. Remember our example from the homomorphism lab? Our first example of a homomorphism was \( f: \mathbb{Z}_{12} \to \mathbb{Z}_3 \); clearly they were not the same group. What OTHER special function properties must isomorphisms have? One answer lies in the kernel.

Question 5

Compute the kernel of both \( f \) and \( h \).

\[
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 
\end{bmatrix}
\]

In other words, both \( f \) and \( h \) are \_\_\_\_-to-one functions.

Functions with kernels that look like the kernels of \( f \) and \( h \) are special classes of functions called \textbf{injections}. Formally, an injection \( \theta \) from \( G \) to \( G' \) satisfies the following:

\[ \theta(a) = \theta(b) \text{ implies that } a = b. \]

This simply means that the function cannot take two different arguments to the same output.
Having an injective homomorphism isn't quite enough either. For example, look at the following function from $\mathbb{Z}_3$ to $\mathbb{Z}_6$ (for simplicity's sake, we can use the integer notations).

$$m := x \to 2 \cdot x$$

So, we are taking the set $\{0, 1, 2\}$ to the set $\{0, 1, 2, \ldots, 5\}$. The function takes each argument and produces a unique output:

$m(0)$

0

$m(1)$

2

$m(2)$

4

So, it is an injective function. It is also a homomorphism. But it is fairly evident that these two groups are not the same (what about the rest of $\mathbb{Z}_6$?). If 0, 2, and 4 were the only elements in $\mathbb{Z}_6$, then we could justify saying the two groups are the same. In addition to being an injective homomorphism, a function must also be surjective -- this means that the image and codomain are equal as sets. Formally, this means that a surjection $f: X \to Y$ satisfies

$$\forall y \in Y, \text{ there exists an } x \in X \text{ with } f(x) = y.$$  

****NOTE****

A surjection is also commonly known as an onto function.

**Question 6**

Show that either $f$ is surjective or $h$ is surjective (pick one).

Functions that are both injective and surjective are called bijections. If a bijection exists between two sets, they must be the same size or cardinality.

**Question 7**

Explain why two finite sets with a bijection between them must be of equal cardinality.

The idea of a surjection is the last puzzle piece for our working definition of an isomorphism.

**Question 8**

Clearly state the definition of an isomorphism.

**Presentation Notation**

Thus far, we've been using matrices to represent our groups. Matrix notation is not very common in group theory texts; a common notation used is called presentation notation, and we can use this to efficiently summarize the group as a whole. This notation first lists the two generators of
the group, and then lists additional relations between those generators. For example, presentation notation for \( \mathbb{Z}_{12} \) would look like this:

\[ \langle x^12 = e \rangle. \]

Think of \( x \) as representing the matrix product \( A \cdot B \); remember that \( (A \cdot B)^{12} = e \).

This means to take an element and to make a group out of it, making sure the relation is obeyed. This means to carry out every possible multiplication to ensure closure.

**Question 9**

List the group elements for the above presentation as powers of \( x \).

Which multiple of \( a \) acts like "1" from the integer notation with addition?

Which acts like "0"?

Give a bijective homomorphism from \( \langle x : x^{12} = e \rangle \) to \( (\{0, 1, \ldots, 11\}, +) \).

Let's look at a previous example of a group, \( D_6 \). Recall that it is generated by the following matrices:

\[
R := \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 \\
\end{bmatrix}
\]

\[
F := \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
\end{bmatrix}
\]
A typical presentation of $D_6$ is $\langle x, y | x^6 = y^2 = e, yxy^{-1} = x^{-1} \rangle$. Notice here that the group has two generators, and two relations to follow, unlike the previous example. The $D_6$ with matrices and presentation of $D_6$ are isomorphic to one another.

**Question 10**

State the isomorphism from $D_6$ with matrices to its presentation notation. Prove it is an isomorphism.

Thus far we have only discussed isomorphisms as a way to justify different notations. This is the core concept of group isomorphisms—functions that show two groups are representations of the same abstract group. If we take one group and write it in a different representation, then we have created a group isomorphic to our first. Consider the claim that $1 = \frac{4}{4} = .999999999999999999999999999999$; they are both the same number, just written in a different way.

More generally, we can write the set of rational numbers in many equivalent ways.

In our specific example, we have two models (representations) of the abstract group (idea, concept, pattern) we call $D_6$.

***NOTE***

For those that are curious, the isomorphism ("isomorphic to" is denoted by $\cong$) defines an equivalence relation:
- Every group is isomorphic to itself; $A \cong A$ (reflexive)
- If group $A \cong B$, then $B \cong A$ (symmetric)
- If group $A \cong B$, and $B \cong C$, then $A \cong C$. (transitive)

A proof of this claim will be part of this week's homework.
Matrix Multiplication

In this lab we will be continuing a concept that many of you are already familiar with: matrix multiplication. The main goals of today's lab are:

* To learn the Maple syntax for multiplication of matrices
* To experiment with some basic properties of matrix multiplication
* To demonstrate closure and lack of commutativity in matrix multiplication
* To introduce the definition of a group

In this lab, we will be working with a small set of matrices shown in the subheading below. For convenience, we'll call this set $D_3$ (the reason for this will be revealed later).

Matrix Set

Our set $D_3$ is generated by these two matrices. [Press ENTER on each matrix to load the matrices into memory.]

\[
A := \begin{bmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix} \\
B := \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]

This is all we'll need to compose our set. The set has matrices $A$ and $B$, along with all possible combinations (via multiplication) of $A$ and $B$. This also includes, for example, $A$ multiplied with itself or $B$ multiplied with itself.

**Question 1**

Predict how many matrices our set will have. (No need to multiply yet, just a rough estimate)

Linear Algebra Inclusion  [Press ENTER on the following line to load the algebra package]

```maple
with(LinearAlgebra)`
Syntax of Multiplication

To multiply two matrices in Maple, we don't use a typical * for multiplication like we do for everything else. To multiply two matrices together, you simply put a period in between them. For example: (press ENTER)

\[ A \cdot B \]

Voila! Matrices A and B have been multiplied together. Bear in mind, however, that the two matrices chosen must be **conformable**. That is, the number of columns in the first matrix must agree with the number of rows in the second. Also, you can use powers with matrices (Maple is smart enough to use the correct multiplication.) Example:

\[ A^2 \]
\[ A\cdot A \]

**Question 2**

Using the period operator, find all possible multiples of A and B. Use the space below for calculation.

What is the total number of matrices in \( D_3 \)?

Basic Properties

Matrix multiplication has a few nice properties which make it useful to work with.

For one, matrix multiplication is **associative**; that is, for any three matrices A, B, and C,

\[ (A \cdot B) \cdot C = A \cdot (B \cdot C) = A \cdot B \cdot C \]

**Question 3**

Verify that matrix multiplication in our set is associative with \( A \cdot (B \cdot A) \), \( (A \cdot B) \cdot A \), and \( A \cdot B \cdot A \).

Also, within the confines of our set \( D_3 \), we can also see that matrix multiplication is **closed**. This means that any multiplication between elements of \( D_3 \) will themselves be elements of \( D_3 \).

**Question 4**

Give a small explanation of why \( D_3 \) is closed under matrix multiplication.

*Hint: Look at how the set is made...you've done the computations for this above.*
The set $D_3$ also has a very special element called the **identity** that, when coupled with matrix multiplication, leaves all other elements unchanged. Some identities you are probably familiar with are 0 with the real numbers and addition, or 1 with the real numbers under multiplication. Formally, the identity element $E$ in a set $S$ satisfies the following:

$$E \cdot A = A \cdot E = A$$

with $A$ being any element of $S$.

**Question 5**
What does the identity in $D_3$ look like? Show that it behaves as an identity element should. Use the space below for calculation.

$$E := \text{Matrix}([[\ ,\ ,\ ],[\ ,\ ,\ ],[\ ,\ ,\ ]]);$$

Finally, the last property of interest we'll explore is that of **inverses**. This is hopefully a familiar topic. When performing an operation, it's useful to have the capacity to "un-do" that operation. For example, an additive inverse of a number is the same number with the opposite sign. The inverse of a matrix $A$, denoted $A^{-1}$ satisfies

$$A \cdot A^{-1} = A^{-1} \cdot A = E$$

with $E$ being the identity matrix.

**CAUTION**: Not all matrices have inverses!

**Question 6**
Find the inverse of each element of $D_3$. Use the space below for calculations. Clearly identify pair of matrix and inverse matrix.

What can we say about how many inverses exist for each element?

While exploring the properties that matrix multiplication can have, we can also talk about a property it does NOT have: **commutativity**, or the ability to switch the order of operation without changing the product. For example, addition and multiplication of real numbers is commutative: we can switch the order of multiplication or addition and still get the same answer. However, matrix multiplication is NOT commutative in general.

**Question 7**
Demonstrate that matrix multiplication is not commutative using elements of $D_3$.

Matrix multiplication and our set $D_3$ form a special type of algebraic structure called a **group**. Within groups, it is possible to solve linear equations of the form
Ax = B. The proper name of $D_3$ is the dihedral group of degree three, otherwise known as the symmetry group of a triangle.

**Question 8**
Keeping in mind the properties above that $D_3$ satisfies, carefully fill out the remainder of the definition of a group.

*A group is a set, $G$, together with a binary operation, $*$, which fulfills these properties:*
Appendix B: Summaries of Groups of Order 12

Group: \( \mathbb{Z}_{12} \)
This is a cyclic group of order 12. Equivalently, it is the group of integers under addition modulus 12. Also, considering symmetries of an object, this group represents all the rotations of a regular 12-gon.

Typical Presentation:
\(< x | x^{12} = e >\)

Group Elements:
\{e, x, x^2, x^3, x^4, ..., x^{11}\}

Product Notation:
\( \mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \)
\( \mathbb{Z}_4 \times \mathbb{Z}_3 \) can be presented in the following way:
\(< a, b | a^4 = b^3 = (ab)^{12} = e, ab = ba >\)

Isomorphism between groups:
\( f : \mathbb{Z}_4 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_{12} \)
\( f(a, b) = ab \)

Group Actions for Matrix Permutation Representation:

Chosen quotient groups:
\( \mathbb{Z}_{12} / \mathbb{Z}_4 = \{ b\mathbb{Z}_4, b^2\mathbb{Z}_4 \} \)
\( \mathbb{Z}_{12} / \mathbb{Z}_3 = \{ a\mathbb{Z}_3, a^2\mathbb{Z}_3, a^3\mathbb{Z}_3 \} \)

Action of \( a \) on quotient groups:
\( a : \{ b\mathbb{Z}_4, b^2\mathbb{Z}_4 \} \rightarrow \{ b\mathbb{Z}_4, b^2\mathbb{Z}_4, b^4\mathbb{Z}_4 \} \)
\( a \sim (1)(2)(3) \)
\( a : \{ b\mathbb{Z}_3, b^2\mathbb{Z}_3, b^3\mathbb{Z}_3, b^4\mathbb{Z}_3 \} \rightarrow \{ a\mathbb{Z}_3, a^2\mathbb{Z}_3, a^3\mathbb{Z}_3, a^4\mathbb{Z}_3 \} \)
\( a \sim (1,2,3,4) \)

Faithful blocking of \( a \):
\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\begin{bmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
\end{bmatrix}
\]

Action of \( b \) on quotient groups:
\( b : \{ b\mathbb{Z}_4, b^2\mathbb{Z}_4 \} \rightarrow \{ b\mathbb{Z}_4, b^2\mathbb{Z}_4, b^4\mathbb{Z}_4 \} \)
\( b \sim (1,2,3) \)
\[ b: \{\mathbb{Z}_3, a\mathbb{Z}_3, a^2\mathbb{Z}_3, a^3\mathbb{Z}_3\} \rightarrow \{\mathbb{Z}_3, a\mathbb{Z}_3, a^2\mathbb{Z}_3, a^3\mathbb{Z}_3\} \]
\[ b \sim (1)(2)(3)(4) \]

**Faithful blocking of** \( b \):

\[
\begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
0 & 0 & 1
\end{bmatrix}
\]

**Subgroups of** \( \mathbb{Z}_{12} \):
- \( \mathbb{Z}_4 \)
- \( \mathbb{Z}_3 \)
- \( \mathbb{Z}_6 \)
- \( \mathbb{Z}_2 \)
Group: $G = \mathbb{Z}_6 \times \mathbb{Z}_2$

This is a group of order 12 made with a direct product of a cyclic group of order 6 and a cyclic group of order 2. Thus, both $\mathbb{Z}_6$ and $\mathbb{Z}_2$ are normal subgroups.

Typical Presentation:

$< a, b | a^6 = b^2 = e >$

Group Elements:

$\{ e, b, a, ab, a^2b, a^3b, a^4b, a^5b \}$

Group Action for Matrix Permutation Representation:

Chosen quotient groups:

$G/\mathbb{Z}_6 = \{ \mathbb{Z}_6, b\mathbb{Z}_6 \}$

$G/\mathbb{Z}_2 = \{ \mathbb{Z}_2, a\mathbb{Z}_2, a^2\mathbb{Z}_2, a^3\mathbb{Z}_2, a^4\mathbb{Z}_2, a^5\mathbb{Z}_2 \}$

Action of $a$ on quotient groups:

$a: \{ \mathbb{Z}_6, b\mathbb{Z}_6 \} \rightarrow \{ \mathbb{Z}_6, b\mathbb{Z}_6 \}$

$a \sim (1)(2)$

$a: \{ \mathbb{Z}_2, a\mathbb{Z}_2, a^2\mathbb{Z}_2, a^3\mathbb{Z}_2, a^4\mathbb{Z}_2, a^5\mathbb{Z}_2 \} \rightarrow \{ a\mathbb{Z}_2, a^2\mathbb{Z}_2, a^3\mathbb{Z}_2, a^4\mathbb{Z}_2, a^5\mathbb{Z}_2, \mathbb{Z}_2 \}$

$a \sim (1,2,3,4,5,6)$

Faithful blocking of $a$:

\[
\begin{bmatrix}
1 & 0 \\
0 & 1 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
1 & 0 \\
\end{bmatrix}
\]

Action of $b$ on quotient groups:

$b: \{ \mathbb{Z}_6, b\mathbb{Z}_6 \} \rightarrow \{ b\mathbb{Z}_6, \mathbb{Z}_6 \}$

$b \sim (1,2)$

$b: \{ \mathbb{Z}_2, a\mathbb{Z}_2, a^2\mathbb{Z}_2, a^3\mathbb{Z}_2, a^4\mathbb{Z}_2, a^5\mathbb{Z}_2 \} \rightarrow \{ a\mathbb{Z}_2, a^2\mathbb{Z}_2, a^3\mathbb{Z}_2, a^4\mathbb{Z}_2, a^5\mathbb{Z}_2, \mathbb{Z}_2 \}$

$b \sim (1)(2)(3)(4)(5)(6)$

Faithful blocking of $b$:

\[
\begin{bmatrix}
0 & 1 \\
1 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
\end{bmatrix}
\]
Subgroups:

- Three “copies” of $\mathbb{Z}_6$
- $\mathbb{Z}_3$
- Three “copies” of $\mathbb{Z}_2$
- $\mathbb{Z}_2 \times \mathbb{Z}_2$
Group: $Dic_3$
This is the dicyclic group of degree three. Together, it represents two separate cycles.

Typical Presentation:
$\langle a, b | a^6 = e, b^2 = a^3, b^{-1}ab = a^{-1} \rangle$ or $\langle a, b, c | a^3 = b^2 = c^2 = e \rangle$

Product Notation: $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$
$\langle x, y | x^3 = y^4 = e, y^{-1}xy = x^{-1} \rangle$

Isomorphism between Groups:
$f: Dic_3 \rightarrow \mathbb{Z}_3 \rtimes \mathbb{Z}_4$
$f(a) = xy^2$
$f(b) = y$

Group Actions for Matrix Permutation Representation:
Chosen quotient groups:
$Dic_3/\mathbb{Z}_3 = \{\mathbb{Z}_3, y\mathbb{Z}_3, y^2\mathbb{Z}_3, y^3\mathbb{Z}_3\}$
$Dic_3/\mathbb{Z}_4 = \{\mathbb{Z}_4, x\mathbb{Z}_4, x^2\mathbb{Z}_4\}$

Action of $x$ on quotient groups:
$x: \{\mathbb{Z}_3, y\mathbb{Z}_3, y^2\mathbb{Z}_3, y^3\mathbb{Z}_3\} \rightarrow \{y\mathbb{Z}_3, y^2\mathbb{Z}_3, y^3\mathbb{Z}_3\}$
$x \sim (1)(2)(3)(4)$

$x: \{\mathbb{Z}_4, x\mathbb{Z}_4, x^2\mathbb{Z}_4\} \rightarrow \{x\mathbb{Z}_4, x^2\mathbb{Z}_4\}$
$x \sim (1,2,3)$

Faithful blocking of $x$:
\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
0 \\
0 \\
0 \\
1
\end{bmatrix}
\]

Action of $y$ on quotient groups:
$y: \{\mathbb{Z}_3, y\mathbb{Z}_3, y^2\mathbb{Z}_3, y^3\mathbb{Z}_3\} \rightarrow \{y\mathbb{Z}_3, y^2\mathbb{Z}_3, y^3\mathbb{Z}_3\}$
$y \sim (1,2,3,4)$

$y: \{\mathbb{Z}_4, x\mathbb{Z}_4, x^2\mathbb{Z}_4\} \rightarrow \{x\mathbb{Z}_4, x^2\mathbb{Z}_4\}$
$y \sim (2,3)$
Faithful blocking of $y$:

$$
\begin{bmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0
\end{bmatrix}
\begin{bmatrix}
0 \\
0 \\
0 \\
0
\end{bmatrix}
\begin{bmatrix}
1 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0
\end{bmatrix}
$$

Subgroups:

- $\mathbb{Z}_2$
- $\mathbb{Z}_3$ (normal)
- Three “copies” of $\mathbb{Z}_4$
- $\mathbb{Z}_6$
**Group:** $D_6$
This is the dihedral group of degree six, meaning it is the group of symmetries of a regular hexagon. In other words, the group describes six rotations and a flipping action on this hexagon.

**Typical Presentation:**
$$< x, y | x^6 = y^2 = e, yxy^{-1} = x^{-1} >$$

**Product Notation:**
$$D_6 \cong C_6 \rtimes C_2$$
$$D_6 \cong D_3 \times \mathbb{Z}_2$$
$$< a, b | a^3 = b^2 = e, bab^{-1} = a^{-1} >x < c | c^2 = e >$$

**Group Actions for Matrix Permutation Representation:**

*Chosen quotient groups:*
$$D_6/C_6 = \{C_6, yC_6\}$$
$$D_6/C_2 = \{C_2, xC_2, x^2C_2, x^3C_2, x^4C_2, x^5C_2\}$$

*Action of x on quotient groups:*
x: $\{C_6, yC_6\} \rightarrow \{C_6, yC_6\}$
x$\sim (1)(2)$
$$x: \{C_2, xC_2, x^2C_2, x^3C_2, x^4C_2, x^5C_2\} \rightarrow \{xC_2, x^2C_2, x^3C_2, x^4C_2, x^5C_2, C_2\}$$
x$\sim (1,2,3,4,5,6)$

*Faithful blocking of x:*

$$\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix}
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0
\end{bmatrix}$$

*Action of y on quotient groups:*
y: $\{C_6, yC_6\} \rightarrow \{yC_6, C_6\}$
y$\sim (1,2)$
$$y: \{C_2, xC_2, x^2C_2, x^3C_2, x^4C_2, x^5C_2\} \rightarrow \{C_2, x^5C_2, x^4C_2, x^3C_2, x^2C_2, yC_2\}$$
y$\sim (2,6)(3,5)$
Faithful blocking of $y$:

\[
\begin{bmatrix}
0 & 1 \\
1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

Subgroups:

- $\mathbb{Z}_6$ (normal)
- Two “copies” of $D_3$ (normal)
- Three “copies” of $\mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathbb{Z}_3$
- Seven “copies” of $\mathbb{Z}_2$
**Group:** $A_4$

This is the alternating group of degree four, or the group of all even permutations on four objects. It is a normal subgroup of $S_4$ and is the kernel of the “sign” homomorphism.

**Typical Presentation:**

$< a, b | a^3 = b^2 = (ab)^3 = e >$

**Product Notation:**

$A_4 = K_4 \rtimes C_3$

**Group Actions for Matrix Permutation Representation:**

*Chosen quotient groups:*

$A_4/K_4 = \{K_4, K_4(2,3,4), K_4(2,4,3)\}$

$A_4/C_3 = \{C_3, C_3(1,2,4), C_3(2,3,4), C_3(2,4,3)\}$

*Action of (1,2,3) on quotient groups:*

$(1,2,3): \{K_4, K_4(2,3,4), K_4(2,4,3)\} \rightarrow \{K_4(1,2,3), K_4(1,2,4)\} = \{K_4(2,3,4), K_4(2,3,4)\}$

$(1,2,3) \sim (1,2,3)$

$(1,2,3): \{C_3, C_3(1,2,4), C_3(2,3,4), C_3(2,4,3)\} \rightarrow \{C_3, C_3(1,3)(2,4), C_3(1,2)(3,4), C_3(1,2)(4)\} = \{C_3, C_3(2,3,4), C_3(2,4,3), C_3(1,2,4)\}$

$(1,2,3) \sim (2,4,3)$

**Faithful blocking of (1,2,3):**

\[
\begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{bmatrix} = 
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]

*Action of (1,2)(3,4) on quotient groups:*

$(1,2)(3,4): \{K_4, K_4(2,3,4), K_4(2,4,3)\} \rightarrow \{K_4(2,3,4), K_4(2,4,3)\}$

$(1,2)(3,4) \sim (1)(2)(3)(4)$

$(1,2)(3,4): \{C_3, C_3(1,2,4), C_3(2,3,4), C_3(2,4,3)\} \rightarrow \{C_3(1,2)(3,4), C_3(2,3,4), C_3(1,2,4), C_3(1,2,3)\} = \{C_3(2,4,3), C_3(2,3,4), C_3(1,2,4), C_3\}$

$(1,2)(3,4) \sim (1,4)(2,3)$

**Faithful blocking of (1,2)(3,4):**

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix} = 
\begin{bmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0
\end{bmatrix}
\]
**Subgroups:**
\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} = K_4 (normal)
-4 “copies” of \(\mathbb{Z}_3\)
-3 “copies” of \(\mathbb{Z}_2\)
Bibliography


[GAP2008]


*All labs prepared and executed in Maple 11, by Maplesoft.
VITA

Mark E. Medwid
740 Nagle Road
Erie, PA, 16511
markmedwid@gmail.com

Education:
Bachelor of Science Degree in Mathematics, Penn State University, Spring 2012
Bachelor of Science Degree in Secondary Ed, Penn State University, Spring 2012
Minor in Statistics
Honors in Mathematics
Thesis Title: Faithful Blockings of Finite Groups and Pedagogical Applications
Thesis Supervisor: Paul E. Becker

Related Experience:
Summer research project
Supervisor: Paul E. Becker
Summer 2010

Teaching field placement at Fort LeBoeuf High School
Supervisor: Robert L. Sensor
Fall 2011

Student teaching placement at Central Tech School
Supervisor: Robert L. Sensor
Spring 2012

Awards:
President’s Freshman Award
Dean’s List
School of Science Scholarship

Presentations/Activities:
Oral presentation at Sigma Xi conference (1st place – oral presentation in math)
Gliding Stars helper (a program for teaching special needs children to ice skate)