Visualizing a Group

Iris Anshel[1]

The need for resilient cryptographic methods has become ubiquitous. Group Theory, a foundational area of mathematics, is classically expressed through symbolic operations and algebraic notation. Given its inherent abstract and broad nature, it serves as a resource and a foundation for essential tools that enables many cryptographic methods. With the goal of making group theory, its applicability, conceptual elegance, and practical versatility approachable, this paper introduces a visual method, partially colored squares, for representing elements in a group, and the operations used to work with said elements.

This paper proceeds as follows: it introduces group elements as sequences of colored squares and the mirror images of these squares; it introduces the universal rules that are intrinsic to any group via these colored squares and their mirror images that represent a group. A given example of a group will have further rules that allow for systematic substitution and manipulation, and the derivation of new relations. It is the presence of these relations that fosters cryptographic security. This paper demonstrates that the visualization represented herein serves two purposes: one, it provides an intuitive educational tool for exploring group structure; and two, it supports a method for obfuscating group elements, which is a key requirement in cryptographic protocols. This visual representation facilitates understanding a rule-based method of transforming a group element, viewed as a sequence, via random substitutions to visual sequences, thereby allowing one to alter the appearance of a group element without changing its underlying identity. This algorithmic transformation of the element can serve as an essential tool in any cryptographic protocol.

Section 1: Introduction to Group Elements

A group can be visualized as a collection of sequences of partially colored squares and their mirror images. In the case of two colors, blue and red, a sequence can take the following form:

Sequences can be combined by juxtaposing one with the other. Let us start with two sequences,

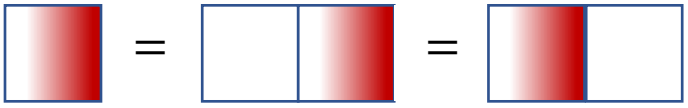
by combining them the following new sequence below is obtained.

In addition to the colored squares and their mirror images, every group contains a unique empty square, which can be considered as an abstraction of the number 0 in addition.

When colored squares are placed next to each other there are universal rules that will always hold, and in addition, there will be specific rules that hold for a particular group. The next section sets forth the Universal Rules.

Section 2: Universal Rules

Universal Rule 1. Any colored square (or its mirror image) when juxtaposed with the empty square remains unchanged. In the two-color case we have the following identities:



The above rule demonstrates why the empty box can be thought of as an abstraction of the number 0 when we view juxtaposition as an abstraction of addition. Thus, for any number n, the analog of the first universal rule is $n = 0 + n = n + 0$.

Universal Rule 2. Juxtaposing any colored square with its mirror image yields the empty square For illustrative purposes, looking at the red square visuals below, we intuitively see the color white abutting white exploding, and similarly, with red abutting red imploding. Using the visual construct above, we see the following:

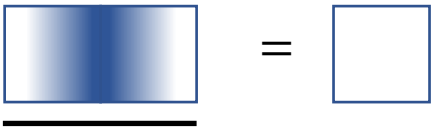
Returning to the arithmetic analogy, the mirror image of n is $-n$, and, thus, for any number n, the analog of the second universal rule is $0 = n + (-n) = -n + n$.

Sequence Simplification. As an example of how the above rules are used consider what happens when the original sequence,

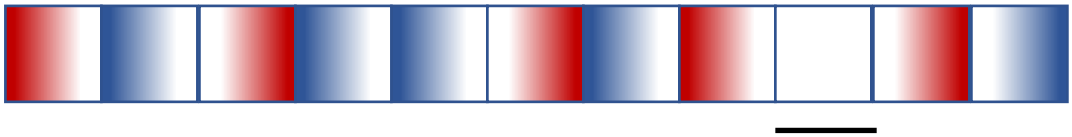
is combined with the following, second sequence.

We first obtain the following longer sequence.

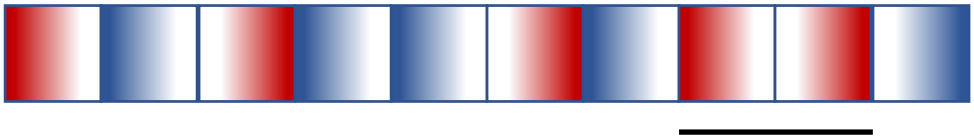
Using Universal Rule 2 the second universal rule, the underlined squares can be replaced by an empty square:



By substituting the empty square for the blue square abutting its mirror image, we obtain an initial simplification:



Given Universal Rule 1, the empty square (which is likewise underlined) can then be deleted using the Universal Rule 1 to yield the next simplification:

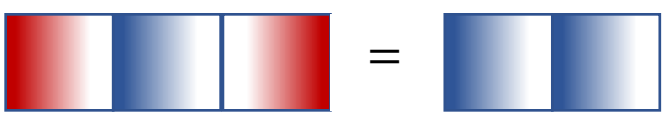


The underlined red squares can be eliminated in the exact same way as we eliminated the blue squares above, yielding the sequence,

where we may yet again eliminate the underlined blue squares. The final sequence obtained is given below.

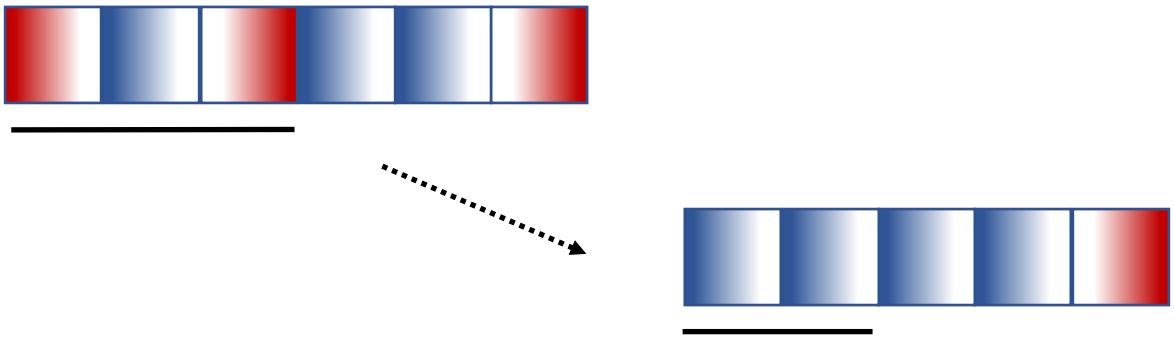
Section 3: Group Relations

To understand group relations, which are, definitionally, additional stipulated rules involving the colored squares and their mirror images, in the context of our visualization we look at an instance of a single group relation (in general, most groups will have many such relations). Consider the following Group Relation (1):

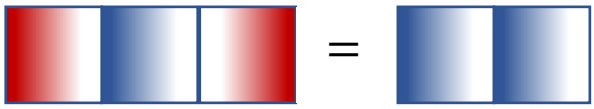


To see the impact of the group relation will have on sequences we look at the following sequence:

The Group Relation (1) allows us to substitute the left side of the relation with the right side of the relation. In the above sequence, the underlined squares coincide with the left part of the Group Relation (1), and hence yields the following transformation (indicated by the dotted arrow).

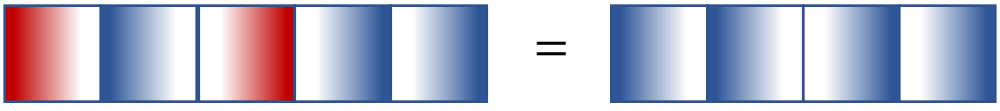


It should be noted that the one group relation, when combined with the universal rules, will generate a collection of new relations that will prove to be very useful. Beginning again with the Group Relation (1),

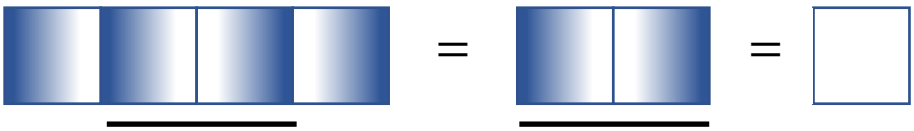


we juxtapose both sides with the sequence

which yields the following identity.



By applying the Universal Rules to the right-hand side of the above identity twice, we see that the right-hand side reduces to the empty square,



and we deduce the following relation:

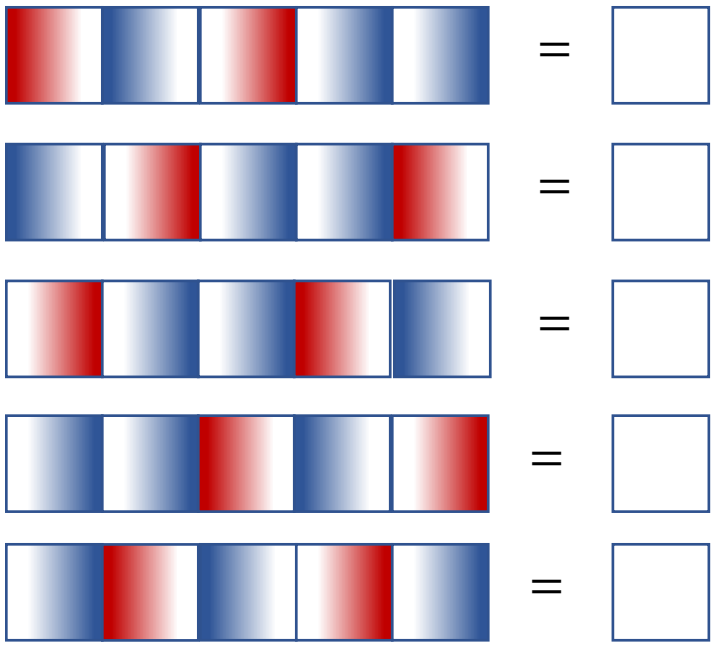
From this relation we now proceed to generate a set of relations by iterating the following process: juxtapose both sides of the relation on the left with the mirror image of the left most square from the left side of the relation.

Again, applying the Universal Rule 2 to the left side and Universal Rule 1 on the right side we obtain the following:

Next, juxtapose both sides of this identity on the right with the mirror image of the square in the right side,

and applying the first universal rule once more to the right-hand side we see that we have derived the following relation.

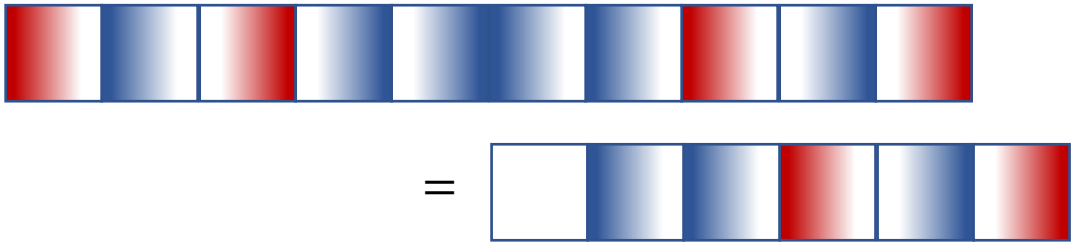
The above routine will produce three additional relations. The complete list is given below.



In addition to the relations above, the initial group relation, which we put in the form,

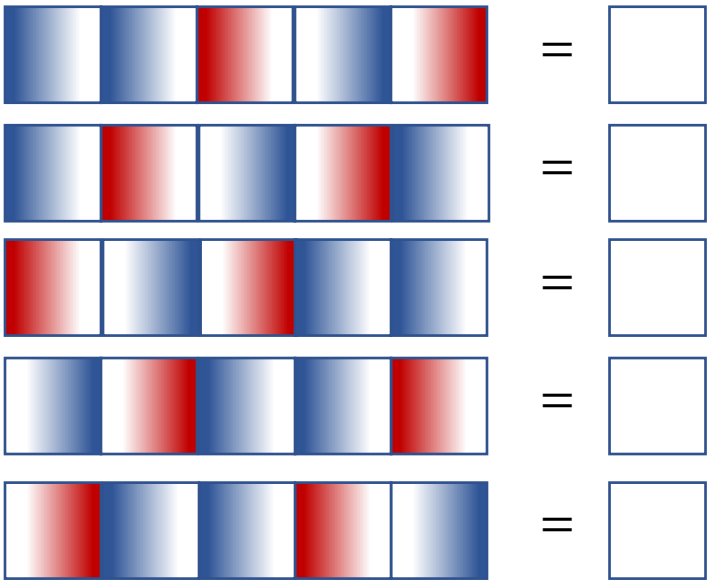
also generates another relation when we take the mirror images of both sides. To see this first note that the mirror image of the empty square is yet again the empty square, and the mirror image of the left hand side of the group relation is given below.

Juxtaposing this latter sequence to the right side of both sides of the relation gives us a new relation: the universal relations, used multiple times, demonstrates that the equality



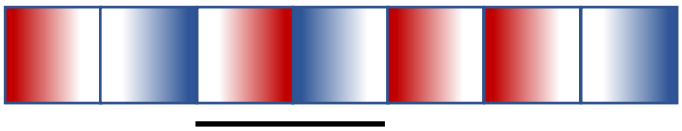
implies that

which is the relation we were seeking to verify. The process of deriving a list of new relations from the original one can be applied here and will yield the following relations.

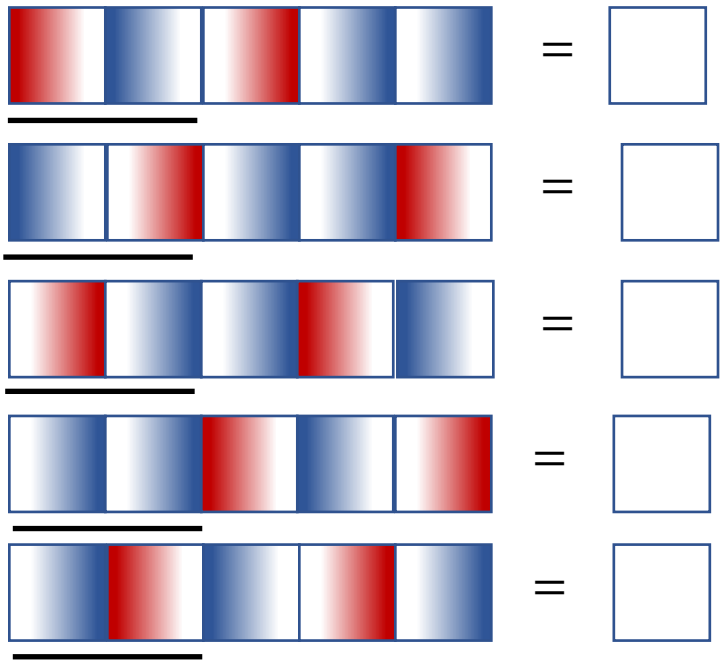


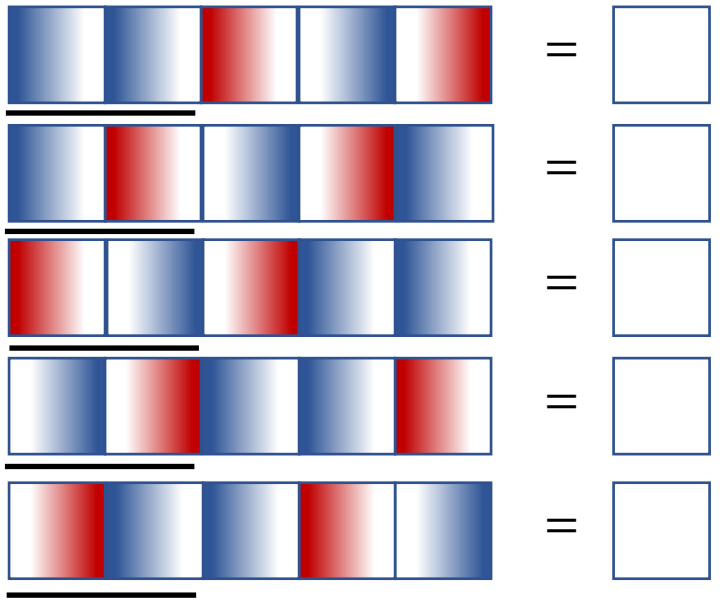
Section 4: Obfuscation Method for Cryptography

When using a group in an environment for a cryptographic process, a collection of relations can be used to obfuscate the structure of an element in the group, e.g., a sequence of colored boxes in our visualization. We illustrate the process with following example: beginning with the sequence



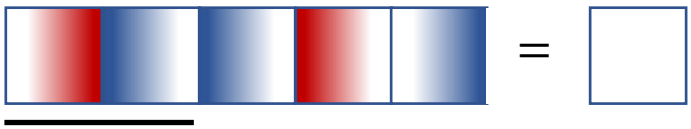
focus on the randomly chosen underlined subsequence. Since there are two squares in the subsequence, the method begins by looking at all the sequences consisting of the first two squares, starting at the left, of each of the relations.





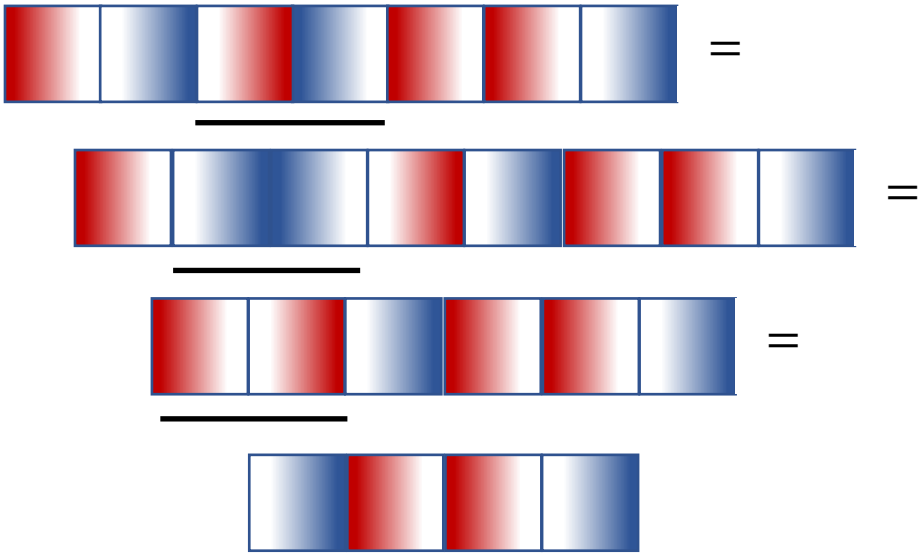
The sequence of two squares, termed a subsequence, we are searching for is,

which appears, reading from the left, at the beginning of the last relation.



From this relation we see that,

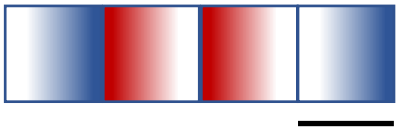
After replacing the left-hand side sequence by the righthand side, and using the universal relations (such areas are underlined), the original sequence becomes



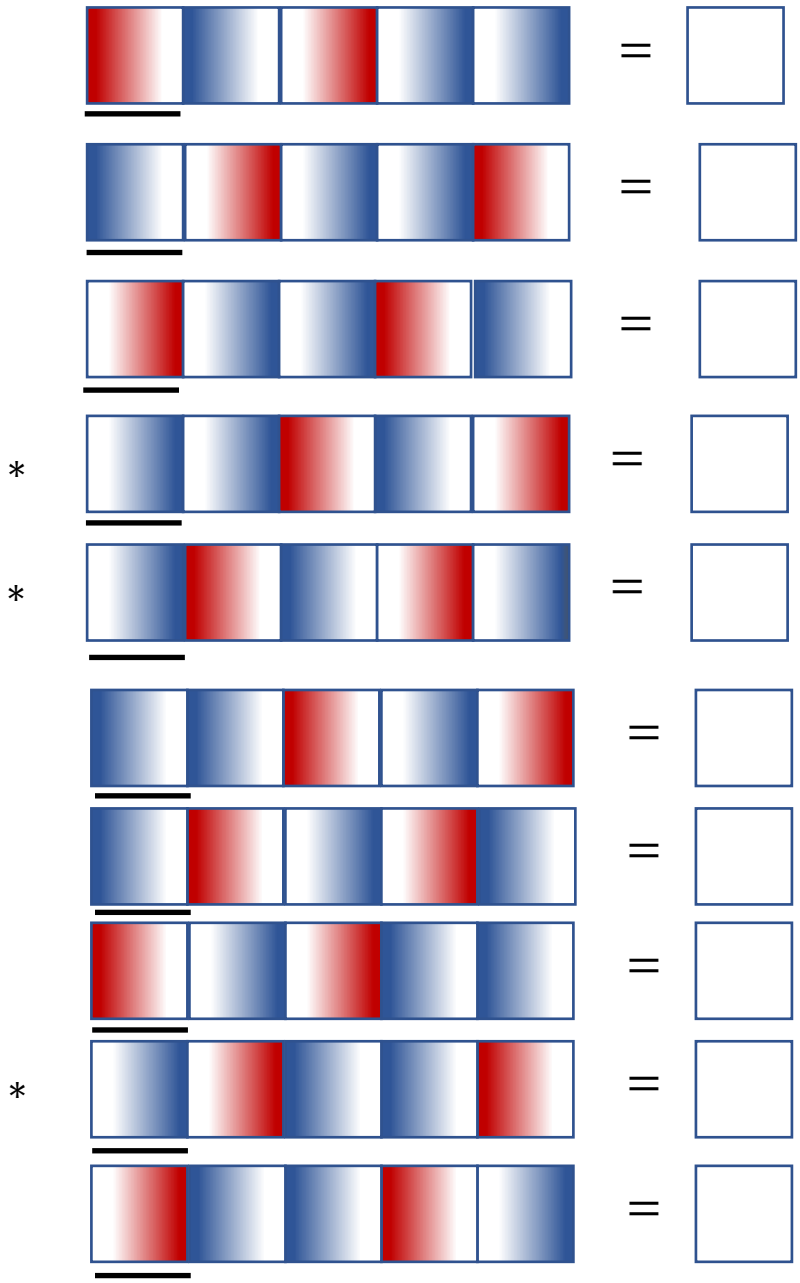
We continue in this way, choosing randomly selected subsequences, and searching for instances of this subsequence at the beginning of each relation. There are times where a given subsequence may be replaced in more than one way. When this situation arises, a random choice is made

between the possibilities. Continuing with the example above, we perform an additional step to make the illustration of the method more complete.

Randomly, we choose the (underlined) subsequence

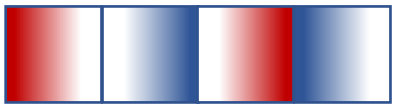


and again, we search through the collections of relations for an appearance of this subsequence starting on the left of each relation

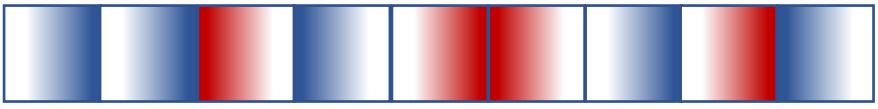


There are three appearances of the underlined subsequence (each marked with a *), and we randomly choose the first of these.

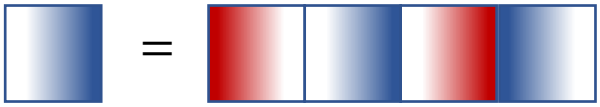
Juxtaposing both sides of the relation on the right with the sequence



we obtain

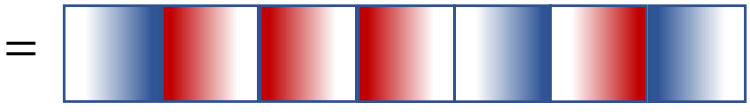


and using the universal rules multiple times, we arrive at the identity below.



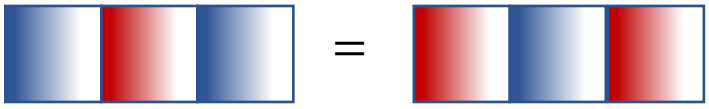
Recalling the original sequence equals

we now conclude the illustration by substituting the rightmost square on the right side of the identity.



Section 5: Transformational Equivalences

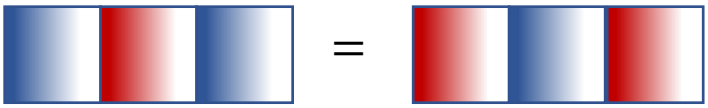
As a final illustration of this visualization method of a group, we consider at a group based, as before, on two colored squares and their mirror images, but this time with the following relation:



Suppose we introduce two new colored squares, yellow and green which are defined to be sequences of the original two:

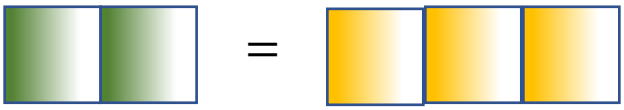
We see that any sequence of green and yellow squares can be turned into a sequence of red and blue squares one using this definition. Notice that,

and, using the relation

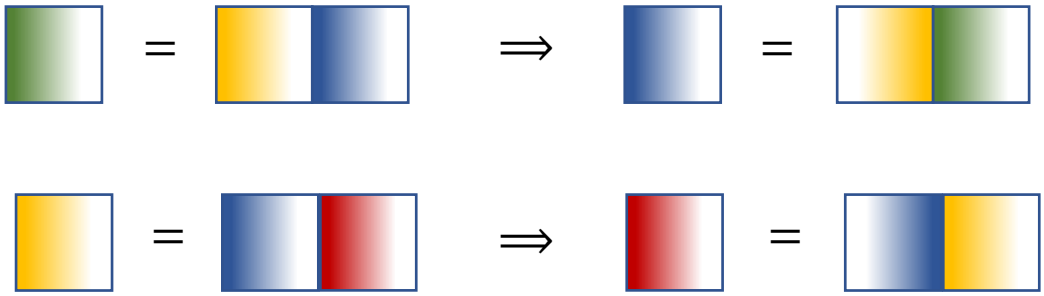


we deduce that

and we have derived the relation between the green and the yellow squares.



This is an alternate way to visualize the original group; we started with red and blue shaded squares and a first relation, and moved to a group based on green and yellow squares with a different relation. For completeness we note that starting with a sequence of red and blue squares, we can make the following substitutions to transform the sequence in one consisting of green and yellow squares. The substitutions we use are given below.



Section 6: Conclusion

Group theory can serve as a basis for cryptography when we transform the key components that emerge in the field, e.g., messages, user chosen passwords, into elements of a group. The methods of transforming the elements of a group, which our visualization approach makes intuitive, are essential. Of particular note are digital signatures of messages which enable authenticity to be verified. When both the message and the signer's chosen passwords are transformed into elements of a group a digital signature can be generated which will be verifiable. A key feature of this process will be an obfuscation method, such as the one depicted via the colored squares.