M_{13}

J. H. Conway

Summary The group M_{12} has no transitive extension, but the object of the title is the next best thing: a *set* of permutations which is an extension of M_{12}. We give an elementary construction, based on a moving-counter puzzle on the projective plane of order 3, and provide easy proofs of some of its properties.

1 Introduction

Long ago I was intrigued by the fact that M_{12}, É. Mathieu's celebrated quintuply transitive group on 12 letters, shares some structure with $L_3(3)$, which acts doubly transitively on the 13 points of the projective plane PG(2, 3), of which it is the automorphism group.

To be more precise, the point-stabilizer in $L_3(3)$ is a group of structure $3^2{:}2S_4$ that permutes the 12 remaining points imprimitively in four blocks of 3, and there is an isomorphic subgroup of M_{12} that permutes the 12 letters in precisely the same fashion. Again, the line-stabilizer in $L_3(3)$ is a group of this same structure that permutes the 9 points not on that line in a doubly transitive manner, while the stabilizer of a triple in M_{12} is an isomorphic group that permutes the 9 letters not in that triple in just the same manner.

In the heady days when new simple groups were being discovered right and left, this common structure inevitably suggested that there should be a new group that contained both M_{12} and $L_3(3)$, various copies of which would intersect in the subgroups mentioned above. Of course this turned out not to be the case, but some years ago I found an almost equally satisfactory explanation — M_{12} and $L_3(3)$ are indeed both subgroups of the same object, but that object is not a group! I call it M_{13}.

Sections 2–6 will be purely descriptive, and contain numbered assertions, which will be proved in Section 7.

2 Definition of M_{13}

Since

M_{12} is a set of $95040 = 12.11.10.9.8$ permutations of 12 letters, (1)

we might expect that

M_{13} is a set of $1235520 = 13.12.11.10.9.8$ permutations of 13 letters; (2)

and since

M_{12} is quintuply transitive, (3)

we might hope that

$$M_{13} \text{ is sextuply transitive.} \tag{4}$$

These expectations turn out to be true, but we must be careful about the meanings of the terms.

Unfortunately, the word "permutation" retains two distinct senses — it may refer either to a particular *arrangement* of n objects, or to a particular operation of *rearranging* them, the latter usage being common among group theorists and the former among the public at large.

We shall define M_{13} to be a particular set of permutations of 13 objects in the lay sense, namely certain ways of putting 12 lettered counters and one hole on the points of a projective plane $P = \mathrm{PG}(2,3)$.

We can think of this in terms of a "13-puzzle" analogous to Sam Loyd's famous 15-puzzle, wherein 15 square tiles and one hole are arranged in a 4×4 tray, the object being to proceed from one given arrangement to another by a sequence of moves in each of which the hole is exchanged with one of the adjacent tiles.

In our 13-puzzle, any counter a determines at any time a line that joins its present position to that of the hole. A move of the puzzle is to put the counter into the hole (that is, onto the "holy point", as we shall call it), *and at the same time to interchange the positions of the other two counters* b *and* c *on this line.* We shall refer to this as the move $a|bc$.

To avoid circumlocution, we refer to the point occupied by the counter labelled a as "point a", and the holy point as "point $\circ$".

M_{13} consists of all the arrangements (of counters and hole) that can be obtained from a given one by moves of this type.

In the language of category theory, M_{13} is a *groupoid*, (a category in which all arrows are invertible), whose objects are the 13 positions of the hole, and whose arrows are the rearrangements produced by legal sequences of moves; the initial and terminal objects of an arrow are the positions of the hole before and after the moves are made.

3 The first few moves

Figures 1–4 show the way we shall draw the projective plane P. In Figure 1, the points of the plane are numbered 0–11 and ∞, and to avoid awkward bends some of the points on some lines are indicated by hooks. We have chosen this particular way of drawing the plane so as to emphasize the close relationship with the "MINIMOG" array (see Figure 2).

Figure 3 shows the usual coordinatization of the plane. The 9 points on the right are those of the corresponding "Euclidean" or "affine" plane, the point marked XY being that with affine coordinates (X,Y) or projective coordinates $(X,Y,1)$. This is extended to the projective plane by adjoining the "line at

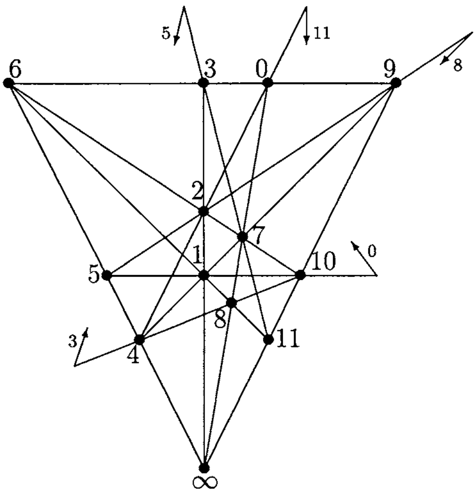


Figure 1: PG(2, 3)

6	3	0	9
5	2	7	10
4	1	8	11

Figure 2: The MINIMOG

infinity" on the left, whose point marked m (for $m = 0, 1, 2$) has projective coordinates $(1, m, 0)$ and lies on the three parallel lines $y = mx + c$, while that marked ∞ has coordinates $(0, 1, 0)$ and lies on the three "vertical" lines $x = c$.

In Figure 4 we display only the y-coordinates of the points other than ∞. There are 4 "vertical" lines (passing through the point ∞), and the 9 others meet these in the points determined by one of the 9 words

$$0\,000,\ 0\,111,\ 0\,222,\ 1\,012,\ 1\,120,\ 1\,201,\ 2\,021,\ 2\,102,\ 2\,210$$

of the "tetracode" (see [3], [2]). The typical tetracode word is

$$m \;\; c\; c+m\; c+2m$$

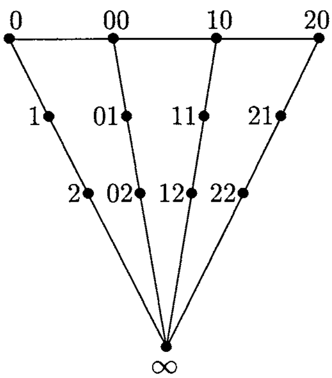


Figure 3: Coordinates

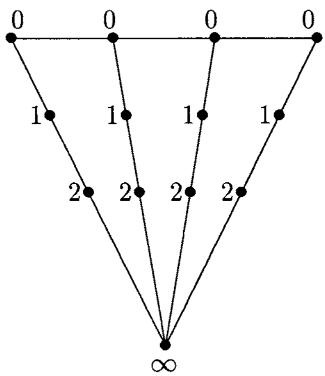


Figure 4: Tetracode coordinates

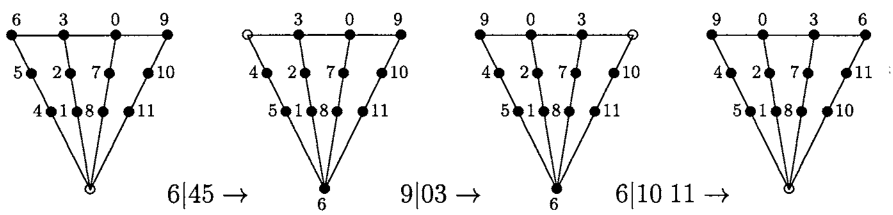
in which the last three digits form an arithmetic progression (mod 3), whose "slope" m is the first digit. For example, the line $\{5, 3, 7, 11\}$ of Figure 1 is called 1 012 in Figure 4.

It should be obvious that the set of permutations of the counters that can be achieved by move sequences that restore the hole to its original position at ∞ forms a group; anticipating a later result, we call this "the group M_{12}".

Figure 5 shows a few successive moves in the 13-puzzle, whose effect is to move the hole around a triangle and restore it to its original position, interchanging the four pairs

$$(4, 5),\ (3, 0),\ (6, 9),\ (10, 11)$$

of counters as it does so. This gives us an element of M_{12}. We call a permutation of this sort a *triangular permutation.*



$$(4\ 5)(6\ 9)(0\ 3)(10\ 11) \in M_{12}$$

Figure 5: A triangular permutation

Look at the action of this permutation on the middle two of the four "vertical" lines. The points $1, 2, 7, 8$ are fixed, and 3 and 0 are interchanged. By symmetry, we see that M_{12} contains a permutation that swaps any two points lying on distinct verticals, and leaves the other four points on these verticals unchanged.

This shows that M_{12} acts transitively on the 12 counters, since we can use one of the above moves to take any given counter off the leftmost vertical (if necessary), and then another to bring it back to the topmost point of that vertical. Indeed it also establishes double transitivity, since two more such moves (at most) are needed to bring the second of two given counters to the second point of the leftwise vertical. One could prove triple transitivity in the same way, but this will not be necessary.

4 The hexads

The classical M_{12} is known to permute a collection of 132 hexads that form a so-called Steiner system $S(5, 6, 12)$. How do we recognize these in our picture?

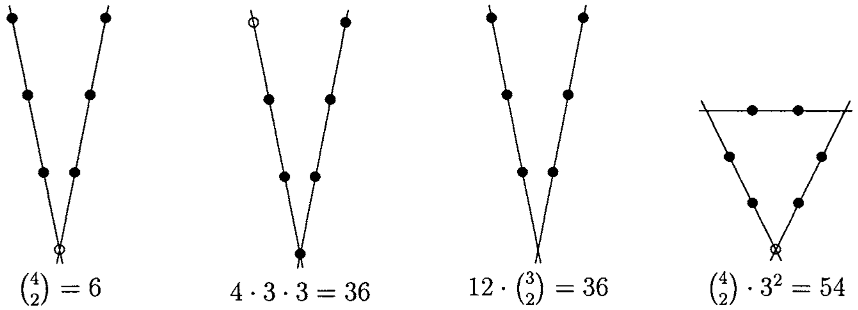


Figure 6: Hexads

Figure 6 shows the answer. At any instant, two lines contain either 6 counters and the hole, in which case these counters form a hexad; or 7 counters, from which we form a hexad by removing the counter at the intersection of the two lines. There is a further type of hexad, consisting of the points (other than the vertices) lying on the lines of a triangle one of whose vertices is the holy point. The Figure shows the four different geometrical appearances that a hexad can assume, and counts the hexads, showing that there are 132 in all.

Note that the triangular permutation shown in Figure 5 fixes the hexad $\{0, 1, 2, 3, 7, 8\}$ and induces the transposition $(0\ 3)$ on it.

One could easily give a case-by-case verification that

> a move of the 13-puzzle takes every hexad to another hexad, although possibly of a different shape. (5)

One could also check that

> no two distinct hexads can contain the same 5 points, and hence the hexads form an $S(5, 6, 12)$, (6)

and that

> M_{12} acts transitively on the hexads. (7)

5 The doublings of M_{13}

The group M_{12} is known to have Schur multiplier of order 2. This reveals itself by the existence of a group $2M_{12}$ that has a homomorphism onto M_{12} with kernel of order 2. This group can be constructed as a group of *monomial permutations* of ± 12 letters: that is to say, it permutes 24 symbols, say

$$+a, -a, +b, -b, \ldots, +k, -k, +l, -l$$

in such a way that we obtain the permutations of M_{12} simply by ignoring the signs. The non-trivial element of the kernel negates all 24 symbols. Is there an analogous $2M_{13}$?

Indeed there is! We can obtain it by labelling the opposite sides of each of our counters with the two signed versions of the appropriate letter. But now when we move some counter into the hole, the two other counters that we interchange must also be turned over. We call this the ± 13-puzzle.

It turns out that

> the monomial permutations realized by sequences of the new moves that return the hole to its original position ∞ do indeed form the usual group $2M_{12}$. (8)

Moreover,

> $2M_{12}$ is *doubly transitive in the monomial sense*; that is, given two pairs a, b and c, d of distinct letters and any signs $\alpha, \beta, \gamma, \delta$, there is an element of $2M_{12}$ which maps αa to γc and βb to δd. (9)

Since we have already shown the double transitivity, it is enough to show that $2M_{12}$ contains an element fixing one counter of the ± 13-puzzle and reversing another. Such an element is easily discovered. For example, the product of the triangular permutations obtained from the triangles $\infty 69$, $\infty 30$, and $\infty 6\ 10$ fixes 4 and negates 3.

The automorphism group of the classical M_{12} is a group $M_{12}.2$ that permutes 24 letters in two sets of 12, with the properties

> each permutation of the original M_{12} extends uniquely to a permutation of the 24 letters, and an outer automorphism interchanges the two sets of 12 letters. (10)

Is there an analogous $M_{13}.2$?

Indeed there is! To obtain it, we enlarge the 13-puzzle to the "26-puzzle" by adjoining an additional hole ◯ and 12 new counters

$$A, B, \ldots, K, L$$

that we associate with the lines of P in the same way as the old ones are associated with the points. However, we also demand that the "holy point" must always be incident with the "holy line". This entails that whenever we make a point-move $a|bc$, the four points involved must form the holy line. Dually, we now have "line-moves", say $A|BC$, for which the four lines involved must pass through the holy point.

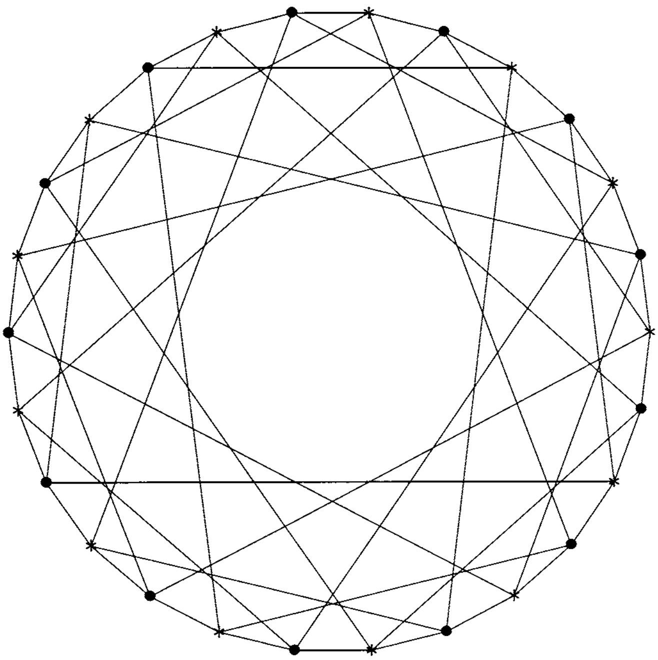
Any sequence of moves in the 26-puzzle yield a legal sequence of moves in the 13-puzzle if we just ignore the line-counters. It might seem that the incidence condition would restrict our freedom; but in fact an arbitrary sequence of point-moves can still be performed, by interleaving them with the appropriate line-moves. Thus, if we wish to follow a point move on the line L_1 by another on a different line L_2, we need merely interpose the line-move that moves the hole from L_1 to L_2.

In this way, for any permutation of M_{12} we can find a sequence of alternating point and line moves that effects that permutation of the point counters, and also restores both holes to their original positions (say, the point ∞ and the line at infinity). It turns out that

> the resulting permutation of the line-counters is uniquely determined, giving the extension of M_{12} to a group on 24 letters, doubly transitive on both sets of counters. (11)

We therefore define $M_{13}.2$ to be the set of *all* permutations of the 26 counters and holes obtainable from the starting position by moves of the 26-puzzle.

The group $M_{12}.2$ has a double cover $2M_{12}.2$ containing the group $2M_{12}$ that we described earlier. This also has an analogue, $2M_{13}.2$, obtained by using both sides of both sets of counters. Provided that $\circ, a, b, c$ lie on the current holy line $\bigcirc$, we can make a point-move $a|bc$ that puts a in the hole and interchanges and negates both b and c; dually, provided $\bigcirc, A, B, C$ pass through the current holy point $\circ$, we can make the line-move $A|BC$ that puts A in the hole and interchanges and negates B and C. We call it the "±26-puzzle".



$\bullet$ = point, $\ast$ = line

Figure 7: The incidence graph of PG(2, 3)

6 The inner product

We regard the symbols on the counters of the ± 26-puzzle as vectors $\pm u$ (for points) and $\pm V$ (for lines), and introduce an *inner product* between the two sets. We define (u, V) to be -1 just if either u and V are incident with each other, or both are incident with the current holes; otherwise $(u, V) = +1$. In terms of the *incidence graph* of the plane (which has vertices that correspond to the points and lines, with edges corresponding to the incident pairs, see Figure 7), (u, V) is equal to -1 just if either is *accessible* from the other — that is to say, if there is a path from u to V that contains no other counter.

It is quite remarkable that

> this inner product is unchanged by making any legal move of the ± 26-puzzle. (12)

To see this, look at the effect of a point-move $a|bc$ in the incidence graph. Figure 8 shows that the same line-counters N, P, Q, R, S, T are accessible from a before and after the move, while those accessible from either b or c before the move are precisely those *not* accessible from $-b$ or $-c$ after it. (Thus, R, S, T, U, V, W are initially accessible from b, while N, P, Q, X, Y, Z become accessible from $-b$.)

It turns out that

> the hexads that were introduced in an *ad hoc* way earlier can now be given a simple uniform definition. (13)

If V and W are labels from any two line-counters, there are 6 point-counters whose labels u satisfy $(u, V) = (u, W)$, which form a hexad $[V, W]$; the remaining 6 satisfy $(u, V) = -(u, W)$ and form the hexad $[V, -W] = [-V, W]$.

Let H be the Gram matrix of the inner product: its rows and columns are indexed by points and lines, the entry in row u and column V being (u, V).

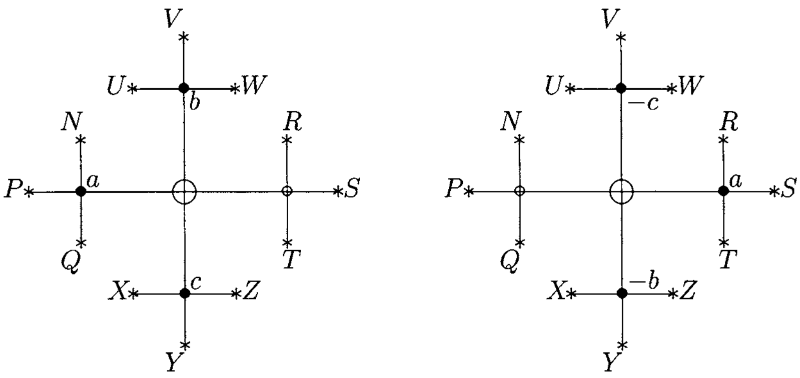


Figure 8: Invariance of the inner product

Then any two columns of H agree and disagree in sets of points forming hexads. So $H^\top H = 12I$, and H is a *Hadamard matrix*.

7 The proofs

It is trivial to check (13): in the new notation, the representative hexads of Figure 6 are as shown in Figure 9. Again, since the hexads are defined in terms of the inner product, (12) immediately implies (5). We can also see that they must be permuted transitively (as claimed in (7)): to move $[V, W]$ to $[X, \pm Y]$ it suffices to move V to X and W to $\pm Y$ (using the dual of (9)).

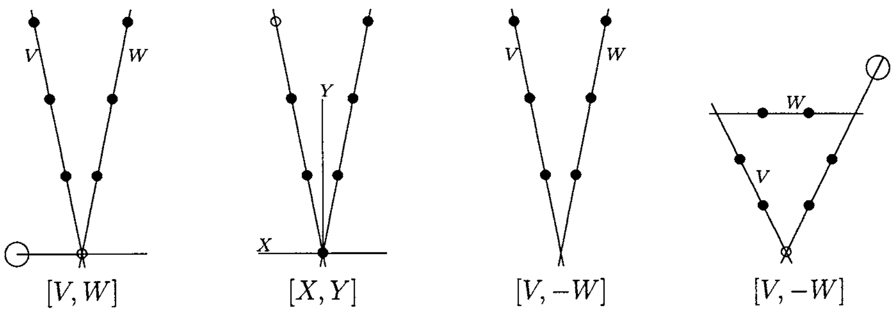


Figure 9: Hexads defined by the inner product

We now prove (10) and (11). Let P and Q be the matrices representing the monomial permutations of points and lines derived from any sequence of moves. Then $P^{-1}HQ = H$, by (12). In particular, $Q = H^{-1}PH$ is uniquely determined by P (since H is invertible). The interchange of point and line counters is effected by a polarity of the plane which swaps the positions of the two holes.

Consider a sequence of point and line moves which leaves every point counter fixed (possibly reversed). Then P is a diagonal matrix with $P^2 = I$. Suppose that $P \neq \pm I$. Since $H^\top PH = 12Q$, we see that P has six entries $+1$ and six entries -1, and the set of six positions where the $+1$s occur meets every hexad in 0, 3 or 6 points. However, no such set can exist. So $P = Q = \pm I$.

The proof of (6) is most easily seen using the Hadamard matrix H, or (for convenience of notation) $H^\top$. By column sign changes, the first three rows of $H^\top$ may be assumed to be

$$\begin{matrix} + & + & + & + & + & + & + & + & + & + & + & + \\ + & + & + & + & + & + & - & - & - & - & - & - \\ + & + & + & - & - & - & + & + & + & - & - & - \end{matrix}$$

If these rows are V, W, X, then clearly $[V, \pm W] \cap [V, \pm X] = 3$. For any other row Y, if Y has a entries $+$ among the first three, then $[V, \pm W] \cap [X, \pm Y]$

is $2a$ or $6-2a$, which is even in either case. So no two hexads can meet in five points. The average number of hexads containing a set of five points is $132.6/\binom{16}{5}=1$; so any five points lie in a unique hexad.

What is the order of M_{12}? We know by (7) that M_{12} acts transitively on hexads. Moreover, the transpositions induced on the hexad $\{0,1,2,3,7,8\}$ by triangular permutations as in Figure 5 generate S_6. Further, the group K fixing a hexad pointwise is trivial (see below). So

$$|M_{12}| = 132.6! = 12.11.10.9.8.$$

Thus, (1) holds. The quintuple transitivity of M_{12} follows: give two 5-tuples, we find $g \in M_{12}$ mapping the hexad $\mathcal{H}$ containing the first tuple to the hexad $\mathcal{H}'$ containing the second; then we may use the symmetric group on $\mathcal{H}'$ to move the tuple to its required position. Thus, (3) holds. The corresponding facts (2) and (4) about M_{13} hold because M_{13} is the union of 13 translates of M_{12}, one for each possible position of the hole.

The fact that the pointwise stabilizer K of a hexad $\mathcal{H}$ is trivial follows from the structure of the Steiner system. Given a *duad* $\{x,y\}\subseteq\mathcal{H}$, the three sets $\mathcal{H}'\setminus\mathcal{H}$, for hexads $\mathcal{H}'\supseteq\mathcal{H}\setminus\{x,y\}$, form a *syntheme* on the complement of $\mathcal{H}$ (a partition into three sets of size 2). Distinct duads give distinct synthemes. Now K fixes all duads on $\mathcal{H}$, and hence all synthemes on the complement; so $K=1$.

Finally, the identification of M_{12} and the related groups with the "classical" versions follow from properties of the classical versions: for example, there is a unique Steiner system, whose automorphism group is M_{12}; and there is a unique Hadamard matrix whose group of monomial automorphisms is $2M_{12}$ (see [2]).

8 Further comments

In view of the fact that

$$13.132 = 1716 = \binom{13}{6},$$

we might wonder if it is possible to partition all the 6-element subsets of a set of size 13 into disjoint copies of $S(5,6,12)$, each omitting one point of the set. In fact this is impossible, even though the analogous partition of 4-element subsets of a 9-element set can be done in two distinct ways [1]. So it is worth seeing how close we get. For each position of the hole, the 132 hexads define a $S(5,6,12)$ on the remaining points. However, not every 6-element set occurs as a hexad in one of these Steiner systems, and some occur more than once. Ignoring the hole, the hexads are of three geometric types. The union of two lines with the intersection removed occurs as a hexad for 7 positions of the hole; the three sides of a triangle with the vertices removed, for 3 positions; and the union of two lines with a point on one line removed, just once.