CDM

Representations

Klaus Sutner

Carnegie Mellon University

Consider a field $\mathbb{F}$ and a vector space V over $\mathbb{F}$. The collection of all bijective linear maps $V \to V$ naturally forms a group under composition, called the general linear group $\mathrm{GL}(V)$.

For our purposes, we will focus on $\mathbb{F}_8$, the 8-element field, considered as a 3-dimensional vector space over the 2-element field $\mathbb{F}_2$. We can think of $\mathbb{F}_8$ as the quotient ring $\mathbb{F}_2[X]/(X^3 + X + 1)$. Naturally, we can interpret the equivalence classes of polynomials as polynomials of degree less than 3, and those as coefficient vectors in $\mathbb{F}_2^3$. By abuse of notation, we can even think of those vectors as binary expansions of naturals $\{0, 1, 2, \ldots, 7\}$.

Exercise

Unpack the last paragraph.

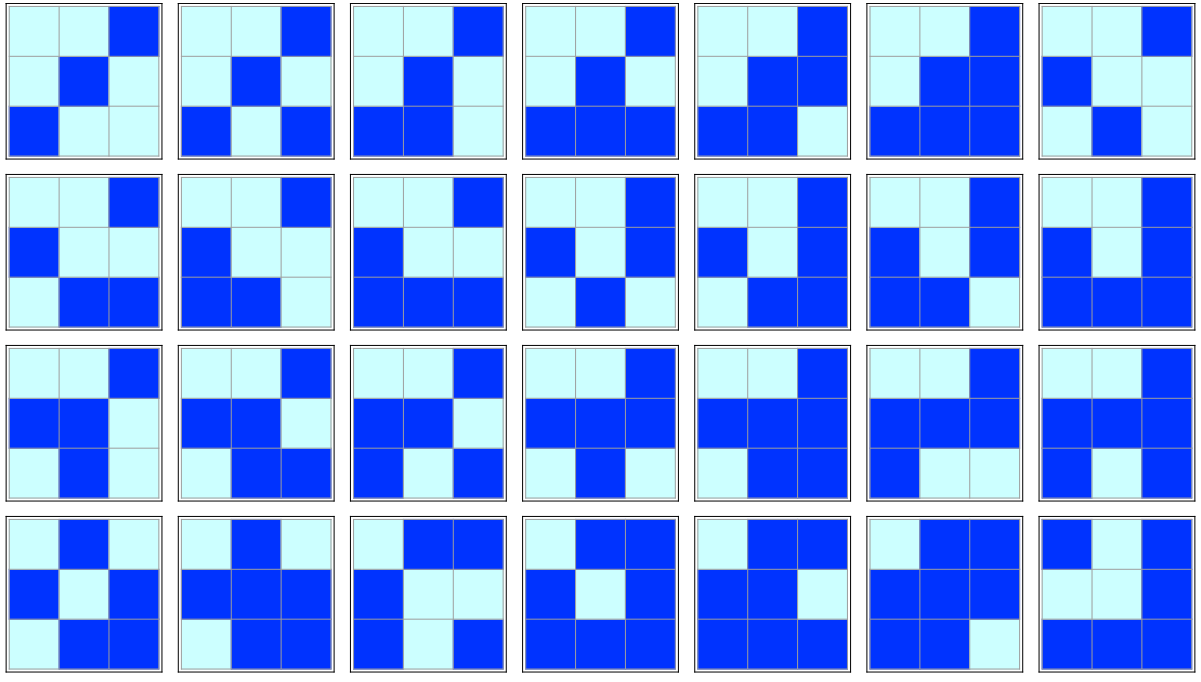
We have a perfectly precise definition of the group $\mathrm{GL}(\mathbb{F}_8)$, but how does one work in this structure? For example, how do we determine its cardinality?

It is rather inconvenient to have to manipulate linear maps directly. A better approach is to resort to linear algebra: by fixing a basis B of $\mathbb{F}_8$, we can represent linear maps as 3×3 matrices over $\mathbb{F}_2$.

Let's use the standard basis $B = (1, X, X^2)$, or, in coefficient vector notation, $B = (100, 010, 001)$.

It is easy to see that there $8^3 = 512$ linear maps $\mathbb{F}_8 \to \mathbb{F}_8$, each described by a matrix in $\mathbb{F}_2^{3\times 3}$. Composition of linear maps here translates nicely into multiplication of matrices.

Alas, we need to filter out the matrices with determinant 1. Brute-force computation shows that there are 168 such matrices, and, up to symmetry only 29. Here are the first 28 of them.

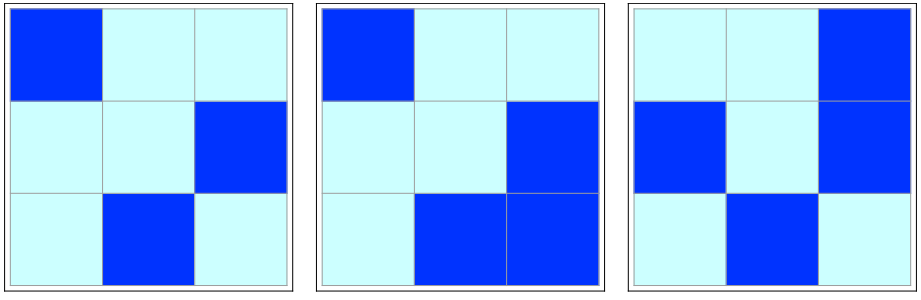


Exercise

Find the missing matrix (this is doable by hand; first figure out how this picture was constructed).

The matrix group is usually referred to as GL$(3,2)$ or GL$(3,\mathbb{F}_2)$. So GL$(3,2) \simeq$ GL$(\mathbb{F}_8)$, and this representation is computationally useful.

As an example, consider the following 3 matrices A_1, A_2 and A_3 representing invertible linear maps f_1, f_2 and f_3:



The corresponding linear maps, in coefficient vector notation:

z	000	100	010	110	001	101	011	111
$f_1(z)$	000	100	001	101	010	110	011	111
$f_2(z)$	000	100	001	101	011	111	010	110
$f_3(z)$	000	010	001	011	110	100	111	101

Question: Can we verify that 168 is the correct order of the two groups?

The first row r_1 of any matrix in M can be chosen freely from 7 non-zero bitvectors of length 3.

The second row r_2 can be chosen freely as long as it is independent from r_1. There are 6 possibilities.

The third row r_3 can be chosen freely as long as it is independent from r_1, r_2. There are 4 possibilities.

Hence the cardinality of M is indeed $7 \cdot 6 \cdot 4 = 168$.

In terms of the q-Pochhammer symbol we likewise get

$$|\mathsf{GL}(n,2)| = \prod_{i=0}^{n-1}(2^n - 2^i) = 2^{n^2}\ \left(2^{-n};2\right)_n$$

For $n = 4$ this is already 20160, so we'll stick to $n = 3$.

One can check computationally the the 3 matrices A_1, A_2 and A_3 from above generate all of GL$(3, 2)$.

To see why, consider A in GL$(3, 2)$. By Gaussian elimination there are elementary matrices E_i such that

$$E_k E_{k-1} \dots E_2 E_1 A = I$$

In our context, elementary matrices are of the following form. Let $1 \leq i \neq j \leq 3$; then $E(i, j)$ has 1's along the diagonal and another 1 in position (i, j).

The effect of $E(i, j) \cdot A$ is to add row j to row i in A.

All these matrices are self-inverse, hence they form a set of generators for GL$(3, 2)$: $A = E_1 \dots E_k$.

Exercise

Show that the 6 matrices $E(i,j)$ really generate $\mathsf{GL}(3,2)$.

Exercise

Show that the matrices A_1, A_2 and A_3 generate $\mathsf{GL}(3,2)$.

Exercise

Find other small sets of generators.

We can select all elements from $\mathrm{GL}(V)$ that have determinant 1, the special linear group $\mathrm{SL}(V)$. Clearly, this produces a subgroup (but note that for the ground field $\mathbb{F}_2$ nothing changes).

We are here interested in $\mathrm{SL}(2,7)$, the group of 2×2 matrices over the field $\mathbb{F}_7$ with determinant 1. One might wonder what on earth this group has to do with $\mathrm{GL}(\mathbb{F}_8)$. Here is a major hint.

Claim

$\mathrm{SL}(2,7)$ *has cardinality 336.*

This can be shown by brute-force, or by counting: consider the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $c = 0$ produces $6 \cdot 7 = 42$ choices, and $c \neq 0$ produces $6 \cdot 7 \cdot 7 = 294$ choices.

So far, we have three groups: $\mathsf{GL}(\mathbb{F}_8)$, $\mathsf{GL}(3,2)$ and $\mathsf{SL}(2,7)$. The first two are isomorphic, and the third, suspiciously, has order twice the order of the first two.

What is really going on? One key idea in understanding groups is that they always describe the symmetries of some object. This is straightforward for some groups like the dihedral groups, but in our case there is a problem.

Big Question: What is this mystery object for $\mathsf{GL}(\mathbb{F}_8)$?

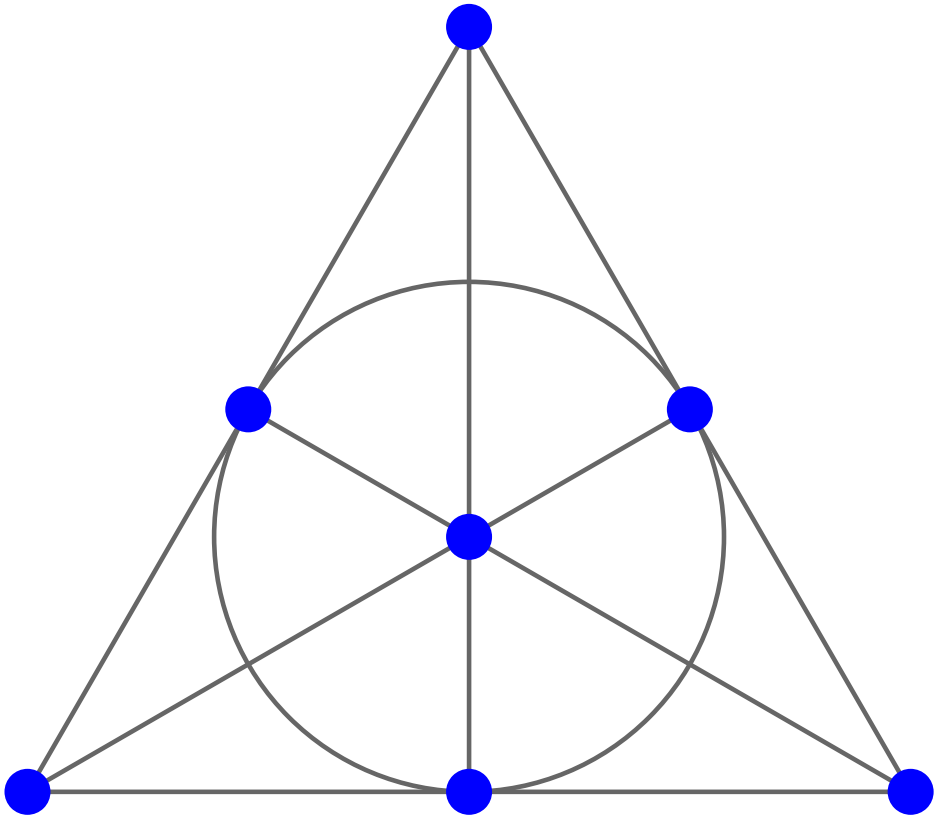
Disclaimer

To fully motivate of our next step one would have to take a major detour into projective geometry, a type of geometry that deals with projections and perspective drawings. This is classical 19th century mathematics, but has recently found applications in computer graphics (how do you render an image of a 3-dimensional scene on a 2-dimensional screen).

For example, two parallel lines (railroad tracks) meet at a point-at-infinity.

More generally, following Klein's Erlanger Programm, projective geometry deals with invariants of projective transformations.

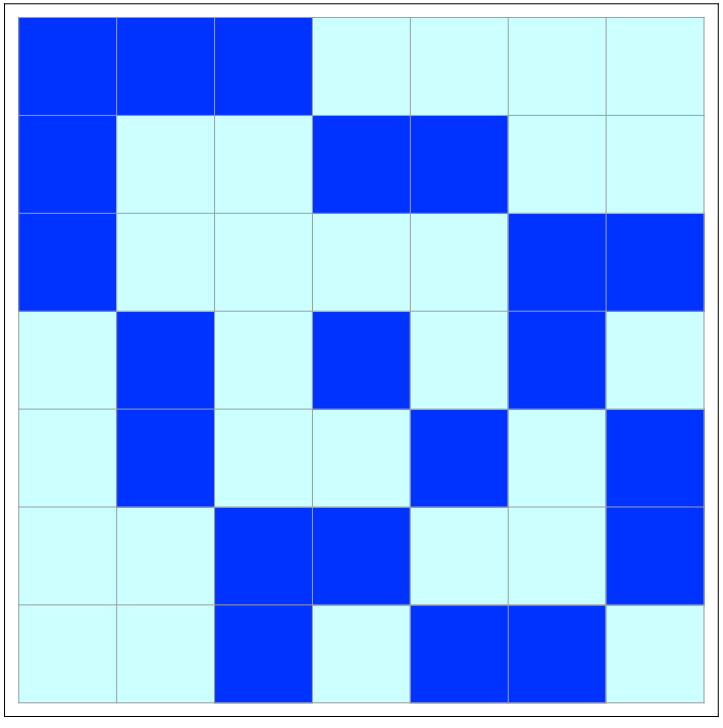
We resist the temptation to inflict mental harm on the student body; take a look at the web if you are interested. Here is the only basic concept we need.



$\mathcal{F}$ is the smallest example of a finite projective plane: 7 points, 7 lines.

More Formally

If you prefer the modern structural approach, there there two types, point and line, plus an incidence relation (point P lies on line ℓ):



Three 1's in each row and column, and symmetry.

Following the current standard, we can axiomatize the properties of this type of structure:

- Every line contains at least 3 points.
- Every two distinct points P and Q determine a unique line.
- Every two distinct lines intersect in exactly one point.
- There exist at least 4 points such that no 3 of them lie on a line.

Exercise

Verify that Fano's plane satisfies these axioms.

Pictures, structures and axioms are great, but how do they help to understand the corresponding object? For example, consider the following

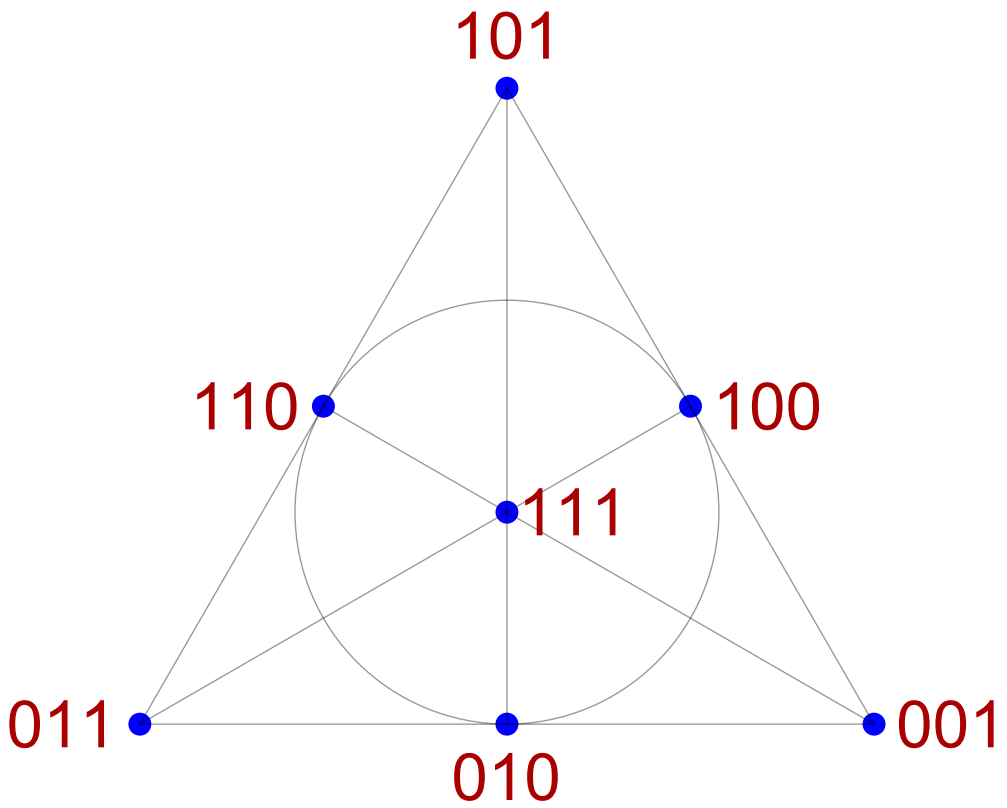
Question:: What are the symmetries of the Fano plane?

Here, a symmetry or automorphism is a permutation of the points that is collinearity preserving: lines are mapped to lines. Clearly, these maps form a group under composition, the automorphism group of the Fano plane, $\mathrm{Aut}(\mathcal{F})$.

Think of these automorphism just as a renaming of the points, there is nothing inherently complicated going on.

Innocent Question: How many are there? What is the order of $\mathrm{Aut}(\mathcal{F})$?

Here is a representation that is useful in answering these questions: identify the points as the non-zero elements of $\mathbb{F}_2^3$. Then points A, B and C form a line iff $A + B + C = 0$.



Since we are in characteristic 2, a line $\{A, B, C\}$ means $A + B = C$.

Claim

Suppose α is a permutation of the points.
Then α is collinearity preserving iff α is linear.

Proof.

Preserving lines means $\alpha(A) + \alpha(B) = \alpha(A + B)$ for all A, B.

□

Lemma

$\mathrm{GL}(3, 2)$ *is isomorphic to* $\mathrm{Aut}(\mathcal{F})$.

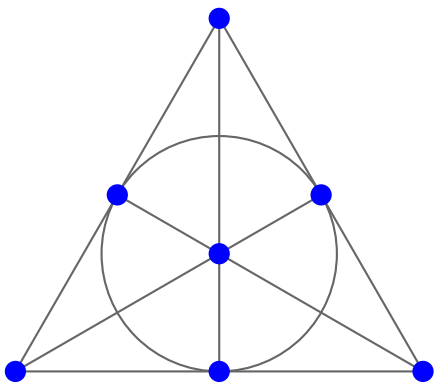
We can associate a line ℓ with a point P_ℓ: $\ell = \{\, Q \mid Q \circ P_\ell = 0 \,\}$. Here $\circ$ denotes the inner product, so these are the non-zero points orthogonal to P_ℓ.

P_ℓ	ℓ
001	$\{010, 100, 110\}$
010	$\{001, 100, 101\}$
011	$\{011, 100, 111\}$
100	$\{001, 010, 011\}$
101	$\{010, 101, 111\}$
110	$\{001, 110, 111\}$
111	$\{011, 101, 110\}$

Exercise

Ponder deeply. There is a duality principle at work.

We can justify our original pretty picture by reading off some of the symmetries of the Fano plane.



The projective lines are suggestively indicated by Euclidean line segments and the circle. We can get a symmetry of the Fano plane by rotating the big triangle by $2\pi/3$ around the center point.

Exercise

Make sure you understand why this really works.

Aut($\mathcal{F}$) has order 168, and the dihedral group D_3 (symmetries of an equilateral triangle) has order 6, so there are lots of elements of Aut($\mathcal{F}$) that do not arise from D_3. What to the others look like?

In the usual cycle notation, here are some permutations that preserve collinearity:

$$(001, 010), (100, 111)$$
$$(001, 010), (100, 101, 111, 110)$$
$$(001, 010, 011), (100, 101, 111)$$
$$(001, 010, 100, 011, 110, 111, 101)$$

All 168 symmetries in Aut($\mathcal{F}$) have a cycle structure like this.

So far we have 3 groups of order 168, all isomorphic:

$$\mathsf{GL}(\mathbb{F}_8) \simeq \mathsf{GL}(3,2) \simeq \mathsf{Aut}(\mathcal{F})$$

But remember, $\mathsf{SL}(2,7)$ had order 336. Hence the quotient group $\mathsf{SL}(2,7)/\{\pm I\}$ has order 168.

We refer to this group as the projective special linear group $\mathsf{PSL}(2,7)$. And we will see that the order is not coincidence.

To see what is going on, consider Moebius transformations, also known as linear fractional transformations. These are maps of the form

$$f(z) = f_{a,b,c,d}(z) = \frac{az+b}{cz+d}$$

where $ad - bc \neq 0$. Note that the coefficients are not uniquely determined by the map f: $f_{a,b,c,d}(z) = f_{\lambda a, \lambda b, \lambda c, \lambda d}(z)$ for $\lambda \neq 0$.

A Moebius transformation is called special if the coefficients can be chosen so that $ad - bc = 1$.

Classically, the ground field is often $\mathbb{C}$ or $\mathbb{R}$, but we will work over the finite field $\mathbb{F}_7$.

More precisely, we will use the projective line over $\mathbb{F}_7$, written $\mathbf{P}^1(\mathbb{F}_7)$.

The idea is to think of $\mathbb{F}_7$ as a line, and adjoin a "point-at-infinity."

Lets start with a representation of $\mathbf{P}^1(\mathbb{F}_7)$ in terms of homogeneous coordinates $[x : y]$ where $x, y \in \mathbb{F}_7$, not both 0.

We can define an equivalence relation on these coordinates via

$$[x_1 : y_1] \equiv [x_2 : y_2] \iff \exists\, \lambda \in \mathbb{F}_7\, (x_1 = \lambda x_2 \wedge y_1 = \lambda y_2)$$

Think of a 2-dimensional $\mathbb{F}_7$ vector space; we are identifying points along lines through the origin.

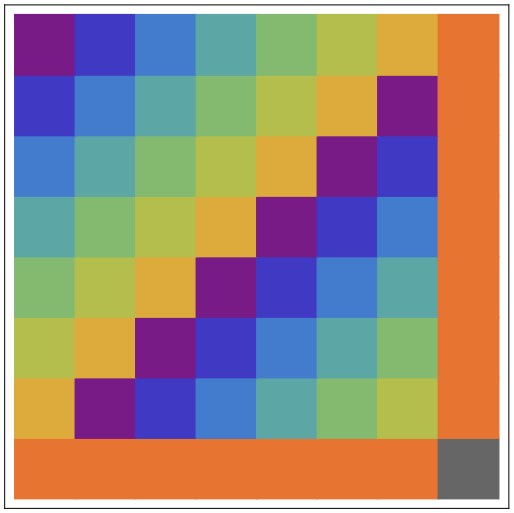
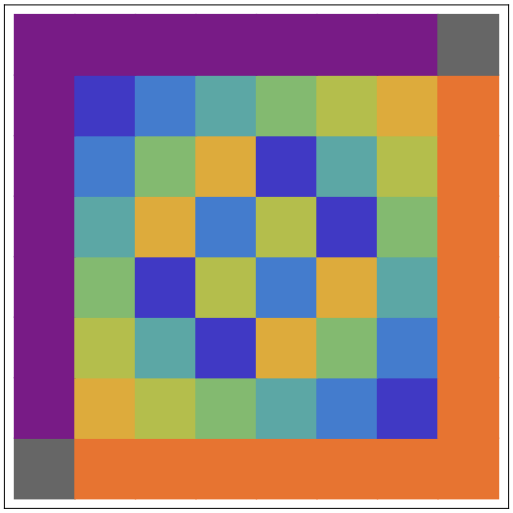
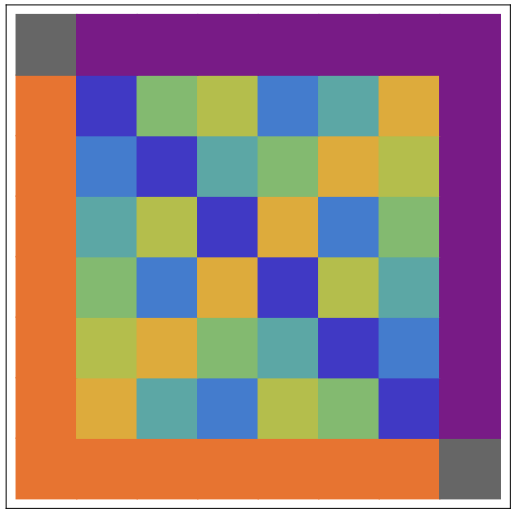
For notation, we ignore the equivalence classes as usual and use representatives $[x : 1]$ and $[1 : 0]$. Even better, write $[x : 1]$ as x, and $[1 : 0]$ as ∞.

So now we have the pleasant carrier set $\{0, 1, \ldots, 6, \infty\}$.

Naked sets are useless, but we can lift the arithmetic from $\mathbb{F}_7$ to $\mathbf{P}^1(\mathbb{F}_7)$.

$$[x_1 : y_1] + [x_2 : y_2] = [x_1 y_2 + x_2 y_1 : y_1 y_2]$$
$$[x_1 : y_1] * [x_2 : y_2] = [x_1 x_2 : y_1 y_2]$$
$$[x_1 : y_1]^{-1} = [x_2 : x_1]$$

So $0^{-1} = \infty$ and $\infty^{-1} = 0$, not unreasonable. Note that $0 * \infty$ and the like are undefined. Here are the (partial) Cayley tables for addition, multiplication and division on our projective line:

Since $\mathbf{P}^1(\mathbb{F}_7)$ is not an algebraic structure in the usual sense, we need to be a bit careful in defining our Moebius transformations $f = f_{a,b,c,d}$. We can use the fraction $f(z) = \frac{az+b}{cz+d}$ from above, except in the following special situations:

Case 1: $c \neq 0$

$$f(-d/c) = \infty$$
$$f(\infty) = a/c$$

Case 2: $c = 0$

$$f(\infty) = \infty$$

Exercise

Verify that these definitions make sense.

Consider the following special Moebius transformations: shift, double and reverse.

$$\sigma(z) = f_{1,1,0,1}(z) = z + 1$$
$$\delta(z) = f_{4,0,0,2}(z) = f_{2,0,0,1}(z) = 2z$$
$$\rho(z) = f_{0,6,1,0}(z) = -1/z$$

The corresponding graphs over $\mathbf{P}^1(\mathbb{F}_7)$ are as follows:

z	0	1	2	3	4	5	6	∞
$\sigma(z)$	1	2	3	4	5	6	0	∞
$\delta(z)$	0	2	4	6	1	3	5	∞
$\rho(z)$	∞	6	3	2	5	4	1	0

And Moebius Transformations?

Let's write SLF(7) for the group of all special Moebius transformations over $\mathbf{P}^1(\mathbb{F}_7)$, a group known as the special linear fractional group.

What do homogeneous coordinates have to do with these transformations? Think of $[z:1]$ as a column vector $\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)$. It is natural to have a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ act like

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} az+b \\ cz+d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} \frac{az+b}{cz+d} \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} f_{a,b,c,d}(z) \\ 1 \end{smallmatrix}\right).$$

Matrix multiplication in $\mathrm{SL}(2,7)$ thus corresponds to composition of Moebius transformations on $\mathbf{P}^1(\mathbb{F}_7)$.

An Epimorphism

Consider the map

$$\phi : \mathsf{SL}(2,7) \to \mathsf{SLF}(7) \qquad \phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = f_{a,b,c,d}$$

Claim

ϕ is a group epimorphism with kernel $\{I, -I\}$.
Hence $\mathsf{PSL}(2,7) = \mathsf{SL}(2,7)/\{\pm I\} \simeq \mathsf{SLF}(7)$.

Exercise

Prove the claim.

The question now is: what is the connection, if any, between SLF(7) and the automorphisms of the Fano plane?

Is there any way to translate a special Moebius transformation on $\mathbf{P}^1(\mathbb{F}_7)$ to a collinearity preserving bijection of the 7-point Fano plane?

We are given some $f = f_{a,b,c,d}$ and need a symmetry $\phi(f)$. Again we represent the points of the plane as non-zero vectors of length 3 over $\mathbb{F}_2$. The key is to think of the points as the set of units in $\mathbb{F}_8$: thus, they form a multiplicative group generated by X. So this should take care of $\{0, 1, \ldots, 6\} \subseteq \mathbb{F}_7$.

The hope is to somehow use zero to deal with the point-at-infinity.

Alas, it's far from clear how to do this in a way that produces an automorphism.

To deal with this problem, we abuse notation and write $X^\infty = 0$.

We can now define ϕ as follows:

$$\phi(f)(z) = X^{f(z)} + X^{f(\infty)}.$$

This guarantees that $\phi(f)(\infty) = 0$, always.

Exercise

Show that $\phi(f)$ is a bijection for all $f \in \mathsf{SLF}(7)$.

Recall our 3 special Moebius transformations: shift, double and reverse.

Claim

σ, δ and ρ generate SLF(7).

Proof.

Note that the matrices associated with these Moebius transformations are none other than A_1, A_2 and A_3 from above. Since these are generators, we are done.

□

Corollary

SLF(7) *is isomorphic to* Aut$(\mathcal{F})$.

name	description	order
GL($\mathbb{F}_8$)	invertible linear maps on $\mathbb{F}_8$	168
GL$(3,2)$	3 by 3 invertible matrices over $\mathbb{F}_2$	168
SL$(2,7)$	2 by 2 invertible matrices over $\mathbb{F}_7$	336
Aut$(\mathcal{F})$	symmetries of the Fano plane	168
PSL$(2,7)$	quotient group of SL$(2,7)$	168
SLF(7)	Moebius transformations on $\mathbf{P}^1(\mathbb{F}_7)$	168