Failure of X_n with non-singular matrices PhL 2.6.13

This was an interesting idea for Chapter 10 that blew up, but record it here anyway.

As our next step, we define X_m to be the restriction of $\mathcal{X}_m$ such that all non-zero matrices must have a non-vanishing determinant.

Since $\mathcal{X}_m$ has p^{m^2} elements, it seems clear that X_m is going to have some smaller number of elements since we require det(X) ≠ 0 for any X in X_m. A 2x2 matrix might have the form $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ and then det(X) = 0 means xt-yz = 0 or f(x,y,z,t) = 0. For real continuous variables, g(x,y,z) = 0 defines a 2D surface in 3D space. Similarly, the determinant condition f(x,y,z,t) = 0 defines a 3D surface in a 4D space. Points on this surface have det(X) = 0. In general the condition det(X) = 0 specifies an m^2-1 dimensional surface in the m^2 dimensional space of the matrix elements. Since the elements of an $\mathcal{X}_m$ matrix are in Z_p, the equation det(X) = 0 defines some kind of "digital surface" which touches a certain number of points and the matrices corresponding to those points must be excluded from X_m . We shall not attempt to calculate the number of matrices in X_m but we know it is some number smaller than p^{m^2} but probably not too much smaller than p^{m^2}. For the case p = 3 and m = 3, there are 3^9 = 19,683 matrices. Of these, exactly 6,891 have det(X) = 0, including the zero matrix, so about 35% of the matrices of $\mathcal{X}_m$ are not present in X_m.

```
> X := matrix(3,3,[a,b,c,d,e,f,g,h,i]):
> p := 3:
> cnt := 0:
> for a from 0 to p-1 do
  for b from 0 to p-1 do
  for c from 0 to p-1 do
  for d from 0 to p-1 do
  for e from 0 to p-1 do
  for f from 0 to p-1 do
  for g from 0 to p-1 do
  for h from 0 to p-1 do
  for i from 0 to p-1 do
  if det(X) = 0 then cnt := cnt + 1 fi;
  od;od;od;od;od;od;od;od;od;
> cnt;
                    6891
```

Fact: The ring X_m of mxm non-singular matrices having elements in Z_p is a field. [wrong!]

Test: Since X_m is I claim a field, and since it has a finite number of elements, it must be some Galois field! That means there must be some prime p and integer m such that

$$p^m = 19{,}683 - 6{,}891 + 1 = 12{,}793$$

Remember that the 6891 includes the all-zero matrix 0, so I want to add it back in. But here is how Maple factors that number

```
ifactors(12793);
                [1, [[11, 1], [1163, 1]]]
```

12,973 = 11 * 1163

so something is wrong in the machine!!!

Proof: The only item missing from the ring-with-identity X_m is the multiplicative inverse. By requiring det ≠ 0 for matrices in X_m, we assure that an inverse for every non-zero element X_m exists. We have closure because if A = BC then det(A) = det(B)det(C) so if B and C are non-singular, A is also non-singular. But how about additive closure!! If A = B + C then we get det(A) = det(B+C). But suppose I select C = - B . The both det(C) and det(B) ≠ 0, but det(B+C) = 0 so things are NOT closed, the whole thing goes blewie! Fine by me. That explains why the numbers above don't work, and it was amusing to do this Maple calculation.