Rational polynomials preserving integer matrices

You may recall that in the fall Asmita described the following problem in the introduction to her talk about her thesis research

Describe the ring $\mathrm{Int}_{\mathbb{Q}}(M_2\mathbb{Z})$ of polynomials $f(x) \in \mathbb{Q}[x] \mid f(M) \subseteq M_n(\mathbb{Z})$ if $M \in M_n\mathbb{Z}$ where $M_n\mathbb{Z}$ is the ring of matrices with entries in $\mathbb{Z}$. In particular find a basis for $\mathrm{Int}(M_n\mathbb{Z})$ as a $\mathbb{Z}$-module in which the n-th basis polynomial has degree n. (a regular basis).

This is an open problem although quite a bit is known, such as examples of polynomials in $\mathrm{Int}\, M_2\mathbb{Z}$ such as

$$f(x) = (x^6 + x^5 + x^3 + x^2)/2$$

How do you see that this $f(x)$ has that property?

Recall the Cayley-Hamilton theorem that any square matrix is a root of its characteristic polynomial. In linear algebra we usually state and prove this over $\mathbb{R}$, but it is true over any ring and in particular over $\mathbb{Z}/(2)$. Thus if $M \in M_2\mathbb{Z}$ and $f(x) \in \mathbb{Z}[x]$ is divisible in $\mathbb{Z}[x]$ by $ch_M(x) = \det(M - xI)$, then M is a root mod 2 of the mod 2 reduction of f, i.e. $f(M) \equiv 0 \ (2)$. Now there are not that many possible characteristic

polynomials mod 2 : $x^2, x^2+x, x^2+1, x^2+x+1$ and if we pick a polynomial divisible by all of them mod 2 eg $q(x) = x^2(x^2+1)(x^2+x+1)$ then $q(M) \equiv 0 \pmod 2$ for any $M \in M_2\mathbb{Z}$

$$x^2(x^2+1)(x^2+x+1) = x^2(x^4+x^3+x+1) = x^6+x^5+x^3+x^2 \quad //$$

In fact this is the best you can do! Any monic polynomial is the characteristic of a matrix, namely its companion matrix

$$x^2+ax+b \longleftrightarrow \begin{bmatrix} 0 & -b \\ 1 & -a \end{bmatrix} \qquad \text{for } n=2$$

$$\begin{bmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ & & 1 & -a_{n-1} \end{bmatrix}$$

and any polynomial vanishing at M is a multiple of $ch_M(x)$ so that

Thm If $f \in Int_a(M_n\mathbb{Z})$ for $q(x)$ with $q \in \mathbb{Z}[x]$ then $q(x)$ is divisible mod c by all monic deg n in $\mathbb{Z}[x]$.

Thus to find our regular bases we need only find, for each c $lcm\{$ monic $g(x) \in \mathbb{Z}/(c)[x]$ deg $n\}$.

What goes wrong? Consider $c=4, n=2$. We could catalog the irreducible polynomials of degree 2 mod 4

There are 4 linear and 6 quadratics

$(x+i)^2$ $i=0,1,2,3$ (x^2+1) (x^2+x+1) (x^2+3x+1)

(x^2+2) (x^2+2x+2) (x^2+2x+3)

and in analogy with the case $c=2$ we could multiply the squares of the linear's with the quadratics and get a polynomial of degree 20 which would be in $Int(M_2\mathbb{Z})$, but certainly not a basis element since we know a polynomial of degree 12 with the same denominator namely $(x^6+x^5+x^3+x^2/2)^2$

The problem is that $\mathbb{Z}_{(2)}[x]$ is a UFD but $\mathbb{Z}/(4)[x]$ isn't and, for example

$(x+1)^2=(x+3)^2$ and $(x^2+2)(x^2+2x+2)=x^3(x+2)$

In fact $Int(M_2\mathbb{Z})$ is not a very well behaved ring and one way of proceeding is to embed it in a larger more tractable ring. It is not integrally closed, which means that there are elements in its quotient field which are integral over $Int(M_2\mathbb{Z})$ without being in the ring. This is a familiar situation to number theorists. When you study the field $\mathbb{Q}[\sqrt{5}]$ you look for its "ring of integers". If you pick $\mathbb{Z}[\sqrt{5}]$ you find it not well behaved and the heart of the problem is there are elements of $\mathbb{Q}[\sqrt{5}]$ which act like integers but aren't in $\mathbb{Z}[\sqrt{5}]$. For example $\frac{1+\sqrt{5}}{2}$ is a root of x^2-x-1 but not in $\mathbb{Z}[\sqrt{5}]$

So instead you study $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \supseteq \mathbb{Z}[\sqrt{5}]$.

This is much easier since it has a division algorithm and so behaves much like $\mathbb{Z}$.

For $\mathrm{Int}(M_n\mathbb{Z})$ much the same thing happens. It's integral closure has a nice description as integervalued polynomials on a more tractable ring, and finding a regular basis here is possible. For $n=2$ this is in a paper of mine and the case $n>2$ is Asmita's thesis project.

So what about $\mathrm{Int}(M_n\mathbb{Z})$ it self? In particular how much bigger is its integral closure? The relation between $\mathbb{Z}[\sqrt{5}]$ and $\mathbb{Z}[(1+\sqrt{5})/2]$ is fairly simple. Here we must proceed computationally, and start by convert the problem: "find a polynomial in $\mathbb{Z}[x]$ divisible mod c by all monic quadratics" into a linear algebra problem

Since the polynomials involved are monic you still have a division algorithm

$$f(x) = (x^2+ax+b)\cdot q(x) + (rx+s).$$

and the coef. of q, and r & s are linear in a, b and the coef. of f.

If $f = \sum f_i x^i$ $\quad \underline{q} = \sum q_i x^i$

Then

$$\begin{bmatrix} 1 & & & & \\ a & \ddots & & 0 & \\ b & & \ddots & & \\ & \ddots & & \ddots & \\ 0 & & b & a & 1 \end{bmatrix} \begin{bmatrix} q_{n-2} \\ \\ q_0 \\ r \\ s \end{bmatrix} = \begin{bmatrix} f_n \\ \\ \\ \\ f_0 \end{bmatrix}$$

$M\underline{q} = \underline{f}$

and so $\underline{q} = M^{-1}\underline{f}$

and the requirement that x^2+ax+b divide $f \bmod c$ is that $\underline{f}$ be in the null space of the bottom two rows of $M^{-1} \bmod c$. In fact there is a fairly simple recurrence for the entries of M^{-1}.

The problem thus becomes looking for a vector in the null space modulo 2^k of this $i2x$ matrix, for every possible choice of a and b, or equivalently of an element in the null space of the $2 \cdot 2^{2n} \times (2n+1)$ matrix composed of all possible pairs rows, call this W

To find this some linear algebra comes in useful: There are unimodular matrices A, B such that $W = ADB$ with D diagonal, called the Smith normal form of W. and since A, B are invertible over $\mathbb{Z}$, the largest power of 2 dividing the diagonal elements of D is the denominator we seek. In fact these diagonal entries satisfy $d_{11} | d_{22} | d_{33} \cdots$ so it is $d_{n,n}$ we look at.

For $n=12$ we get $d_{12,12} = 12 = 2^2 \cdot 3$ so the square of our 6 degree polynomial f_6^2 is the best we can do

but for

$n=16$ $d_{16,16} = 24 = 2^3 \cdot 3$, so f_6^3 is not a regular basis element

Unfortunately Smith Normal Form is expensive to compute, both in time + memory, and this method only works up to about deg. 20

To go further we resort to using a matrix W' with only some of the pairs of rows, for a randomly selected set of pairs (a,b). How many is enough?

We are picking pairs from $(\mathbb{Z}/2^k)^2$ and the result will give the same span as the full matrix W if the set of pairs forms a $\mathbb{Z}/2^k$ spanning set of $(\mathbb{Z}/2^k)^{n+1}$. Since such a set spans iff it does mod 2^k we are left with the combinatorial problem:

If m vectors are picked at random from $(\mathbb{Z}/p)^{n+1}$ what is the probability that they span? For $m<n$ the answer clearly is 0 and for $m>n$ it is

$$\prod_{m-n} \left(1-\frac{1}{p^s}\right)$$