Matrix Actions on Bivariate Polynomials

Michelle Bergeron

Abstract. Using a matrix action, matrices in the group SL_2 mod n can act on homogenous polynomials in two variables. We find homogenous (bivariate) polynomials of any given degree are closed under the matrix action, and that the mappings from a polynomial $p \in R[x, y]_k$ to $p\mathcal{A}$ lay the foundation for certain patterns that we describe.

1. Mathematical Foundations

When matrices and polynomials interact, usually the polynomial acts on the matrix by an operation and changes its entries. However, if we define a matrix action, then the matrix can act on polynomials unchanged. In particular, we will define an action for matrices in special linear groups of degree 2 mod n to act on bivariate polynomials.

1.1. Special linear groups of degree 2 mod n.

Special linear groups are a specific type of group that can be defined over any commutative ring with unity. We are interested in the case where the ring is $\mathbb{Z}/n$, the integers mod n.

Definition 1.1. The special linear group SL_2 mod n is defined as all 2x2 matrices with determinant 1 comprised of entries mod n.

For example, SL_2 mod 2 is made up of the matrices:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

1.2. Polynomials with coefficients mod n.

We claim that the matrices in SL_2 mod n can act on polynomials. To do that, we must define a specific set of polynomials to work with. We thus define the set of polynomials that the matrices act on:

Definition 1.2. Let $R[x, y]$ be the ring of polynomials in two variables, x and y, with coefficients in $R = \mathbb{Z}/n\mathbb{Z}$. An element of $R[x, y]$ of the form $ax^m y^n$, with a in R, is called a monomial. Define the degree of the monomial $ax^m y^n$ to be $m + n$. Say that an element p in $R[x, y]$ is homogeneous if p is a sum of monomials all of the same degree. (Say that 0 is homogeneous of every degree, since $0 = 0x^m y^n$ for all m and n.) Write $R[x,y]_k$ for the set of polynomials in $R[x,y]$ that are homogeneous of degree k.

For now, we will consider R to be positive integers mod 2. That is, $R = \mathbb{Z}/2$. The monomials of degree k in $R[x,y]$ are $x^k, x^{k-1}y, \cdots, xy^{k-1}, y$.These monomials span $R[x,y]_k$ as an R-module. This means that any element of $R[x,y]_k$ can be written as $\sum_{j=0}^{k} a_j x^{k-j} y^j$ for some a_j in R.

Proposition 1.1. *The number of elements in $R[x,y]_k$ is equal to n^{k+1}. This is because for each polynomial, there are n options for each coefficient and k + 1 terms.*

To further illustrate these concepts, take the example below.

Example 1.1. Let $R = \mathbb{Z}/2$. Let $n = 2$. Our goal is to generate $R[x,y]_2$. According to the above, every element in $R[x,y]_2$ has the form $a*x^2+b*xy+c*y^2$ for some $a, b, c \in R$.

We form all combinations of this equation by plugging the elements of R into a, b, and c:

$$\begin{aligned}
0x^2 + 0xy + 0y^2 &= 0\\
1x^2 + 0xy + 0y^2 &= x^2\\
0x^2 + 1xy + 0y^2 &= xy\\
0x^2 + 0xy + 1y^2 &= y^2\\
1x^2 + 0xy + 1y^2 &= x^2 + y^2\\
1x^2 + 1xy + 0y^2 &= x^2 + xy\\
0x^2 + 1xy + 1y^2 &= xy + y^2\\
1x^2 + 1xy + 1y^2 &= x^2 + xy + y^2
\end{aligned}$$

Since $R = \mathbb{Z}/2$, $r = 2$. By the argument in Proposition 1.1, we can verify in $R[x,y]_2$ is equal to $2^{2+1} = 8$.

2. Matrix Actions on R[x,y]$_k$

So far, we have constructed special linear groups of matrices and sets of polynomials with coefficients mod n. This section details how the matrices in SL_2 mod n can act on polynomials in $R[x,y]_k$.

2.1. Preliminaries. For a polynomial in $R[x,y]_k$ and a matrix in SL_2 mod n, the matrix acts on the polynomial according to the following rule, $\mathcal{A}$:

$$x\begin{bmatrix} a & b \\ c & d \end{bmatrix} = xa + yb$$

$$y\begin{bmatrix} a & b \\ c & d \end{bmatrix} = xc + yd$$

However, most of the polynomials we are working with are more complex than simply x and y. Therefore, we need to establish how to use the matrix action $\mathcal{A}$ on more complicated polynomials.

Definition 2.1. For $p, q \in R[x, y]$ and $r \in R$, require:

(1) $(p+q)\mathcal{A} = p\mathcal{A} + q\mathcal{A}$
(2) $pq\mathcal{A} = (p\mathcal{A})(q\mathcal{A})$
(3) $rp\mathcal{A} = r(p\mathcal{A})$

Example 2.1. Apply the action using the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ in SL_2 mod 2 to the polynomial $xy + y^2$ in $R[x, y]_2$.
Begin with using $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, we will first take $xy\mathcal{A} + y^2\mathcal{A}$: First, compute $xy\mathcal{A}$ using the multiplication rule:

$$x\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = 0x + 1y = y$$

$$y\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = 1x + 0y = x$$

to get $xy\mathcal{A} = (y * x)$ mod $2 = xy$.

Next, compute $y^2\mathcal{A}$:
We know that $y\mathcal{A} = x$, so we can multiply $(x * x)$ mod $2 = y^2$. Thus, we combine our results of $xy\mathcal{A} + y^2\mathcal{A}$ with the addition rule to get $(xy + y^2)\mathcal{A} = x^2 + xy$.

2.2. Orbits. When we allow every matrix in SL_2 mod n to act on all polynomials in $R[x, y]_k$for fixed values of n and k , patterns begin to emerge. One can observe that some polynomials in $R[x, y]_k$generate the same result after being acted on by every matrix in SL_2 mod n.

Example 2.2. Apply the matrices in SL_2 mod 2 to the polynomials in $R[x, y]_2$
We demonstrate the process with $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, mapping $p \mapsto p\mathcal{A}$ for $p \in R[x, y]_2$:

$$\begin{gathered} 0 \to 0, \\ y^2 \to x^2, \\ xy \to xy, \\ xy + y^2 \to xy + x^2, \\ x^2 \to y^2, \\ x^2 + y^2 \to x^2 + y^2, \\ xy + x^2 \to xy + y^2, \\ xy + x^2 + y^2 \to xy + x^2 + y^2 \end{gathered}$$

Performing this on the rest of the matrices in SL_2 mod n are omitted.

If one continues applying $\mathcal{A}$ to $R[x, y]_2$ using the rest of the matrices in SL_2 mod 2, we see that two polynomials in $R[x, y]_2$ are always mapped to themselves:

0 and $x^2 + xy + y^2$. Upon closer inspection, the terms fall into three groups: $\{0\}, \{x^2, y^2, x^2 + y^2\}$ and $\{x^2 + xy + y^2\}$. The terms within each group always map to each other. We call these groupings ***orbits***.

3. Irreducible Polynomial Sets

To further understand the properties of these polynomial sets, we introduce the notion of irreducibility. First, we define alternate notation for $R[x, y]_k$ to make it easier to use to use with irreducible polynomial sets.

Definition 3.1. $R[x, y]_k = \underline{k+1}$

What does it mean for such a set to be irreducible?

Definition 3.2. A set $\underline{k}$ of the form $R[x, y]_{k-1}$ is irreducible if the only $SL_2(R)$ submodules are $\underline{k}$ and $\{0\}$.

Definition 3.3. $U \subset R$ is a $SL_2(R)$ submodule of $\underline{k}$ if the following two criteria hold:

(1) $p\mathcal{A} \in U$ for $p \in U$ and $\mathcal{A} \in SL_2(R)$
(2) $rp + sq \in U$ for $r, s \in R$; $p, q \in U$

Therefore, $R[x, y]_0 = \underline{1}$, $R[x, y]_1 = \underline{2}$, etc. In this form, Proposition 1.1 argues that the number of elements in $\underline{k} = n^k$. Using this new notation, we can then illustrate an example of polynomial set irreducibility.

Note that in SL_2 mod 2, there are two matrices which can generate the entire set by operating on each other, which we will call S and T. In this case, $S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. The reader is encouraged to verify that operations between these two matrices can generate the entirity of SL_2 mod 2. Consequently, these generator matrices are all that are required to test irreducibility because the rest of the group can be derived from them.

Example 3.1. In SL_2 mod 2, $\underline{1}$ and $\underline{2}$ are irreducible. To show that a set is irreducible, we need to show that the only submodules they contain is $\{0\}$ and itself.

$\underline{\mathbf{1}} = \{0, 1\}$: 0 and $\underline{1}$ are the trivial submodules. We will show that they are the only submodules by contradiction: Assume that $\{1\}$ is a submodule. Take $0 \cdot 1$. This should generate an element of $\{1\}$. However, $0 \cdot 1 = 0$. $0 \notin \{1\}$. Contradiction! Therefore, the only submodules of $\underline{1}$ are $\{0\}$ and itself. $\underline{1}$ is hence irreducible. □

$\underline{\mathbf{2}} = \{0, x, x+y, y\}$. Once again, we need to show that the only two submodules are the trivial submodules, $\{0\}$ and $\underline{2}$. Choose $V < \underline{2}$. If $x \in V$, then we know that $(x + y) \in V$ because $x\mathcal{T} = (x + y)$. We also know that $y \in V$ because $x\mathcal{S} = y$. One can repeat this argument by beginning with $(x + y)$ and y instead of with x, so V must be equal to $\underline{2}$. Therefore, we conclude that the only submodules are $\{0\}$ and $\underline{2}$. □

3.1. Reducible Polynomial Sets. We have shown that there exist irreducible polynomial sets such as $\underline{1}$ and $\underline{2}$ in SL_2 mod 2. However, we can also illustrate that sets of higher degree can be condensed to irreducibles. If one looks closely enough, there are "copies" of $\underline{1}$ and $\underline{2}$ in $\underline{3}$, $\underline{4}$, and beyond. That is, one can find elements in $\underline{k}$ that behave like elements in $\underline{1}$ and $\underline{2}$. The best way to illustrate what this means is by example:

Example 3.2. In SL_2 mod 2, we can find $\underline{1}$ and $\underline{2}$ within $\underline{3}$.

Recall that $\underline{1} = \{0, 1\}$, $\underline{2} = \{0, x, x + y, y\}$, and $\underline{3} = \{0, x^2, y^2, xy, x^2 + xy, x^2 + y^2, x^2 + xy + y^2\}$. To find a copy of $\underline{1}$ within $\underline{3}$, we must find elements in $\underline{3}$ that behave like those in $\underline{1}$. $0 \in \underline{1}$ will clearly correspond to $0 \in \underline{3}$. Next, we need to find an element that matches $1 \in \underline{3}$. $1 \in \underline{1}$ and $(x^2 + xy + y^2)$ fixed by $< S, T >$; hence, these elements correspond. We have shown that there is a copy of $\underline{1}$ within $\underline{3}$. □

We thus repeat the process for each of the elements of $\underline{2}$.

There are copies of $\underline{1}$ and $\underline{2}$ within $\underline{3}$; therefore, we write that $\underline{3} \cong \underline{1} \bigoplus \underline{2}$. In this case, $0 \in \underline{2} \mapsto 0 \in \underline{3}$, $x \in \underline{2} \mapsto x^2 \in \underline{3}$, $(x + y) \in \underline{2} \mapsto (x^2 + y^2) \in \underline{3}$, and $y \in \underline{2} \mapsto y^2 \in \underline{3}$.

By the same argument, one can verify that $\underline{4}$ contains two copies of $\underline{1}$ and one copy of $\underline{2}$.

We can continue this process for the rest of $R[x, y]_k$.

3.2. Generalization of irreducible behavior in SL_2 mod 2. In the examples, it is clear that $\underline{1}$ and $\underline{2}$ are irreducible within SL_2 mod 2. We have observed that in polynomial sets in $R[x, y]_k$ of higher powers (greater values of k), then we can find copies of $\underline{1}$ and $\underline{2}$ within each of them. Therefore, such sets of higher powers are reducible under SL_2 mod 2.

Observe that for an arbitrary set $\underline{k}$ under SL_2 mod 2, the values of the copies it contains add up to k. For example, we show above that $\underline{3} \cong \underline{1} \bigoplus \underline{2}$. Note that 1 + 2 = 3.

As k grows, we can see a pattern begin to emerge. We can examine our findings so far by arranging them in a table.

Polynomial set	# of $\underline{1}$	# of $\underline{2}$
$\underline{1}$	1	0
$\underline{2}$	0	1
$\underline{3}$	1	1
$\underline{4}$	2	1
$\underline{5}$	1	2
$\underline{6}$	2	2
$\underline{7}$	3	2
$\underline{8}$	2	3
$\underline{9}$	3	3

$\vdots$

In SL_2 mod 2, to determine row $\underline{h}$'s contents, there is the following formula. Note that there is a pattern in the table periodic every three rows. Therefore, there are three different cases for each row within the pattern.

PROPOSITION 3.1. *To determine row $\underline{h}$'s contents, first take h mod 3.*

h *mod* 3	# *of* $\underline{1}$	# *of* $\underline{2}$
0	$h/3$	$h/3$
1	$\lceil h/3 \rceil$	$\lfloor h/3 \rfloor$
2	$\lfloor h/3 \rfloor$	$\lceil h/3 \rceil$

3.3. Irreducibles in SL_2 mod 3. We can easily find the irreducible terms in SL_2 mod 3. By the same argument used in SL_2 mod 2, $\underline{1}, \underline{2}$ and $\underline{3}$ are irreducible. Below is the table that shows the number of copies of each irreducible set within higher dimensional sets. In order to better see the pattern, there are two "dummy rows", $\underline{-1}$ and $\underline{0}$ that exist solely to provide padding.

Polynomial Set	# of $\underline{1}$	# of $\underline{2}$	# of $\underline{3}$
$\underline{-1}$	0	0	0
$\underline{0}$	0	0	0
$\underline{1}$	1	0	0
$\underline{2}$	0	1	0
$\underline{3}$	0	0	1
$\underline{4}$	0	2	0
$\underline{5}$	2	0	1
$\underline{6}$	0	3	0
$\underline{7}$	1	0	2
$\underline{8}$	0	4	0
$\underline{9}$	3	0	2
$\underline{10}$	0	5	0

$\vdots$

PROPOSITION 3.2. *As in SL_2 mod 2, we can define formulas for row h. Take h mod 4:*

h *mod* 4	# *of* $\underline{1}$	# *of* $\underline{2}$	# *of* $\underline{3}$
0	0	$h/2$	0
1	$\lceil h/4 \rceil$	0	$\lfloor h/4 \rfloor$
2	0	$h/2$	0
3	$\lfloor h/4 \rfloor$	0	$\lceil h/4 \rceil$

Polynomial Set	# of $\underline{1}$	# of $\underline{2}$	# of $\underline{3}$	# of $\underline{4}$	# of $\underline{5}$
$\underline{1}$	1	0	0	0	0
$\underline{2}$	0	1	0	0	0
$\underline{3}$	0	0	1	0	0
$\underline{4}$	0	0	0	1	0
$\underline{5}$	0	0	0	0	1
$\underline{6}$	0	1	0	1	0
$\underline{7}$	2	0	0	0	1
$\underline{8}$	0	2	0	1	0
$\underline{9}$	1	0	1	0	1
$\underline{10}$	0	1	0	2	0
$\underline{11}$	1	0	0	0	2
$\underline{12}$	0	2	0	2	0
$\underline{13}$	3	0	0	0	2
$\underline{14}$	0	3	0	2	0
$\underline{15}$	2	0	1	0	2

$$\vdots$$

3.4. Irreducibles in SL_2 mod 5. We repeat creating the table for the case of SL_2 mod 5:

Note the connection between the table for SL_2 mod 5 and the one for SL_2 mod 2. Hidden within the odd rows of column $\underline{5}$, there is a copy of row $\underline{2}$ in SL_2 mod 2. Both have the pattern 1, 1, 1, 2, 2, 2, 3, 3, 3, ... In the even rows of column $\underline{2}$ in SL_2 mod 5, there is a copy of column $\underline{1}$ in SL_2 mod 2. Both have the pattern 1, 0, 1, 2, 1, 2, 3, 2, 3, ...

Proposition 3.3. *Again we define formulas for row h in terms of h mod $n+1$. Take h mod 6:*

h mod 6	*# of* $\underline{1}$	*# of* $\underline{2}$	*# of* $\underline{3}$	*# of* $\underline{4}$	*# of* $\underline{5}$
0	0	$h/6$	0	$h/6$	0
1	$\lceil h/6 \rceil$	0	0	0	$\lfloor h/6 \rfloor$
2	0	$\lceil h/6 \rceil$	0	$\lfloor h/6 \rfloor$	0
3	$\lfloor h/6 \rfloor$	0	$h/3$	0	$\lceil h/6 \rceil$
4	0	$\lfloor h/6 \rfloor$	0	$\lceil h/6 \rceil$	0
5	$\lfloor h/6 \rfloor$	0	0	0	$\lceil h/6 \rceil$

3.5. Irreducible behavior in SL_2 mod n. We have noticed that for the cases of SL_2 mod n for $n = 2$, 3, and 5, the sets $\underline{1}$, ..., $\underline{n}$ are irreducible. We posit that this is true for any n.

Proposition 3.4. *In SL_2 mod n, sets $\underline{1}$, ..., $\underline{n}$ are irreducible.*

Thus far in SL_2 mod n for $n = 2$ and $n = 3$, the table we have drawn has a pattern that is periodic every $n+1$ rows. This will be true for any value of n.

Proposition 3.5. *SL_2 mod n, the table displaying the number of copies of each irreducible set will have a pattern that has a period of $n+1$ rows.*

Also, in SL_2 mod n, rows with even values of h can only have nonzero entries in even columns. Rows with odd values of h can only have nonzero entries in odd columns.

Using the information found in SL_2 mod 2, 3, and 5, then we can conjecture the behavior in SL_2 mod n.

4. Conclusion

When matrices in SL_2 mod n can act on polynomials $R[x, y]_k$, patterns begin to emerge. When one examines polynomials of lower orders, distinctive mappings called orbits begin to appear. As the order increases, we find that polynomial sets contain copies of lower order sets. In fact, SL_2 mod n, sets $\underline{1}$, ..., $\underline{n}$ are irreducible. We find that it is possible to find how many copies of the irreducibile sets each higher order set can be decomposed into and to discern what will happen as k approaches infinity.

Department of Mathematics, Case Western Reserve University, Cleveland, OH,
E-mail address: mrb113@case.edu