Lecture 3: Latin Squares and Groups

In our last lecture, we came up with some fairly surprising connections between finite fields and Latin squares. This, in a sense, leads us to wonder whether other algebraic objects can be used to study Latin squares: i.e. can we use the concept of **groups** to study Latin squares?

Perhaps unsurprisingly by this point, the answer is yes! In this lecture, we will study the deeply strange ways in which we can make this connection.

1 Turning Groups into Latin Squares

We start by restating the definition of a group, for people who haven't seen them before:

Definition. Take a set G, along with an operation $\cdot$ that gives you some way to "combine" two elements in your group into a new element. Suppose that this operation $+$ satisfies the following four properties that the integers, $\mathbb{Z}$, also did with respect to $+$: namely,

- **Closure(+)**: $\forall a, b \in G$, we have $a + b \in G$.
- **Identity(+)**: $\exists 0 \in G$ such that $\forall a \in G$, $0 + a = a$.
- **Associativity(+)**: $\forall a, b, c \in G, (a + b) + c = a + (b + c)$.
- **Inverses(+)**: $\forall a \in G, \exists$ a unique $(-a) \in G$ such that $a + (-a) = 0 = (-a) + a$.

We call this kind of thing a **group**.

There are many groups that you already know and love: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ with respect to addition, and $\mathbb{Q}$ and $\mathbb{R}$ with respect to multiplication if you remove 0. More interestingly for our purposes, there are many types of **finite groups**: i.e. groups with finitely many elements. For example, we have $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n, which forms a group with respect to addition mod n:

$+$	0	1	2	$\dots$	$n-1$
0	0	1	2	$\dots$	$n-1$
1	1	2	3	$\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$n-1$	$n-1$	0	1	$\dots$	2

Another common example of a finite group is the **dihedral group** of order $2n$, the group made by taking all of the rotations or flips that send a regular n-gon to itself, and combining two group elements via composition (i.e. $a \circ b$ is the symmetry that first does b

and then a to the n-gon.) For $n = 3$, this is the set of symmetries of a triangle ABC, which we present below:

$\circ$	id	rot_{120CW}	rot_{240CW}	flip_A	flip_B	flip_C
id	id	rot_{120CW}	rot_{240CW}	flip_A	flip_B	flip_C
rot_{120CW}	rot_{120CW}	rot_{240CW}	id	flip_B	flip_C	flip_A
rot_{240CW}	rot_{240CW}	id	rot_{240CW}	flip_C	flip_A	flip_B
flip_A	flip_A	flip_C	flip_B	id	rot_{240CW}	rot_{120CW}
flip_B	flip_B	flip_A	flip_C	rot_{120CW}	id	rot_{240CW}
flip_C	flip_C	flip_B	flip_A	rot_{240CW}	rot_{120CW}	id

Why do we mention groups in a Latin squares class? Well: if you look at the group tables above, it's not too hard to see that in both cases, the $n \times n$ squares made by taking the results from each of these group tables are themselves Latin squares! This is relatively easy to prove:

Proposition. Any group table is a Latin square.

Proof. Take a row indexed by the group element a. Suppose that two elements in this row are equal: in other words, that there are two columns c, d such that $ac = ad$. If we multiply by a^{-1} on the left, this gives us $c = d$; i.e. that these were in fact the same columns, and therefore that there are no repetitions in this row. The same logic tells us that there are also no repetitions in any column; therefore, this is a Latin square.

Given this, you might hope that we can possibly "go backwards" with this reasoning: i.e. if we can turn groups into Latin squares, maybe we can also turn Latin squares into groups! To omit somewhat dumb counterexamples and simplify matters, suppose that our Latin squares have their first row and column equal to $(0, g_1, \ldots g_{n-1})$, where 0 is the identity in our group and the g_i's are the other elements. Can we always turn a Latin square into a group?

As a quick test, examine the following two Latin squares of order 4. One of these turns out to be a Latin square that we can get from a group, while the other does not. Which is which?

$$\begin{bmatrix} I & a & b & c \\ c & I & a & b \\ b & c & I & a \\ a & b & c & I \end{bmatrix}, \quad \begin{bmatrix} I & a & b & c & d \\ a & d & c & I & b \\ b & I & a & d & c \\ c & b & d & a & I \\ d & c & 0 & b & a \end{bmatrix}.$$

By examination, we can see that the first square is actually the group $\mathbb{Z}/4\mathbb{Z}$ in disguise: let $I = 0, b = 1, c = 2$, and $d = 3$.

The second square is weirder. Suppose that it was a group table: then for some ordering $[f, g, h, i, j]$ of our group elements and another ordering $[v, w, x, y, z]$, we have

$+$	v	w	x	y	z
f	0	a	b	c	d
g	a	d	c	0	b
h	b	0	a	d	c
i	c	b	d	a	0
j	d	c	0	b	a

.

One of f, g, h, i, j is the identity: therefore, one of the five rows of our Latin square must be $[v, w, x, y, z]$! In particular, we can actually assume that our top row is formed by taking f^{-1} and adding it to every element of $[0, a, b, c, d]$, because the row $[0, a, b, c, d]$ is just adding f to $[v, w, x, y, z]$.

If we do this, we can now notice the following useful observation: take any two rows of our table. Think of these as permutations of the row $[0, a, b, c, d]$: i.e. for example, the row corresponding to g, $[a, d, c, 0, b]$, can be though of as the map $\begin{pmatrix} 0 & a & b & c & d \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ a & d & c & 0 & b \end{pmatrix}$. Using this idea, we can now define an operation to compose two rows, by simply composing their permutations: i.e. the composition of the rows

$$h = \begin{pmatrix} 0 & a & b & c & d \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ b & 0 & a & d & c \end{pmatrix}, g = \begin{pmatrix} 0 & a & b & c & d \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ a & d & c & 0 & b \end{pmatrix}$$

is the permutation

$$h \circ g = \begin{pmatrix} 0 & a & b & c & d \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ a & d & c & 0 & b \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & c & d & b & a \end{pmatrix}.$$

What does this correspond to? Well: h corresponds to adding $h + f^{-1}$ to the elements of the row $[0, a, b, c, d]$, while i corresponds to adding $i + f^{-1}$ to the elements of $[0, a, b, c, d]$. The composition of h and i, then, is just adding $h + f^{-1} + i + f^{-1}$ to each element of the row $[0, a, b, c, d]$! But $h + f^{-1} + i + f^{-1}$ is some element of our group: therefore, there must be some row that corresponds to this resulting composition!

Furthermore, simply saying that the composition of any two rows is a third row is equivalent to asking that our group is associative, because (if we pick the "base" row, i.e. the row that we picked $[0, a, b, c, d]$ as above, to be the row corresponding to adding the identity element) this is just claiming that composing rows a and b is the same as the row $a + b$: i.e. that for every c in our base row, $a + (b + c) = (a + b) + c$.

So, we've actually proven the following:

Theorem. A Latin square is a group table if and only if the composition of any two rows is another row (with composition defined via the "base row" idea above.)

In particular, this tells us that the 5×5 square we were studying above cannot have resulted from a group table: as we calculated, the composition $h \circ g$ of the rows g and h yielded $[0, c, d, b, a]$, which is not a row in our Latin square (even though we'd expect it to correspond to whatever element $h + f^{-1} + i + f^{-1}$ is, if commutativity held.)

So, surprisingly enough, associativity fails! This is kinda surprising; if you've gone through the introductory group theory courses, you may be used to things like inverses being the difficult part of insuring something's a group, while associativity is the "boring detail that always works." For Latin squares, the opposite is true! In fact, Latin squares correspond precisely to the tables of **quasigroups**: an algebraic structure that consists of the group axioms, minus the associativity part.

Because they're not associative, they're pretty horrible to work with, so let's not do that. Instead, let's try something perhaps even sillier: we tried making Latin squares out of groups. Why not make groups out of Latin squares?

2 Making Groups out of Latin Squares

To do this, we're going to need to generalize a bit:

Definition. A **row-Latin** square is a $n \times n$ grid filled with the symbols $1 \dots n$, so that no symbol is repeated in any row. Column repeats are fine.

These are far easier to count than Latin squares:

Proposition. There are $(n!)^n$-many row-Latin squares of order n.

Proof. You have n rows, and $n!$ many choices of a permutation of $(1, \dots n)$ to put in each row.

Surprisingly, it turns out that we can turn these into a group! To explain precisely how, we need to introduce the **symmetric group**, which we do here:

Definition. The **symmetric group** S_n is the collection of all bijections from $\{1, \dots n\}$ to itself, with the group operation of **composition**. Often, people will write an element of S_n as a permutation: i.e. as some ordered subset of the numbers $\{1, \dots n\}$, like $(2, 4, 3)$ or some such thing. When they do this, they are denoting by shorthand some map $f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$, such that $2 \to 4 \to 3 \to 2$: i.e.

$$f = (2, 4, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 2 & 4 \end{pmatrix}$$

In other words, writing (a, b, c) denotes the permutation that sends a to b, b to c, and c to a, while leaving everything else unchanged.

In this notation, the composition of two such maps is just the function that you get by combining these two maps. For example, if $f = (2, 4, 3, 1)$ and $g = (4, 3)$, we have that $f \circ g$

is

$$f \circ g = (2,4,3,1) \circ (4,3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 4 & 1 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

i.e. the map that sends 1 to 2, 2 to 3 , 3 to 1, and leaves 4 alone. You can write this in this permutation notation as $(1,2,3)$

The identity map $i(x) = x$ is clearly the identity under this group operation; as well, we clearly have inverses (just take the map that undoes whatever bijection you're trying to find an inverse for) and associativity (because function composition doesn't care about associativity.) So it's a group!

So, with this idea defined, we can now turn row-Latin squares into a group in the following way:

Proposition. Take the collection of all $n \times n$ row-Latin squares R_n, and define the following group operation on R_n: given any two elements A, B of R_n, write

$$A = \begin{pmatrix} a_1 \\ \dots \\ a_n \end{pmatrix}, B = \begin{pmatrix} b_1 \\ \dots \\ b_n \end{pmatrix}$$

where the elements a_i, b_i are all permutations of $(1, \dots n)$: i.e. elements of S_n.

Then, we can define

$$A \circ B = \begin{pmatrix} a_1 \circ b_1 \\ \dots \\ a_n \circ b_n \end{pmatrix},$$

where by each $a_i \circ b_i$ we mean the permutation in S_n given by $a_i \circ b_i$.

We have an identity: specifically, the matrix

$$I = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & \dots & n \end{pmatrix}.$$

We have inverses: given a row-Latin square

$$A = \begin{pmatrix} a_1 \\ \dots \\ a_n \end{pmatrix},$$

let

$$A = \begin{pmatrix} (a_1)^{-1} \\ \dots \\ (a_n)^{-1} \end{pmatrix},$$

where these $(a_i)^{-1}$'s come from taking inverses in S_n. We also have associativity, because we're basically doing things over in S_n, which we claimed was associative.

We can define a pair A, B of row-Latin squares to be **orthogonal** in the exact same way that Latin squares are orthogonal: if every possible ordered pair of symbols occurs in the cells of A superimposed upon B. Usefully, this concept of orthogonality gives us a way of telling when a row-Latin square is a Latin square:

Proposition. If A is a row-Latin square that is orthogonal to the identity row-Latin square $I = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & \dots & n \end{pmatrix}$, then A is a Latin square.

Proof. If A is orthogonal to the identity, this is just saying that in any column i of A, we get all possible pairs of the form (i, k): in other words, that we cannot repeat any symbol k in this column. We already know by definition that there are no repeats in A's rows; therefore, it's a Latin square.

Using this, we can prove the following useful lemma:

Proposition. If $A_1, \dots A_n$ is a set of of mutually orthogonal row-Latin squares, then given any other row-Latin square X, the set $X \circ A_1, \dots X \circ A_n$ is another set of mutually orthogonal Latin squares.

Proof. Take any two squares $X \circ A_b, X \circ A_c$. Suppose that there are two distinct cells $(i, j), (k, l)$ such that when we superimpose these two squares, we see the same pairs of symbols: i.e. suppose that

- $X \circ A_b$'s cell (i, j) is the same as $X \circ A_b$'s cell (k, l) , and
- $X \circ A_c$'s cell (i, j) is the same as $X \circ A_c$'s cell (k, l).

If x_i, x_k are the ith and kth rows of X, while b_i, b_k and c_i, c_k the ith and kth rows of A_b, A_c respectively, this is specifically saying that

- The jth entry of $x_i \circ b_i$ is equal to the lth entry of $x_k \circ b_k$, and
- The jth entry of $x_i \circ c_i$ is equal to the lth entry of $x_k \circ c_k$.

But, if we multiply by $(x_i)^{-1}, (x_j)^{-1}$ respectively, this tells us that

- The jth entry of $(x_i)^{-1} \circ x_i \circ b_i$ is equal to the lth entry of $(x_k)^{-1} \circ x_k \circ b_k$, and
- The jth entry of $(x_i)^{-1} \circ x_i \circ c_i$ is equal to the lth entry of $(x_k)^{-1} \circ x_k \circ c_k$;

in other words, if we simplify, we have

- The jth entry of b_i is equal to the lth entry of b_k, and

- The jth entry of c_i is equal to the lth entry of c_k.

But this is impossible if A_b, A_c are orthogonal: therefore, we must have that $X \circ A_b, X \circ A_c$ are orthogonal as well. Because we have shown this for any pair A_b, A_c, we've in fact shown that the whole set $X \circ A_1, \ldots X \circ A_n$ is a collection of mutually orthogonal Latin squares.

Proposition. Two row-Latin squares A, B are orthogonal if and only if there is a proper Latin square L such that $AL = B$.

Proof. If L is a Latin square, L is orthogonal to I, the identity row-Latin square. Therefore, the set $\{I, L\}$ is a pair of mutually orthogonal row-Latin squares; by the above result we have that $\{A \circ I, A \circ L\} = \{A, B\}$ is a pair of orthogonal row-Latin squares.

Conversely: if A, B are orthogonal, then (because the set of row-Latin squares is a group) there is a row-Latin square L such that $AL = B$. Let B^{-1} be the inverse of B: then, we have

$$B^{-1}A = L, B^{-1}B = I;$$

as well, by our earlier proposition, we know that this set $\{L, I\}$ is also an orthogonal set. Therefore, L is orthogonal to I; i.e. L is a Latin square!

A quick corollary of this property is the following:

Proposition. Given a row-Latin square A, suppose that m is the smallest positive integer such that A^m is not latin. Then the set $A, A^2, \ldots A^{m-1}$ is a collection of MOLS.

The reason we care about this is the following:

Proposition. For any n, expand n using its unique factorization into primes: i.e. write $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots p_k^{n_k}$, such that $p_1 < \ldots p_n$.

Let $G = \mathbb{Z}/n\mathbb{Z}$, and L be the Latin square associated to G. Then $L, L^2, \ldots L^{p-1}$ is a set of MOLS.

Proof. So, first notice that any integer $\leq p_1 - 1$ is relatively prime to n; as well, notice that L^k, because it's formed by simply multiplying L by itself k times, is just the following group table:

$+$	0	k	$2k$	$\ldots$	$(n-1)k$
0	0	k	$2k$	$\ldots$	$(n-1)(k)$
k	k	$2k$	$3k$	$\ldots$	$(n-1)(2k)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
$(n-1)k$	$(n-1)k$	$(n-1)(2k)$	$(n-1)(3k)$	$\ldots$	$(n-1)(n-1)(k)$

Take any row. I claim that there are no repeats within this row. To see why, simply notice that if you did, say in row i in columns x, y, this is saying that

$$ixk \equiv iyk \mod n.$$

Because k is relatively prime to n, we know that we can divide by it without affecting the validity of the above equation; therefore, we have

$$ix \equiv iy \mod n.$$

But this only happens when $x = y$, because our original group table has ix and iy in row i, columns x, y. So there are no repetitions in this row; nor are there any repetitions in any column.

This gives us tons of lower bounds on numbers of MOLS: i.e. we can use this to deduce that there is a pair of MOLS of order 15. Which is pretty neat!

Latin Squares — Instructor: Padraic Bartlett

Homework 4: Groups and Graph Theory

Week 2 — *Mathcamp 2012*

Attempt all of the problems that seem interesting, and let me know if you see any typos! (+) problems are harder than the others. (++) problems are currently open.

1. For what values of n can you find a Latin square that does not come from a group table?

2. Using the finite field methods we described today, make 7 MOLS of order 8. (Don't explicitly write them out; rather, write out their general form, and write out two to test that they're actually orthogonal.)

3. Using the groups and graph theory methods we described today (if we finished them!), create 2 MOLS of order 15.

4. Which of the following Latin squares are multiplication tables of groups?

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \\ 2 & 3 & 1 & 5 & 6 & 4 \\ 5 & 6 & 4 & 1 & 2 & 3 \\ 6 & 4 & 5 & 3 & 1 & 2 \\ 4 & 5 & 6 & 2 & 3 & 1 \end{bmatrix}.$$