Affine and Projective Planes and Latin Squares (Explanation of Section 17.4)

What was Bóna talking about in this section? I'll explain how it is similar to ordinary analytic geometry. I'll omit all proofs, even the short ones.

1. Modular Arithmetic

I'll use the general example of $\mathbb{Z}_p$ where p is a prime number. In $\mathbb{Z}_p$ arithmetic is carried out *modulo* p, which means that we consider two integers the same if they differ by a multiple of p. Technically, we say m and n are *congruent modulo* p, written $m \equiv n \pmod{p}$, if $p|n-m$ ($|$ means "divides"). For instance, $p \equiv 0$ and $p-1 \equiv -1 \pmod{p}$. p is called the *modulus*.

I will write "$m = n$ in $\mathbb{Z}_p$" instead of "$m \equiv n \pmod{p}$".

$\mathbb{Z}_p$ has several important properties.

(1) Addition and multiplication are commutative and associative; multiplication is distributive over addition.
(2) There are an additive identity, 0, and a multiplicative identity, 1.
(3) Each element has a negative, $-m$, which is the same (in $\mathbb{Z}_p$) as $p-m$. For instance, -1 is the same as $p-1$ and -3 is the same as $p-3$.
(4) Each element except 0 has a multiplicative inverse. (This is why p must be a prime number.)

    For instance, in $\mathbb{Z}_5$, $3 \cdot 2 = 1$ so $2^{-1} = 3$ and $3^{-1} = 2$. N.B. Don't write $1/3$ for 3^{-1}. It will confuse you and me, both. 3^{-1} in $\mathbb{Z}_5$ is not a fraction.

These are the defining properties of a *field*. $\mathbb{Z}_p$ is an example of a finite field, because it's a field and it's a finite set. We call it the *finite field of order* p. There is a finite field of each order q that is a prime power, for instance order $2^2 = 4$ (which Bóna uses in Chapter 17), but it is not $\mathbb{Z}_q$ unless q is a prime number. For instance, $\mathbb{Z}_4$ is not a field, because it fails the last property (multiplicative inverses). The field of order 4 is more complicated and I won't try to describe it.

However, for affine and projective planes it's useful to know that a finite field of order q exists for any prime power q, and *only* for prime powers, and there is only one finite field of order q for each prime power q. (The proof is one of the great theorems of modern algebra. It's surprisingly easy—that doesn't exactly mean easy!—once you know the techniques. It's based on linear algebra.) Note that a finite field of q elements is $\mathbb{Z}_p$ if $q = p$ (a prime number) but *not* if q is not itself prime.

N.B. There will not be any questions on the final exam about finite fields, except $\mathbb{Z}_p$.

2. Affine Planes

You all know about $\mathbb{R}^2$, the ordinary Euclidean plane, whose point set is $\mathbb{R}^2 := \{(x, y) : x, y \in \mathbb{R}\}$ and whose lines are given by linear equations, $y = mx + b$ and (the vertical lines) $x = a$. m is the slope (and the slope of a vertical line is ∞), and lines are parallel (definition: non-intersecting) if and only if they have the same slope. This is an example of an affine plane: it is the *affine plane over* $\mathbb{R}$ and it is infinite: it has infinitely many points.

We do exactly the same for an affine plane over $\mathbb{Z}_p$. The point set is $\mathbb{Z}_p \times \mathbb{Z}_p = \{(x, y) : x, y \in \mathbb{Z}_p\}$. A line is given by a linear equation, either $y = mx + b$ where $m, b \in \mathbb{Z}_p$, or $x = a$ where $a \in \mathbb{Z}_p$. We call m the slope of the line, and we say $x = a$ has slope ∞; we call a line with slope 0 *horizontal* and a line with slope ∞ *vertical*. Lines are defined to be *parallel*

if they don't intersect, and we can prove (by solving two linear equations in $\mathbb{Z}_p$) that lines are parallel if and only if they have the same slope. The sets of points and of lines together make the *affine plane over* $\mathbb{Z}_p$, which I will write $\mathrm{AP}(\mathbb{Z}_p)$.

Now I want to prepare a table of all the points on all the lines with slope 2 in $\mathrm{AP}(\mathbb{Z}_5)$. I'll do this by making a list of all the x values in one column and having a column for each line, where I put the y value corresponding to that x value. The lines have the equations $y = 2x + b$ for each possible value of b, so there are $p = 5$ lines with slope 2. For instance, the line $y = 2x + 1$ is the point set $\{(0, 1), (1, 3), (2, 0), (3, 2), (4, 4)\}$.

	$y = 2x + 0$ $b = 0$	$y = 2x + 1$ $b = 1$	$y = 2x + 2$ $b = 2$	$y = 2x + 3$ $b = 3$	$y = 2x + 4$ $b = 4$
$x = 0$	0	1	2	3	4
$x = 1$	2	3	4	0	1
$x = 2$	4	0	1	2	3
$x = 3$	1	2	3	4	0
$x = 4$	3	4	0	1	2

TABLE 2.1. The y-coordinates of the points in each line of a parallel class in $\mathrm{AP}(\mathbb{Z}_5)$.

The intersection of the lines $y = 2x+1$ and $y = 3x+3$ is the point (x, y) obtained by solving the equations. That is, $2x + 1 = 3x + 3$, so $x = -2 = 5 - 2 = 3$ and $y = 2 \cdot 3 + 1 = 7 = 2$. Thus, the intersection point is $(3, 2)$.

A plane $\mathrm{AP}(\mathbb{Z}_p)$ gives a $(p^2,\ p,\ 1)$-design, in full a $(p^2 + p,\ p^2,\ p + 1,\ p,\ 1)$-design. The point set of the design is the point set of the plane, and the blocks of the design are the lines of the plane. Every line has p points, so we say the plane has *order* p.

PROJECTIVE PLANES

People who look at landscape pictures often say "parallel lines meet at infinity". In art this is called "perspective painting". You can see it in Renaissance paintings where the painters were excited about perspective. The classic example (currently) is the parallel tracks of a straight railway line receding into the distance. In projective geometry we invent actual points at infinity where parallel lines meet.

The point set of the *projective plane* $\mathrm{PP}(\mathbb{Z}_p)$ is the point set of the affine plane together with one new point for each parallel class of lines, i.e., one for each slope. We call these *points at infinity*. Let's name these points ∞_m where $m \in \mathbb{Z}_p$ or $m = \infty$, and add ∞_m as a new point on every line with slope m. For instance, ∞_0 is a new point that's on every horizontal line, ∞_1 is a new point on every line of slope 1, and ∞_∞ is a new point on every vertical line. The lines of $\mathrm{PP}(\mathbb{Z}_p)$ are the lines of $\mathrm{AP}(\mathbb{Z}_p)$ with the new points added in, and one entirely new line called the *line at infinity*,

$$l_\infty := \{\infty_0, \infty_1, \ldots, \infty_{p-1}, \infty_\infty\}.$$

This is the projective plane of order p.

$\mathrm{PP}(\mathbb{Z}_p)$ has some very nice symmetry. Any two lines meet in exactly one point. Any two points lie on exactly one line. Every line has $p+1$ points, and every point lies on $p+1$ lines.

Therefore, $\mathrm{PP}(\mathbb{Z}_p)$ is a symmetric $(p^2+p+1,\ p^2+p+1,\ p+1,\ p+1,\ 1)$-design, where we take the points of the design to be the points of the plane, and the blocks of the design are the blocks of the plane. We say this projective plane has *order* p, the same as the associated affine plane.

Remarks.

1. An important point is that any projective plane can be constructed from an affine plane (by adding points at infinity), and any affine plane can be constructed from a projective plane (as a residual design). So, in some sense, projective and affine planes are equivalent, although they are not the same thing.

2. You'll have noticed that the book defines an affine plane as a residual design of a projective plane. In other words, the book goes from a projective plane to an affine plane. I went the other way: first I defined an affine plane (over $\mathbb{Z}_p$) and then derived the projective plane (over $\mathbb{Z}_p$) from the affine plane. Both methods are correct.

3. The book defines a projective plane as a symmetric $(n^2+n+1,\ n+1,\ 1)$-design. That definition doesn't mention finite fields. Not all projective planes come from affine planes constructed using $\mathbb{Z}_p$ or other finite fields. See the last section, "Looking Ahead".

4. The book's construction is pretty mysterious. I'll explain it just to give you a better idea of what it's doing, but if you don't understand it don't worry; I don't expect you to know this. First of all, let's skip general finite fields and only work with $\mathbb{Z}_p$. We are doing linear algebra over the field $\mathbb{Z}_p$. That's just like linear algebra over $\mathbb{R}$, but finite. (You see this in Modern Algebra.) Bóna says to take ordered triples, $(x,y,z) \in \mathbb{Z}_p^3$, but exclude $(0,0,0)$. Then, set up an equivalence relation: $(x,y,z) \sim (x',y',z')$ if there is a scalar α (an element of $\mathbb{Z}_p$) such that $(x,y,z) = \alpha(x',y',z')$. Then he says each equivalence class is a point of the projective plane $\mathrm{PP}(\mathbb{Z}_p)$. For instance, $(1,2,1)$ and $(3,1,3)$ are equivalent over $\mathbb{Z}_5$ (with $\alpha = 3$), so they represent only one point in $\mathrm{PP}(\mathbb{Z}_5)$. (We write $[x,y,z]$ for the projective point that contains the triple (x,y,z); it is an equivalence class of triples. For instance, $[1,2,1]$ or $[3,1,3]$ or $[2,4,2]$, ...—they are all the same projective point.) Bóna does something similar for lines but to keep from getting too complicated I'll ignore that.

   But wait, now we can forget about points like $(3,1,3)$ (where $z \neq 1$) and just work with points like $(1,2,1)$, where $z = 1$. (Why? Because $(3,1,3) = 3 \cdot (1,2,1)$ by scalar multiplication in the 3-dimensional vector space over $\mathbb{Z}_5$, which we call $\mathbb{Z}_5^3$, just like $\mathbb{R}^3$.) That's not completely true, since there are vectors such as $(2,3,0)$ where no scalar multiple has $z = 1$, but let's put those aside temporarily. Now, here's one way to get the affine plane $\mathrm{AP}(\mathbb{Z}_p)$: delete the points with $z = 0$, keeping only those with $z = 1$. So, we have points that look like $(x,y,1)$. Now don't write the 1; you have the point (x,y). That's the affine plane $\mathrm{AP}(\mathbb{Z}_5)$. And what about the deleted points? They are the points at infinity in the projective plane! (I'm cutting a corner by not explaining exactly how that's true.)

Latin Squares

If you look at the y-values in Table 2.1 you'll see that they form a Latin square of order 5 with symbol set $\mathbb{Z}_5$. (The reason is that since we have slope $m \neq 0, \infty$, there is no repetition of a y value in any one line of the parallel class. If we made a similar table with $m = 0$, each

column would have only one number since $y = 0x + b$. If we took $m = \infty$, each row would have only one number.)

Let's make a similar table of the y-values of points in the lines with slope 1, combined with the table for $m = 2$.

	$b = 0$	$b = 1$	$b = 2$	$b = 3$	$b = 4$
$x = 0$	0 0	1 1	2 2	3 3	4 4
$x = 1$	1 2	2 3	3 4	4 0	0 1
$x = 2$	2 4	3 0	4 1	0 2	1 3
$x = 3$	3 1	4 2	0 3	1 4	2 0
$x = 4$	4 3	0 4	1 0	2 1	3 2

TABLE 2.2. The y-coordinates of the points in the lines $y = mx + b$ of two parallel classes in $\mathrm{AP}(\mathbb{Z}_5)$. In each box the first number represents the y-coordinate for a line $y = 1x + b$ and the second number is the y-coordinate for a line $y = 2x + b$. Every ordered pair appears exactly once.

We get two Latin squares. Notice that the same (ordered) pair of numbers never appears twice. (Also, every pair appears once. That must be so if no pair is repeated, because there are p^2 boxes and p^2 ordered pairs). That means we have an *orthogonal pair of Latin squares*. (There's a definition in Ch. 17, Exercise 20.) If you filled in four numbers in each box using slopes 1, 2, 3, and 4, you would find that you had four mutually orthogonal Latin squares (MOLS)—which means any two of them are orthogonal.

Theorem 1. *The Latin squares formed from the y-coordinates of lines of each parallel class in $\mathrm{AP}(\mathbb{Z}_p)$, excluding slopes 0 and ∞, form a set of $p - 1$ MOLS.*

This is one of the main ways to get large sets of MOLS, which are valuable for experimental design. Note that if $p = 2$, we only get one square in a set of MOLS; that means there are no two Latin squares of order 2 that are orthogonal to each other. When $p = 3$, we can get a set of 2 MOLS.

I'm omitting the proof, but the reason is basically that two lines with different slopes intersect in one and only one point.

The number $p - 1$ in Theorem 1 is the best possible. The theorem that says so is Exercise 21 in Chapter 17.

Theorem 2. *Suppose there is a set of k MOLS of order n. Then $k \leq n - 1$.*

The theorem *does not say* that $n - 1$ MOLS exist. For many values of n there are not that many. For instance, the largest set of MOLS of order 6 has only 2 squares. Also, it does not say you can choose the squares arbitrarily. For instance, in order 4 there is a square that is not orthogonal to any other square, but there is also a square that is orthogonal to two other squares and the three of them form a set of three MOLS.

There is a converse to Theorem 1; it is Theorem 3.

Latin squares and addition and multiplication operations.

Latin squares are related to algebraic operations. The addition table of $\mathbb{Z}_n$ (that is, addition modulo n) is an $n \times n$ Latin square. The subtraction table is another. The multiplication table of $\mathbb{Z}_n \setminus \{0\}$ (that is, omit the row and column of 0) is an $(n-1) \times (n-1)$ Latin square if n is prime, but not if n is composite.

A quick remark for those who had Modern Algebra: The multiplication table of any finite group (that means a binary operation that is associative and has an identity and has inverses, such as multiplication on the set $\mathbb{Z}_p \setminus \{0\}$ for prime p) is a Latin square. Not every Latin square is the multiplication table of a group. Every Latin square defines a "multiplication" operation but it may not be associative and it may not have an identity element.

Looking Ahead

There is a beautiful subject of finite geometry that concerns affine and projective planes and higher-dimensional spaces, and Latin squares. Design theory gets into it, too.

1. Using finite fields we can construct an affine plane of order q for any prime power q. The construction is just like the one we showed for $\mathbb{Z}_p$ (but we cannot use $\mathbb{Z}_q$ unless q is a prime; we use a "finite field" $\mathbb{F}_q$ with q elements; $\mathbb{F}_p = \mathbb{Z}_p$ when $q = p$, a prime number, but not otherwise). From the plane we get a set of $q-1$ MOLS.

2. The amazing thing is that there's a converse. If you have a set of $n-1$ MOLS of order n (the most one can possibly hope for, by Exercise 17.21), you can build an affine plane of order n.

Theorem 3. *There exists an affine plane of order n if and only if there exists a set of $n-1$ MOLS of order n.*

To explain the importance of the theorem, I have to tell you that there are affine planes that are not built from finite fields the way we did it. There's a direct combinatorial definition of an affine plane which is a bit too complicated to state here, but an indirect combinatorial definition is that an affine plane is a residual design of a projective plane. So, when we talk about affine planes, we don't necessarily mean they have prime power order.

3. However, *no one knows whether an affine plane with non-prime-power order exists*! Since there is a projective plane of order n if and only if there is an affine plane of order n, we have the same ignorance about the existence of projective planes of non-prime-power order. This is a famous unsolved problem in combinatorics.

The first non-prime-power is 6; this can be ruled out by a complicated theorem. The next is 10; this was ruled out about a dozen years ago through massive computation after much theoretical simplification. The next non-prime-power is 12. *No one knows whether there is an affine plane of order 12.*

Postscript

There will be questions about affine and projective planes and Latin squares on the final exam but nothing about projective coordinates (the $[x, y, z]$ discussed above and in Section 17.4).