Modern Geometry Homework.

1. Constructing examples of affine planes.

We are now going to use the usual coordinate geometry we all know and love from high school to construct examples of affine geometries. I am assuming that you are familiar with the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the rational numbers $\mathbb{Q}$. We will use $\mathbb{F}$ to denote any one of these and refer to it as the ***base field***. We define affine plane $\mathbb{A}^2$ such that the set of points of $\mathbb{A}^2$ is just the set of ordered pairs (x, y) with $x, y \in \mathbb{F}$ and define the lines of of $\mathbb{A}^2$ to be the zero sets of linear equations. To start let

$$\mathbb{A}^2 := \{(x, y) : x, y \in \mathbb{R}\}.$$

Probably the case you want to keep in mind is when $\mathbb{F} = \mathbb{R}$ in which case $\mathbb{A}^2$ is just the usual plane with its x-y coordinates.

We now want to define lines by their equations. One way to get an equation for a line is the ***slope intercept*** form

$$y = mx + \beta$$

where m is the slope of the line and β is the y-intercept. See Figure 1

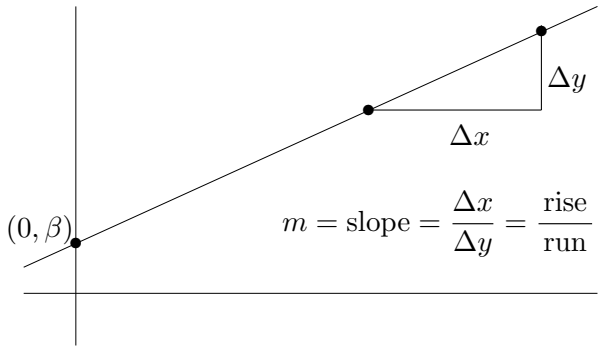

Figure 1. The line $y = mx + \beta$ has y-intercept $(0, \beta)$ and slope m.

This is nice in that for each line that is not vertical we get a unique equation. The problem is that for some limes (the vertical ones) there is no equation. As a bit of review, and to motivate what is coming, we look at other forms of equations of lines. One is the ***point slope form***: the equation of the line through (x_0, y_0) with slope m is

$$y = y_0 + m(x - x_0),$$

see Figure 2.

Problem 1. Find the y-intercept of $y = y_0 + m(x - x_0)$. □

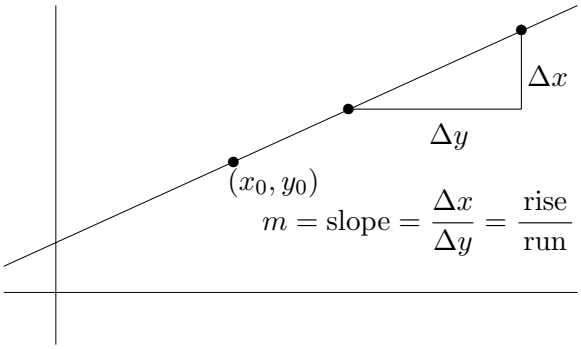

FIGURE 2. The equation of the line through (x_0, y_0) with slope m is $y = y_0 + m(x - x_0)$

Anther form is the two point form. If a line goes through the points (x_0, y_0) and (x_1, y_1) where $x_0 \neq y_0$ then the equation through these points has the equation

$$y = y_0 + m(x - x_0) \qquad \text{where} \qquad m = \frac{y_1 - y_0}{x_1 - x_0},$$

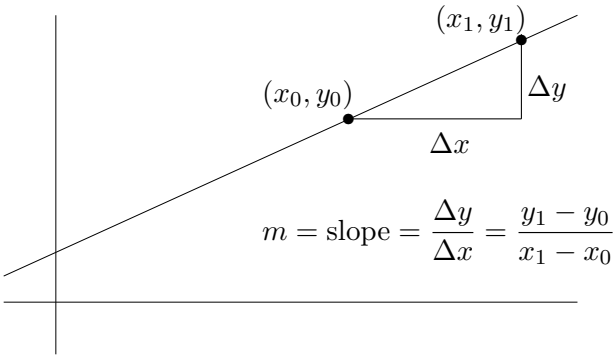

FIGURE 3. The equation of the line through the points (x_0, y_0) and (x_1, y_1) with $x_0 \neq x_1$.

Problem 2. Let (x_0, y_0) and (x_1, y_1) be points of $\mathbb{A}^2$ with $x_1 \neq x_0$. Show that the slope intercept form of the equation of the line through these points is

$$y = mx + \beta \qquad \text{with} \qquad m = \frac{y_1 - y_0}{x_1 - x_0} \quad \text{and} \quad \beta = \frac{x_1 y_0 - x_0 y_1}{x_1 - x_0}. \qquad \square$$

All of these forms of the equations of lines we have just given have the problem that they do not represent vertical.

The other standard form of equations for lines

$$ax + by + c = 0$$

where a and b are not both zero.

Problem 3. Why do we rule out the case where $a = b = 0$? □

This has the advantage that every line in the plane has an equation of this form. The draw back is that there is more than one such equation for each line. For example

$$x + 2y + 3 = 0, \quad -x - 2y - 3 = 0, \quad 2x + 4y + 6 = 0, \quad 42x + 82y + 126 = 0$$

are all equations for the same line. Still this is the definition we will use.

Remark 1. Let use recall a bit of vector algebra. If we want to find the line, call it ℓ, through the point $P_0 = (x_0, y_0)$ and perpendicular to the vector $\vec{n} = \langle a, b\rangle$. Let $P = (x, y)$ be any arbitrary point on ℓ. Then the vector

$$\vec{P_0P} = \langle x - x_0, y - y_0\rangle$$

is perpendicular to the vector $\vec{n} = \langle a, b\rangle$. This means that that dot product of these two vectors is zero. That is

$$0 = \langle a, b\rangle \cdot \vec{P_0P} = \langle a, b\rangle \cdot \langle x - x_0, y - y_0\rangle = ax + by + (-ax_0 - by_0)$$

which gives us an equation for the required line. See Figure 4. □

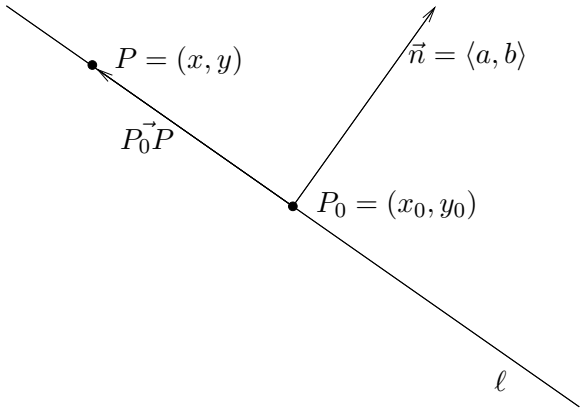

FIGURE 4. To find the line ℓ through the point P_0 and perpendicular to the vector $\vec{n}$, we have that for any point P on ℓ the vector $\vec{P_0P}$ will be perpendicular to $\vec{n}$. Thus the dot product of $\vec{n}$ and $\vec{P_0}$ will be zero. The equation $\vec{P_0} \cdot \vec{n} = 0$ can be expanded into an x-y equation for the line.

Problem 4. It is often useful to be able to find a vector perpendicular to a given vector $\langle a, b\rangle$. Show that $\langle -b.a\rangle$ is such a perpendicular. *Hint:* Show that their dot product is zero. □

Remark 2. To review some more vector algebra, let us look for the equation of the line through $P_0 = (x_0, y_0)$ and $P_1 = (x_1, y_1)$. Then, see Figure 5, the

vector $\vec{n} = \langle -(y_1 - y_0), (x_1 - x_0)\rangle$, should be perpendicular to the line. Thus the construction of Remark 1 gives that an equation of the line should be

$$-(y_1 - y_0)x + (x_1 - x_0)y + ((y_1 - y_0)x_0 - (x_1 - x_0)y_0) = 0. \qquad (1)$$

□

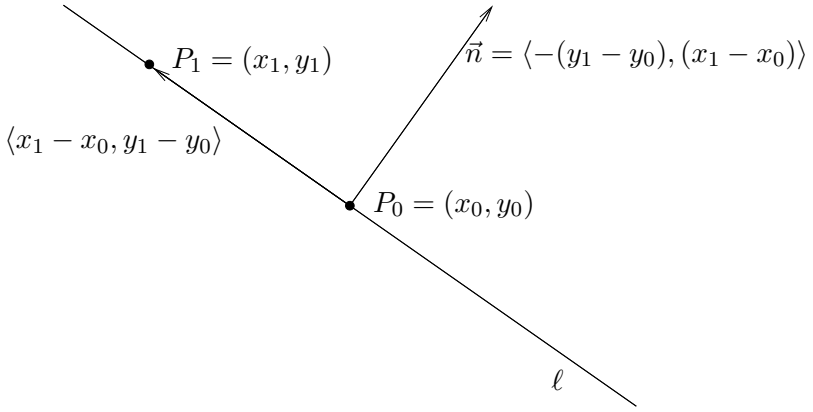

FIGURE 5. To find an equation of the line ℓ through the point $P_0 = (x_0, x_1)$ and $P_1 = (x_1, y_1)$ we note that the vector $\vec{P_0P_1} = \langle x_1 - x_0, y_1 - y_0\rangle$ is parallel is parallel to the line we are looking for. Thus, by Problem 4, the vector $\vec{n} = \langle -(y_1 - y_0), (x_1 - x_0)\rangle$ is perpendicular to the line. We can now use the construction of Remark 1 to find an equation of the line.

Problem 5. Simplify Equation 1 and verify that (x_0, y_0) and (x_1, y_1) satisfy this equation. □

We now define what will be the lines in our geometry.

Definition 3. If $a, b, c \in \mathbb{F}$ and a and b are not both zero, then let $L(a, b, c)$ be the subset of $\mathbb{A}^2$ defined by

$$L(a, b, c) := \big\{(x, y) : ax + by + c = 0\big\}.$$

We call such subsets the ***lines*** in $\mathbb{A}^2$. □

From now on when we write $L(a, b, c)$ we will assume that a and b are not both zero. For the rest of this section when we say "line" we mean a subset of the form $L(a, b, c)$ with a and b not both zero.

Here are some examples:

Problem 6. In the case the base field is $\mathbb{F} = \mathbb{R}$, so that $\mathbb{A}^2$ is the usual coordinate plane,

(a) Graph $L(1, 2, 3)$.
(b) Graph $L(1, 0, 4)$.
(c) Graph $L(0, 1, -2)$.

(d) Find a, b and c such that $L(a,b,c)$ contains both the points $(1,2)$ and $(-2,3)$. (There are more than one choice for (a,b,c) can you figure out how they are realted?) *Hint:* See Remark 2.
(e) Given $x_0, y_0 > 0$, find a and b such that $L(a,b,-1)$ contains the points $(x_0,0)$ and $(0,y_0)$. □

We now what to show that $\mathbb{A}^2$ with this definition of a line satisfies the axioms for an affine plane. While not hard, we will do this in small steps.

Proposition 4. *If $\lambda \neq 0$ then for any a,b,c with a and b not both zero*

$$L(a,b,c) = L(\lambda a, \lambda b, \lambda c).$$

Problem 7. Prove this. *Hint:* Do not make this hard. This really does not say anything more than that for $(x,y) \in \mathbb{A}^2$ and $\lambda \neq 0$ that we have $ax+by-c=0$ if and only if $\lambda ax + \lambda by - \lambda c = 0$. □

Lemma 5. *For any two distinct points $P_0 = (x_0,y_0)$ and $P_1 = (x_1,y_1)$ there is at least one line containing P_0 and P_1. That is we can find $a,b,c \in \mathbb{F}$ with a and b not both zero and with P_0 and P_1 on $L(a,b,c)$.*

Problem 8. Prove this. *Hint:* Look at Problem 4. While in that problem we were assuming that the field $\mathbb{F} = \mathbb{R}$, it is not hard to see that the equation for the line your got works in the general case. □

Remark 6. If you are familiar with determinants, here is an outline of anther way to prove the last lemma. Consider distinct points (x_0,y_0) and (x_1,y_1) and the 3×3 determinant

$$f(x,y) = \begin{vmatrix} x & y & 1 \\ x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \end{vmatrix}$$

Expanding along the first row gives

$$\begin{aligned} \begin{vmatrix} x & y & 1 \\ x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \end{vmatrix} &= x \begin{vmatrix} y_0 & 1 \\ y_1 & 1 \end{vmatrix} - y \begin{vmatrix} x_0 & 1 \\ x_1 & 1 \end{vmatrix} + 1 \begin{vmatrix} x_0 & y_0 \\ x_1 & y_1 \end{vmatrix} \\ &= (y_0 - y_1)x + (x_1 - x_0)y + (x_0 y_1 - x_1 y_0) \\ &= ax + by + c \end{aligned}$$

where this defines a, b, and c. Note that $a = 0$ only when $y_0 = y_1$ and $b = 0$ only when $x_0 - x_1$. As the points are distinct we have that at least one of a or b is nonzero. And the punch line is that if two rows of a determinant are equal, then the determinant is zero. Thus $(x,y) = (x_0,y_0)$ the the first two rows are the same and so $f(x_0,y_0) = 0$. Likewise if $(x,y) = (x_1,y_1)$ then the first and third rows are the same and thus $f(x_1,y_1) = 0$. Therefore we see that

$$L(y_0 - y_1, x_1 - x_0, x_0 y_1 - x_1 y_0)$$

contains both the points (x_0,y_0) and (x_1,y_1). □

We still need to show that the line through two distinct points is unique.

Problem 9. Show that the set of points (x, y) satisfying $y = mx + \beta$ is the same as the line $L(m, -1, \beta)$. □

Lemma 7. *Let (x_0, y_0) and (x_1, y_1) be points of $\mathbb{A}^2$ with $x_0 \neq x_1$. Assume these points are both on $L(a, b, c)$ where a and b are not both zero. That is*

$$ax_0 + by_0 + c = 0 \qquad \text{and} \qquad ax_1 + by_1 + c = 0.$$

Then $b \neq 0$ and

$$L(a, b, c) = L(m, -1, \beta)$$

where

$$m = \frac{y_1 - y_0}{x_1 - x_0}, \qquad \text{and} \qquad \beta = \frac{x_1 y_0 - x_0 y_1}{x_1 - x_0}.$$

Problem 10. Prove this along the following lines:

(a) Show $a(x_1 - x_0) + b(y_1 - y_0) = 0$.
(b) Show $b \neq 0$. *Hint:* If $b = 0$ what does this say about a?
(c) Show $\dfrac{-a}{b} = \dfrac{y_1 - y_0}{x_1 - x_0} = m$
(d) Use $\lambda = -1/b$ in Proposition 4 to conclude

$$L(a, b, c) = L\Big(\frac{-a}{b}, -1, \frac{-c}{b}\Big).$$

(e) Show

$$\frac{-c}{b} = \frac{x_1 y_0 - x_0 y_1}{x_1 - x_0}.$$

(f) Assemble the parts above to finish the proof. □

Lemma 8. *If (x_0, y_0) and (x_1, y_1) are distinct points of $\mathbb{A}^2$ with $x_0 = x_1$ and these points are both on $L(a, b, c)$ then*

$$L(a, b, c) = L(1, 0, -x_0)$$

Problem 11. Prove this. *Hint:* Start by noting that as the points are distinct that $y_0 \neq y_1$ and use this to show $b = 0$. Thus $a \neq 0$ (why?). Therefore $L(a, b, c) = L(a, 0, c)$. Also $L(a, 0, c) = L(1, 0, c/a)$ (why?). Finally use that (x_0, y_0) is on $L(1, 0, c/a)$ to conclude $c/a = -x_0$. □

Lemma 9. *If (x_0, y_0) and (x_1, y_1) are distinct points of $\mathbb{A}^2$ and they are on $L(a, b, c)$ and $L(a', b', c')$, then*

$$L(a, b, c) = L(a', b', c').$$

Problem 12. Prove this. *Hint:* If $x_0 \neq x_1$ then by Lemma 7

$$L(a, b, c) = L\Big(\frac{y_1 - y_0}{x_1 - x_0}, -1, \frac{x_1 y_0 - x_0 y_1}{x_1 - x_0}\Big).$$

What does Lemma 7 say about $L(a', b', c')$? If $x_0 = x_1$ use Lemma 8 and the same line of reasoning. □

Theorem 10. *The first axiom of Affine Geometry holds in $\mathbb{A}^2$ when we use the sets $L(a,b,c)$ as lines. That is given any two points P and Q of $\mathbb{A}^2$ there is a unique set of the form $L(a,b,c)$ that contains both P and Q.*

Problem 13. Assemble the lemmas above to give a proof of this. □

We now have to come to grips with when lines are parallel and when they intersect in this setting.

Lemma 11. *Given $L(a,b,c)$ and $L(a',b',c')$ with $ab'-a'b\neq 0$ then these lines have exactly one point in common.*

Problem 14. Prove this. *Hint:* This is the same as showing that the system

$$\begin{aligned} ax+by+c&=0 \\ a'x+b'y+c'&=0 \end{aligned} \tag{2}$$

has exactly on solution $(x,y)\in\mathbb{A}^2$. Multiply the first of these by b' and the second by b to get

$$\begin{aligned} ab'x+bb'y+cb'&=0 \\ a'bx+bb'y+bc'&=0 \end{aligned}$$

Now subtract:

$$(ab'-a'b)x+cb'-bc'=0$$

which, as $ab'-a'b\neq 0$, gives a x value of

$$x=\frac{bc'-cb'}{ab'-a'b}.$$

Do a similar calculation get a formula for y that has $ab'-a'b$ in the denominator. This shows that there is at most one solution (why?). Now plug your formulas for x and y back into the system (2) to that there is at least one solution. □

Lemma 12. *Let $a,b,a',b'\in\mathbb{F}$ with a and b not both zero and a' and b' not both zero. Assume*

$$ab'-a'b=0.$$

Then show there is a $\lambda\in\mathbb{F}$, with $\lambda\neq 0$, such that

$$a'=\lambda a \qquad \textit{and} \qquad b'=\lambda b.$$

(In vector form this is $\langle a',b'\rangle=\lambda\langle a,b\rangle$.)

Problem 15. Prove this. *Hint:* As a and b are not both zero, consider two cases. First if $a\neq 0$ show that this implies $a'\neq 0$ and show that $\lambda=\frac{a'}{a}$ works. Do something similar when $b\neq 0$. □

Lemma 13. *Given $L(a,b,c)$ and $L(a',b',c')$ with $ab'-a'b=0$, show that $L(a,b,c)$ are parallel. (Recall that under our definition this means that either the two have not point in common or they are equal.)*

Problem 16. Prove this. *Hint:* By Lemma 12 there is a $\lambda \neq 0$ such that $a' = \lambda a$ and $b' = \lambda b$. Show if $c' = \lambda c$ then $L(a, b, c) = L(a', b', c')$ and if $c' \neq \lambda c$ that $L(a, b, c)$ and $L(a', b', c')$ have no points in common. □

Lemma 14. *Given a point $P = (x_0, y_0)$ and $a, b \in \mathbb{F}$ with a and b not both zero, show there is a c such that P is on $L(a, b, c)$.*

Problem 17. Prove this. □

Theorem 15. *The second axiom of affine geometry holds in $\mathbb{A}^2$. Explicitly this is the parallel axiom which in this setting says that given any line $L(a, b, c)$ and a point $P = (x_0, y_0)$ not on this line that there is a unique line through P and parallel to $L(a, b, c)$.*

Problem 18. Prove this. *Hint:* By Lemma 14 there is a $c' \in \mathbb{F}$ such that P is on $L(a, b, c')$. Show that the line $L(a, b, c')$ is parallel to $L(a, b, c)$ and that it is the only parallel to $L(a, b, c)$ through this point. □

Theorem 16. *The third axiom of affine geometry holds in $\mathbb{A}^2$. That is there are four points of $\mathbb{A}^2$ with no three on the same line.*

Problem 19. Prove this. *Hint:* You might try the four points $(0, 0)$, $(1, 0)$, $(0, 1)$, and $(1, 1)$. □

We can now say when two of the lines $L(a, b, c)$ and $L(a'b'c')$ are equal (although this is implicit in some of the results above).

Proposition 17. *The two lines $L(a, b, c)$ and $L(a', b', c')$ are equal if and only if there is a $\lambda \neq 0$ such that*

$$a' = \lambda a, \qquad b' = \lambda b, \qquad c' = \lambda c.$$

Problem 20. Prove this. □

2. Fields and their basic properties.

In the last section we construct the affine planes from sets of ordered pairs (x, y) where $x, y \in \mathbb{F}$ and $\mathbb{F}$ was either the real numbers $\mathbb{R}$, the rational numbers, $\mathbb{Q}$, or the complex numbers, $\mathbb{C}$. If you look at what we did you can see that the only properties we used for elements of $\mathbb{F}$ were that they satisfy the usual rules for addition, subtraction, multiplication, and division we familiar with from basic high school algebra. This motivates the following:

Definition 18. A ***field*** is a set $\mathbb{F}$ with two operations $+$ (addition) and $\cdot$ (multiplication) that satisfy the following definition. The ***associative laws***

$$x + (y + z) = (x + y) + z \qquad x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

hold. The ***communicative laws***

$$x + y = y + x \qquad x \cdot y = y \cdot x$$

hold. The ***distributive law***

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

holds. There are two elements 0 (zero) and 1 (unity or one) such that for all $x \in \mathbb{F}$

$$x + 0 = x \qquad x \cdot 1 = 1$$

and $0 \neq 1$. For each $x \in \mathbb{F}$ there is an ***additive inverse*** $-x$ of x such that

$$x + (-x) = 0.$$

For each $x \in \mathbb{F}$ with $x \neq 0$ there is an ***inverse***, x^{-1}, of x such that

$$x \cdot (x^{-1}) = 1.$$

□

We will simplify the notation a bit and write xy for $x \cdot y$. We also use abbreviation

$$a + (-b) = a - b$$

and call this ***subtraction***. We also have a natural definition of ***division***

$$\frac{a}{b} = a(b^{-1}).$$

We now give some examples of fields other that might be new to you. First let $\mathbb{Q}(\sqrt{2})$ be the subset of the real numbers given by

$$\mathbb{Q}(\sqrt{2}) := \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \right\}$$

Proposition 19. *If $a, b \in \mathbb{Q}$ and*

$$a + b\sqrt{2} = 0$$

then

$$a = b = 0.$$

Proof. If $a = 0$, then $b\sqrt{2} = 0$ which implies $b = 0$. If $b = 0$ then $a = a + b\sqrt{2} = 0$. So if the proposition does not hold we have that both a and b are not zero. But then $a + b\sqrt{2} = 0$ implies

$$\sqrt{2} = \frac{-a}{b}$$

and $\frac{-a}{b}$ is a rational number, contradicting the well known fact that $\sqrt{2}$ is irrational. □

Also $\mathbb{Q}(\sqrt{2})$ is closed under sums and products: if $a + b\sqrt{2}$ and $a' + b'\sqrt{2}$ are in $\mathbb{Q}(\sqrt{2})$ then the sum is

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}$$

which is back in $\mathbb{Q}(\sqrt{2})$, and the product is

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2}$$

and as the numbers $(aa' + 2bb')$ and $(ab' + a'b)$ are rational this is back in $\mathbb{Q}(\sqrt{2})$. More subtle is that $\mathbb{Q}(\sqrt{2})$ is closed under taking inverses. Let

$a + b\sqrt{2}$ be a nonzero element of $\mathbb{Q}(\sqrt{2})$. Then by the last proposition at least one of a or b is nonzero and whence $a^2 + 2b^2 \neq 0$. Therefore

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a}{a+2b^2} + \frac{-b}{a^2+2b^2}\sqrt{2}.$$

But $\frac{a}{a+2b^2}$ and $\frac{-b}{a^2+2b^2}$ are rational numbers which shows that $\frac{1}{a+b\sqrt{2}}$ is an element of $\mathbb{Q}(\sqrt{2})$. These facts can be put together to get

Proposition 20. *The subset $\mathbb{Q}(\sqrt{2})$ if $\mathbb{R}$ is a field. (More precisely a subfield of $|R$.)* □

There was nothing special about $\sqrt{2}$. The same line of reasoning shows

Proposition 21. *If d is a positive integer such that $\sqrt{d}$ is irrational, then the set*

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$$

is a subfield of $\mathbb{R}$. □

Then using $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ in the construction of $\mathbb{A}^2$ as in Section 1 gives us many more examples of affine planes.

There are also many finite fields. To find some of them recall the construction of the integers mod n. If n is a positive integer a is any integer let $a \bmod n$ be the remainder when a is divided by n. For example

$$5 \bmod 2 = 1 \qquad 6 \bmod 2 = 0 \qquad 17 \bmod 5 = 2$$
$$-7 \bmod 5 = 3 \qquad 100 \bmod 9 = 1 \qquad 853{,}462 \bmod 100 = 62.$$

We can then define addition and multiplication mod n by reducing mod n. Therefore if $n = 6$ we have that mod 6 addition and multiplication look like

$$1 + 2 \bmod 6 = 3 \bmod 6 = 3$$
$$3 + 4 \bmod 6 = 7 \bmod 6 = 2$$
$$2 \cdot 6 \bmod 6 = 6 \bmod 6 = 1$$
$$3 \cdot 4 \bmod 6 = 12 \bmod 6 = 2$$

The full addition and multiplication tables looks like

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

We call this $\mathbb{Z}_6$. For any $n \geq 2$ we can make the corresponding addition and multiplication tables. We call the resulting number system $\mathbb{Z}_n$, the ***integers modulo*** n.

If $\mathbb{F}$ is a field and $a, b \in \mathbb{F}$ with $ab = 0$, then $a = 0$ or $b = 0$. To see this note that if $a = 0$, then we are done. So assume that $a \neq 0$. Then multiply both sides of $ab = 0$ by a^{-1} to get $a^{-1}ab = a^{-1}0$ which simplifies to $b = 0$. Thus we from the multiplication table above that $\mathbb{Z}_6$ is *not* a field as $2 \cdot 3 = 0$ in $\mathbb{Z}_6$.

Let us look at $n = 7$. Then the tables are

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

If you are very energetic you can check that this is a field. (What takes the most work is showing that the associative laws hold.) What makes this a field while $\mathbb{Z}_6$ is not is that 7 is a prime number. In general we have

Theorem 22. *If p is a prime number then $\mathbb{Z}_p$ is a field.* □

Thus for each prime we can construct an affine plane

$$\mathbb{A}^2 := \{(x, y) : x, y \in \mathbb{Z}_p\}.$$

When $p = 2$ this gives the four point plane from Homework 1. When $p = 3$ this gives the nine point plane from Homework 1.

It is now natural to ask if this gives all the finite fields. The answer is no.

Theorem 23. *If $n = p^k$ is a power of a prime number, there is field of order n. Any two fields of the same order are isomorphic, so that there is essential only one field of order $n = p^k$.* □

That a field of order p^k exists was shown by Evariste Galois around 1830. That these are the only finite fields was shown by E. H. Moore in 1893. Moore was one of the first American mathematicians to gain an international reputation.