MOOC de Criptología Matemática. Geometría sobre Cuerpos Finitos

Leandro Marín

Módulo III. Sesión 1.
Dificultad Media

Definiciones Básicas

- Sea K un cuerpo cualquiera y n un número natural.

Definiciones Básicas

- Sea K un cuerpo cualquiera y n un número natural.
- Podemos construir el conjunto K^n formado por tuplas ordenadas $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ que llamaremos vectores.

Definiciones Básicas

- Sea K un cuerpo cualquiera y n un número natural.
- Podemos construir el conjunto K^n formado por tuplas ordenadas $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ que llamaremos vectores.
- Estos elementos se pueden sumar con la operación

$$(\lambda_1, \lambda_2, \cdots, \lambda_n) + (\mu_1, \mu_2, \cdots, \mu_n) = (\lambda_1 + \mu_1, \lambda_2 + \mu_2, \cdots, \lambda_n + \mu_n)$$

Definiciones Básicas

- Sea K un cuerpo cualquiera y n un número natural.
- Podemos construir el conjunto K^n formado por tuplas ordenadas $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ que llamaremos vectores.
- Estos elementos se pueden sumar con la operación

$$(\lambda_1, \lambda_2, \cdots, \lambda_n) + (\mu_1, \mu_2, \cdots, \mu_n) = (\lambda_1 + \mu_1, \lambda_2 + \mu_2, \cdots, \lambda_n + \mu_n)$$

- También podemos multiplicar un elemento de K por un vector de la siguiente forma:

$$\alpha \cdot (\lambda_1, \lambda_2, \cdots, \lambda_n) = (\alpha\lambda_1, \alpha\lambda_2, \cdots, \alpha\lambda_n)$$

Definiciones Básicas

- Sea K un cuerpo cualquiera y n un número natural.
- Podemos construir el conjunto K^n formado por tuplas ordenadas $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ que llamaremos vectores.
- Estos elementos se pueden sumar con la operación

$$(\lambda_1, \lambda_2, \cdots, \lambda_n) + (\mu_1, \mu_2, \cdots, \mu_n) = (\lambda_1 + \mu_1, \lambda_2 + \mu_2, \cdots, \lambda_n + \mu_n)$$

- También podemos multiplicar un elemento de K por un vector de la siguiente forma:

$$\alpha \cdot (\lambda_1, \lambda_2, \cdots, \lambda_n) = (\alpha\lambda_1, \alpha\lambda_2, \cdots, \alpha\lambda_n)$$

- El conjunto K^n con estas operaciones forma lo que se denomina un espacio vectorial.

El caso finito

- Es muy probable que conozcas espacios vectoriales como por ejemplo $\mathbb{R}^n$.

El caso finito

- Es muy probable que conozcas espacios vectoriales como por ejemplo $\mathbb{R}^n$.
- Lo que hemos hecho aquí es considerar un cuerpo K cualquiera. Podemos tomar un cuerpo finito.

El caso finito

- Es muy probable que conozcas espacios vectoriales como por ejemplo $\mathbb{R}^n$.
- Lo que hemos hecho aquí es considerar un cuerpo K cualquiera. Podemos tomar un cuerpo finito.
- Cuando estamos en un cuerpo finito funcionan bien casi todas las propiedades (salvo las relacionadas con distancias y ángulos).

El caso finito

- Es muy probable que conozcas espacios vectoriales como por ejemplo $\mathbb{R}^n$.
- Lo que hemos hecho aquí es considerar un cuerpo K cualquiera. Podemos tomar un cuerpo finito.
- Cuando estamos en un cuerpo finito funcionan bien casi todas las propiedades (salvo las relacionadas con distancias y ángulos).
- Podemos describir rectas, planos, sistemas de ecuaciones, etc. El problema es que perdemos la visión intuitiva que tenemos sobre esos conceptos.

El caso finito

- Es muy probable que conozcas espacios vectoriales como por ejemplo $\mathbb{R}^n$.
- Lo que hemos hecho aquí es considerar un cuerpo K cualquiera. Podemos tomar un cuerpo finito.
- Cuando estamos en un cuerpo finito funcionan bien casi todas las propiedades (salvo las relacionadas con distancias y ángulos).
- Podemos describir rectas, planos, sistemas de ecuaciones, etc. El problema es que perdemos la visión intuitiva que tenemos sobre esos conceptos.
- Sin embargo, para criptografía son mucho más útiles los cuerpos finitos, porque nos permiten representar información mediante el número finito casos posibles.

Ejemplo

- Consideremos por ejemplo el caso $K = \mathbb{Z}_2$ y $n = 3$.

Ejemplo

- Consideremos por ejemplo el caso $K = \mathbb{Z}_2$ y $n = 3$.
- En este caso el número de vectores posibles es 8.

$$\{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$$

Ejemplo

- Consideremos por ejemplo el caso $K = \mathbb{Z}_2$ y $n = 3$.
- En este caso el número de vectores posibles es 8.

$$\{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$$

- El producto $\alpha(\lambda_1, \lambda_2, \lambda_3)$ será, según α sea 0 ó 1,

$$0 \cdot (\lambda_1, \lambda_2, \lambda_3) = (0,0,0)$$

$$1 \cdot (\lambda_1, \lambda_2, \lambda_3) = (\lambda_1, \lambda_2, \lambda_3).$$

Ejemplo

- Consideremos por ejemplo el caso $K = \mathbb{Z}_2$ y $n = 3$.
- En este caso el número de vectores posibles es 8.

$$\{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$$

- El producto $\alpha(\lambda_1, \lambda_2, \lambda_3)$ será, según α sea 0 ó 1,

$$0 \cdot (\lambda_1, \lambda_2, \lambda_3) = (0,0,0)$$

$$1 \cdot (\lambda_1, \lambda_2, \lambda_3) = (\lambda_1, \lambda_2, \lambda_3).$$

- Si recordamos que en $\mathbb{Z}_2$ la operación $+$ coincide con el *o exclusivo* (XOR), tenemos que la suma vectorial coincide con la operación XOR sobre los números representados por los vectores.

Número de Vectores

- Sea K un cuerpo de p elementos y n un número natural.

Número de Vectores

- Sea K un cuerpo de p elementos y n un número natural.
- El número de vectores del espacio K^n será el número de posibles tuplas $(\lambda_1, \lambda_2, \cdots, \lambda_n)$.

Número de Vectores

- Sea K un cuerpo de p elementos y n un número natural.
- El número de vectores del espacio K^n será el número de posibles tuplas $(\lambda_1, \lambda_2, \cdots, \lambda_n)$.
- Como tenemos p posibles elecciones para λ_1, para cada una de ellas p elecciones para λ_2. Para cada elección de λ_1 y λ_2 tenemos otras p elecciones para λ_3.

Número de Vectores

- Sea K un cuerpo de p elementos y n un número natural.
- El número de vectores del espacio K^n será el número de posibles tuplas $(\lambda_1, \lambda_2, \cdots, \lambda_n)$.
- Como tenemos p posibles elecciones para λ_1, para cada una de ellas p elecciones para λ_2. Para cada elección de λ_1 y λ_2 tenemos otras p elecciones para λ_3.
- Siguiendo este proceso, vemos que el número total de vectores es precisamente p^n.

Rectas en el Plano Vectorial

- Llamaremos plano vectorial al espacio vectorial K^2.

Rectas en el Plano Vectorial

- Llamaremos plano vectorial al espacio vectorial K^2.
- Dentro de él encontraremos conjuntos que llamaremos rectas.

Rectas en el Plano Vectorial

- Llamaremos plano vectorial al espacio vectorial K^2.
- Dentro de él encontraremos conjuntos que llamaremos rectas.
- Si $v = (\lambda_1, \lambda_2)$ es un vector de K^2 distinto de 0, la recta vectorial generada por v es el conjunto de puntos

$$\{\alpha v : \alpha \in K\} = \{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$$

Rectas en el Plano Vectorial

- Llamaremos plano vectorial al espacio vectorial K^2.
- Dentro de él encontraremos conjuntos que llamaremos rectas.
- Si $v = (\lambda_1, \lambda_2)$ es un vector de K^2 distinto de 0, la recta vectorial generada por v es el conjunto de puntos

$$\{\alpha v : \alpha \in K\} = \{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$$

- El número de puntos de esta recta es el mismo que el de elementos de K, puesto que si $\alpha \neq \beta$ se tiene que $\alpha v \neq \beta v$, es decir, todos los puntos αv son distintos.

Rectas en el Plano Vectorial

- Llamaremos plano vectorial al espacio vectorial K^2.
- Dentro de él encontraremos conjuntos que llamaremos rectas.
- Si $v = (\lambda_1, \lambda_2)$ es un vector de K^2 distinto de 0, la recta vectorial generada por v es el conjunto de puntos

$$\{\alpha v : \alpha \in K\} = \{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$$

- El número de puntos de esta recta es el mismo que el de elementos de K, puesto que si $\alpha \neq \beta$ se tiene que $\alpha v \neq \beta v$, es decir, todos los puntos αv son distintos.
- Llamaremos representación paramétrica de la recta a esta forma de darla en términos de un vector y un parámetro α.

Representación Implícita de las Rectas

- Si tenemos una recta $\{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$ y llamamos x a la primera coordenada e y a la segunda, tenemos:

$$x = \alpha\lambda_1 \quad y = \alpha\lambda_2$$

Representación Implícita de las Rectas

- Si tenemos una recta $\{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$ y llamamos x a la primera coordenada e y a la segunda, tenemos:

$$x = \alpha\lambda_1 \quad y = \alpha\lambda_2$$

- Por lo tanto $\lambda_2 x = \alpha\lambda_1\lambda_2 = \lambda_1 y$

Representación Implícita de las Rectas

- Si tenemos una recta $\{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$ y llamamos x a la primera coordenada e y a la segunda, tenemos:

$$x = \alpha\lambda_1 \quad y = \alpha\lambda_2$$

- Por lo tanto $\lambda_2 x = \alpha\lambda_1\lambda_2 = \lambda_1 y$
- La representación de la recta como la ecuación $\lambda_1 y = \lambda_2 x$ o equivalentemente $\lambda_2 x - \lambda_1 y = 0$ es lo que se llama representación implícita de la recta.

Representación Implícita de las Rectas

- Si tenemos una recta $\{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$ y llamamos x a la primera coordenada e y a la segunda, tenemos:

$$x = \alpha\lambda_1 \quad y = \alpha\lambda_2$$

- Por lo tanto $\lambda_2 x = \alpha\lambda_1\lambda_2 = \lambda_1 y$
- La representación de la recta como la ecuación $\lambda_1 y = \lambda_2 x$ o equivalentemente $\lambda_2 x - \lambda_1 y = 0$ es lo que se llama representación implícita de la recta.
- En el caso en que $\lambda_1 \neq 0$, también podemos poner $y = \lambda_2\lambda_1^{-1}x$.

Representación Implícita de las Rectas

- Si tenemos una recta $\{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$ y llamamos x a la primera coordenada e y a la segunda, tenemos:

$$x = \alpha\lambda_1 \quad y = \alpha\lambda_2$$

- Por lo tanto $\lambda_2 x = \alpha\lambda_1\lambda_2 = \lambda_1 y$
- La representación de la recta como la ecuación $\lambda_1 y = \lambda_2 x$ o equivalentemente $\lambda_2 x - \lambda_1 y = 0$ es lo que se llama representación implícita de la recta.
- En el caso en que $\lambda_1 \neq 0$, también podemos poner $y = \lambda_2\lambda_1^{-1}x$.
- El valor $\lambda_2\lambda_1^{-1}$ se llama pendiente de la recta.

Rectas en el Plano $\mathbb{Z}_5^2$

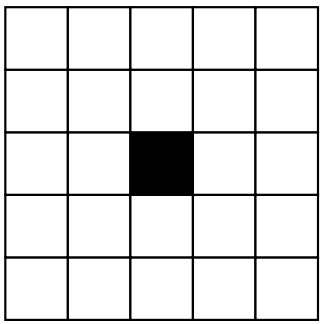
- Vamos a ver como ejemplo todas las rectas en el plano $\mathbb{Z}_5^2$.

Rectas en el Plano $\mathbb{Z}_5^2$

- Vamos a ver como ejemplo todas las rectas en el plano $\mathbb{Z}_5^2$.
- Como $-1 \equiv 4(mod\ 5)$ y $-2 \equiv 3(mod\ 5)$, vamos a hacer la representación de los valores en el siguiente orden $-2, -1, 0, 1, 2$.

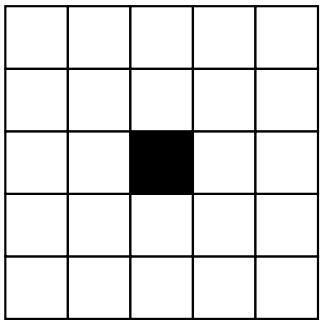
Rectas en el Plano $\mathbb{Z}_5^2$

- Vamos a ver como ejemplo todas las rectas en el plano $\mathbb{Z}_5^2$.
- Como $-1 \equiv 4(mod\ 5)$ y $-2 \equiv 3(mod\ 5)$, vamos a hacer la representación de los valores en el siguiente orden $-2, -1, 0, 1, 2$.
- Utilizaremos el eje horizontal y vertical tal y como se usa en $\mathbb{R}^2$. Así por ejemplo el $(0, 0)$ será el siguiente vector:



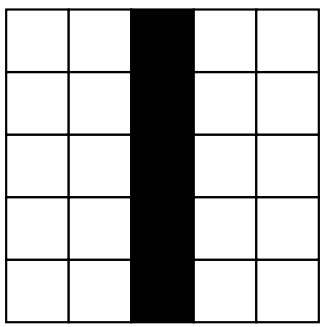
Rectas en el Plano $\mathbb{Z}_5^2$

- Vamos a ver como ejemplo todas las rectas en el plano $\mathbb{Z}_5^2$.
- Como $-1 \equiv 4(mod\ 5)$ y $-2 \equiv 3(mod\ 5)$, vamos a hacer la representación de los valores en el siguiente orden $-2, -1, 0, 1, 2$.
- Utilizaremos el eje horizontal y vertical tal y como se usa en $\mathbb{R}^2$. Así por ejemplo el $(0, 0)$ será el siguiente vector:



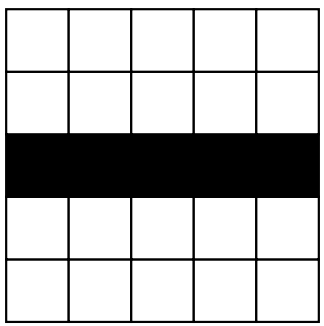
- Esta representación la usaremos en diversas ocasiones a lo largo de este curso.

Recta $x = 0$



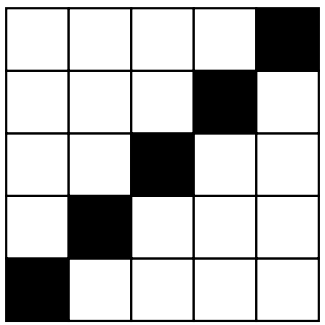
Esta es la recta vertical, formada por los puntos $\{(0,-2),(0,-1),(0,0),(0,1),(0,2)\}$ y que podemos generar por medio del vector $(0,1)$ (por ejemplo) ya que la recta coincide con los puntos $\{\alpha(0,1) : \alpha \in \mathbb{Z}_5\}$.

Recta $y = 0$



Esta es la recta horizontal.

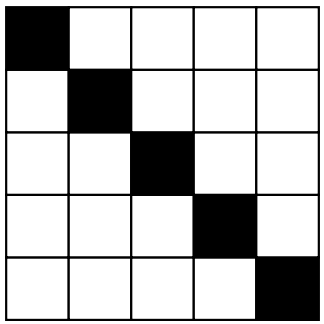
Recta $-x + y = 0$



Esta es la recta que podríamos entender como diagonal principal. Está generada por el vector $(1, 1)$ (por ejemplo) ya que son los puntos

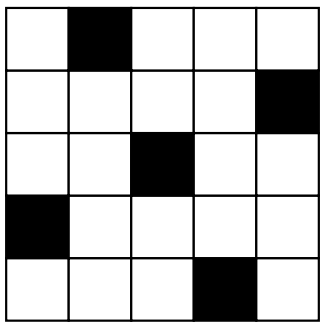
$$\{(\alpha, \alpha) : \alpha \in \mathbb{Z}_5\}$$

Recta $x + y = 0$



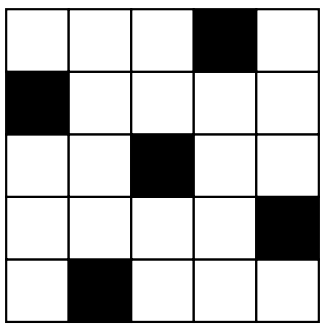
Esta es la otra diagonal, generada por el vector $(1, -1)$.

Recta $2x + y = 0$



Esta es otra recta, aunque pueda parecer que no lo es, cumple perfectamente la ecuación de una recta en este plano finito. Esta pérdida de la intuición gemétria es el problema que nos aparece en el caso finito, en el que nos tendremos que basar más en las propiedades algebraicas que en la idea intuitiva.

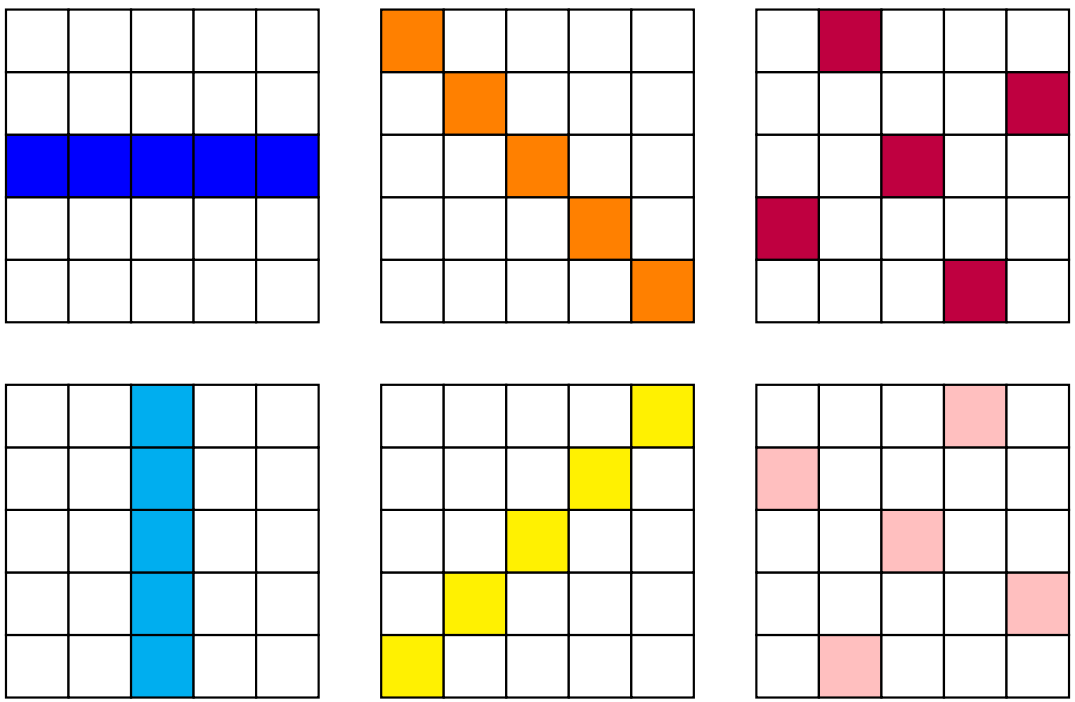
Recta $-2x + y = 0$



Esta última recta es la simétrica de la anterior.

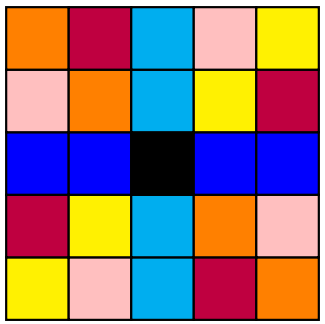
Rectas vectoriales del plano $\mathbb{Z}_5^2$

Veamos las 6 rectas vectoriales de este plano conjuntamente.



Algunas Propiedades

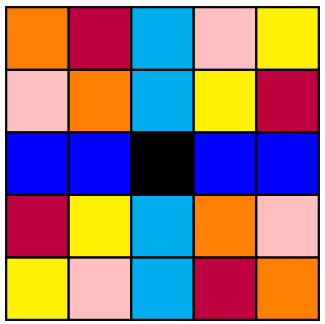
Si vemos las seis rectas superpuestas en un único dibujo obtenemos lo siguiente:



de donde podemos deducir que

Algunas Propiedades

Si vemos las seis rectas superpuestas en un único dibujo obtenemos lo siguiente:

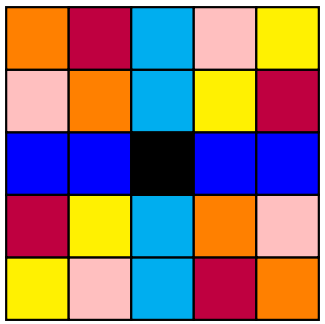


de donde podemos deducir que

- El $(0,0)$ es común a todas las rectas.

Algunas Propiedades

Si vemos las seis rectas superpuestas en un único dibujo obtenemos lo siguiente:

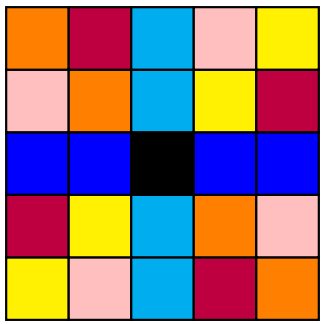


de donde podemos deducir que

- El $(0,0)$ es común a todas las rectas.
- Este es el único vector común a todas ellas.

Algunas Propiedades

Si vemos las seis rectas superpuestas en un único dibujo obtenemos lo siguiente:

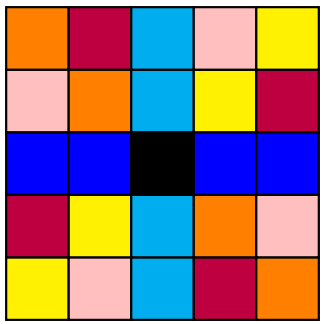


de donde podemos deducir que

- El $(0,0)$ es común a todas las rectas.
- Este es el único vector común a todas ellas.
- Las 6 rectas cubren todo el plano.

Algunas Propiedades

Si vemos las seis rectas superpuestas en un único dibujo obtenemos lo siguiente:



de donde podemos deducir que

- El $(0,0)$ es común a todas las rectas.
- Este es el único vector común a todas ellas.
- Las 6 rectas cubren todo el plano.
- Todas ellas tienen 5 puntos (el mismo número de elementos que el cuerpo $\mathbb{Z}_5$).

Representaciones Equivalentes

- Hemos visto que una recta viene dada por un vector no nulo $v = (\lambda_1, \lambda_2)$ con la fórmula

$$r = \{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$$

Representaciones Equivalentes

- Hemos visto que una recta viene dada por un vector no nulo $v = (\lambda_1, \lambda_2)$ con la fórmula
$$r = \{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$$
- Supongamos que v y w son dos vectores no nulos tales que $v = \mu w$, entonces las rectas generadas por v y por w son la misma, veámoslo:

Representaciones Equivalentes

- Hemos visto que una recta viene dada por un vector no nulo $v = (\lambda_1, \lambda_2)$ con la fórmula
$$r = \{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$$
- Supongamos que v y w son dos vectores no nulos tales que $v = \mu w$, entonces las rectas generadas por v y por w son la misma, veámoslo:
  - Si (x, y) está en la recta generada por v es porque existe α tal que $(x, y) = \alpha v$, pero como $v = \mu w$ podemos deducir que $(x, y) = \alpha v = \alpha\mu w$, es decir, que (x, y) es igual a un elemento de K (concretamente $\alpha\mu$) multiplicado por el vector w, o lo que es lo mismo, (x, y) está en la recta generada por w.

Representaciones Equivalentes

- Hemos visto que una recta viene dada por un vector no nulo $v = (\lambda_1, \lambda_2)$ con la fórmula
$$r = \{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$$
- Supongamos que v y w son dos vectores no nulos tales que $v = \mu w$, entonces las rectas generadas por v y por w son la misma, veámoslo:
  - Si (x, y) está en la recta generada por v es porque existe α tal que $(x, y) = \alpha v$, pero como $v = \mu w$ podemos deducir que $(x, y) = \alpha v = \alpha\mu w$, es decir, que (x, y) es igual a un elemento de K (concretamente $\alpha\mu$) multiplicado por el vector w, o lo que es lo mismo, (x, y) está en la recta generada por w.
  - Recíprocamente, supongamos que tenemos (x, y) en la recta generada por w, es decir, $(x, y) = \beta w$ para alún $\beta \in K$. Escribiendo $w = \mu^{-1} v$ deduciremos que $(x, y) = \beta\mu^{-1} v$ y por tanto está en la recta generada por v.

Representaciones Equivalentes

- Hemos visto que una recta viene dada por un vector no nulo $v = (\lambda_1, \lambda_2)$ con la fórmula
$$r = \{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$$
- Supongamos que v y w son dos vectores no nulos tales que $v = \mu w$, entonces las rectas generadas por v y por w son la misma, veámoslo:
  - Si (x, y) está en la recta generada por v es porque existe α tal que $(x, y) = \alpha v$, pero como $v = \mu w$ podemos deducir que $(x, y) = \alpha v = \alpha\mu w$, es decir, que (x, y) es igual a un elemento de K (concretamente $\alpha\mu$) multiplicado por el vector w, o lo que es lo mismo, (x, y) está en la recta generada por w.
  - Recíprocamente, supongamos que tenemos (x, y) en la recta generada por w, es decir, $(x, y) = \beta w$ para alún $\beta \in K$. Escribiendo $w = \mu^{-1} v$ deduciremos que $(x, y) = \beta\mu^{-1} v$ y por tanto está en la recta generada por v.
- Dos vectores no nulos v y w diremos que son equivalentes cuando exista $\mu \in K$ tal que $v = \mu w$.

Representaciones Equivalentes

- Hemos visto que una recta viene dada por un vector no nulo $v = (\lambda_1, \lambda_2)$ con la fórmula
$$r = \{(\alpha\lambda_1, \alpha\lambda_2) : \alpha \in K\}$$
- Supongamos que v y w son dos vectores no nulos tales que $v = \mu w$, entonces las rectas generadas por v y por w son la misma, veámoslo:
  - Si (x, y) está en la recta generada por v es porque existe α tal que $(x, y) = \alpha v$, pero como $v = \mu w$ podemos deducir que $(x, y) = \alpha v = \alpha\mu w$, es decir, que (x, y) es igual a un elemento de K (concretamente $\alpha\mu$) multiplicado por el vector w, o lo que es lo mismo, (x, y) está en la recta generada por w.
  - Recíprocamente, supongamos que tenemos (x, y) en la recta generada por w, es decir, $(x, y) = \beta w$ para alún $\beta \in K$. Escribiendo $w = \mu^{-1} v$ deduciremos que $(x, y) = \beta\mu^{-1} v$ y por tanto está en la recta generada por v.
- Dos vectores no nulos v y w diremos que son equivalentes cuando exista $\mu \in K$ tal que $v = \mu w$.
- Otra forma de verlo es que dos vectores son equivalentes si y sólo si generan la misma recta.

Vectores Equivalentes y Normalización

- Un vector no nulo v diremos que está normalizado si su última coordenada no nula es 1.

Vectores Equivalentes y Normalización

- Un vector no nulo v diremos que está normalizado si su última coordenada no nula es 1.
- Por ejemplo, $(\alpha, 1)$ es un vector normalizado, pero también lo es $(1, 0)$.

Vectores Equivalentes y Normalización

- Un vector no nulo v diremos que está normalizado si su última coordenada no nula es 1.
- Por ejemplo, $(\alpha, 1)$ es un vector normalizado, pero también lo es $(1, 0)$.
- Todo vector es equivalente a uno normalizado porque si $v = (\lambda_1, \lambda_2)$ con $\lambda_2 \neq 0$ podemos escribir $v = \lambda_2(\lambda_1\lambda_2^{-1}, 1)$ y por lo tanto v sería equivalente a $(\lambda_1\lambda_2^{-1}, 1)$. Los vectores no nulos de la forma $(\gamma, 0) = \gamma(1, 0)$ serán equivalentes al $(1, 0)$.

Vectores Equivalentes y Normalización

- Un vector no nulo v diremos que está normalizado si su última coordenada no nula es 1.
- Por ejemplo, $(\alpha, 1)$ es un vector normalizado, pero también lo es $(1, 0)$.
- Todo vector es equivalente a uno normalizado porque si $v = (\lambda_1, \lambda_2)$ con $\lambda_2 \neq 0$ podemos escribir $v = \lambda_2(\lambda_1\lambda_2^{-1}, 1)$ y por lo tanto v sería equivalente a $(\lambda_1\lambda_2^{-1}, 1)$. Los vectores no nulos de la forma $(\gamma, 0) = \gamma(1, 0)$ serán equivalentes al $(1, 0)$.
- Dos vectores normalizados son equivalentes si y sólo si son iguales.

Número de Rectas en el Plano

- Para contar el número de rectas en el plano, no tenemos más que contar cuantos vectores normalizados distintos tenemos.

Número de Rectas en el Plano

- Para contar el número de rectas en el plano, no tenemos más que contar cuantos vectores normalizados distintos tenemos.
- Por un lado tendremos los vectores $(\alpha, 1)$ con $\alpha \in K$ (de los cuales tendremos tantos como elementos de K) y también tendremos el $(1, 0)$.

Número de Rectas en el Plano

- Para contar el número de rectas en el plano, no tenemos más que contar cuantos vectores normalizados distintos tenemos.
- Por un lado tendremos los vectores $(\alpha, 1)$ con $\alpha \in K$ (de los cuales tendremos tantos como elementos de K) y también tendremos el $(1, 0)$.
- En total, si K tiene p elementos, tendremos $p + 1$ rectas.

Número de Rectas en el Plano

- Para contar el número de rectas en el plano, no tenemos más que contar cuantos vectores normalizados distintos tenemos.
- Por un lado tendremos los vectores $(\alpha, 1)$ con $\alpha \in K$ (de los cuales tendremos tantos como elementos de K) y también tendremos el $(1, 0)$.
- En total, si K tiene p elementos, tendremos $p + 1$ rectas.
- Estas son precisamente las que habíamos obtenido en el caso $p = 5$, un total de 6 rectas.

El Plano Afín

- En el plano vectorial existe un punto especial, que es el origen de coordenadas.

El Plano Afín

- En el plano vectorial existe un punto especial, que es el origen de coordenadas.
- Todas las rectas vectoriales $\{\alpha v : \alpha \in K\}$ contienen a este vector, puesto que siempre podemos poner $\alpha = 0$.

El Plano Afín

- En el plano vectorial existe un punto especial, que es el origen de coordenadas.
- Todas las rectas vectoriales $\{\alpha v : \alpha \in K\}$ contienen a este vector, puesto que siempre podemos poner $\alpha = 0$.
- El plano afín diferencia dos conceptos, puntos y vectores, aunque ambos se representarán por pares $(x, y) \in K^2$.

El Plano Afín

- En el plano vectorial existe un punto especial, que es el origen de coordenadas.
- Todas las rectas vectoriales $\{\alpha v : \alpha \in K\}$ contienen a este vector, puesto que siempre podemos poner $\alpha = 0$.
- El plano afín diferencia dos conceptos, puntos y vectores, aunque ambos se representarán por pares $(x, y) \in K^2$.
- Una recta vendrá definida por un punto base y una dirección.

El Plano Afín

- En el plano vectorial existe un punto especial, que es el origen de coordenadas.
- Todas las rectas vectoriales $\{\alpha v : \alpha \in K\}$ contienen a este vector, puesto que siempre podemos poner $\alpha = 0$.
- El plano afín diferencia dos conceptos, puntos y vectores, aunque ambos se representarán por pares $(x, y) \in K^2$.
- Una recta vendrá definida por un punto base y una dirección.
- De esta forma podemos desplazar el origen de coordenadas a cualquier punto del plano e introducir conceptos como el paralelismo.

Rectas en el Plano Afín

- Sea $P = (P_1, P_2) \in K^2$ un punto del plano y L una recta vectorial en el plano K^2.

Rectas en el Plano Afín

- Sea $P = (P_1, P_2) \in K^2$ un punto del plano y L una recta vectorial en el plano K^2.
- Definiremos la recta afín que pasa por P en la dirección de L al conjunto de puntos:

$$r = \{P + v : v \in L\}$$

Rectas en el Plano Afín

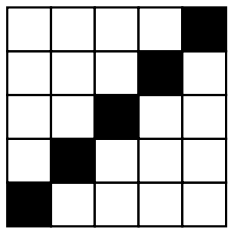
- Sea $P = (P_1, P_2) \in K^2$ un punto del plano y L una recta vectorial en el plano K^2.
- Definiremos la recta afín que pasa por P en la dirección de L al conjunto de puntos:

$$r = \{P + v : v \in L\}$$

- La representación de las rectas mediante un punto base y una dirección no es única.

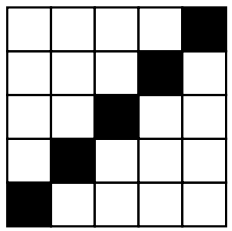
Ejemplo I

- Consideremos L la recta vectorial sobre el cuerpo $K = \mathbb{Z}_5$ dada por la fórmula $y = x$.

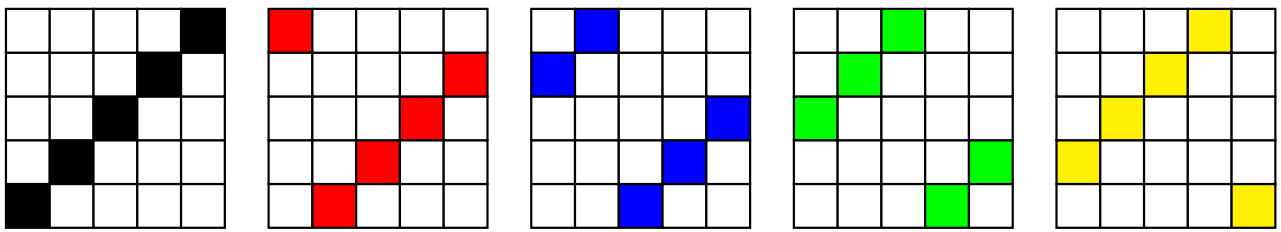


Ejemplo I

- Consideremos L la recta vectorial sobre el cuerpo $K = \mathbb{Z}_5$ dada por la fórmula $y = x$.

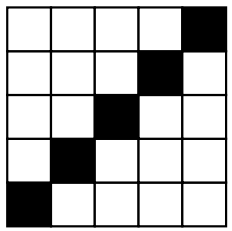


- Vamos a dibujar para cada uno de los puntos $(0,0)$, $(1,0)$, $(2,0)$, $(3,0) = (-2,0)$ y $(4,0) = (-1,0)$ las rectas afines que pasan por ellos en la dirección de L.

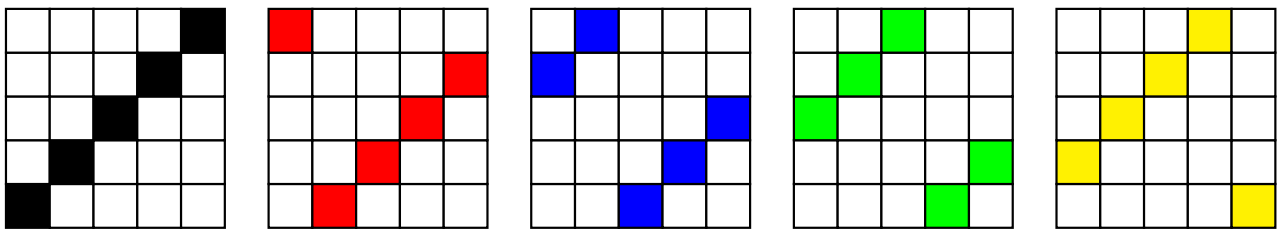


Ejemplo I

- Consideremos L la recta vectorial sobre el cuerpo $K = \mathbb{Z}_5$ dada por la fórmula $y = x$.



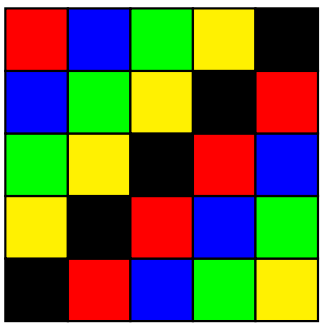
- Vamos a dibujar para cada uno de los puntos $(0,0)$, $(1,0)$, $(2,0)$, $(3,0) = (-2,0)$ y $(4,0) = (-1,0)$ las rectas afines que pasan por ellos en la dirección de L.



- Estas rectas no tienen ningún punto en común, son rectas paralelas.

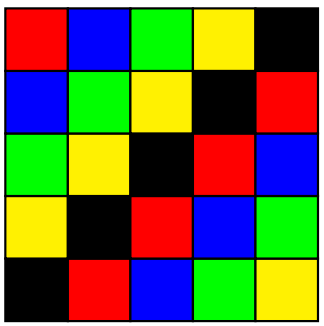
Ejemplo II

- Si juntamos las 5 rectas en un solo dibujo obtenemos lo siguiente:



Ejemplo II

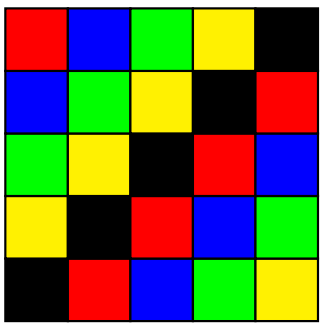
- Si juntamos las 5 rectas en un solo dibujo obtenemos lo siguiente:



- Esto nos muestra que estas cinco rectas paralelas cubren todo el plano.

Ejemplo II

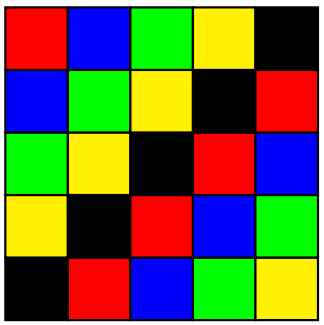
- Si juntamos las 5 rectas en un solo dibujo obtenemos lo siguiente:



- Esto nos muestra que estas cinco rectas paralelas cubren todo el plano.
- O lo que es lo mismo, que dado cualquier punto del plano, podemos encontrar una recta paralela a la recta $y = x$ que pasa por ese punto.

Ejemplo II

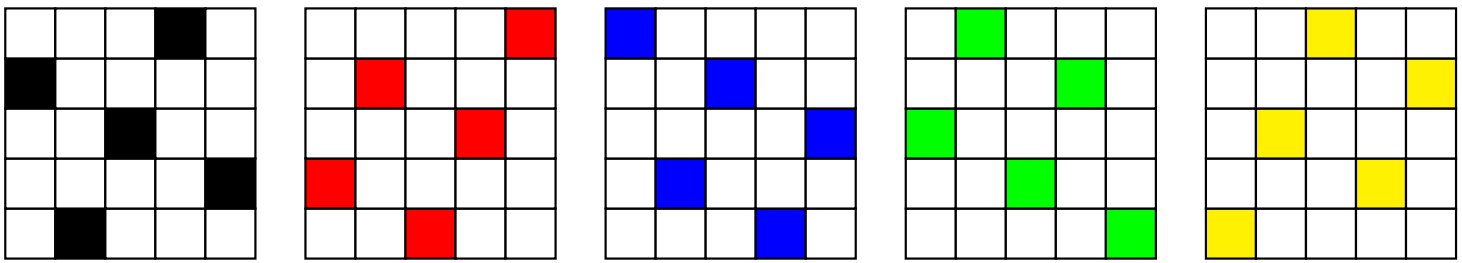
- Si juntamos las 5 rectas en un solo dibujo obtenemos lo siguiente:



- Esto nos muestra que estas cinco rectas paralelas cubren todo el plano.
- O lo que es lo mismo, que dado cualquier punto del plano, podemos encontrar una recta paralela a la recta $y = x$ que pasa por ese punto.
- Este tipo de propiedades son las habituales del paralelismo y de las rectas en cualquier plano.

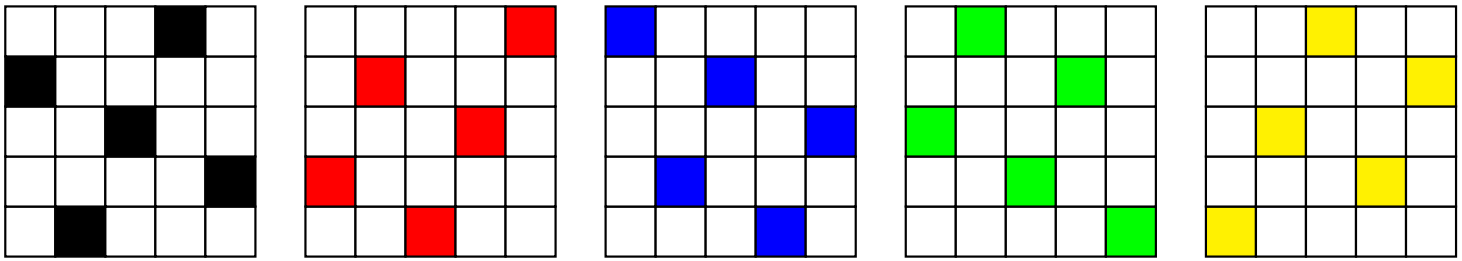
Ejemplo III

- Lo mismo sucede con la recta $y = 2x$ sobre el cuerpo $\mathbb{Z}_5$

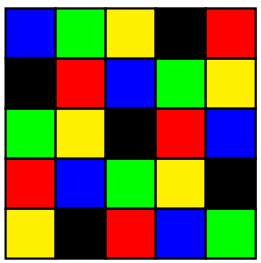


Ejemplo III

- Lo mismo sucede con la recta $y = 2x$ sobre el cuerpo $\mathbb{Z}_5$

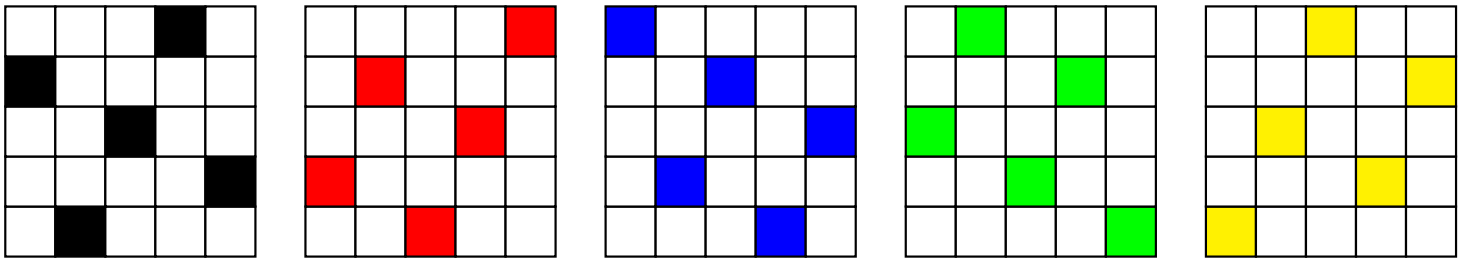


- Poniendo las cinco rectas paralelas en el mismo plano, vemos que cubre todo el plano

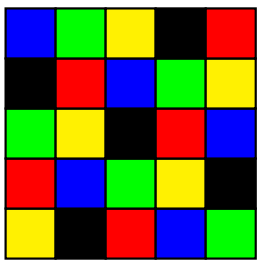


Ejemplo III

- Lo mismo sucede con la recta $y = 2x$ sobre el cuerpo $\mathbb{Z}_5$



- Poniendo las cinco rectas paralelas en el mismo plano, vemos que cubre todo el plano



- En este caso, la idea de rectas y paralelismo no se ve tan clara, pero desde el punto de vista algebraico es similar.

Ecuación Implícita de la Recta Afín

- Sea $P = (x_0, y_0)$ un punto del espacio afín, L la recta $ax + by = 0$

Ecuación Implícita de la Recta Afín

- Sea $P = (x_0, y_0)$ un punto del espacio afín, L la recta $ax + by = 0$
- La recta $r = P + L$ estará formada por los puntos (x, y) tales que $(x - x_0, y - y0) \in L$, es decir $a(x - x_0) + b(y - y_0) = 0$.

Ecuación Implícita de la Recta Afín

- Sea $P = (x_0, y_0)$ un punto del espacio afín, L la recta $ax + by = 0$
- La recta $r = P + L$ estará formada por los puntos (x, y) tales que $(x - x_0, y - y0) \in L$, es decir $a(x - x_0) + b(y - y_0) = 0$.
- Esta ecuación o la equivalente $ax + by = ax_0 + by_0$ es lo que llamaremos ecuación implícita de la recta afín.

Curvas en el Plano Afín

- Igual que se definen rectas, podemos definir otro tipo de curvas en el plano K^2 sobre un cuerpo finito.

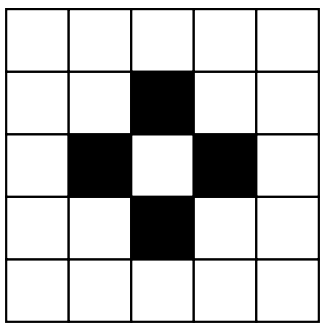
Curvas en el Plano Afín

- Igual que se definen rectas, podemos definir otro tipo de curvas en el plano K^2 sobre un cuerpo finito.
- Podemos aplicar polinomios en dos variables x e y y tomar los puntos (x, y) que cumplen la ecuación.

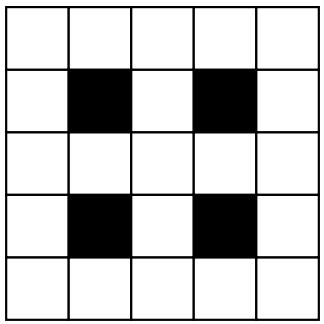
Curvas en el Plano Afín

- Igual que se definen rectas, podemos definir otro tipo de curvas en el plano K^2 sobre un cuerpo finito.
- Podemos aplicar polinomios en dos variables x e y y tomar los puntos (x, y) que cumplen la ecuación.
- Vamos a ver algunos ejemplos de curvas de grado dos.

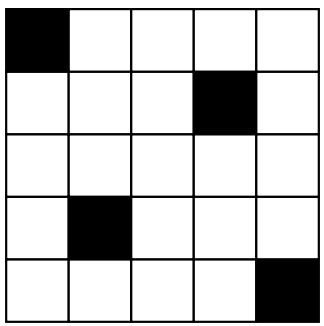
Curva $x^2 + y^2 = 1$



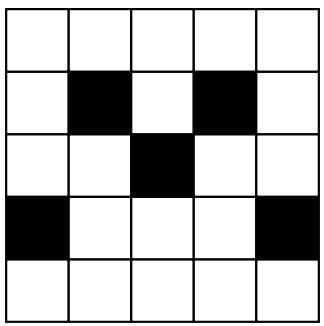
Curva $x^2 + y^2 = 2$



Curva $xy = 1$



Curva $y = x^2$



Vectores Equivalentes y Normalización

- Dados dos vectores no nulos $v = (v_1, v_2, v_3)$ y $w = (w_1, w_2, w_3)$, diremos que son equivalentes si existe $\mu \in K$ tal que $v = \mu w$.

Vectores Equivalentes y Normalización

- Dados dos vectores no nulos $v = (v_1, v_2, v_3)$ y $w = (w_1, w_2, w_3)$, diremos que son equivalentes si existe $\mu \in K$ tal que $v = \mu w$.
- Esta es la misma definición que hicimos para vectores del plano, pero con tres coordenadas.

Vectores Equivalentes y Normalización

- Dados dos vectores no nulos $v = (v_1, v_2, v_3)$ y $w = (w_1, w_2, w_3)$, diremos que son equivalentes si existe $\mu \in K$ tal que $v = \mu w$.
- Esta es la misma definición que hicimos para vectores del plano, pero con tres coordenadas.
- Un vector no nulo diremos que está normalizado cuando su última coordenada no nula sea un 1.

Vectores Equivalentes y Normalización

- Dados dos vectores no nulos $v = (v_1, v_2, v_3)$ y $w = (w_1, w_2, w_3)$, diremos que son equivalentes si existe $\mu \in K$ tal que $v = \mu w$.
- Esta es la misma definición que hicimos para vectores del plano, pero con tres coordenadas.
- Un vector no nulo diremos que está normalizado cuando su última coordenada no nula sea un 1.
- Al conjunto de vectores normalizados lo llamaremos plano proyectivo y lo denotaremos $\mathbb{P}^2(K)$.

Puntos del Plano Proyectivo

- Sea K un cuerpo de p elementos. Tendremos tres tipos de puntos en el plano proyectivo, los de la forma $(x, y, 1)$ donde x e y pueden tomar cualquier valor de K, por lo tanto tendremos p^2 puntos de este tipo. Estos puntos te llamarán puntos afines y los identificaremos con el plano afín.

Puntos del Plano Proyectivo

- Sea K un cuerpo de p elementos. Tendremos tres tipos de puntos en el plano proyectivo, los de la forma $(x, y, 1)$ donde x e y pueden tomar cualquier valor de K, por lo tanto tendremos p^2 puntos de este tipo. Estos puntos te llamarán puntos afines y los identificaremos con el plano afín.
- Por otro lado tendremos los del tipo $(x, 1, 0)$ con x cualquier valor de K (de este tipo tendremos p puntos) y por último tendremos el punto $(1, 0, 0)$.

Puntos del Plano Proyectivo

- Sea K un cuerpo de p elementos. Tendremos tres tipos de puntos en el plano proyectivo, los de la forma $(x, y, 1)$ donde x e y pueden tomar cualquier valor de K, por lo tanto tendremos p^2 puntos de este tipo. Estos puntos te llamarán puntos afines y los identificaremos con el plano afín.
- Por otro lado tendremos los del tipo $(x, 1, 0)$ con x cualquier valor de K (de este tipo tendremos p puntos) y por último tendremos el punto $(1, 0, 0)$.
- En total tendremos $p^2 + p + 1$ puntos en el plano proyectivo, de los cuales p^2 serán puntos afines y los otros los denominaremos puntos del infinito.

Coordenadas Proyectivas

- Para evitar confusiones entre los puntos del plano afín y la representación proyectiva en la que incluimos una última coordenada, escribiremos $(X : Y : Z)$ para denotar las clases de equivalencia de los vectores.

Coordenadas Proyectivas

- Para evitar confusiones entre los puntos del plano afín y la representación proyectiva en la que incluimos una última coordenada, escribiremos $(X : Y : Z)$ para denotar las clases de equivalencia de los vectores.
- Así por ejemplo, $(X : Y : Z) = (\mu X : \mu Y : \mu Z)$ para cualquier $\mu \neq 0$, puesto que son vectores equivalentes.

Coordenadas Proyectivas

- Para evitar confusiones entre los puntos del plano afín y la representación proyectiva en la que incluimos una última coordenada, escribiremos $(X : Y : Z)$ para denotar las clases de equivalencia de los vectores.
- Así por ejemplo, $(X : Y : Z) = (\mu X : \mu Y : \mu Z)$ para cualquier $\mu \neq 0$, puesto que son vectores equivalentes.
- Si $Z \neq 0$ entonces $(X : Y : Z) = (X/Z : Y/Z : 1)$ que corresponde al punto del plano afín $(x, y) = (X/Z, Y/Z)$ (en este caso separados por una coma).

Coordenadas Proyectivas

- Para evitar confusiones entre los puntos del plano afín y la representación proyectiva en la que incluimos una última coordenada, escribiremos $(X : Y : Z)$ para denotar las clases de equivalencia de los vectores.
- Así por ejemplo, $(X : Y : Z) = (\mu X : \mu Y : \mu Z)$ para cualquier $\mu \neq 0$, puesto que son vectores equivalentes.
- Si $Z \neq 0$ entonces $(X : Y : Z) = (X/Z : Y/Z : 1)$ que corresponde al punto del plano afín $(x, y) = (X/Z, Y/Z)$ (en este caso separados por una coma).
- Este tipo de coordenadas la denominaremos coordenadas proyectivas.

Coordenadas Proyectivas

- Para evitar confusiones entre los puntos del plano afín y la representación proyectiva en la que incluimos una última coordenada, escribiremos $(X : Y : Z)$ para denotar las clases de equivalencia de los vectores.
- Así por ejemplo, $(X : Y : Z) = (\mu X : \mu Y : \mu Z)$ para cualquier $\mu \neq 0$, puesto que son vectores equivalentes.
- Si $Z \neq 0$ entonces $(X : Y : Z) = (X/Z : Y/Z : 1)$ que corresponde al punto del plano afín $(x, y) = (X/Z, Y/Z)$ (en este caso separados por una coma).
- Este tipo de coordenadas la denominaremos coordenadas proyectivas.
- Un punto diremos que está en coordenadas proyectivas cuando nos lo den con tres valores X, Y y Z, pudiendo no estar normalizado. Un punto afín (x, y) para ponerlo en coordendadas proyectivas únicamente necesita añadir una última coordenada igual a 1.

Las Rectas Paralelas se cortan en el Infinito

- Si planteamos las ecuaciones de dos rectas paralelas, por ejemplo $x + y + 1 = 0$ y $x + y + 2 = 0$ podemos ver que no hay ningún punto (x, y) que satisfaga al mismo tiempo ambas ecuaciones, es decir, nunca se cortan.

Las Rectas Paralelas se cortan en el Infinito

- Si planteamos las ecuaciones de dos rectas paralelas, por ejemplo $x + y + 1 = 0$ y $x + y + 2 = 0$ podemos ver que no hay ningún punto (x, y) que satisfaga al mismo tiempo ambas ecuaciones, es decir, nunca se cortan.
- Sin embargo nosotros tenemos la intuición geométrica de que esas rectas se cortan si las vemos en perspectiva, pero lo hacen en un punto infinitamente lejano, lo que llamaríamos un punto del infinito.

Las Rectas Paralelas se cortan en el Infinito

- Si planteamos las ecuaciones de dos rectas paralelas, por ejemplo $x + y + 1 = 0$ y $x + y + 2 = 0$ podemos ver que no hay ningún punto (x, y) que satisfaga al mismo tiempo ambas ecuaciones, es decir, nunca se cortan.
- Sin embargo nosotros tenemos la intuición geométrica de que esas rectas se cortan si las vemos en perspectiva, pero lo hacen en un punto infinitamente lejano, lo que llamaríamos un punto del infinito.
- Esa intuición que se puede formalizar con geometría proyectiva sobre el cuerpo de los números reales, también funciona sobre cuerpos finitos.

Las Rectas Paralelas se cortan en el Infinito

- Si planteamos las ecuaciones de dos rectas paralelas, por ejemplo $x + y + 1 = 0$ y $x + y + 2 = 0$ podemos ver que no hay ningún punto (x, y) que satisfaga al mismo tiempo ambas ecuaciones, es decir, nunca se cortan.
- Sin embargo nosotros tenemos la intuición geométrica de que esas rectas se cortan si las vemos en perspectiva, pero lo hacen en un punto infinitamente lejano, lo que llamaríamos un punto del infinito.
- Esa intuición que se puede formalizar con geometría proyectiva sobre el cuerpo de los números reales, también funciona sobre cuerpos finitos.
- Para ello lo que tenemos que hacer es poner las ecuaciones en forma homogénea y resolver el sistema de ecuaciones, pero ahora en valores $(X : Y : Z)$.

Las Rectas Paralelas se cortan en el Infinito

- Si planteamos las ecuaciones de dos rectas paralelas, por ejemplo $x + y + 1 = 0$ y $x + y + 2 = 0$ podemos ver que no hay ningún punto (x, y) que satisfaga al mismo tiempo ambas ecuaciones, es decir, nunca se cortan.
- Sin embargo nosotros tenemos la intuición geométrica de que esas rectas se cortan si las vemos en perspectiva, pero lo hacen en un punto infinitamente lejano, lo que llamaríamos un punto del infinito.
- Esa intuición que se puede formalizar con geometría proyectiva sobre el cuerpo de los números reales, también funciona sobre cuerpos finitos.
- Para ello lo que tenemos que hacer es poner las ecuaciones en forma homogénea y resolver el sistema de ecuaciones, pero ahora en valores $(X : Y : Z)$.
- Vamos a ver este proceso con estas rectas.

Homogenización I

- Dada una ecuación en coordenadas afines (x, y), llamaremos ecuación homogénea a aquella que resulta de sustituir x por X/Z e y por Y/Z y eliminar denominadores multiplicando la ecuación por la potencia de Z más baja necesaria.

Homogenización I

- Dada una ecuación en coordenadas afines (x, y), llamaremos ecuación homogénea a aquella que resulta de sustituir x por X/Z e y por Y/Z y eliminar denominadores multiplicando la ecuación por la potencia de Z más baja necesaria.
- Así por ejemplo, $x + y + 1 = 0$ se escribiría $X/Z + Y/Z + 1 = 0$ y multiplicando por Z quedaría $X + Y + Z = 0$, que sería su correspondiente ecuación homogénea.

Homogenización I

- Dada una ecuación en coordenadas afines (x, y), llamaremos ecuación homogénea a aquella que resulta de sustituir x por X/Z e y por Y/Z y eliminar denominadores multiplicando la ecuación por la potencia de Z más baja necesaria.
- Así por ejemplo, $x + y + 1 = 0$ se escribiría $X/Z + Y/Z + 1 = 0$ y multiplicando por Z quedaría $X + Y + Z = 0$, que sería su correspondiente ecuación homogénea.
- En el caso de $x + y + 2 = 0$ la ecuación homogénea sería $X + Y + 2Z = 0$.

Homogenización I

- Dada una ecuación en coordenadas afines (x, y), llamaremos ecuación homogénea a aquella que resulta de sustituir x por X/Z e y por Y/Z y eliminar denominadores multiplicando la ecuación por la potencia de Z más baja necesaria.
- Así por ejemplo, $x + y + 1 = 0$ se escribiría $X/Z + Y/Z + 1 = 0$ y multiplicando por Z quedaría $X + Y + Z = 0$, que sería su correspondiente ecuación homogénea.
- En el caso de $x + y + 2 = 0$ la ecuación homogénea sería $X + Y + 2Z = 0$.
- Si resolvemos el sistema de ecuaciones $X + Y + Z = 0, X + Y + 2Z = 0$ obtenemos $Z = 0$ y $X = -Y$, que es el punto proyectivo $(Y : -Y : 0)$.

Homogenización I

- Dada una ecuación en coordenadas afines (x, y), llamaremos ecuación homogénea a aquella que resulta de sustituir x por X/Z e y por Y/Z y eliminar denominadores multiplicando la ecuación por la potencia de Z más baja necesaria.
- Así por ejemplo, $x + y + 1 = 0$ se escribiría $X/Z + Y/Z + 1 = 0$ y multiplicando por Z quedaría $X + Y + Z = 0$, que sería su correspondiente ecuación homogénea.
- En el caso de $x + y + 2 = 0$ la ecuación homogénea sería $X + Y + 2Z = 0$.
- Si resolvemos el sistema de ecuaciones $X + Y + Z = 0, X + Y + 2Z = 0$ obtenemos $Z = 0$ y $X = -Y$, que es el punto proyectivo $(Y : -Y : 0)$.
- Como estamos en coordenadas proyectivas Y no puede ser 0 y este punto normalizado es $(-1 : 1 : 0)$, el punto del infinito que es intersección de estas dos rectas paralelas.

Homogenización II

- Este mismo método se puede utilizar para calcular puntos del infinito de otras ecuaciones que no son rectas, por ejemplo curvas de segundo o tercer grado.

Homogenización II

- Este mismo método se puede utilizar para calcular puntos del infinito de otras ecuaciones que no son rectas, por ejemplo curvas de segundo o tercer grado.
- Consideremos la parábola $y = x^2$, si homogeneizamos tenemos $Y/Z = X^2/Z^2$ o lo que es lo mismo $ZY = X^2$, que es la ecuación homogénea de la parábola.

Homogenización II

- Este mismo método se puede utilizar para calcular puntos del infinito de otras ecuaciones que no son rectas, por ejemplo curvas de segundo o tercer grado.
- Consideremos la parábola $y = x^2$, si homogeneizamos tenemos $Y/Z = X^2/Z^2$ o lo que es lo mismo $ZY = X^2$, que es la ecuación homogénea de la parábola.
- Si queremos calcular sus puntos del infinito, debemos hacer $Z = 0$ de donde obtenemos $X^2 = 0$ y por lo tanto $X = 0$.

Homogenización II

- Este mismo método se puede utilizar para calcular puntos del infinito de otras ecuaciones que no son rectas, por ejemplo curvas de segundo o tercer grado.
- Consideremos la parábola $y = x^2$, si homogeneizamos tenemos $Y/Z = X^2/Z^2$ o lo que es lo mismo $ZY = X^2$, que es la ecuación homogénea de la parábola.
- Si queremos calcular sus puntos del infinito, debemos hacer $Z = 0$ de donde obtenemos $X^2 = 0$ y por lo tanto $X = 0$.
- Las soluciones posibles son $(0 : Y : 0)$, que al ser un punto proyectivo es equivalente a $(0 : 1 : 0)$.

Homogenización II

- Este mismo método se puede utilizar para calcular puntos del infinito de otras ecuaciones que no son rectas, por ejemplo curvas de segundo o tercer grado.
- Consideremos la parábola $y = x^2$, si homogeneizamos tenemos $Y/Z = X^2/Z^2$ o lo que es lo mismo $ZY = X^2$, que es la ecuación homogénea de la parábola.
- Si queremos calcular sus puntos del infinito, debemos hacer $Z = 0$ de donde obtenemos $X^2 = 0$ y por lo tanto $X = 0$.
- Las soluciones posibles son $(0 : Y : 0)$, que al ser un punto proyectivo es equivalente a $(0 : 1 : 0)$.
- Dicho de otro modo, la parábola es una curva que tiene un punto en el infinito.

Transformaciones Proyectivas

- Igual que podemos deformar un plano afín, girarlo, hacer simetrías, etc., también podemos transformar el plano proyectivo.

Transformaciones Proyectivas

- Igual que podemos deformar un plano afín, girarlo, hacer simetrías, etc., también podemos transformar el plano proyectivo.
- Estas transformaciones pueden llevar puntos del infininito al plano finito y viceversa. De esta forma podemos transformar por ejemplo una circunferencia en una parábola llevando uno de sus puntos al infinito.

Transformaciones Proyectivas

- Igual que podemos deformar un plano afín, girarlo, hacer simetrías, etc., también podemos transformar el plano proyectivo.
- Estas transformaciones pueden llevar puntos del infininito al plano finito y viceversa. De esta forma podemos transformar por ejemplo una circunferencia en una parábola llevando uno de sus puntos al infinito.
- Aunque es un tema interesante, no profundizaremos en este tipo de cálculos porque alargarían excesivamente este curso.