Review from last time:

- Functions
- Intuitive idea of a group
  - shuffles of a deck of 52 cards
- Groups of symmetries – geometry –

The symmetric group S_n is the group of permutations of $\{1, 2, 3, \dots, n\}$

bijection from set to itself

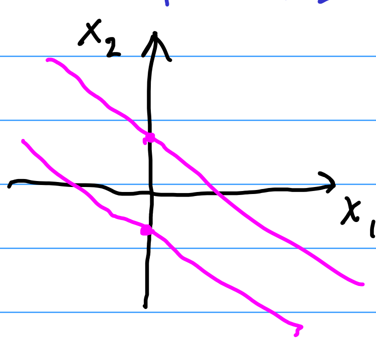
Lecture 3:

$$\boxed{\text{Groups coming from algebraic equations}}$$

An algebraic equation is something like

$$\underbrace{p(x_1, x_2, \dots, x_n)}_{\text{polynomial}} = 0$$

Ex: $x_1^2 + 2x_1x_2 + x_2^2 - 1 = 0$

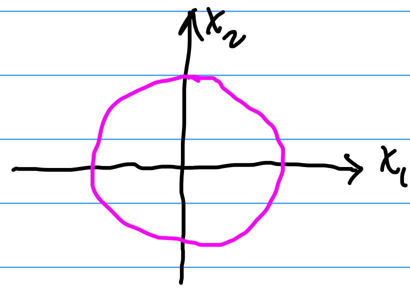


$(x_1 + x_2)^2 = 1$

$x_1 + x_2 = \pm 1$

$x_2 = -x_1 \pm 1$

Ex: $x_1^2 + x_2^2 - 1 = 0$



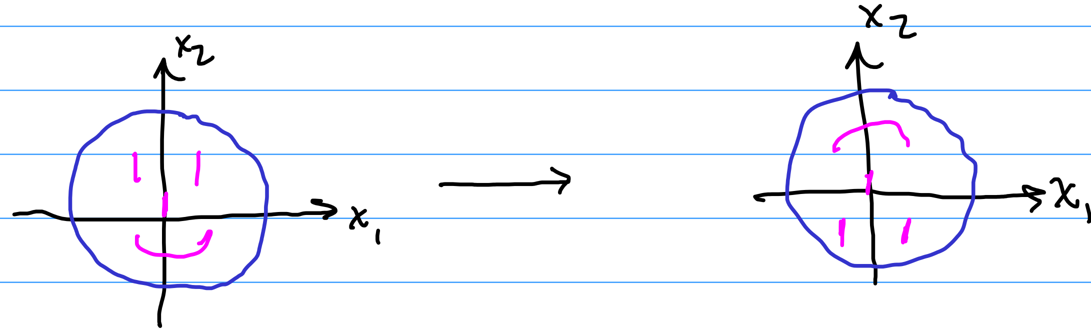
Let $Z(p)$ denote the set of solutions of $p(x_1,\dots,x_n)=0$.

Def: An automorphism of $Z(p)$ is a sequence of rational functions $\rho_1(x_1,\dots,x_n),\dots,\rho_n(x_1,\dots,x_n)$ such that

$$\rho(x_1,\dots,x_n) = (\rho_1(x_1,\dots,x_n),\dots,\rho(x_1,\dots,x_n))$$

restricts to a bijection of $Z(p)$.

Ex:



Roots of unity:

Def: An n'th root of unity is a solution of the algebraic equation $z^n = 1$

In other words, it's an element of $Z(p)$ for $p(z)=z^n-1$

Q: What are the automorphisms of $Z(p)$?

Looking for rational functions $\rho(z)$ with

$$\rho(Z(p)) = Z(p)$$

Example of one $\rho(z) = z^2$

Make sure $\rho(Z(p)) = Z(p)$

Take z with $z^n = 1$.

$p(z) = z^2$. $(z^2)^n = z^{2n} = (z^n)^2 = 1^2 = 1$

I get that $p(Z(p)) \subseteq Z(p)$.

As long as n and 2 are relatively prime

$$p(Z(p)) = Z(p)$$

In general: define $\rho_k : z \mapsto z^k$ $\quad (\rho_k(z) = z^k)$

$$\boxed{\mathrm{Aut}(Z(p)) = \{\rho_k \mid k \text{ and } n \text{ are relatively prime}\}}$$

Multiplication $\rho_j \cdot \rho_k = \rho_j \circ \rho_k = \rho_{jk}$

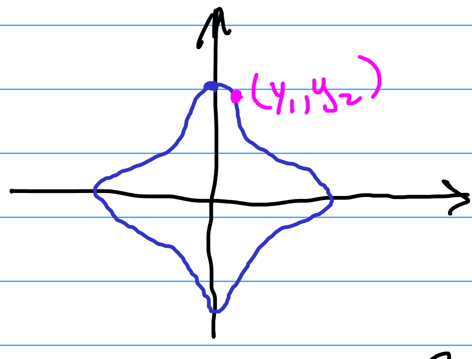
$$(\rho_j \circ \rho_k)(z) = \rho_j(\rho_k(z)) = \rho_j(z^k) = (z^k)^j = \rho_{jk}$$

Edwards curve:

$$\cancel{x_1^2 + x_2^2 = 1 - a x_1^2 x_2^2}$$

$a \geq 0$ constant

$$x_1^2 + x_2^2 + a x_1^2 x_2^2 - 1 = 0$$



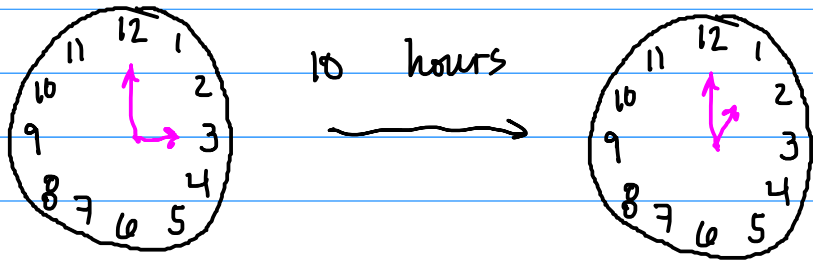
What are the automorphisms?

Given (y_1, y_2) define $\rho_{(y_1,y_2)}(x_1, x_2) = \left(\frac{x_1 y_2 + x_2 y_1}{1 - a x_1 x_2 y_1 y_2}, \frac{x_2 y_2 - x_1 y_1}{1 + a x_1 x_2 y_1 y_2}\right)$

Defines a bijection of $Z(p)$!

Define $(x_1, x_2) + (y_1, y_2) = \rho_{(y_1, y_2)}(x_1, x_2)$

<u>Number Theory</u>: modular arithmetic



"$3 + 10 = 1$"

addition modulo 12

$\mathbb{Z}_{12} = \{0, 1, \dots, 11\}$

$a +_{12} b$ = remainder of $\frac{a+b}{12}$

$3 +_{12} 10$ = remainder of $\frac{3+10}{12}$ = 1

<u>Ex</u>: $2 +_5 3 = 0$

$8 +_2 5 = 1$

$4 +_7 9 = 4 +_7 2 = 6$

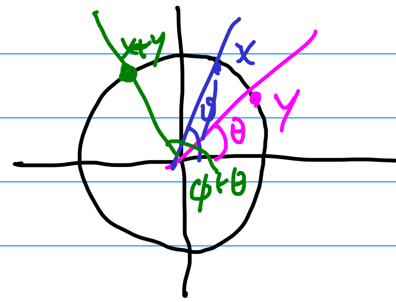
This defines a group structure on $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

$(j, k) \longmapsto j \oplus_n k$

More generally $\mathbb{R}_r = [0, r)$ $\quad x +_r y = \begin{cases} x+y, & x+y < r \\ x+y-r, & x+y \geq r \end{cases}$

Ex: $\sqrt{2} +_3 2 = \sqrt{2}+2-3 = \sqrt{2}-1$

$$7\pi/4 +_{2\pi} \pi/2 = \frac{9\pi}{4} - 2\pi = \frac{\pi}{4}$$

$[0, 2\pi) \approx$ 

Binary Operations

Def: A binary operation on a set G is a function $m: G\times G \to G$ $\quad m(a,b) = a*b$

Example: $G=\mathbb{R}$ define $a*b = a+b$
perfectly good binary operation!

Alternatively, define $a*b = ab$
also perfectly good (different) binary operation!

Crazy example $a*b = a^2+\cos(b)$

Example: $G = \{A \mid A \text{ is a } 5\times 5 \text{ real matrix}\}$.

$A*B = AB$ is a binary operation

Example: $G=\mathbb{R}$, $a*b = a/b$ something's wrong!
$1*0$ not defined

Example: $G=\mathbb{N}$, $a*b = a-b$
$0*1 = -1$ NOT in G! Not well defined

Definition: A binary operation is associative if $a*(b*c) = (a*b)*c$ for all $a, b, c \in G$.
It's called commutative if $a*b = b*a$ for all $a, b \in G$.

Ex: $G = \mathbb{R}$ $\quad a*b = a-b$
is well defined!

not associative
$$\begin{cases} (1*0)*1 = (1-0)*1 = 1*1 = 1-1 = 0 \\ 1*(0*1) = 1*(0-1) = 1*-1 = 1-(-1) = 2 \end{cases}$$

$5*3 = 5-3 = 2$ but $3*5 = 3-5 = -2$
not commutative