Remark

$x \in \mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \cdots \subseteq \mathbb{F}_{p^{n!}} \subseteq \cdots$

$\overline{\mathbb{F}}_p = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$ field inclusion

$q = p^k$

$y \in \mathbb{F}_q \subseteq \mathbb{F}_{q^{2!}} \subseteq \cdots \subseteq \mathbb{F}_{q^{n!}} \subseteq$

$$\overline{\mathbb{F}}_q = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{q^{n!}}$$

note: $\overline{\mathbb{F}}_p = \overline{\mathbb{F}}_q$

could also define

$\overline{\mathbb{F}}_p = \mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^4}$

$\subseteq \cdots \subseteq \mathbb{F}_{p^{2^n}} \subseteq$

$$\iff \quad s \mid t$$

Recall $\quad 0 := \emptyset$

$1 = \{\emptyset\}$

$2 := \{\emptyset, \{\emptyset\}\}$

$\vdots$

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$$

Def: A relation on a set X is a subset $R \subseteq X \times X$.

When $(x, y) \in R$ we denote $x R y$ or $x \sim_R y$.

Ex: a function $f: X \to X$

gives rise to a relation:

$$x \sim_R y \iff f(x) = y.$$

Def: A relation R on X is called an equivalence relation if

1) Reflexive: $\forall x \in X,\ x \sim_R x$.

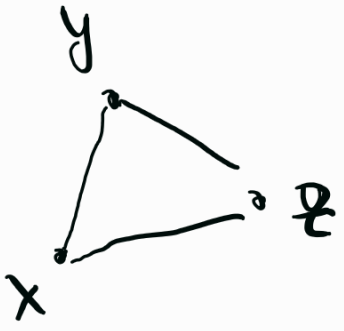
2) Symmetric: $\forall x, y \in X,\ x \sim_R y$

$$\iff y \sim_R x.$$

3) Transitive: $\forall x, y, z \in X$

$$x \sim_R y \wedge y \sim_R z$$

$$\Rightarrow x \sim_R z$$



Ex: if $f: X \to X$, $f \neq id_X$

ie $\exists\ x_0 \in X$ s.th $f(x_0) \neq x_0$

Then the relation $x \sim_R y$

$\iff$ $f(x) = y$ is not reflexive.

Ex $X = \mathbb{Z}$, $n \in \mathbb{N}$

$R = \equiv \pmod n$

ie for $x, y \in \mathbb{Z}$

$x \sim_R y \iff x \equiv y \pmod n$.

1) $\forall\ x \in \mathbb{Z}$ $x \equiv x \pmod n$

2) $\forall_{x,y} \in \mathbb{Z}$ $x \equiv y \pmod n$

$\iff$ $y \equiv x \pmod n$

3) $\forall_{x,y,z}$ if $x \equiv y \pmod n$

and $y \equiv z \pmod n$

then $x \equiv z \pmod n$.

Construction Let $\sim$ be an equivalence relation on a set X. For $x \in X$, denote

$$[x] = \{ y \in X \mid x \sim y \} \subseteq X$$

and call it equivalence class of X

eg $X = \mathbb{Z}$, $\sim$ is (mod n)

$$[n+1] = [1] = \{ 1, n+1, 2n+1, \cdots \quad (\text{mod } n)$$

$$1-n, 1-2n, \cdots \}$$

Note: 1) if $a, b \in [x]$ then

$$a \sim x \wedge b \sim x$$

$\overset{\text{sym}}{\Rightarrow}\ x \sim b \overset{\text{Trans.}}{\Rightarrow} a \sim b$

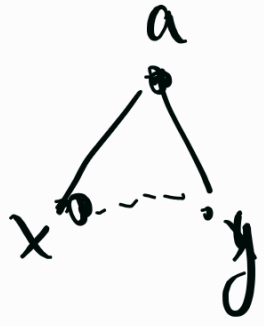
2) If $x, y \in X$ are s.th

$[x] \neq [y]$. If $a \in [x] \cap [y]$

Then $a \sim x \wedge a \sim y$

$\Rightarrow x \sim a \wedge a \sim y$

$\overset{\text{Tr.}}{\Rightarrow} x \sim y$



$\Rightarrow [x] = [y]$

(bcs if $t \in [x]$ $t \sim x$

then since $x \sim y$ it

follows that $t \sim y$ i.e.

$t \in [y]$)

So $[x] = [y] \iff x \sim y$

and if $[x] \neq [y]$

as subsets of X then

$$[x] \cap [y] = \emptyset.$$

Thus, the collection (of sets)

$$\underline{\underline{Q}} = \{ [x] \subseteq X \mid x \in X \}$$

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

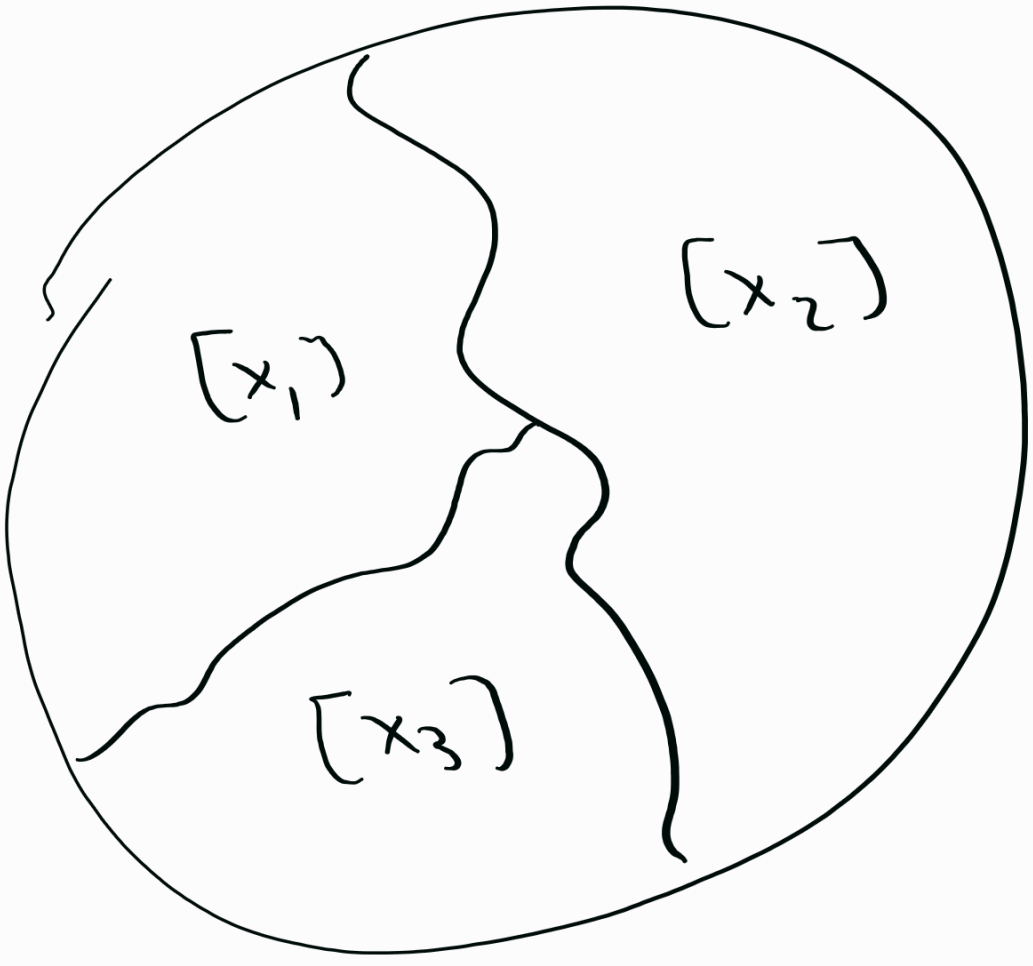
is a <u>partition</u> of X

in that $\bigcup_{x \in X} [x] = X$

and $\forall x, y \in X$, either

$$[x] = [y] \quad \text{or}$$

$$[x] \cap [y] = \emptyset$$



Ex: $X = \mathbb{Z}$, w/ $(\bmod n)$

$$\mathbb{Z} = \{ [x] \mid x \in \mathbb{Z} \}$$

$= \{\ldots, [-1], [0], [1], [2], \ldots\}$

---

remove repetitions.

$= \{[0], [1], \ldots, [n-1]\}$

$\mathbb{Z}_n$

$= \{[n], [n+1], \ldots, [2n-1]\}$

$= \ldots$

Notation: Given a set X w/ an equivalence rel. $\sim$

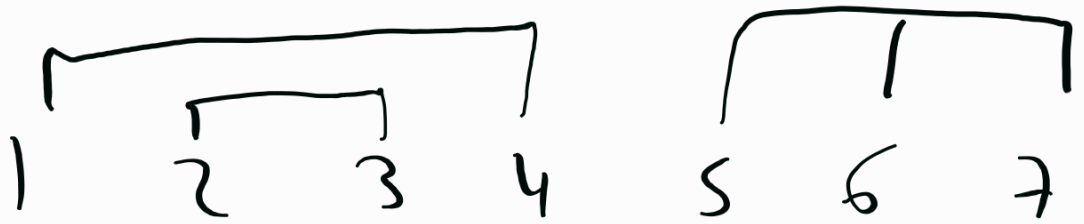
We denote

$$X/_\sim := Q = \{[x] \mid x \in X\}$$

and call it the quotient set

Set:

Ex: $X = \{1, \dots, 7\}$



$$X/\sim = \{[1], [2], [5]\}$$

$$= \{[4], [3], [6]\}.$$

Note if $\mathcal{P}$ is a partition of a set X, ie

$$\mathcal{P} = \{U_i\}_{i \in I}$$

and $\forall i, j \in I$ if $i \neq j$

then $U_i \cap U_j = \emptyset$

+ $\bigcup_{i \in I} U_i = X$

We can define an equivalence rel. on X by

for $x, y \in X$, $x \sim y$

$\iff \exists\, i \in I$ s.th

$x, y \in U_i$

$\Rightarrow$ 1-1 correspondence

$$\left\{ \text{equivalence rel's on } X \right\}$$

bijection $\longleftrightarrow$ $\left\{ \text{Partitions of } X \right\}$

Recall: If $(G, \cdot)$ is an abelian gp and $H \leq G$.

for $x \in G$, the H coset of x is

$(x+H)$ $\quad x \cdot H = \{ x \cdot h \mid h \in H \}$.

We defined $G/H = \{ xH \}_{x \in G}$

Lemma $xH = yH \iff x \cdot y^{-1} \in H$

G/H has an abelian gp structure, given by

unit $= e \cdot H = H$

mult $(xH) \cdot (yH) = (xy)H$

$= \{ (xy)h \mid h \in H \}$

$= \{ x(yh) \mid h \in H \}$ ...

inverse of xH is $x^{-1}H$

Claim: The collection $\{ xH \mid x \in G \}$ is a partition of G.

$\cup xH \subseteq G \Leftarrow xH \subseteq G$

$\bigcup_{x \in G} xH \overset{?}{=} G$

Proof: 1) Want: $\bigcup_{x \in G} xH = G$

indeed, if $x \in G$

then $x = x \cdot e \in xH$ $(e \in H)$ //

2) if $x, y \in G$ and

$xH \neq yH$. Want: $xH \cap yH = \emptyset$

Suppose (towards contradiction)

that $a \in xH \cap yH$.

Then $\exists h, h' \in H$ s.th

$$x \cdot h = a = y \cdot h'.$$

Thus $x = y(h'h^{-1}) \in yH$

$$y = x(h(h')^{-1}) \in xH$$

Finally: if $a = xh_1 \in xH$

Then $a = y(h'h^{-1}) \cdot h_1 \in yH$

and similarly if $\beta = yh_2 \in yH$

then $\beta = x(h(h')^{-1}) \cdot h_2 \in xH$

so $xH \subseteq yH$ $\Rightarrow$

$\wedge$ $yH \subseteq xH$

$xH = yH$. $\square$ //

$h \in \mathbb{N}$

Ex: $G = \mathbb{Z}$, $H = n\mathbb{Z}$

$G/H = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$

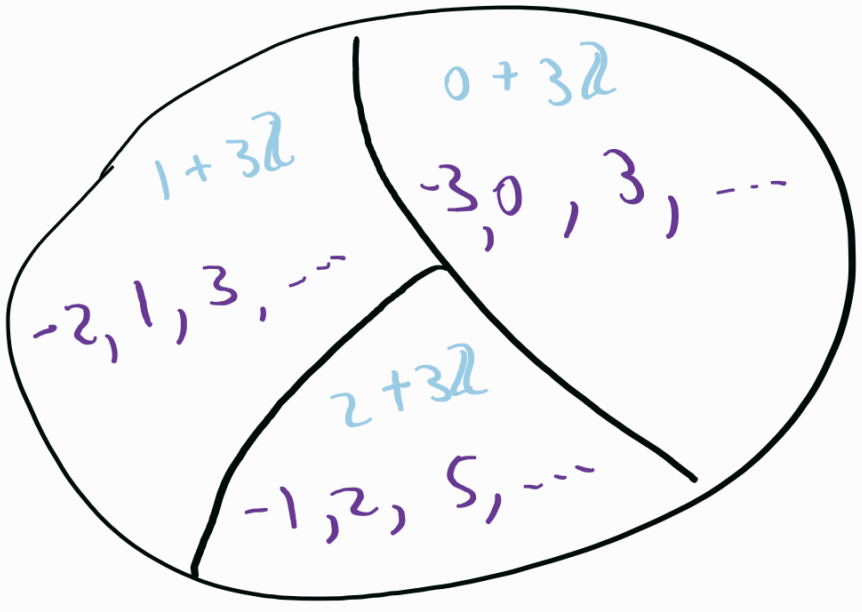
By the above

G/H is a partition

G/H

of $\mathbb{Z}$ hence gives rise to an <u>equivalence relation</u>:

eg $X = \mathbb{Z}$ $n = 3$



$a, b \in \mathbb{Z}$ $a \sim b$

$(=)$ $a \equiv b \pmod 3$

<u>Example</u>: $\mathbb{F}$ a field

$\phi(x) \in \mathbb{F}[x]$ $\deg \phi = n$

$$\mathbb{F}[x]/(\phi) \overset{\text{as set}}{=}$$

$$\left\{ r(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \;\middle|\; a_i \in \mathbb{F} \right\}$$

if ϕ is prime then

mod-ϕ arithmetic defines

a field structure on

$K = \mathbb{F}[x]/(\phi)$ ← $\phi(X) = (X-\alpha)\psi(X)$

We could set: for

$f(x), g(x) \in \mathbb{F}[x]$

$f \sim g \iff f \equiv g \pmod{\phi}$

ϕ g

Exercise: $\sim_\phi$ is an equivalence relation

$$\boxed{\mathbb{F}[x]}/\sim_\phi = \{ [f] \mid f \in \mathbb{F}[x] \}$$

$$= \{ [r] \mid \deg r < n = \deg \phi \}$$

$$[f] = [g] \iff$$

$$f \sim_\phi g$$

$$\iff f \equiv g \pmod{\phi}$$

$$f = q_1 \phi + r_1 \qquad \deg r_1 < n$$

$$g = q_2 \phi + r_2 \qquad \deg r_2 < n$$

$$f \equiv g \mod \phi$$

$$(=) \quad r_1 = r_2$$

if $r_1 \neq r_2$

then $[r_1] \neq [r_2]$

ie

$$F[x] / \sim_\phi \qquad \deg \phi = n$$

$$= \{ [r] \mid \deg r < n \}$$

no q

repetitions.

$$\mathbb{Z}_n = \{0, \dots, n-1\}$$

$$+ \quad \text{mod } n$$

$$\mathbb{Z}/_{\sim_{\text{mod } n}} = \{[0], \dots, [n-1]\}$$

$$+$$

$$[a] + [b]$$

$$= [a+b]$$

$$= [a+b \bmod n]$$

$$\mathbb{F}[x]/_{(\emptyset)}$$

$= \{ r \mid \text{remainder poly's} \}$

↑ mod ϕ

$F[x] / \sim_\phi$ ⇐

$= \{ [r] \mid \text{remainder poly's} \}$

↑ mod ϕ

$[r_1] + [r_2] := [r_1 + r_2]$

$[r_1] \cdot [r_2] = [r_1 \cdot r_2]$

↑