$f: A \to B$

$g: B \to C$

$A \xrightarrow{f} B \xrightarrow{g} C$

$g(f(x))$ or $(x)fg$

Permutations

$f: S \to S$

f is bijection

we call f a permutation

permutation

$S = \{1,2,3\}$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$[3,1,2]$

$f: S \to S$

$g: S \to S$

f, g are ~~bij~~

$g \circ f$ $f \circ g$ are also bij.

$G_S = \{f : S \to S \mid f \text{ is a bij}\}$

$G_S \neq \emptyset$ $\because id_S \in G_S$.

if $f, g \in G_S$, then $f \circ g$ & $g \circ f \in G_S$.

G_S is closed under functional composition.

$id_S \circ f = f$ $f \circ id_S = f$

if $f \in G_S$, then $\exists\, g = f^{-1}$ s.t. $g \circ f = id$, $f \circ g = id$

a, b, c

$\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$

$S = \text{range}(10)$

$\begin{pmatrix} 0 & \cdots & 9 \\ @ & \cdots & 9 \text{ many} \end{pmatrix}$

$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 0 & 2 \end{pmatrix}$

$0\ 1\ 2\ 3\ 4$

$[1,3,4,0,2]$

$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

$f \circ f^{-1}$ $f^{-1} \circ f$

$f \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ $f^{-1} \circ f$ $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

Thm (

$f, g, h \in G_S$, then $f \circ (g \circ h) = (f \circ g) \circ h$

Def A group G is a set together with an operation $*: G \times G \to G$ s.t.

1) $\exists\, e \in G$ s.t. $\forall g \in G$ $g * e = e * g = g$ (we call e the identity) often people write 1
2) $\forall g, h, k \in G$ $(g * h) * k = g * (h * k)$ (Associative)
3) $\forall g \in G$ $\exists\, g^{-1} \in G$ s.t. (such that) $g * g^{-1} = e = g^{-1} * g$

What's missing?

Groups do not have to have $f * g = g * f$

If G is commutative we call G abelian or commutative Abel abelian

(X)

$\mathbb{R}$ with $*$ is this a group? No, 0^{-1} does not exist

$\mathbb{R} - \{0\}$ with $*$. Group? Yes

Abelian? Yes

$\mathbb{N}, *$? Group? No No No, 1000 * No

$\mathbb{N}, +$ No

$\mathbb{Z}, +$ Yes $e = 0$, $-n + n = 0$, $n + (-n) = 0$ Assoc

Abelian? Yes

$\mathbb{Q}, *$, No $\because 0 \in \mathbb{Q}$

$\mathbb{Q} - \{0\}, *$, Yes

$\mathbb{Z}, *$, Not a group $\because 0$

$\mathbb{Z} - \{0\}, *$, No inverse

$\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$

$\mathbb{Z}_7$ has $+, *$

is $\mathbb{Z}_7, +$ a group?

$\mathbb{Z}_7, *$ a group? No

$\mathbb{Z}_7 - \{0\}, *$ a group? $1 = e$, Assoc.

$1^{-1} = 1$

$2^{-1} = 4 \quad 4^{-1} = 2$

$3^{-1} = 5 \quad 5^{-1} = 3$

$6^{-1} = 6$

Abelian? Yes

$\mathbb{Z}_8 - \{0\}, * \quad 2 * 4 = 0$

$\mathbb{Z}_p - \{0\}$, p prime } Conjecture
is a group

$\mathbb{Z}_n - \{0\}^*$, n composite
is not a group
$n = a * b$
$a * b = 0$ mod n

$\mathbb{Z}_8 - \{0\}, \quad \{1,3,5,7\} \quad 1^{-1} = 1 \quad 3^{-1} = 5$
$5^{-1} = 3 \quad 7^{-1} = 7$

GCD(a,b)
if a%b == 0:
return b
return GCD(b, a%b)

$a = q * b + r \qquad r = a - q * b$

127

$\mathbb{Z}_p - \{0\}$, p a prime

$g = GCD(a,b)$

$\exists\, s,t$ s.t. $g = s*a + t*b$.

Extended GCD

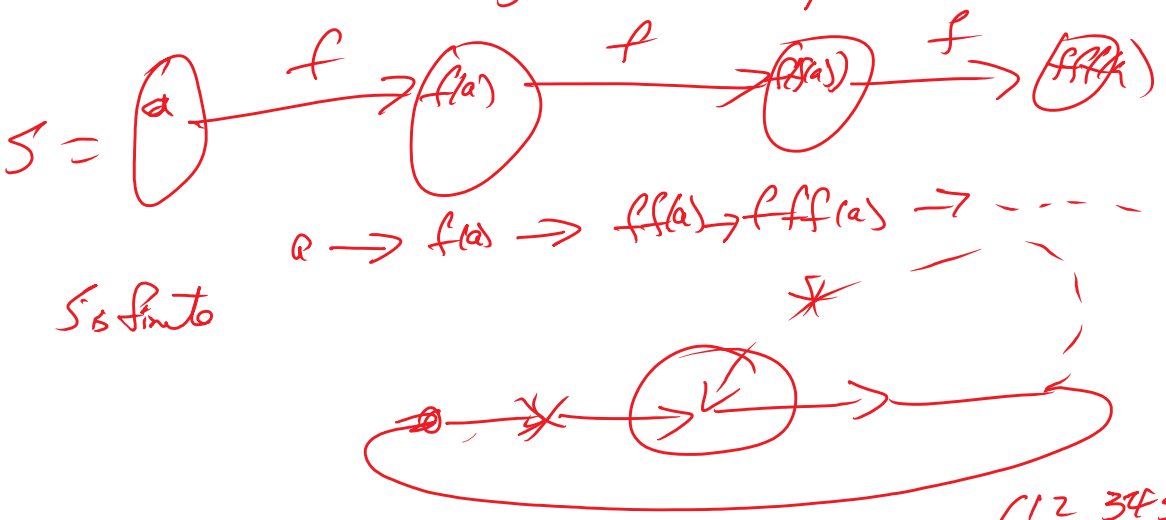
$GCD(63, 45) = GCD(45, 18) = GCD(18, 9) = 9$

$s*63 + t*45 = 9$ (You do this)

a rel prime to p

$s*a + t*p = 1$

$s*a = 1 \mod p$



$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \to (13)(254) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$

$(254)(13)$

$(23)(254)$ $\quad 1 \to 2$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$ $\quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$

convert to cycle notation

X R is an equiv relation on

X R is reflexive $\forall x \in X \; xRx$

symmetric $\forall xy \in X, \; xRy \Rightarrow yRy$

transitive $\forall xyz, \; xRy \; \& \; yRz \Rightarrow xRz$

If R is an ~~ER~~ equiv Rel on X, then

R partitions X

A partition of a set X is a set of subsets of X, $X_1, \ldots, X_k$ s.t. (disjoint)

1) $X_i \cap X_j = \emptyset \quad \forall i \neq j$

2) $\bigcup_{i=1}^{k} X_i = X$

R $\Longrightarrow$ mod k Partion. $\{[x] \mid x \in X\}$

$x \in X, \quad [x] = \{y \mid xRy\}$ (equiv class of x)

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

$[x] \neq \emptyset$ ∵ xRx

$[x] \cap [y] \neq \emptyset \Rightarrow \exists z \in [x] \cap [y]$

$\rightarrow xRz \; \& \; yRz \Rightarrow xRz$

$\Rightarrow xRz \;\&\; yRz \Rightarrow xRz$

	Reason
$xRz \;\&\; zRy$	$z \in [x] \cap [y]$
xRy	R is sym
yRx	R is trans
$[x] = [y]$	R is symmetric

R trans xRy, yRx

Have partition, then get equiv relation?

$P = \{X_1, X_2, \ldots, X_k\}$, $X_i \cap X_j = \emptyset \; \forall i \neq j$, $\bigcup X_i = A$

xRy iff $\exists i$ s.t. $x, y \in X_i$

xRx : $\bigcup X_i = A$, $x \in X_i$ for some i

$xRy \Rightarrow yRx$? X_i unique

$xRy \;\&\; yRz \Rightarrow xRz$

---

mod 7

xRy iff $x \bmod 7 = y \bmod 7$

$x \bmod 7 = x \bmod 7$

$x \bmod 7 = y \bmod 7 \Rightarrow y \bmod 7 = x \bmod 7$

$x \bmod 7 = y \bmod 7 \;\&\; y \bmod 7 = z \bmod 7 \Rightarrow x \bmod 7 = z \bmod 7$

Equivalence Relations $\longleftrightarrow$ Partitions

$n \times m$ matrix

$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \times \begin{bmatrix} 3 & 1 & 2 \\ 4 & 6 & 5 \end{bmatrix} = \begin{bmatrix} 3 & 2 & 6 \\ 16 & 30 & 30 \end{bmatrix}$ Matrix $+$ $\times$

G is a group.

$|G|$ = order of G.

$|\mathbb{Z}| = \aleph_0$

$|\mathbb{Q}| = \aleph_0$

$|\mathbb{R}| = \aleph_1$

$g \in G$ order of g is the smallest n s.t. $g^n = e$ (if n exists) else $\text{ord}(g) = \infty$

$(\mathbb{Z}, +)$ order $(1) = ?$ ∞

$(\mathbb{Z}_q, +)$ order $(1) = q$ $\text{ord}(g) < \infty$

If $|G|$ is finite, & $g \in G$, $\text{order}(g) \mid |G|$

$a \mid b \Rightarrow b \% a = 0$

$g, g \times g = g^2, g^3 \ldots \ldots$ can't all be different.

so $\exists\, i, j$ $i \neq j$ s.t. $g^i = g^j$

assume $i < j$ $g^i g^{-i} = e$

$g^{-1} g = e$ $\underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{i} \underbrace{g g g \cdots}_{i} = e$

$g^{-i} g^j = g^{-i} g^i g^j$

$g^{-i} g^j = g^{-i} g^j$

$e = g^{j-i}$ $\quad j - i \neq 0$

order(g) = order(g^{-1})

G is <u>cyclic</u> iff $\exists\, g \in G$ s.t. order(g) = |G|

$G = e, g, g^2, \ldots, g^{|G|-1}$

<u>Thm</u> if G is cyclic then G is abelian

$g^i \cdot g^j = g^{(i+j)\%|G|}$ $\quad g^j \cdot g^i = g^{j+i} = g^{i+j}$

If G is cyclic & order(g) = |G|, g is called a generator of G.

Are generators unique?

$\mathbb{Z}$ of 4 $\quad$ 1, 2, 3, 0 $\quad$ order 4

2, 0, 2, 0, ... $\quad$ order 2

3, 2, 1, 0 $\quad$ order 4

0 $\quad$ order 1

$\mathbb{Z}_{16}$ $\quad$ 1 order 16

$(\mathbb{Z}_{16}^{\times} - \{0\}, *)$ $\qquad$ $(\mathbb{Z}_{16}^{*}, *)$

$\mathbb{Z}_{16}^{*} = \{ n \in \text{range}(16) \mid GCD(n, 16) = 1 \}$.

$= \{1, 3, 5, 7, 9, 11, 13, 15\}$

$1^{-1} = 1$ $\quad 7^{-1} = 7$

$3^{-1} = 11$ $\quad 9^{-1} = 9$

$5^{-1} = 13$

$(\mathbb{Z}/\mathbb{Z}_{16})^*$

order of $\mathbb{Z}_k^*$ is $\phi(k)$

Euler ϕ function.

if p is prime $\phi(p) = p-1$

How to compute $\phi(k)$?

Subgroup Let $(G, *)$ be a group.

$H \subseteq G$ is a subgroup iff $\forall\, h, k \in H$, $h * k \in H$, $1 \in H$

Does every Group have a subgroup?

$\{1\}$ is always a subgroup.

G is a subgroup.

Are there always other subgroups?

A subgroup $H < G$ s.t. $1 < |H| < |G|$ $\quad$ N/D

is called a proper subgroup

A group without proper subgroups is called a simple group

Question. Do the relatively prime elements of $(Z_k, *)$ form a group?

What does rel prime mean

$\{r \mid GCD(k,r) = 1\}$

Group Prop
- $*$ is assoc ✓
- identity ✓ 1 is rel prime to K
- inverse
- closed ✓ r, s are rel prime to K

r is relatively to K

What is r^{-1}?

r*s is rel prime to K

why?

Subgroups $G \supseteq H$ $h_1 * h_2 \in H$

$1 \in H$

$h \in H \Rightarrow h^{-1} \in H$

$(Z, +)$

What are the subgroups of $(Z, +)$?

Even are a subgroup:

odd are not. Closed under +, 0 ∉ odd

$(nZ, +)$ is a subgroup. Even $2\mathbb{Z}$

$Z = 1Z$

$3Z = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

Question are nZ the only subgroups of Z?

Extended GCD $(a, b \in \mathbb{N})$

~~not GCD(a,b)~~

GCD(0,0) not defined

GCD(0,5) = 5

Extended GCD ($a, b \in \mathbb{N}$)

GCD(0,0) not defined

GCD(0,5) = 5

```
def GCD(a,b):
    if (a%b)==0:
        return b
    :
    return GCD(b, a%b)
```

Goal $g = GCD(a,b)$ $\exists\ s,t \in \mathbb{Z}$, s.t. $g = sa + tb$

```
def EGCD(a,b):
    if (a%b)==0:
        return (b,0,1)
    else
        temp = EGCD(b, a%b)
        return (temp[0], temp[2],
        temp[1] - (a//b) * temp[2])
```

returns (g,s,t)

$g = sa + tb$.

```
# b = s*a + t*b
# r = a%b
temp = (g, k, q)
= EGCD(b, r)
```

① $kb + qr = g$

② $sa + tb = g$

③ $r = a - wb$

$a = wb + r$

① + ③ $\Rightarrow$

$kb + q(a - wb) = g$

$qa + (k - wq)b = g$

$w = a//b$

What is a^{-1} in $(\mathbb{Z}_k^*, *)$ $\quad \mathbb{Z}_k^* = \{y \in \mathbb{Z}_k \mid GCD(k,y) = 1\}$

$GCD(k,y) = 1$ $\exists$ s,t s.t. $sk + ty = 1$

Take $\bmod k$ $\quad 0 + (ty) \bmod k = 1$

Solution to Quest 1

Solution to Quest 1

Question 2?

$G \subseteq \mathbb{Z}_n$ G is a subgroup $\neq \{0\}$

Pick $k = \min\{y \in G \mid y > 0\}$ $\mathbb{N}$ is well-ordered.

A well-ordered set is a set with a partial order s.t. every non-empty subset has a smallest element.

$\mathbb{N}$ is well-ordered & every non-empty subset of a well-ordered set is well-ordered

G has a smallest positive value call it v

Let $w \in G$, $w > 0$. $w \geq v$ Why?

$w = qv + r$. If $r = 0$, w is a multiple of v

if $r \neq 0$, $v > r > 0$, $r \in G$ $r = w - qv$

impossible so $r = 0$

$G = v\mathbb{Z}$

Let G be a group and H a subgroup.

Let $g \in G$, what does gH look like?

$gH = \{gh_1, gh_2, \ldots, gh_k\}$ where $H = \{h_1, \ldots, h_k\}$

are these all different?

$gh_i = gh_k$

$g^{-1}gh_i = g^{-1}gh_k$

$h_i = h_k$

is $gH = H$ iff $g \in H$

$gH = H$ iff $g \in H$

What about $gH = kH$

$g \in gH$ $ge = g$ $k \in kH$

$g = kh$ for ~~some~~ $h \in H$

$k^{-1}g \in H$

$z \in gH$ & $z \in kH$ claim $gH = kH$

$z = gh_1$ $z = kh_2 = gh_1$

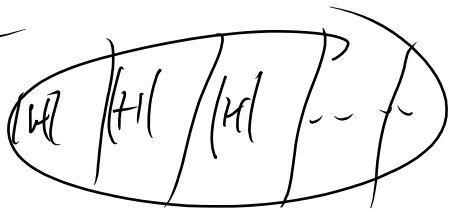
$g = kh_2h_1^{-1}$

$gh_3 = k(h_2h_1^{-1}h_3)$ $k = gh_1h_2^{-1}$

$kh_4 = gh_1h_2^{-1}h_4$ $gH = kH$

gH is a called a coset. $|gH| = |H|$

Cosets form a partition



$G = \bigcup_{g \in G} gH$ $g \in gH$

$\frac{|G|}{|H|}$ = an integer

$|G|$ is a prime the only subgroups of G are $\{e\}$ and G.

---

order(H) | order(G) if $H \leq G$

$g \in G$, order(g) | order(G) $\{1, g, g^2, \ldots, g^{k-1}, g^k = 1\}$

order$(\{1, g, \ldots, g^{k-1}\}) = k$ = order(g)

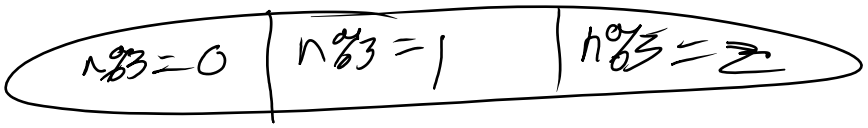
order(g) | order(G)

$H < G$

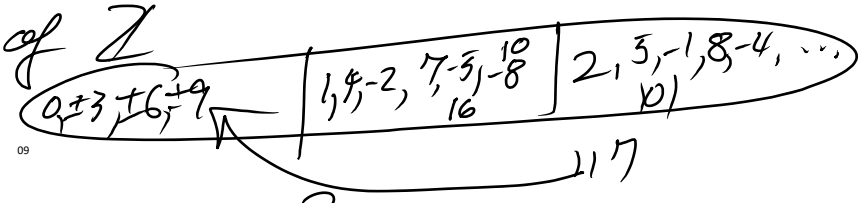
G

$\mathbb{Z}_3$

$\mathbb{Z}$



$3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$



09

$\{0,1,2\}$

G

$g_1H \cdot g_2H = g_1g_2H$?

$gH \cdot kH = gkH$

$gh_1 \cdot kh_2 = gkh_3$

G is a group

$H < G$ subgroup

$H * H = H$

$H * H \subseteq H$

Why $H * H = H$?

$1 \in H$

~~$g_1 H * g_2 H = g_1 g_2 H$~~

$g_1 h_1 g_2 h_2 = g_1 g_2 h_3$

g_1^{-1} $\quad h_1 g_2 h_2 = g_2 h_3$ ←

g_2^{-1} $\quad g_2^{-1} h_1 g_2 h_2 = h_3$

$g_2^{-1} h_1 g_2 = h_3 h_2^{-1}$

$h_1 g_2 h_2 = g_2 h_3$

$h_1 g_2 = g_2 h_3 h_2^{-1}$

$h_1 = g_2 (h_3 h_2^{-1}) g_2^{-1}$

$\in H$

$H < G$ is called a normal subgroup iff

$\forall g \in G \quad gHg^{-1} = H$

We write $H \triangleleft G$ instead of $H < G$

A group is simple iff it has no non-trivial normal subgroups. $\{1\}$ & G are normal

$g 1 g^{-1} = 1$

If $H \triangleleft G$, we can create a new group

$G/H = \{gH \mid g \in G\}$ $\quad gH = g_1 g_2 H$

$g_1 H g_2 H = g g_2 H$ ...

$H \triangleleft G \quad g_1 H g_1^{-1} = H \Rightarrow g_1 H = H g_1$

G/H is a group.

If G is abelian and $H < G \Rightarrow H \triangleleft G$

$g H g^{-1} = g g^{-1} H = H$ if G is abelian

$\mathbb{Z}/n\mathbb{Z}$ modular group

$\{gH\}$ are the left cosets of H

$\{Hg\}$ right cosets

in general $gH \neq Hg$

When is $gH = Hg$?

$g H g^{-1} = H$

Left cosets = Right cosets if H is normal.

$H < G \Rightarrow |H| \mid |G|$

$|G| =$ prime

G is cyclic and any $g \neq 1$ generates

$G \quad |G| = pR$

Homomorphisms.

G_1, G_2 are groups

$f: G_1 \longrightarrow G_2$

$f(1_{G_1}) = 1_{G_2}$

$f(a *_1 b) = f(a) *_2 f(b)$

$f(1) = 1$

$f(a*b) = f(a) * f(b)$

$f(g^{-1}) = f(g)^{-1}$

$1 = g g^{-1}$

$1 = f(1) = f(g g^{-1}) = f(g) f(g^{-1})$

$1 = f(g) f(g^{-1})$ so $f(g^{-1}) = f(g)^{-1}$

$g = g \cdot 1$ $\quad f(g) = f(g) * f(1)$

$1 = f(1)$

G_1 & G_2 groups

$f: G_1 \to G_2$ hom

$\ker(f) = \{ g \mid f(g) = 1 \}$

Thm $f: G_1 \to G_2$ is a hom

$\ker(f) < G_1$

Pf: $f(1) = 1$ so $1 \in \ker(f)$

$a, b \in \ker(f)$ $\quad f(a) = 1$ & $f(b) = 1$

$f(ab) = f(a) * f(b) = 1 * 1$

$g, b \in \ker(f) \Rightarrow ab \in \ker(f)$

so $\ker(f)$ is a subgroup of G_1

Thm $\ker(f) \lhd G$

$a \in \ker(f)$ $\quad f(a) = 1$

$f(gag^{-1}) = f(g) f(a) f(g^{-1}) = f(g) f(g^{-1}) = 1$

$a \in \ker(f)$ $\quad gag^{-1} \in \ker(f)$ $\forall g \in G$

$G / \ker(f)$

Rings

Groups have one operation $*$

Rings have two operations $+, *$

$(R, +, *)$ is a ring iff

$(R, +)$ is an abelian group

and $*$ is associative with identity and the distributive laws

R is a ring iff $(R, +)$ is Abelian group

$0 \in R$ (+ identity) $\quad 0 + a = a + 0 = a$

$1 \in R \quad 1 * r = r * 1 = r$

$*$ is associative

$r(s+t) = r*s + r*t$

$(s+t)*r = s*r + t*r$

What's missing?

no / not — inverses for $*$

commutative

$$s*0 = 0$$

$$s*(0+0) = s*0$$

$$= s*0 + s*0$$

$$s*0 + s*0 = s*0$$

$$g + g = g$$

$$g = 0$$

Examples of Rings

$(\mathbb{Z}, +, *)$ $(\mathbb{Q}, +, *)$ $(\mathbb{R}, +, *)$

Polynomials

$\mathbb{Z}[x]$

$\mathbb{Q}[x]$

$\mathbb{R}[x]$

$x^3 + 5x^2 - 7x + 3$

$-x^3 - 5x^2 + 7x - 3$

1.2

$\mathbb{K}[x]$

$\frac{f(x)}{g(x)}$ with $f(x), g(x) \in \mathbb{Q}[x]$, $g(x) \neq 0$

$(\mathbb{C}, +, *)$ $\mathbb{C}[x]$

$\frac{f(x)}{g(x)}$ $f, g \in \mathbb{C}[x]$, $g \neq 0$

$n \times n$ matrices $M = [m_{ij}]$ $N = [n_{ij}]$

$M + N =$

$M + N = [m_{ij} + n_{ij}]$

$M * N = [m_{ij} * n_{ij}]$

$M \times N = [\sum_{k=1}^{n} m_{ik} n_{kj}]$

$CF = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is continuous}\}$

$+$

$*$

Ring Homomorphism

$f : R_1 \to R_2$

$f(a+b) = f(a) + f(b)$

$f(ab) = f(a) f(b)$

$f(x) = ?$

$f(a+b+c) = f(a)+f(b)+f(c)$

$f(0) = f(0+0) = f(0)f(0)$

$f(0) = 0$

$f(1) = ?$

$f(a) = f(a \cdot 1) = f(a)f(1)$

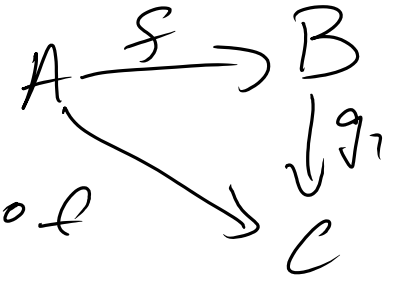
Not every definition of ring includes 1.

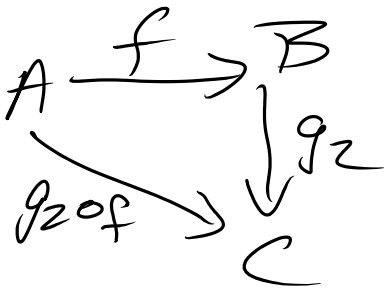
f mono $\Rightarrow$ $(f \circ g_1 = f \circ g_2) \Rightarrow g_1 = g_2$

$f : A \to B$

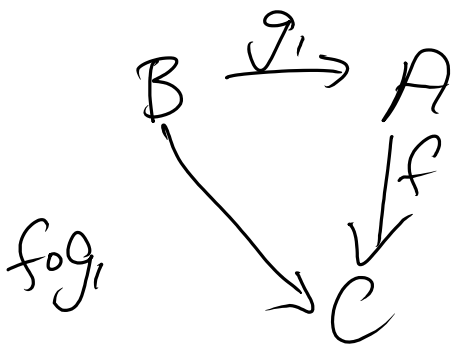
$g_1 : B \to C$

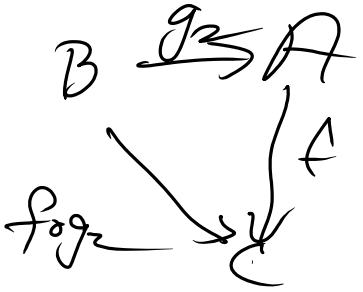
$g_2 : B \to C$





In the Category of ~~Sets~~ f is inj iff f is a monomorphism





f is inj $\iff$ f is mono

f is inj

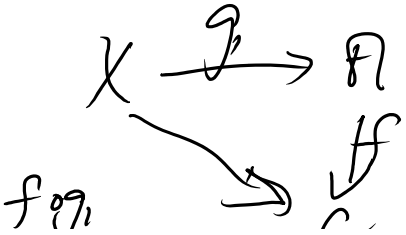
$f(g_1(x)) = f(g_2(x)) \quad \forall x \in B$

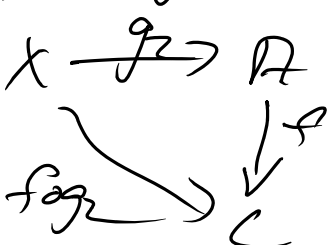
$\Downarrow$

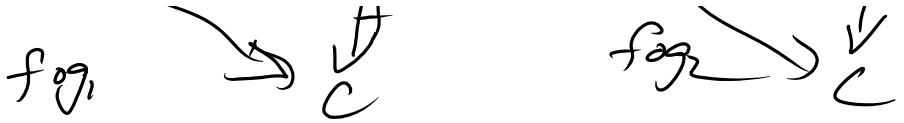
$g_1(x) = g_2(x) \quad \forall x \in B$

$\Rightarrow g_1 = g_2$

f mono







$fog_1 = fog_2 \Rightarrow g_1 = g_2$

f is injective. Suppose f not injective

$\exists y, z \in A$ s.t. $f(z) = f(y)$

Let $X = \{1\}$ $g_1(1) = z$ $g_2(1) = y$

$g_1 \neq g_2$

$f(g_1(1)) = f(z) = f(y)$ $f(g_2(1)) = f(z) = f(y)$

$fog_1 = fog_2$ but $g_1 \neq g_2$ so

f is not a mono. Contradiction

$(1+x+x^2)(x+x^3)$

$= x+x^2+x^3+x^4+x^5$

$\mod(1+x^4)$

$x^4+1 \;\big|\; x^5+x^4+x^2+x$

$x^5 \qquad\qquad +x$

x^4+x^2

$x^4 \qquad\qquad +1$

x^2+x+1

$x^5+x^4+x^2+x = (x+1)(x^4+1)$

x^4+1 irreducible over $\mathbb{Z}_2$ $\mathbb{F}_2$

$x^4+1 = x \cdot x^3+1$

$x+1 \;\big|\; x^4+1$

x^4+x^3

x^3+1

x^3+x^2

x^2+1

x^2+x

$x+1$

x^3+x^2+x+1

$x \qquad x+1$

$x+1$

x^3+x^2+x+1

$x^4+x^3+x^2+x$

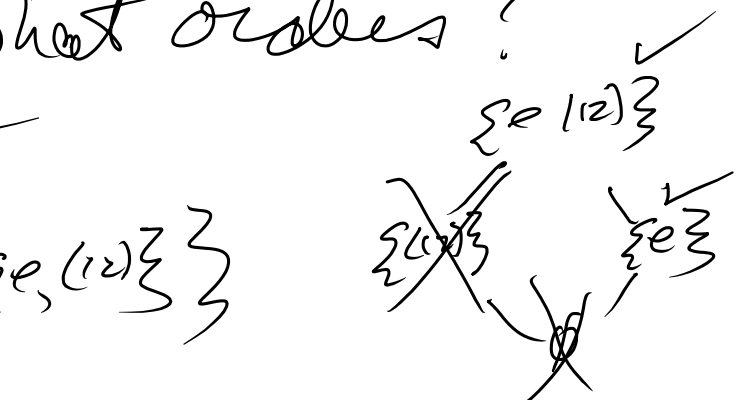
x^4+1

$S_2 = \{e, (12)\}$ $|S_2| = 2$

Subgroups of S_2 have what orders?

order 1 $\{e\}$

order 2 $\{e, \{e, (12)\}\}$



$|S_3| = 6$ Subgroups can have what order? 1, 2, 3, 6

How subsets of S_3? 64

K	Subsets of size	Subgroups
0	1	0
1	6	1
2	15	3 $\{e,(12)\}$ $\{e,(13)\}$ $\{e(23)\}$
3	20	1 $\{e,(123),(132)\}$
4	15	0
5	6	0
6	1	1

Pairs on 1, 2, 3

$\{e, P\}$ $P^2 = e$ $P^2 = e$

1 2 3
a b c

$1 \to 2 \to 1$
$2 \to 1 \to 2$

1 2 3
1 3 2

$S_3 = \{\{e\}, \{e,(12)\}, \{e,(13)\}, \{e,(23)\}, \{e,(123),(132)\}\}$

$(123)(132) = (1)$

S_4 $|S_4| = 2^4 = 16$ mill+ 8 mill+ because must contain $1\ 2\ 3\ 4$

1

8 will + because must contain

order 1 $= \{e\}$

order 2 $= \{e, p\}$ $p^2 = 1$

$p =$ (12) (12)(34)
(13) (13)(24)
(14) (14) (23)
(23) ~~(23) (14)~~
(24)
(34)

order 3 $\{e, (123), (132)\}$

$\{e, (124)$

$$\left(\frac{127}{547}\right) = -\left(\frac{547}{127}\right) = -\left(\frac{39}{127}\right)$$

$$= -\left(\frac{3}{127}\right)\left(\frac{13}{127}\right)$$

$$= -\left(\frac{127}{3}\right)\left(\frac{127}{13}\right)$$

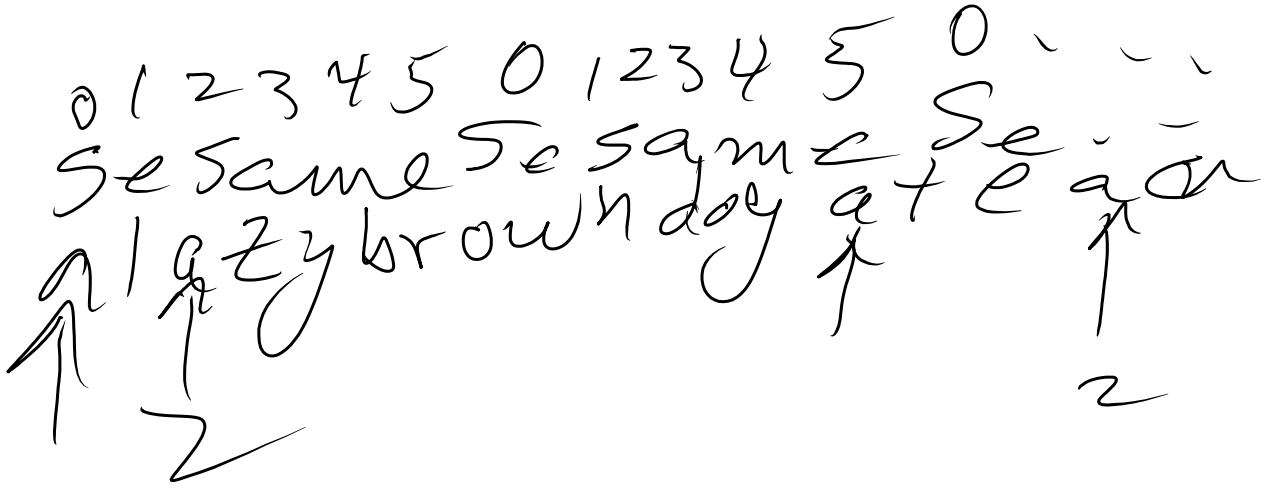
$$= \left(\frac{127}{3}\right)\left(\frac{127}{13}\right)$$

$$= \left(\frac{1}{3}\right)\left(\frac{10}{13}\right) = \left(\frac{10}{13}\right)$$

127 = 4 · 32 + 39

547 = 509 + 39

$\left(\frac{2}{13}\right)(-1)$ $\left(\frac{5}{13}\right)(-1) = 1$


0 1 2 3 4 5 0 1 2 3 4 5 0
Sesame Sesame Se
a lazy brown dog ate a

a) A group is a pair $(G, *)$ where G is a set and $*: G \times G \to G$ is an operation s.t.
$\exists 1 \in G$ s.t. $\forall g \in G \quad 1*g = g*1 = g$
$\forall g \in G, \exists g^{-1}$ s.t. $g * g^{-1} = g^{-1} * g = 1$
$*$ is associative.

b) A permutation on a set S is a bijection from $S \to S$.

c) Let S_n be the set of all bijections from range$(n) \to$ range(n) with functional composition
1) functional comp. is closed
2) The identity map is the identity under composition
3) Every bijection has an inverse function

d) $H \lhd G$ iff $\forall g \in G, \quad gHg^{-1} = H$

e) A group hom between G_1 & G_2 is a function $f: G_1 \to G_2$ s.t. $f(a*b) = f(a) * f(b)$

f) If $f: G_1 \to G_2$ is a group hom, $\ker(f) = \{g \in G_1 \mid f(g) = e\}$. $k_1, k_2 \in \ker(f)$ $f(k_1 k_2) = f(k_1) f(k_2) = e * e = e$ so $k_1 k_2 \in \ker(f)$ so it's a subgroup. $\ker f$ is normal because ~~if~~ if $k \in \ker(f)$, $g \in G_1$ $f(gkg^{-1}) = f(g) f(k) f(g^{-1})$
$= f(g) e f(g^{-1})$
$= f(g) f(g^{-1}) = e$

So $\ker(f) \lhd G_1$

(a) The Ext GCD is an algorithm that, in addition to calculating GCD(a,b) also calculates s & t s.t. $sa + tb = GCD(a,b)$

(b) Just like GCD(a,b) uses GCD(b, a%b) if $a\%b \neq 0$, EGCD(a,b) computes the GCD and coefficients from EGCD(b, a%b) if $a\%b \neq 0$

$g = s_1 b + t_1 r$
$a = qb + r$
$r = a - qb$
$g = s_1 b + t_1 (a - qb)$
$g = t_1 a + (s_1 - qt_1) b$

(c)
```
def eGCD(a,b):
    if a%b == 0:
        return (b,0,1)
    else:
        g,s1,t1 = eGCD(b, a%b)
        return (g,t1,s1-a//b*t1)
```

a) $\mathbb{Z}_n^* = \{ m \in \mathbb{Z}_n \mid \gcd(m,n) = 1 \}$

$\mathbb{Z}_n^*$ differs from $\mathbb{Z}_n$: it doesn't contain 0.

b) $(\mathbb{Z}_n^*, *)$ is a group :

$*$ is associative

$1 \in \mathbb{Z}_n^*$

m & n are coprime and q & n are coprime $\Rightarrow mq$ & n are coprime so $\mathbb{Z}_n^*$ is closed under $*$

$\forall m \in \mathbb{Z}_n^*$ by the extended GCD algorithm $\exists$ s, t s.t $sm + tn = 1$. $sm = 1 \pmod n$

s is the inverse of m.

c) $\mathbb{Z}_n^* \not\subseteq \mathbb{Z}_n$ $\mathbb{Z}_n$ is a group under $+$

$\mathbb{Z}_n^*$ " " " " $*$

d) $|\mathbb{Z}_n^*| = \phi(n)$ $\phi(pq) = (p-1)(q-1)$

$\phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1)$

a) CRT if s & t are coprime then map $f: \mathbb{Z}_{s*t} \to \mathbb{Z}_s \times \mathbb{Z}_t$ given by $f(n) = (n \% s, n \% t)$ is a bijection.

b) CRT Proof: Claim f is an injection.

assume $f(n) = f(m)$ $\quad (n \% s, n \% t) = (m \% s, m \% t)$

$n = m \pmod s$ $\quad n = m \pmod t$

$(n-m) = 0 \pmod s$ $\quad (n-m) = 0 \pmod t$

$(n-m)$ divisible by s $\quad n-m$ divisible by t

s & t are coprime $\Rightarrow (n-m) = 0 \pmod{s*t}$

$n = m \pmod{s*t}$

$|\mathbb{Z}_{s*t}| = s*t$ $\quad |\mathbb{Z}_s \times \mathbb{Z}_t| = s*t$

an injection between two sets of equal sizes is a bijection.

a) The value of 8000 is 60's from the μ. So by Chebyshev this is likely to happen $1/36$-th of the time. Unusual.

b) Sample Space is the 128 positions that the Small Disk can have relative to the large disk.

$Matches: S \to \mathbb{R}$

$Matches(position) = \#$ of Matches

Introduce $Match_j(p) = 1$ if sector j in position p Matches sector below

$= 0$ else

$$Matches = \sum_{j=0}^{127} Match_j$$

Assume Smaller disk has 32 R 96 W

$E(Match_j) = \frac{3}{4}$ if sector j is red $\frac{96}{128}$

$= 1/4$ if sector j is white

$$E(Matches) = 32 \times \frac{3}{4} + 96 \times \frac{1}{4} = \frac{96+96}{4} = \frac{96}{2} = 48$$

Since $E(Matches) = 48$, $Matches(p) \geq 48$ for some position p.

a) A ring is a triple $(R, +, *)$ where R is a set, $+ : R \times R \to R$, $* : R \times R \to R$ and $(R, +)$ is an abelian group. $*$ is associative and $\forall a, b, c$ $a*(b+c) = a*b + a*c$
$(b+c)*a = b*a + c*a$

b) a commutative ring is a ring s.t. $*$ is commutative

c) A field F is a comm ring with an identity "1" for $*$ and $\forall f \in F - \{0\}$ $\exists f^{-1}$ s.t. $ff^{-1} = 1$

d) $\mathbb{Z}_n$ is a commutative ring because $*$ is commutative. In general not a field because if n is not prime $\exists$ zero divisors

e) $\mathbb{Z}_p$ is a field if p prime because by Problem 2(b), $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ ~~result~~ if p is prime

f) 1) Can add two polynomials to get another polynomial
2) 0 is additive inverse
3) Product of polynomials is commutative and a poly
4) All ops are associative (closed under algebra)

g) If degree $f <$ deg g, $f = 0 * g + f$
Otherwise let $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$
$g = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$

let $C(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$

Let $f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$

$f_1(x)$ has degree $< n$.

Can repeat until degree $< m$

$f(x) = g(x) q(x) + r(x)$ with

$\deg r(x) < m$.

Equiv Relation R

1) Reflexive
2) Symm
3) Trans

$xRx \quad \forall x$

$xRy \Rightarrow yRx$

$xRy \;\&\; yRz \Rightarrow xRz$

R is reflexive $xx^{-1} = e \in H$ ∴ H is a subgroup.

xRx

R is symm $xRy \Rightarrow xy^{-1} \in H \Rightarrow (xy^{-1})^{-1} \in H \Rightarrow yx^{-1} \in H \Rightarrow yRx$

R is transitive $xRy \Rightarrow xy^{-1} \in H$, $yRz \Rightarrow yz^{-1} \in H$

$\Rightarrow xy^{-1}yz^{-1} = xz^{-1} \in H \Rightarrow xRz$

(b) Cosets $xy^{-1} \in H \quad x \in Hy$

c) R partitions G. Each coset has size $|H|$

$|G| = k|H|$ for k cosets & $|H|$ divides $|G|$

$f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2$ mono

$g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2$ epi

Prob 1

a) $g^2 = e \quad \forall g \in G$

$ab = ba$

$a^2 = e$

$b^2 = e$

$(ab)^2 = abab = e$

$ab = aeb = a(abab)b = a^2ba b^2 = ba$

b) $(ab)^2 = a^2b^2 \Rightarrow abab = a^2b^2$

$\Rightarrow ba = ab$

c) if $|G| = 4$, then every elt has order 1, 2, or 4 ∴ the order of every elt has to divide the order of the group.

If ∃ an elt of order 4, then G is a cyclic group, and is abelian.

If ∄ an elt of order 4, then G is abelian by Part (a).

d) $e^2 = e \quad g \neq e.$

$g \longleftrightarrow g^{-1} \qquad g^2 = e$

$\text{Set} = \{\{g, g^{-1}\} \mid g \in G\}$

$|\{g, g^{-1}\}| = 1 \text{ or } 2$

Define aRb iff $b = a$ or $b = a^{-1}$

Define aRb iff $b=a$ or $b=a^{-1}$

R is an equiv.

This partitions G into equivalence classes

$|[e]|=1$ $\quad |G| = \sum_{g \neq g^{-1}} |[g]| + \sum_{g=g^{-1}} |[g]|$

$|G| = 2k + j \qquad j>1$

even even $\qquad |[e]|=1$

So $\exists g \neq e$ s.t. $|[g]|=1$ so $g^2=e$

Prob 2 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longleftrightarrow abcd$

$\mathbb{Z}_2$ $ad - bc \neq 0$

Let $X = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0 \right\}$ ~~det~~

$ad - bc \neq 0$ $ad + bc$

abcd

bc	ad
1001	0110
1101	1110
1011	0111

b) Because $Det(M_1 \times M_2) = Det(M_1) \times Det(M_2)$
All matrices of det 1 are closed under matrix multiplication
Matrix mult is assoc by Lin Alg.
Matrix mult preserves Det
Assoc
1001 is Identity

Inverse Brute Force
By Lin Alg or if $Det(M) \neq 0$ $\exists$
M^* s.t. $M \times M^* = Id$ →

Why is $Det(M^*) = 1$?

$Det(M) \times Det(M^*) = Det(Id)$

$1 \times x = 1 \Rightarrow x = 1$

$M^* \subset G$.

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \end{pmatrix}$

$f_{a,b} : \mathbb{R} \to \mathbb{R}$ $\quad f_{a,b}(x) = ax + b$.

Prove its a group!

$f_{c,d}(f_{a,b}(x)) = c(ax+b)+d = acx + bc + d = f_{ac,\,bc+d}$

$bc+d \in \mathbb{R}$

$ac \in \mathbb{R}$

$f_{a,b}^{-1} = f_{c,d}$ $\quad acx + bc + d = x$

$ac = 1 \quad c = \frac{1}{a}$ (OK since $a \neq 0$)

$bc + d = 0 \quad \frac{b}{c} + d = 0 \quad d = -\frac{b}{a}$

$f_{a,b}^{-1} = f_{1/a,\,-b/a}$ $\quad f_{a,b}\left(f_{\frac{1}{a},-\frac{b}{a}}\right) \quad a\left(\frac{1}{a}x - \frac{b}{a}\right) + b = x - b + b = x$

$e = f_{1,0}$

functional is Assoc.

So we have a group.

1) closed under func comp $ac \neq 0$ if $a \neq 0$ & $c \neq 0$
2) Assoc $\because$ func comp is assoc
3) Id is $f_{1,0}$
4) Inverse is $f_{\frac{1}{a},-\frac{b}{a}}$

Part b) $\quad f_{a,b} \circ f_{c,d} = f_{ac,\,bc+d}$ $\quad acx + da + b$

$bc+d \quad ac \quad dc+d$

$ac + \ldots$ $\quad bc + d = ad + b$

$c = 0, d = 0$ $\quad 0 \neq 1$
$b = 1$

Part c H is a subgroup $\because f_{1,0} \in H$

$f_{a,b} \in H \Rightarrow f_{1/a, -b/a} \in H$

$a \in \mathbb{R} \Rightarrow \frac{1}{a} \in \mathbb{Q}$

$f_{a,b}, f_{c,d} \in \mathbb{Q} \Rightarrow f_{a,b} \circ f_{c,d} \in \mathbb{Q}$

$a, c \in \mathbb{Q} \Rightarrow ac \in \mathbb{Q}$

(Part d) Normal Yes

$f_{c,d} \circ f_{a,b} \circ f_{\frac{1}{c}, -\frac{d}{c}} = c \cdot a \frac{1}{c} V_t - \ldots$

$= a V_t + \ldots$

What could you check on Prob 4

$p(x) = m(x)g(x) + r(x)$

$p(x)$

$g(x)$

$GCD(p, g)$

$f(a +_R b) = f(a) +_S f(b)$

$f(a *_R b) = f(a) *_S f(b)$

$f(0) = f(0 +_R 0) = f(0) +_S f(0) \Rightarrow f(0) = 0_S$

$0 \in \ker f$

$f(0) = 0$

$r, s \in \ker f \quad f(r +_R s) = f(r) +_S f(s) = 0_S$

$f(r) = 0$

$f(ar) = f(a) \cdot f(r) = f(a) * 0 = 0$

$f(ra) = f(r) * f(a) = 0 * f(a) = 0$

$\sum a + H \mid a \in$

3) Sample Space

$$= \{(f, k\text{-heads in a row}), (f, \text{Not } k \text{ heads}), (b, k\text{-heads}), (b, \text{Not } k \text{ heads})\}$$

a: $\frac{1}{2^{k+1}}$ b: $\frac{1}{2} - \frac{1}{2^{k+1}}$ c: $\frac{1}{2}$ d: 0

Prob Space

$2^k/2^k + 1 = 2$

$2^k/(2^k+1)$

Event A Biased coin picked $A = \{c, d\}$

Event B k heads in a row $B = \{a, c\}$

$$\text{Prob}(A|B) = \frac{\text{Prob}(A|B)}{\text{Prob}(B)} = \frac{\text{Prob}(\{c\})}{\text{Prob}(a,c)} = \frac{1/2}{1/2 + 1/2^{k+1}} \cdot \frac{2^{k+1}}{2^{k+1}}$$

$$= \frac{2^k}{2^{k+1} - 1} = \frac{2^{k+1}}{2^{k+1}} - \frac{1}{2^{k+1}} = 1 - \frac{1}{2^{k+1}}$$

iff

A ⇒ B if f is an epimorphism in the Category of Sets then f is a surjection.

B ⇒ A if f is a surjection then it is an epimorphism in the Category of sets.

Don't invent your own language this category is epimorphic ???

A ⇒ B Proof by Contradiction

Assume f is an epimorphism but Not a surjection $f: A \to B$

f an epimorphism ⇒ ∀ sets C & functions $g_1: B \to C$, $g_2: B \to C$, if $g_1 \circ f = g_2 \circ f$, then $g_1 = g_2$. Since f not a surj ∃ $b \in B$ s.t. $f(a) \neq b \ \forall a \in A$

Let $C = \{0, 1\}$, Let $g_1: B \to C$ be $g_1(x) = 0$ ∀ $x \in B$. $g_2: B \to C$ be $g_2(x) = 0$ if $x \neq b$, $g_2(b) = 1$

$g_1 \circ f = g_2 \circ f \ \forall a \in A$

but $g_1 \neq g_2$

B ⇒ A $f: A \to B$ is a surjection

$g_1, g_2: B \to C$

s.t. $g_1 \circ f = g_2 \circ f$. Pick $q \in B$. ∃ $a \in A$ s.t. $f(a) = q$ $g_1 \circ f(a) = g_2 \circ f(a)$

$\Rightarrow g_1(q) = g_2(q)$, $\forall q \in B \Rightarrow g_1 = g_2$

b) In the Cat of sets bij $\iff$ bimorph

From a) in the Cat of sets surj $\iff$ epimorph

inj $\iff$ monomorph

From Hotel

bij $\overset{\text{iff}}{\iff}$ surj & inj $\overset{\text{iff}}{\iff}$ epimorph & monomorph

$\iff$ bimorph

c) Category of Graphs.

Objects = undirected Graphs

Morphisms? $G_1 = (V_1, E_1)$ $G_2 (V_2, E_2)$

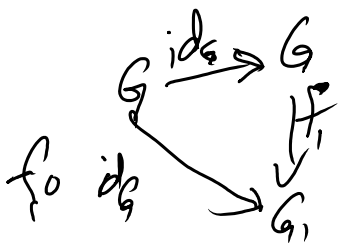
a morphism is a map $f: V_1 \to V_2$ s.t.

$(a,b) \in E_1 \implies (f(a), f(b)) \in E_2$

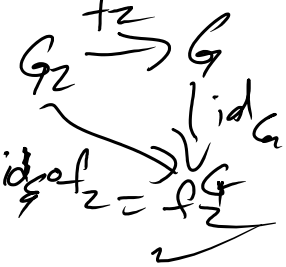
What's the identity $G = (V, E)$

$id_G : V \to V$ $id_G(v) = v$

$f_1 : G \to G_1$ or $f_2 : G_2 \to G$



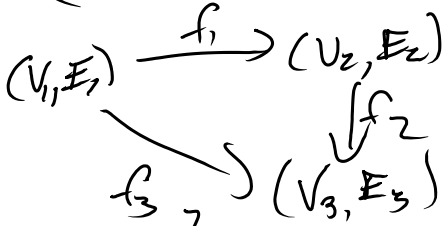
$f_1 \circ id_G = f_1$ ✓



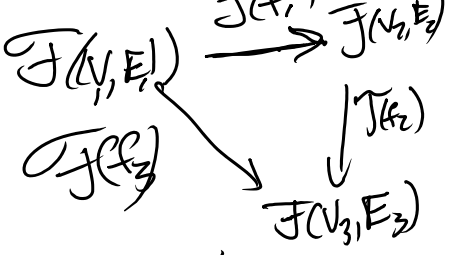
✓

d) Graphs (V, E) Digraphs (V, A)

$\mathcal{F}((V,E)) = (V, A)$ $A = \{(v,w) \mid \{v,w\} \in E\}$



$f_3 = f_2 \circ f_1$



$\mathcal{F}(f_1)(a,b) = (f(a), f(b))$

$f_1 : V_1 \to V_2$

$f_3((a,b)) = \{f(a), f(b)\}$

$f_p([a,b]) = \{f_1(a), f(a)\}$ $\quad f_1 : U_1 \to U_2$ $\quad \mathcal{J}(f_1)(a,b) = (f(a), f(b))$

Prob 3 Produce all groups of orders $1, 2, \cdots, 7$

Order $1 = \{e\}$

$2, 3, 5, 7$ are primes so the only groups of those sizes are C_j (C_j is the cyclic group of order j) for $j = 2, 3, 5, 7$

Leaves order $= 4$ & order $= 6$

Order 4 $(\mathbb{Z}_4, +)$

Let G be a group of order 4

Every elt of G has order $1, 2,$ or 4

If elt has order 4, then $G \cong (\mathbb{Z}_4, +)$

Only case left is every elt has order 1 or 2

$\{1, a\}$ is a subgroup. Pick $b \in G - \{1, a\}$

$b^2 = 1$ $\{1, a, b, ab\}$ $ab \neq 1$ $a^2 = 1$

$ab \neq a$ $ab = a^2$

What is $ba \neq 1$ $ab \neq b$ $b = a$

$\neq a$

$\neq b$

$ba = ab$

Group is comm.

$ab = c$ $\{1, a, b, c\}$

abelian $ab = c$

$bc = a$

$ca = b$

So for order $= 4$ $\exists$ two non-isomorphic groups.

Both Abelian

Order 6 orders of elts must be $1, 2, 3,$ or 6

Order 6 Order of elts must be 1, 2, 3, or 6

If element has order 6, $G = (\mathbb{Z}_6, +)$

Abelian or Non-Abelian Limiting our groups so elts only

Abelian of order 1, 2, 3

Assume all elements have only order 1 or 2

$\{1, a, b, ab\}$ is subgroup of order 4 in a group of order 6 ?!? Impossible $4 \nmid 6$

$\exists$ an element a of order 3.

$\{1, a, a^2\}$

Let $b \in G - \{1, a, a^2\}$

$S = \{1, a, a^2, b, ab, a^2b\}$

$b = ab$? $\Rightarrow a = 1$

$b = a^2b \Rightarrow a^2 = 1$

$ab = a^2b \Rightarrow a = 1$

$ab = a \Rightarrow b = 1$

$a^2b = a \Rightarrow ab = 1 \Rightarrow b = a^2$

$|S| = 6$ What is $b^2 = ?$

Case $b^2 = 1$ Imp $1, ab, a^2, a^2b^3, a^4b^4, b, a, a^5b^5 = a^6b, a^6b = 1$

Look at order(ab)

$b^2 \neq b$

$\neq ab$

$\neq a^2b$

$b^2 \neq 1$

$b^3 = 1$

$b^2 = a$

$b^2 = a^2$

$b^2 = a$

$b^4 = a^2$ $b^3 \neq 1$

$a^2 = b^4 = b^3 \cdot b = b$

$b^2 = a^2$

$b^4 = a$

The only abelian group of order 6 is $(\mathbb{Z}_6, +)$