Abstract Algebra - Revision

1- Functions

- A function has 3 parts;
  - domain X
  - codomain Y
  - rule $f(x) = y$

} $\forall x \in X \quad \exists$ a unique $y \in Y$ st $f(x) = y$

- Example 1.1 - $f : \mathbb{Z} \to \mathbb{R} \quad f(x) = \sqrt{x}$

$-1 \in \mathbb{Z} \quad f(-1) = \sqrt{-1} \notin \mathbb{R}$

$\Rightarrow$ not a function

fix $\to$ $g : \mathbb{N} \to \mathbb{R} \quad g(x) = \sqrt{x}$ edit domain

$h : \mathbb{Z} \to \mathbb{C} \quad h(x) = \sqrt{x}$ edit codomain

- Example 1.2 - $f : \mathbb{Z} \to \mathbb{Z} \quad f(x) = \frac{x}{2}$

$1 \in \mathbb{Z} \quad f(1) = \frac{1}{2} \notin \mathbb{Z}$

$\Rightarrow$ not a function

Fix $\to$ $g : 2\mathbb{Z} \to \mathbb{Z} \quad g(x) = \frac{x}{2}$ edit domain

$h : \mathbb{Z} \to \{\frac{n}{2} \mid n \in \mathbb{N}\} \quad h(x) = \frac{x}{2}$ edit codomain

- Example 1.3 - $f : \mathbb{Z} \to \mathbb{Z} \quad f(x) = \begin{cases} x+1 & x \geq 0 \\ x-1 & x \leq 0 \end{cases}$

$0 \geq 0 \Rightarrow f(0) = 0+1 = 1$

$0 \leq 0 \Rightarrow f(0) = 0-1 = -1$

$\Rightarrow$ not a function (not well defined)

fix $\to$ $g : \mathbb{Z} \to \mathbb{Z} \quad g(x) = \begin{cases} x+1 & x \geq 0 \\ x-1 & x < 0 \end{cases}$

edit function to make well defined

- Example 1.4 - $f: \mathbb{Q} \to \mathbb{Z}$ $\quad f\left(\frac{a}{b}\right) = a \cdot b$

$$f\left(\tfrac{3}{7}\right) = 3 \cdot 7 = 21$$

$$f\left(\tfrac{6}{14}\right) = 6 \cdot 14 = 84$$

Two ways to write the same element of $\mathbb{Q}$ → $\frac{3}{7} = \frac{6}{14}$ $\quad f\left(\frac{3}{7}\right) \neq f\left(\frac{6}{14}\right)$

$\Rightarrow$ not well defined

can you see how we could fix this? can we specify a unique way to write fractions?

- Example 1.5 - $f: \mathbb{Q}\setminus\{0\} \to \mathbb{Q}$ $\quad f\left(\frac{a}{b}\right) = \frac{b}{a} + 1$

$*$ $\frac{a}{b} \in \mathbb{Q} \Rightarrow f\left(\frac{a}{b}\right) = \frac{b}{a} + 1 = \frac{b}{a} + \frac{a}{a}$

$$= \frac{b+a}{a} \in \mathbb{Q}$$

$$\Rightarrow \forall x \in X \quad f(x) \in Y$$

$*$ Is this well defined (is $f(x)$ unique?)

we need to check f is well defined as there are multiple ways to express fractions

Let $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ with $\frac{a}{b} = \frac{c}{d}$

$$\Rightarrow ad = bc$$

$$\Rightarrow \frac{ad}{ac} = \frac{bc}{ac}$$

$$\Rightarrow \frac{d}{c} = \frac{b}{a}$$

$$\Rightarrow \frac{d}{c} + 1 = \frac{b}{a} + 1$$

$$\Rightarrow f\left(\tfrac{c}{d}\right) = f\left(\tfrac{a}{b}\right)$$

$\Rightarrow$ well defined

- Example 1.6 - Let $N \trianglelefteq G$ We'll revisit normal SGs in §3

$$F: G/N \times G/N \to G/N \qquad F(Nx, Ny) = Nxy$$

$$x, y \in G \implies xy \in G$$
$$\implies Nx, Ny \in G/N \implies N(xy) \in G$$

There are multiple ways to express cosets so we need to check that F is well defined

Let $Nx, Nx', Ny, Ny' \in G/N$ with

$$Nx = Nx' \quad \text{and} \quad Ny = Ny'$$
$$\implies xx'^{-1} \in N \qquad yy'^{-1} \in N$$
$$\implies \exists n, m \in N \text{ with}$$
$$xx'^{-1} = n \qquad yy'^{-1} = m$$
$$\implies x = nx' \qquad y = my'$$
$$\implies xy = nx'my'$$
$$= nx'mx'^{-1}x'y'$$
$$\implies (xy)(x'y')^{-1} = \underbrace{n}_{n \in N}\underbrace{x'mx'^{-1}}_{x'mx'^{-1} \in N \text{ since } N \trianglelefteq G}$$
$$\implies nx'mx'^{-1} \in N$$
$$\implies (xy)(x'y')^{-1} \in N$$
$$\implies Nxy = Nx'y'$$
$$\implies \text{well defined}$$ ☺

2 - Congruences

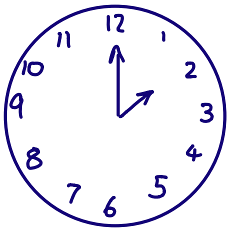
2.1 - Definitions

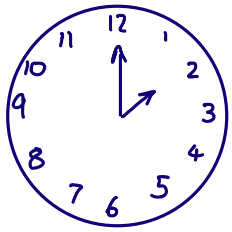
- Let $m \in \mathbb{Z}$ with $m > 1$, let $a, b \in \mathbb{Z}$

  $a \equiv b \bmod m \iff m$ divides $(a-b)$
  $\iff$ a and b have the same remainder when divided by m

- example clocks -

  Let $\boxed{02:00}$ $\boxed{14:00}$ be 2 times in 24-hour time

  $\boxed{02:00}$ = 

  $\boxed{14:00}$ = 

- Congruence classes = equiv classes under $a \sim b \iff a \equiv b \bmod m$

  $$[a] = \{km + a \mid k \in \mathbb{Z}\}$$
  $$= \{\ldots.\ a-2m, a-m, a, a+m, a+2m, \ldots\}$$

  The "standard" set of equiv classes are

  $[0], [1], \ldots, [m-1]$

- $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$
  $= \{0, 1, \ldots, m-1\}$

  we sometimes drop the $[\cdot]$ notation

  $[a] + [b] = [a+b]$ $\qquad$ $[a]\cdot[b] = [ab]$

- Example - $m = 5$ $\qquad$ $[1] = \{\ldots.\ -9, -4, 1, 6, 11, \ldots\}$

  $\mathbb{Z}_5 = \{[0], [1], \ldots, [4]\}$

  $[1] + [3] = [4]$ $\qquad$ $[2]\cdot[4] = [8] = [3]$

  $[2] + [3] = [5] = [0]$

2.2 – Groups, Rings + Fields

(See lecture notes for proofs)

- $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ is a commutative ring
- $m = p$ prime $\Rightarrow$ $\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is a field

  $\mathbb{F}_p^* = \mathbb{Z}_p \backslash \{0\}$ is a group under $\times$

- $m = ab$ $1 < a, b < m$ (m composite) $\Rightarrow$ $\mathbb{Z}_m$ is a ring but <u>not</u> a field

  $\mathbb{Z}_m \backslash \{0\}$ is <u>not</u> a group

  $U_m = \{ a \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1 \}$ is a group

2.3 – Finding Solutions

- Let p prime, $c \neq 0$

  $cx \equiv d \mod p \Rightarrow$ unique soln

  $c \in \mathbb{Z}_p \backslash \{0\}$ (a group)

  $\Rightarrow c^{-1}$ exists

  $\Rightarrow x \equiv c^{-1} d \mod p$

  $\Rightarrow x = [c^{-1} d]$

Solve $2x \equiv 5 \mod 7$

Lets find 2^{-1} in $\mathbb{Z}_7 \backslash \{0\}$

$2 \cdot 1 = 1$ $\quad 2 \cdot 2 = 4$ $\quad 2 \cdot 3 = 6$ $\quad 2 \cdot 4 = 8 \equiv 1$

$\Rightarrow 4 \cdot 2x \equiv 4 \cdot 5 \mod 7$

$\Rightarrow x \equiv 20 \equiv 6 \mod 7$

$\Rightarrow x = [6]$

- $m = ab$, $1 < a, b < m$ (m comp)

  $cx \equiv d \mod m$

  * $\gcd(c, m) = 1 \Rightarrow$ unique soln

  $\gcd(c, m) = 1 \Rightarrow c \in U_m$

  $\Rightarrow c$ has an inverse

  $\Rightarrow x \equiv c^{-1} d \mod p$

  $\Rightarrow x = [c^{-1} d]$

Solve $3x \equiv 4 \mod 10$

$\gcd(3, 10) = 1$

$\Rightarrow 3 \in U_{10}$, let's find 3^{-1}

$3 \cdot 1 = 3$ $\quad 3 \cdot 2 = 3$ ..... $\quad 3 \cdot 7 = 21 \equiv 1$

$\Rightarrow x \equiv 7 \cdot 4 \mod 10 \equiv 8 \mod 10$

$\Rightarrow x = [8]$

* $\gcd(c,m)=t \quad t \nmid d$
$\Rightarrow$ no solns

$cx \equiv d \mod m$
$\Rightarrow \exists y \in \mathbb{Z}$ st
$cx - my = d$

$t \mid c, t \mid m \Rightarrow t \mid LHS$
$t \nmid d \Rightarrow t \nmid RHS$
#

Show that $10x \equiv 8 \mod 20$
has no solns
(try this yourself)

* $\gcd(c,m)=t \quad t \mid d$
$\Rightarrow$ t solns

$cx \equiv d \mod m$
$\Rightarrow$ solve $cx - my = d$
Find $x_0 =$ initial soln
all solns;
$x_i = x_0 + \left(\frac{m}{t}\right) i \quad i = 0, \dots, t-1$

$6x \equiv 8 \mod 20$
$\gcd(6,20) = 2 \qquad 2 \mid 10$
$\Rightarrow$ 2 solns
$6 \cdot 1 = 6, \dots, \quad 6 \cdot 8 = 48 \equiv 8$
$\Rightarrow x_0 = 8$
$x_0 = [8] \qquad x_1 = [8 + (\frac{20}{2})1]$
$= [18]$

3- Normal Subgroups + Quotients

- Let $N \leq G$, then N is normal write $N \trianglelefteq G$ if one of the following holds;

  ① $\forall x \in N, \forall g \in G \quad g^{-1} x g \in N$

  ② $\forall g \in G \quad g^{-1} N g = N$

  ③ $\forall g \in G \quad Ng = gN$

  ④ set of left cosets = set of right cosets

  Thm 10.12

- Example 3.1 (normal SG) - If $H \leq G$ with $[G:H]=2$ then $H \trianglelefteq G$
  - Let $g \in G \setminus H$ then;
  $\{H, Hg\}$ = right cosets $\quad \{H, gH\}$ = left cosets
  $H = H \Rightarrow Hg = gH$
  $\Rightarrow$ right costes = left cosets
  $\Rightarrow$ normal by ④

- $D_{2n} = \langle \sigma, \rho \rangle$
reflection rotation

$\langle \rho \rangle$ has index 2 in D_{2n}

$\Rightarrow \langle \rho \rangle \trianglelefteq D_{2n}$

- Example 3.2 - (normal SG) If G is abelian and $H \leq G \Rightarrow H \trianglelefteq G$

  - Let $g \in G$ $x \in H$

    $g^{-1}xg = g^{-1}gx = 1x = x \in N \Rightarrow$ normal by ①

    Can you check N is normal by ②-④?

  - klein 4 $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$
    addition componentwise mod 2

    $\langle (0,1) \rangle = \{(0,0), (0,1)\} \leq \mathbb{Z}_2 \times \mathbb{Z}_2$

    $\mathbb{Z}_2 \times \mathbb{Z}_2$ abelian $\Rightarrow \langle (0,1) \rangle \trianglelefteq \mathbb{Z}_2 \times \mathbb{Z}_2$

- Example 3.3 - (quotients) Let p prime, $n \in \mathbb{N}$

  Let $G = GL_n(p)$ $N = SL_n(p)$

  Let $\phi : G \to \mathbb{F}_p^*$ $\phi(g) = \det(g)$

  Then ϕ is a homomorphism with kernel N

  (can you check this yourself)

  What is G/N?

  * By the 1^{st} isomorphism thm

  $$G/\ker\phi \cong \operatorname{im}\phi$$

  $$\Rightarrow G/N \cong \operatorname{im}\phi$$

  what is $\operatorname{im}\phi$?

Let $a \in \mathbb{F}_p^*$ then $\phi\begin{pmatrix} a & & \\ & 1 & \\ & & \ddots & \\ & & & 1\end{pmatrix} = a$

$\Rightarrow \phi$ surjective

$\Rightarrow \operatorname{im}\phi = \mathbb{F}_p^*$

$\Rightarrow G/N \cong \mathbb{F}_p^*$

* can we see this another way?

$G/N = \{ Ng \mid g \in G \}$

$Ng \cdot Nh = N(gh)$

$\#$ cosets $= [G : N] = \dfrac{|G|}{|N|} = p-1$ ___ $(+)$

Lets find these cosets

let $g_a = \begin{pmatrix} a & & \\ & 1 & \\ & & \ddots & \\ & & & 1\end{pmatrix}$

$Ng_a = \{ n g_a \mid n \in N \}$

$\det(ng_a) = \det(n)\det(g_a)$
$= 1 \cdot a$
$= a$

$\Rightarrow a \neq b$ then $g_b = \begin{pmatrix} b & & \\ & 1 & \\ & & \ddots & \\ & & & 1\end{pmatrix} \notin Ng_a$

$\Rightarrow$ Ng_a and Ng_b are distinct cosets

$\Rightarrow N = Ng_1, Ng_2, \dots, Ng_{p-1}$
are $p-1$ distinct cosets

$\Rightarrow$ by $(+)$ these are all the cosets

$\Rightarrow G/N = \{ Ng_1, Ng_2, \dots, Ng_{p-1} \}$

What does the multiplication look like?

$$Ng_a \cdot Ng_b = Ng_a g_b$$

$$= N\begin{pmatrix} a & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}\begin{pmatrix} b & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

$$= N\begin{pmatrix} a\cdot b & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

$$= Ng_{ab}$$

$\Rightarrow \; Ng_a \cdot Ng_b = Ng_{ab}$

so if we write $\boxed{a} = Ng_a$ then

$G/N = \{\boxed{1}, \boxed{2}, \ldots, \boxed{p-1}\}$ and

$\boxed{a} \cdot \boxed{b} = \boxed{a\cdot b}$

Can you see that this now "looks like" the group $\mathbb{F}_p^*$?