Recall,

$$U(n) = \{[a] \in \mathbb{Z}_n \mid [a] \text{ has an inverse under } \cdot \}$$

is an abelian group under multiplication.

<u>Thm</u>: Let $a \in \mathbb{Z}$. Then $[a] \in U(n)$ if and only if $\gcd(a,n) = 1$.

<u>Proof</u>: $[a] \in \mathbb{Z}$ if and only if the equation

$$ax \equiv 1 \pmod{n}$$

has a solution $x \in \mathbb{Z}$ (since then $[a]^{-1} = [x]$).

($\Rightarrow$) Suppose such $x \in \mathbb{Z}$ exists. Then $ax - 1 = ny$ for some $y \in \mathbb{Z}$. So

$$ax + n(-y) = 1,$$

proving $\gcd(a,n) = 1$.

($\Leftarrow$) Conversely, suppose $\gcd(a,n)=1$. Then there exist $x,y \in \mathbb{Z}$ such that

$$ax + ny = 1.$$

Thus,

$$ax - 1 = n(-y),$$

proving that

$$ax \equiv 1 \pmod{n}.$$

$\blacksquare$

Ex: By the theorem, $U(8) = \{1, 3, 5, 7\}$. The Cayley table is

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

HW 3

Invertible matrices

Let

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A \text{ is invertible}\}.$$

$\Updownarrow$

$\det A \neq 0$

Then $GL_n(\mathbb{R})$ is a group under matrix multiplication, called the <u>general linear group</u> of degree n over $\mathbb{R}$.

<u>Why?</u> It's clear that

1. Matrix multiplication is associative;
2. $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ is the identity element; and
3. Each $A \in GL_n(\mathbb{R})$ has an inverse $A^{-1} \in GL_n(\mathbb{R})$.

The one thing to check is that matrix multiplication is a binary operation on $GL_n(\mathbb{R})$.

This follows from the fact that if $A, B \in GL_n(\mathbb{R})$ are invertible matrices, then

$$(AB)^{-1} = B^{-1}A^{-1}$$

and so $AB \in GL_n(\mathbb{R})$ also.

Since matrix multiplication is not commutative, $GL_n(\mathbb{R})$ is a non-abelian group (for $n \geq 2$).

More basic properties of groups

Note: Going forward, we will write the group operation in a generic group as multiplication.

$$\boxed{\text{For } g,h \in G, \quad gh \text{ means } g*h.}$$

Of course, if a familiar group uses other notation (e.g., $\mathbb{Z}_n$ uses $+$), then we will use that notation when working with that group.

Prop: Let G be a group and $g,h \in G$. Then there exists a unique $x \in G$ such that

$$gx = h.$$

Similarly, there is a unique $y \in G$ such that

$$yg = h.$$

Proof: Let $x = g^{-1}h$. Then

$$gx = g(g^{-1}h) = (gg^{-1})h = eh = h,$$

so x solves the equation.

For uniqueness, suppose $gx_1 = h$ and $gx_2 = h$. Then

$$x_1 = g^{-1}gx_1 = g^{-1}h = g^{-1}gx_2 = x_2.$$

Similarly, $y = hg^{-1} \in G$ is the unique solution to $yg = h$.

$\blacksquare$

Prop (Cancellation laws): Let G be a group. For all $a,b,c \in G$,

$ab = ac$ implies $b = c$, and

$ba = ca$ implies $b = c$.

Proof: Suppose $ab = ac$. If we call this element h, then

$$ax = h$$

is solved by both $x = b$ and $x = c$. By the previous proposition, $b = c$. ∎

Order + Exponentiation

Let G be a group and $g \in G$. For $n \in \mathbb{N}$, we will write

$$g^n := \underbrace{g \cdot g \cdots g}_{n \text{ times}}$$

and

$$g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}.$$

Note: This is OK by associativity.

We will also write $g^0 := e$.