Integers (mod n)
Z_n denotes the integers mod n.

1. If $a, b \in Z_n$, $a+b$ (mod n) is k s.t. $a+b \equiv k$ (mod n)
2. Usual arithmetic hold but not all have multiplicative inverse. Eg. In $Z_8, 2$ does not have a multiplicative inverse. $\nexists k$ s.t. $2k \equiv 1$ (mod 8).

The following hold for Z_n,

1. $a+b \equiv b+a$ (mod n) and same for ab
2. $(a+b)+c \equiv a+(b+c)$ (mod n) and same for $(ab)c$
3. $a+0 \equiv a$ (mod n) and $a \cdot 1 \equiv a$ (mod n)
4. $\exists -a$ s.t. $a+(-a) \equiv 0$ (mod n)
5. $gcd(a,n)=1 \iff \exists b$ s.t. $ab \equiv 1$ (mod n)

Symmetry

1. A triangle has 6 symmetries, essentially 3! the permutations of the vertices.
2. In the multiplication table for symmetries of a triangle, for every motion there is an inverse.

Groups
A group $(G, \circ)$ is a set G with a law of composition $(a,b) \to a \circ b$ s.t.

1. $\forall a, b \in G, a \circ b \in G$
2. $(a \circ b) \circ c = a \circ (b \circ c)$
3. $\exists e \in G$ s.t. $\forall a \in G, e \circ a = a \circ e = e$
4. $\forall a \in G, \exists a^{-1} s.t., a \circ a^{-1} = a^{-1} \circ a = e$

If $a \circ b = b \circ a$ then the group is abelian.

- Z is a group under addition.
- $(Z_n, +)$ is a group but Z_n is not with modular multiplication
- The group of units $U(n)$ is all $a \in Z_n$ that are coprime with n. So $U(8) = \{1,3,5,7\}$. It is a group under multiplication.
- $M_2(R)$ is set of all 2×2 matrices. Then $GL_2(R)$ the general linear group is the subset that consists of all invertible matrices. The identity of the group is just I. It is a non-abelian group.
- S_3 the symmetry group is $\{(1),(12),(23),(13),(123),(132)\}$

A group is finite if it has finite order. The order of a finite group is number of elements. $|Z_5| = 5$

Properties of Groups

- Inverse is unique; Identity is unique
- $(ab)^{-1} = b^{-1}a^{-1}$; $(a^{-1})^{-1} = a$
- $ba = ca \vee ab = ac \Rightarrow b = c$

Law of exponents hold as follows,

- $g^m g^n = g^{m+n}$; $(g^m)^n = g^{mn}$
- $(gh)^n = (h^{-1}g^{-1})^{-n}$

$(gh)^n = g^n h^n$ only if G is abelian.

Subgroups
A subgroup H of G is a subset H s.t. H is a group under the same operation on G. Every group with at least two elements will have at least two subgroups. $H = \{e\}$ (trivial subgroup) and $H = G$ (proper subgroup)
- $Q^* = \{p/q : p, q \neq 0\}$ is a subgroup of R^*
- $SL_2(R)$ is a subset of $GL_2(R)$ s.t. determinant is 1. It is a sugroup of $GL_2(R)$
A subset H of G can be a group but not a subgroup (essentially a group under a diff operation)

Subgroup Theorems
H is a subgroup of G if and only if

- e of G is in H
- $h_1, h_2 \in H$ then $h_1 \circ h_2 \in H$
- $h \in H$ then $h^{-1} \in H$

H is a subgroup of G if and only if $H \neq \phi$ and for $g, h \in H, gh^{-1} \in H$

Cyclic Subgroups
If G is a group and a is an element of G then, $\langle a \rangle = \{a^k : k \in Z\}$ is a subgroup of G, the smallest containing a.
We call a the generator of the subgroup. The order of a is the smallest n such that $a^n = e$ and $|a| = n$. If order of a is $|G|$ then a is a generator of G.
Eg. Both 1 and 5 generate Z_6. 1 generates Z and any Z_n

- If a generates G then $a^k = e$ if and only if n divides k if G is of order n.
- if $a \in G$ is a generator. If $b = a^k$ then order of b is n/d where $d =$ gcd(k,n)

To find the order of any element $a \in G$ we have, $|a| = n/gcd(a,n)$
A normal subgroup is N s.t. $g \in G$ and $n \in N$ we have $gng^{-1} \in N$

Cosets
A left coset of H with a given $g \in G$ is, $gH = \{gh : h \in H\}$
A right coset of H with a given $g \in G$ is, $Hg = \{hgh \in H\}$ The following are equivalent for $g_1, g_2 \in G$

1. $g_1 H = g_2 H$
2. $Hg_1^{-1} = Hg_2^{-1}$
3. $g_1 H \subset g_2 H$
4. $g_2 \in g_1 H$
5. $g_1^{-1} g_2 \in H$

The cosets of a subgroup partition the larger group G (always).
The **index** of H in G is the number of left cosets of H in G which is $[G : H]$
Eg. $G = Z_6$ and $H = \{0,3\}$ then $[G : H] = 3$

lagranges theorem
H is a subgroup of G and with $g \in G$ the map $\phi : H \to gH$, $\phi(h) = gh$ is bijective. So $|H| = |gH|$.

1. If H is a subgroup of G then $|G|/|H| = [G : H]$
2. Order of $g \in G$ must divide number of elements in G
3. $|G| = p$ then any $g \in G \neq e$ is a generator and G is cyclic.

Homomorphisms
A homomorphism between $(G, \circ_1)$ and $(H, \circ_2)$ is a map $\phi : G \to H$ s.t. $\phi(g_1 \circ_1 g_2) = \phi(g_1) \circ_2 \phi(g_2)$
The relation is stronger if its isomorphic.
Eg. $\phi : Z \to G$ s.t. $\phi(n) = g^n$ is a homomorphism from Z to G.
The following hold,

1. e is identity of G_1 then $\phi(e)$ is of G_2
2. For any $g \in G_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$
3. H_1 is a subgroup of G_1 then $\phi(H_1)$ is a subgroup of G_2
4. If H_2 is a subgroup of G_2 then $\phi^{-1}(H_2) = \{g \in G_1 : \phi(g) \in H_2\}$ is a subgroup of G_1.

The subgroup $H = \phi^{-1}(\{e\})$ is called the kernal of ϕ