Definition 0.1. (Group). A group is a set G with a binary operation "$\circ$" such that

- G is closed under $\circ$.
- G is associative.
- There is an Identity Element: $\exists e \in G \mid x \circ e = e \circ x - x \; \forall x \in G$.
- Inverses: $\forall x \in G \; \exists y \in G \mid x \circ y = y \circ x = e$.

Definition 0.2. (Abelian Group). If $\circ$ is commutative in group G, we call G Abelian. In that case, G is often written additively; i.e. we use "$+$" for "$\circ$".

(If $\circ$ is not commutative, we often write G multiplicatively.)

Definition 0.3. (Subgroup). Let G be a group, and $\emptyset \neq H \subseteq G$. Then H is called a subgroup of G if H is also a group.

Definition 0.4. (Cyclic). A group G is called cyclic if $\exists g \in G$ (called generator) such that $G = \{g^n \mid n \in Z\}$.

Definition 0.5. (Equivalence). Let G be a group and H a subgroup. Define the relation $x \sim y$ if $xy^{-1} \in H$.

Definition 0.6. (Index). $[G : H]$ is the number of equivalence relations, which is called the index of H in G.

$$[G : H] = \frac{|G|}{|H|}.$$

Definition 0.7. (Order of an element). Let G be a group and $g \in G$. Then the order of $o(g)$ is the smallest positive integer n such that $g^n = e$. (May be infinite)

Definition 0.8. (Group Homomorphism). Let G_1, G_2 be groups. Then $\varphi : G_1 \to G_2$ is called a group homomorphism if

$$\varphi(xy) = \varphi(x)\varphi(y) \tag{0.1}$$

for all $x, y \in G_1$.

Definition 0.9. (Additional Terminology). There are some additional classifications of homomorphisms:

φ is called an isomorphism if φ is 1-1 and onto.

φ is called automorphism if φ is an isomorphism and $G_1 = G_2$

Definition 0.10. (Kernel and Image). Similar to linear algebra and linear transformations, we have kernel and image.

$$\ker\varphi \overset{\text{def}}{=} \{x \in G_1 \mid \varphi(x) = e_2\} \text{ where } e_2 \text{ is the identity in } G_2$$
$$\mathrm{im}\varphi \overset{\text{def}}{=} \{\varphi(x) \mid x \in G_1\}$$

We call G_2 the "codomain" of φ.

Definition 0.11. (Normal Subgroups). Let H be a subgroup of G. H is called normal if ghg^{-1} for all $g \in G$, $h \in H$.

$$gHg^{-1} \subseteq H \tag{0.2}$$

Definition 0.12. (Ideals). Let I be a proper (non-trivial) ideal in a commutative ring R.

- I is called prime ideal if for all $a, b \in R$, $ab \in I \Rightarrow a \in I$ or $b \in I$.
- I is called maximal ideal if for all ideals J with $I \subseteq J \subseteq R$, $J = I$ or $J = R$.

Definition 0.13. (Ring Homomorphism). Let R and S be commutative rings. A function $\phi : R \longrightarrow S$ is called a ring homomorphism if

$$\phi(a + b) = \phi(a) + \phi(b) \tag{0.3}$$

and

$$\phi(ab) = \phi(a)\phi(b) \tag{0.4}$$

for all $a, b \in R$.

A ring homomorphism that is one-to-one and onto is called an isomorphism. If there exists an isomorphism from R onto S, we say R is isomorphic to S, and write $R \cong S$.

Definition 0.14. (***). Let R, S be commutative rings. $\varphi : R \longrightarrow S$ a homomorphism. Then ${}^{R}/_{\ker(\varphi)} = \{[r] \mid r \in R\}$ where $r \sim s$ if $r - s \in \ker(\varphi)$. (or $\varphi(r) = \varphi(s)$).

Definition 0.15. (Witness). If p is not a prime, it is not necessarily true that $a^{p-1} \equiv 1 \pmod{()}p$. In that case we call "$a$" a <u>witness</u> for the compositeness of p.

Definition 0.16. (Discrete Logarithm). Given $g \in \mathbb{F}_p$ a primitive root (i.e. generator) and $a \in \mathbb{F}_p$, such that $a = g^n$, $n \in Z$, we say

$$n = \log_g(a). \tag{0.5}$$

By F.ℓ.T., if n_0 staisfies $a = g^{n_0}$, then so does $n = n_0 + (p-1)k$. We shall pick the unique solution of n in $\mathbb{Z}_{p-1}$ for the logarithm.