Appendix

(Groups)

A group $G = (S, \cdot)$ is a set S with a binary operator $(\cdot): S \times S \to S$ such that

1. $(\cdot)$ is associative, i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c \;\; \forall a, b, c \in S$
2. There exists an identity element $e \in S$ such that
$$e \cdot a = a = a \cdot e \quad \forall a \in S$$
3. Every element $a \in S$ has an inverse a^{-1} such that
$$a \cdot a^{-1} = e = a^{-1} \cdot a$$

Ex.

1. The set of $n \times n$ unitary matrices $U(n)$ together with matrix multiplication forms a group:
   1. $A(BC) = (AB)C$
   2. $IA = A = AI$, I is identity matrix
   3. $A^{-1} = A^{+}$ for any $A \in U(n)$

2. The set of integers modulo N together with addition forms a group, denoted $(\mathbb{Z}_N, +)$
   1. $a + (b + c) \equiv (a + b) + c \mod N$
   2. $0 + a \equiv a \equiv a + 0 \mod N$
   3. $a^{-1} = N - a \Rightarrow a + a^{-1} \equiv a + (N - a) \equiv N \equiv 0 \mod N$

E.g. for $N = 5$, $4^{-1} = 1$ since $4 + 1 = 5 \equiv 0 \mod N$

3. If N is prime, then the integers mod N together with integer multiplication mod N also forms a group, denoted $(\mathbb{Z}_N, \cdot)$

1. $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot c \mod N$
2. $1 \cdot a \equiv a \equiv a \cdot 1 \mod N$
3. $a^{-1} = x$ where $ax \equiv 1 \mod N$, which exists if a is coprime to N

E.g. for $N=5$, $4^{-1} = 4$ since $4 \cdot 4 = 16 \equiv 1 \mod 5$

4. What if $N = 10$? What is the multiplicative inverse of 2 mod 10? We would need ℓ, k satisfying

$$2 \cdot \ell = 1 + 10k$$

which is impossible since 2ℓ is even and $1+10k$ is odd.
In general, a has a multiplicative inverse mod N if and only if a & N are coprime.

For non-prime N, $(\mathbb{Z}_N^\times, \cdot)$ where $\mathbb{Z}_N^\times$ consists of the numbers $[0, N-1]$ which are coprime to N is a group.

(Notation)
We call $(\mathbb{Z}_N, +)$ the additive group of $\mathbb{Z}$ mod N and $(\mathbb{Z}_N^\times, \cdot)$ the multiplicative group of $\mathbb{Z}$ mod N.

More generally, we call G an additive group if the binary operation is most commonly thought of as addition, and in particular if it is commutative:

$$a + b = b + a$$

A group (not neccessarily additive) with a commutative operator (e.g. both $(\mathbb{Z}_N, +)$ and $(\mathbb{Z}_N^\times, \cdot)$ but <u>not</u> $U(n)$) is called an Abelian group.

(Order)

Let $G=(S,\cdot)$ be a group. The order of $a\in S$, denoted $|a|$, is the smallest integer r such that

$$a^r = \overbrace{a\cdot a\cdot\cdots\cdot a}^{r\text{ times}} = e$$

If no such integer exists, $|a|$ is infinite.

(Order of a group)

Let $G=(S,\cdot)$ be a group. The order of G is

$$|G|=|S|$$

Theorem

Let $G=(S,\cdot)$ be a finite group. For any $a\in S$,

$$|a| \mid |G| \quad (|a| \text{ divides } |G|)$$

Corollary

For any $a\in(\mathbb{Z}_N^\times,\cdot)$, $a^{\varphi(N)}\equiv 1 \mod N$.

Note that $|\mathbb{Z}_N^\times|=\varphi(N)$.

(Subgroups)

Let $G=(S,\cdot)$ be a group. Then $H=(T,\cdot)$ where $T\subseteq S$ and multiplication in H is the same as in G is a subgroup of G if

- $e\in T$
- $a\cdot b\in T$ for any $a, b\in T$
- $a^{-1}\in T$ for any $a\in T$

Ex.

Consider the group $(\mathbb{Z}_{10}, +)$. Its members are $S = \{0, 1, \ldots, 9\} = \mathbb{Z}_{10}$

Let $T = \{0, 2, 4, \ldots, 8\} = 2\mathbb{Z}_{10}$

Then $(2\mathbb{Z}_{10}, +)$ is a subgroup of $(\mathbb{Z}_{10}, +)$ since

- $0 \in T$
- $2a + 2b = 2(a+b) \in T \quad \forall 2a, 2b \in T$
- $(2a)^{-1} = 10 - 2a = 2(5-a) \in T \quad \forall 2a \in T$

Ex.

Let $G = \{U_1, U_2, \ldots, U_k\}$ be an inverse-closed set of $n \times n$ unitary matrices. We denote bi $\langle G \rangle$ the group generated by G which consists of all finite products of gates in G. Then $\langle G \rangle$ is a subgroup of $U(n)$.

- $I \in \langle G \rangle$ since I is the empty product.
- $UV \in \langle G \rangle \quad \forall U, V \in \langle G \rangle$ since UV itself is a finite product over G.
- $(U_1 \cdots U_k)^{-1} = U_k^{-1} \cdots U_1^{-1} \in \langle G \rangle \quad \forall U_1 \cdots U_k \in \langle G \rangle$

Theorem (Lagrange)

Let H be a subgroup of G. Then

$$|H| \mid |G| \quad (|H| \text{ divides } |G|)$$

(Cosets)

Let H be a subgroup of G and $a \in G$. The left coset of a and H is

$$a \cdot H = \{a \cdot b \mid b \in H\}$$

Note that if:

right coset $\{b \cdot a \mid b \in H\}$

- $a \in H$, then $a \cdot H = H$
- H & G are abelian, then $a \cdot H = \overbrace{H \cdot a}$

A subgroup H of G is called Normal, denoted

$$H \triangleleft G$$

if $a \cdot H = H \cdot a$ for all $a \in G$.

The left (resp. right) cosets of any subgroup H partition the group G. Normal subgroups however admit the important property that the set of cosets itself is a group defined as

$$G/H = \{a \cdot H \mid a \in G\}$$
$$(a \cdot H)(b \cdot H) = (a \cdot b) \cdot H$$

This group is called the quotient or factor group, and is informally the group of equivalence classes "mod H" — that is

$$a \sim_H b \iff a \in b \cdot H$$

Ex.

The group $(\mathbb{Z}_2, \oplus)$ is more accurately defined as

$$\mathbb{Z}/2\mathbb{Z}$$

where $\mathbb{Z} = (\mathbb{Z}, +)$ and $2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\}$

(Cyclic groups)

A group G is cyclic if it is generated by integer powers of a single element g. That is,

$$h = g^k = \overbrace{g \cdot g \cdots g}^{k} \quad \text{for some } k \in \mathbb{Z}$$

whenever $h \in G$.

Ex.

The group $(\mathbb{Z}_n, +)$ is cyclic for any n, since

$$a = a \cdot 1 = \overbrace{1 + 1 + \cdots + 1}^{a}$$

for any $a \in \mathbb{Z}_n$.

Another cyclic group is the multiplicative group of n^{th} roots of unity, $G = \{e^{2\pi i/n \cdot k} \mid k = 0, 1, \ldots, n-1\}$

(Group homomorphisms)

A group homomorphism from $(G, \cdot_G) \longrightarrow (H, \cdot_H)$ is a function $h : G \rightarrow H$ that preserves the group structure — in that

1. $h(e_G) = e_H$
2. $h(a^{-1}) = h(a)^{-1}$
3. $h(a \cdot_G b) = h(a) \cdot_H h(b)$

Two groups G & H are said to be isomorphic if there is a homomorphism from $G \rightarrow H$ and from $H \rightarrow G$. We say $G \simeq H$ in this case and view them as the same group up to representation.

Ex.

Let G be the multiplicative group of n^{th} roots of unity. Then $G \simeq \mathbb{Z}_n$ with isomorphisms

$$a \longleftrightarrow e^{2\pi i/n \, a\cdot b}, \quad b \in \{1, \dots, n-1\}$$

The representation of $a \in \mathbb{Z}_n$ as $e^{2\pi i/n \, a\cdot b} \in \mathbb{C}$ is an example of a character, which we use in the Fourier analysis of finite groups.

The next and final theorem, which is important in generalizations of Shor's algorithm, establishes that every finite Abelian group is a product, e.g.

$$\mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n}$$

of cyclic groups, and thus has a simple Fourier theory

(Fundamental theorem of finite Abelian groups)

Let G be a finite Abelian group. Then

$$G \simeq \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_k}$$

where each N_i is a prime power.