CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Tuesday, February 20 - Lecture 7.1

Reading: Appendix 2

Agenda:

1. Groups
2. Cosets, Quotient, etc.
3. Representations
4. Group algebra and regular representations

1 Groups

Intuition: "A group is an abstract symmetry type"

Definition. *A group G is a set with a binary operation*

$$\cdot : G \times G \to G$$

that satisfies the following axioms:

1. *Associativity*
2. *There exists an identity element e such that $ge = eg = g$ for all $g \in G$.*
3. *There exists an inverse for all $g \in G$ and $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$*

G is finite if $|G| < \infty$. We call $|G|$ the *order* of G. The *order* of $g \in G$ is $|g| = min\{k \geq 1 | g^k = e\}$.

A subgroup of G is a subset $H \subseteq G$ such that:

1. For all $h \in H$, $h^{-1} \in H$.
2. For all $h_1, h_2 \in H$, $h_1 h_2 \in H$

We write $H \leq G$ if it is a subgroup.
Given $x_1, ..., x_k \in G$ the sub group generated by them is:

$$\langle x_1, ..., x_k \rangle = \bigcap_{H \leq G} H$$

.
We call $\langle x \rangle$ the cyclic subgroup generated by x, since it consists of all powers of x (positive, negative and 0 powers).
Lemma: If $g \in G$, then $|g| = |\langle g \rangle|$.

Theorem 1 (Lagrange's Theorem)**.** *If $H \leq G$, then $|H|$ divides $|G|$.*

A group G is **abelian** or commutative, if for all $g_1, g_2 \in G$ we have $g_1 g_2 = g_2 g_1$.

1.1 Examples of Groups

1.1.1 $(\mathbb{Z}/N\mathbb{Z}, +)$

This is the group of addition mod N. It will be of great importance later when $N = 2^n$.

1.1.2 $((\mathbb{Z}/2\mathbb{Z})^n, +)$

Given $a_1, ...a_n$ and $b_1, ...b_n$, then $(a_1, ...a_n) + (b_1, ...b_n) = a_1 + b_1, ..., a_n b +_n$ where the addition is mod N.

Fact: Every finite abelian group is isomorphic to a group of the form

$$\bigoplus_{i=1}^{k} \mathbb{Z}/N_i\mathbb{Z}$$

where the $N_i s$ are positive integers. Here, note that if A and B are two groups, then

$$A \oplus B = \{(a, b) | a \in A, b \in B\}$$

is also a group. If we apply the Chinese remainder theorem, we can classify finite abelian groups as sums of cyclic groups of prime power order.

1.1.3 U(d)

This is the unitary group of $d \times d$ unitary matrices. Of course $|U(d)| = \infty$ In fact, it is uncountably infinite. Better yet,$U(d)$ is a "Lie group" meaning it is both a grup and smooth manifold, and can be understood rather well using its associated Lie algebra. It also has a subgroup $SU(d) \subseteq U(d)$.

$U(d)$ is not abelian unless $d = 1$.

1.1.4 S_n

The symmetric group on n elements. That is, the set of all permutations of the set $\{1, \ldots, n\}$:

$$S_n = \{F : \{1, ..., n\} \to \{1, ..., n\} \mid F \text{ is a bijection}\}.$$

S_n is not abelian unless $n = 2$.

Definition. *A* homomorphism *is a function*

$$\phi : G_1 \to G_2$$

such that

$$\phi(xy) = \phi(x)\phi(y)$$

for all $x, y \in G_1$. If ϕ is bijective, then it is called an isomorphism.

Theorem 2. *(Cayley's Theorem) Let $|G| = n$ and fix an enumeration of the elements of G, $G = \{x_1, ..., x_n\}$, for each $g \in G$, define*

$$L_g : \{1, ..., n\} \to \{1, ..., n\}$$

where j is the unique index such that $gx_i = x_j$. Then L_g is a well-defined bijective function. Moreover, the function

$$G \to S_n$$
$$g \mapsto L_g$$

is an injective group homomorphism.

Thus, every (finite) group is a subgroup of a permutation group.

1.2 Cosets, etc.

Given $H \leq G$ and $g \in G$, the left H-coset of g is

$$gh = \{gh | h \in H\}$$

Lemma: $g_1 H = g_2 H$ iff there exists $h \in H$ such that $g_2 = g_1 h$.

The set of all left H-cosets is denoted

$$G/H = \{gH | g \in G\}$$

Note: G/H is a partition of G in which each part has size $|H|$. This proves Lagrange's theorem.

We can also similarly define right H-cosets.

We say H is a *normal* subgroup if for all $g \in G$, $gH = Hg$. We denote this $H \trianglelefteq G$.

Theorem. *The following are equivalent*

- $H \trianglelefteq G$
- *The function* $(G/H) \times (G/H) \to G/H$ *and* $(g_1 H, g_2 H) \mapsto (g_1 g_2)H$ *is well defined and makes* G/H *a group. We call* G/H *with this group operation the quotient group (of G by* H*).*

Note for abelian G, all subgroups are normal.

If $\phi : G_1 \to G_2$ is a homomorphism, then the kernel is $\ker \phi = \{x \in G_1 | \phi(x) = 1\}$

Theorem 3. *(First Isomorphism theorem)*
If $\phi : G_1 \to G_2$ *is a homomorphism, then* $\phi(G_1) \leq G_2$, $\ker \phi \trianglelefteq G_1$ *and* $\phi(G_1) \cong G_1 / \ker \phi$.

2 Representations

Let V be a vector space over the complex numbers $\mathbb{C}$. Define the general linear group of V to be

$$GL(V) = \{F : V \to V \mid F \text{ is linear and bijective}\}.$$

If $V = \mathbb{C}^n$ we write $GL(n, \mathbb{C}) = GL(\mathbb{C}^n)$.

A *representation of a group* G on V is a homomorphism

$$\rho : G \to GL(V)$$

Suppose

$$\rho_1 : G \to GL(V_1)$$

$$\rho_2 : G \to GL(V_2)$$

are two representations. We say ρ_1 and ρ_2 are *isomorphic* if there exists an isomorphism of vector spaces

$$\Phi : V_1 \to V_2$$

such that

$$\rho_2(g) = \Phi \circ \rho_2(g) \circ \Phi^{-1}$$

for all $g \in G$. In other words for all $g \in G$ the following diagram commutes:

$$\begin{tikzcd} V_1 \arrow[r, "\rho(g)"] \arrow[d, "\Phi"'] & V_1 \arrow[d, "\Phi"] \\ V_2 \arrow[r, "\rho(g)"'] & V_2 \end{tikzcd}$$

A representation $\rho : G \to GL(v)$ is *unitary* if V is a finite-dimensional Hilbert space and $\rho(G) \subseteq U(V) \subseteq GL(V)$.

Lemma: Every representation over $\mathbb{C}$ of a finite group is isomorphic to a unitary representation.

Goal of representation theory:

1. Classify the representations of a group.
2. Understand how the representation of G reflects the underlying structure of G.

To this end, there are two types of representations we are interested in:

1. Faithful:
   $\rho : G \to GL(v)$ such that ρ is injective.
2. Irreducible, which we will define momentarily.

Note: Neither property implies the other.

A representation $\rho : G \to GL(v)$ is *reducible* if there exists a non-trivial, proper W such that $\rho(g)(W) \subseteq W$ for all $g \in G$.

An irreducible representation is a representation that is not reducible and not 0-dimensional. We often call these "irreps."

Lemma: Every 1-dimensional representation is an irrep.

In particular, the trivial 1-dimensional representation

$$\begin{aligned} \rho : G &\to GL(\mathbb{C}) = \mathbb{C}^\times = \mathbb{C} - \{0\} \\ g &\mapsto 1 \end{aligned}$$

is always irreducible.

Definition. *A conjugacy class if G is a subset of $C \subseteq G$ such that*

$$C = \{xgx^{-1} | x \in G\}$$

for some $g \in G$.

Theorem 4. *If G is a finite group, then the number of complex irreps of G (considered up to isomorphism) equals the number of conjugacy classes of G.*

The best way to prove this is by using "character theory". Given any representation $\rho : G \to GL(v)$, the *character* of ρ is

$$\begin{aligned} Tr_\rho : G &\to \mathbb{C} \\ g &\mapsto Tr(\rho(g)) \end{aligned}$$

Note: Tr_ρ is not a homomorphism. (It us a "class function," meaning it is constant on the conjugacy classes of G.)

Moreover, given any rep $\rho : G \to GL(v)$, there exists a unique collection of irreps $\rho_1, ..., \rho_k$ (possibly with multiplicities) such that

$$\rho \cong \bigoplus_{i=1}^{k} \rho_i$$

Corollary: If A is abelian, then it has $|A|$ many irreps.

Lemma: If A is abelian and $\rho : G \to GL(v)$ is irrep, then $\dim V = 1$.

Proof: By prior lemma, we can assume ρ is unitary. In particular for all $a \in A$, $\rho(a)$ is unitary. However, we know that unitary matrices are diagonalizable. Since A is Abelian, the $\rho(a)$ are simultaneously diagonalizable. Now, let $\beta = \{\vec{v}_1, ..., \vec{v}_n\}$ be basis for which we have a diagonal representation for each $i = 1, ..., n$ in the one-dimensional subspace. Clearly span$\{\vec{v}_i\}$ is invariant under the A action. Because ρ is assumed to be irreducible, we conclude that $\vec{v}_i$ must span all of V. In other words, V is 1-dimensional, as desired.

Thus, the irreps of an abelian group A are the same thing as a homomorphism $A \to U(1)$.

Definition. . *If A is a (finite) abelian group, then the* dual group *is the set of all irreducible representations of A:*

$$\hat{A} := Hom(A, U(1))$$

The group operation is defined as follows. Given

$$\rho_1 : A \to U(1)$$

$$\rho_2 : A \to U(1)$$

define

$$\begin{aligned} \rho_1 \otimes \rho_2 : A &\to U(1) \\ a &\mapsto \rho_1(a)\rho_2(a) \end{aligned}$$

Theorem 5. *(Pontryagin duality) Let A be a finite abelian group, then*

1. *$\otimes$ makes $\hat{A}$ into an abelian group.*
2. *$\hat{A} \cong A$ (But NOT naturally)*
3. *$\hat{\hat{A}} \cong A$ (Naturally)*