Lecture 2
Background - Discrete mathematical structures: Groups

MIEFis - Quantum Computation, L. S. Barbosa, 2020-21

Summary

Reversibility. Groups as a prototypical algebraic structure. Groups of permutations. Cayley's theorem. Action of a group. Cosets.

Basic definitions

A group (G, θ, u) is a set G with a binary operation θ which is associative, and equipped with an identity element u and an inverse:

$$a^{-1}\theta a \;=\; u \;=\; a\theta a^{-1}$$

Note that a *monoid* lacks inverse, and a *semigroup* also drops the identity element.

A morphism $h : (G, \theta, u) \longrightarrow (G', \theta', u')$ between two groups is a function $h : G \longrightarrow G'$ between their carriers preserving the binary operation, i.e.

$$h(a\theta b) \;=\; h(a)\theta' h(b)$$

Properties:

1. left cancellation: $a\theta b = a\theta c \;\Rightarrow\; b = c$ because

$$\begin{array}{ll} & a\theta b = a\theta c \\ \Rightarrow & \quad \{\ x = y \Rightarrow z\theta x = z\theta y\ \} \\ & a^{-1}\theta(a\theta b) = a^{-1}\theta(a\theta c) \\ = & \quad \{\ \theta \text{ associative}\ \} \\ & (a^{-1}\theta a)\theta b = (a^{-1}\theta a)\theta c \\ = & \quad \{\ \text{definition of inverse}\ \} \\ & u\theta b = u\theta c \\ = & \quad \{\ \text{unit}\ \} \\ & b = c \end{array}$$

   Right cancellation: $b\theta a = c\theta a \;\Rightarrow\; b = c$

2. $a^{-1^{-1}} \;=\; a$. because

$$\begin{array}{ll} & a^{-1}\theta a^{-1^{-1}} = u = a^{-1}\theta a \\ = & \quad \{\ \text{cancellation}\ \} \\ & a^{-1^{-1}} = a \end{array}$$

3. $(a\theta b)^{-1} = b^{-1}\theta a^{-1}$. Indeed $b^{-1}\theta a^{-1}$ is the inverse of $a\theta b$ because

$$
\begin{array}{cl}
 & (b^{-1}\theta a^{-1})\theta(a\theta b) \\
\Rightarrow & \qquad \{\ \theta \text{ associative} \} \\
 & b^{-1}\theta(a^{-1}\theta a)\theta b \\
= & \qquad \{\ \text{definition of inverse} \} \\
 & b^{-1}\theta u\theta b \\
= & \qquad \{\ \text{identity} \} \\
 & b^{-1}\theta b \\
= & \qquad \{\ \text{definition of inverse} \} \\
 & u
\end{array}
$$

4. The equation $a\theta x = b$ has a unique solution $x = a^{-1}\theta b$. First confirm it is indeed a solution:

$$
\begin{array}{cl}
 & a\theta(a^{-1}\theta b) \\
\Rightarrow & \qquad \{\ \theta \text{ associative} \} \\
 & (a\theta a^{-1})\theta b \\
= & \qquad \{\ \text{definition of inverse} \} \\
 & u\theta b \\
= & \qquad \{\ \text{identity} \} \\
 & b
\end{array}
$$

   Then, cancellation entails uniqueness. Suppose y is another solution; then,

$$a\theta x = b = a\theta y$$

   which, by cancellation, entails $x = y$.

The cancellation law also proves a basic property of morphisms: that every group morphism preserves the group structure. If h is a group morphism, it preserves the binary operation, by definition. But it also preserves unit and inverse. Indeed,

$$h(a)\theta h(a^{-1}) = h(a\theta a^{-1}) = h(u) = u' = h(a)\theta(h(a))^{-1}$$

which entails $h(a^{-1}) = (h(a))^{-1}$ by cancellation. On the other hand

$$h(u)\theta h(u) = h(u\theta u) = h(u) = h(u)\theta u'$$

which entails $h(u) = u'$.

Examples

- Both $(\mathbb{R}^+, \times, 1)$ and $(\mathbb{R}^+, +, 0)$ are groups. Functions ln_e and e^- are the components of a bijection between them.
- The additive group of integers modulo 2 is isomorphic to the multiplicative group over $\{-1, 1\}$ through the correspondence $0 \mapsto 1, 1 \mapsto -1$.
- Permutations also form a group:

  $$S_n = (\{\sigma : n \longrightarrow n \mid \sigma \text{ is a permutation}\}, \cdot, id)$$

  is called the *symmetry group of degree* n. Clearly, it has $n!$ elements: the image of the first element is chosen arbitrarily; the second can be chosen in $n - 1$ ways, and so on.

Permutations over the set of all points of a two-dimensional geometrical figure that preserves distances (i.e. the distance between points a and b is the same as the distance between their images) are called *symmetries*. For example, consider an equilateral triangle. There are six ways in which its vertices may be re-arranged corresponding to rotations of 120°, 240° and 360°, and reflections in the altitudes through the three vertices. Since any symmetry of the equilateral triangle is determined by its effect on the vertices, this set contains all the symmetries of the triangle.

Groups can also be formed from other groups. For example the *product* of two groups G_1 and G_2 is still a group, with

$$\begin{aligned} (a, b)\theta(c, d) &= (a\theta_1 c), (b\theta_2 d) \\ u &= (u_1, u_2) \end{aligned}$$

Another important notion is that of a *subgroup*: A group H is a subgroup of another group G if the carrier of H is a subset of the carrier of G and the inclusion is a group morphism. In an equivalent way one may say that a subset of the carrier of a group G is the carrier of a subgroup of G iff it is closed for the group binary operation, its unit and inverse.

As an exercise you may prove that the intersection of two subgroups of the same group is still a subgroup.

Cayley's Theorem

The set of bijections $f : X \longrightarrow X$ over a set X with functional composition forms a group of *transformations* (which is the identity? And the inverse?), which is called a transformation group. For example, the group of symmetries of a planar figure (e.g. the equilateral triangle discussed above) is a transformation group on the set of points of this figure.

The following is a main result in the theory of groups:

Theorem.

Every group is isomorphic to a group of transformations

Proof.

Let (G, θ, u) be a group. For each element a of G define a map $f_a : G \longrightarrow G$ such that $f_a(x) = a\theta x$.

Let us show that a new group T can be defined over the set of transformations above:

1. The (functional) composition of two elements of T is in T:

$$(f_a \cdot f_b)(x) = f_a(f_b(x)) = f_a(b\theta x) = a\theta(b\theta x) = (a\theta b)\theta x = f_{a\theta b}(x)$$

2. For identity,

$$f_u(x) = u\theta x = x$$

3. For inverse,

$$f_a \cdot f_{a^{-1}}(x) = a\theta(a^{-1}\theta x) = (a\theta a^{-1})\theta x = u\theta x = x$$

We have proved that T is a group (note that axioms are inherited from the properties of function composition restricted to bijections). It remains to show that T is *isomorphic* to G. Let $h : G \longrightarrow T$ be defined by $h\,(a) = f_a$.

- Clearly $h(a\theta b) = f_{a\theta b} = f_a \cdot f_b = h(a) \cdot h(b)$, $h(u) = f_u$ (which is the identity) and $ha^{-1} = f_{a^{-1}} = h(a^{-1})$. Thus h is a homomorphism between both groups.
- T is entirely composed of bijections f_a for every element $a \in G$, thus h is a surjection.
- If $a \neq b$, then $h(a) = f_a \neq f_b = h(b)$; thus h is injective.

□

If (G, θ, u) is a finite group, this isomorphism can be depicted in a tabular form: each f_a is the permutation

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ a\theta x_1 & a\theta x_2 & \cdots & a\theta x_n \end{bmatrix}$$

which means, in other words, that f_a is the permutation given by row a in the table for θ.

A morphism of a group (G, θ, u) to a transformation group is called a *representation* of G. Of course, a group may have a number of different representations. The specific one built for the proof of Cayley's theorem is usually called the *left regular representation* of G.

Action of a group

A group (G, θ, u) acts over a set X through a function (the action) $\tau : G \times X \longrightarrow X$ which satisfies the following properties:

$$\tau(u, x) = x \quad \text{and} \quad \tau(g\theta f, x) = \tau(g, (\tau(f, x))$$

For example, if G is a transformation group consisting of permutations p on a set X, a function mapping

$$(p, x) \ \mapsto \ p(x)$$

for all p in G and $x \in X$, defines an action of G on set X.

As an exercise, show that every group (G, θ, u) acts over itself through the map $(g, x) \mapsto g\theta x\theta g^{-1}$. Exemplify with $G = (\mathbb{N}, +, 0)$.

Cosets

Given an element a of a group (G, θ, u) and a subgroup H of G, the set

$$aH \ = \ \{a\theta h \mid h \text{ in } H\}$$

is called the (left) *coset* of H in G wrt element a. Similarly a right coset is defined as follows

$$Ha \ = \ \{h\theta a \mid h \text{ in } H\}$$

The two notions coincide for Abelian groups.

Examples

- for $G = (\{-1, 1\}, \times, 1)$ and $H = (\{1\}, \times, 1)$, the cosets for elements -1 and 1 are, respectively, $\{-1\}$ and $\{1\}$.
- for $G = (\mathbb{Z}, +, 0)$ and a subgroup $H = (m\mathbb{Z}, +, 0)$, for an integer m, where

  $$m\mathbb{Z} \ = \ \{\cdots, -2m, -m, 0, m, 2m, \cdots\}$$

  The (left) cosets are the sets $m\mathbb{Z}$, $m\mathbb{Z} + 1$, ..., $m\mathbb{Z}(m - 1)$, where

  $$m\mathbb{Z} + x \ = \ \{\cdots, -2m + x, -m + x, x, m + x, 2m + x, \cdots\}$$

  Note that the number of cosets is exactly m because $m\mathbb{Z} + m = m(\mathbb{Z} + 1) = m\mathbb{Z}$.

The notion of a coset is a fundamental tool in the study of groups. Basically, it provides a way to decompose the carrier of a group into disjoint, equal-size subsets. To further discuss this first observe the following result:

Theorem. For H a subgroup of G

$$Ha = Hb \quad \Leftrightarrow \quad a\theta b^{-1} \text{ in } H$$

(or, dually, $aH = bH \;\Leftrightarrow\; b^{-1}\theta a$ in H)

Proof.

- If $Ha = Hb$, then $a = u\theta a \in Ha = Hb$, and so there is x in H with $a = x\theta b$, i.e. $a\theta b^{-1} = x$ in H.
- Conversely, assume $a\theta b^{-1} = s$ in H, i.e. $a = s\theta b$. To prove that $Ha = Hb$ consider again two cases:
  - If $x \in Ha$, then $x = z\theta a$ for some z in H. Thus, $x = z\theta s\theta b \in Hb$.
  - Similarly, if $y \in Hb$, then $y = z'\theta b$ for some z' in H, and $y = z'\theta s^{-1}\theta a \in Ha$.

□

A second observations is the following:

Theorem. Any two right (or any two left) cosets of H in G are either identical or disjoint.

Proof. This is proved by showing that if there is an element $x \in Ha \cap Hb$, then $Ha = Hb$. This element has the form $z\theta b = x = w\theta a$ for z, w in H. Thus, $a\theta b^{-1} = w^{-1}z$ in H and, by the previous result $Ha = Hb$.

□

This property tells that the right cosets of a subgroup H of G forms a partition of G: each such coset is nonempty, and G is their disjoint union. Indeed, the right cosets of H in G are the equivalence classes of the following equivalence relation over the carrier of G:

$$a \equiv b \quad \Leftrightarrow \quad a\theta b^{-1} \text{ in } H$$

Actually, a similar result holds for left cosets. Moreover, the number of right cosets of H in G is equal to the number of left cosets of H in G. This number is called the *index* of H in G. In a finite group this number measures the relation between the cardinality of the carrier of G (called the *order* of G) and that of H.

To see this, recall that G can be partitioned into its right cosets:

$$G \;=\; Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n$$

and, thus, $\sum_i |Hx_i|$ gives the cardinality of G. Function $\phi_i : H \longrightarrow Hx_i$ given by $\phi_i a = a\theta x_i$ is a bijection, making $|Hx_i|$ equal to the order of H. So, we conclude that $|G| = n|H|$ where n is the index of H in G. In group thoery, this result is known as the *theorem of Lagrange*.