Lecture 10  Subgroups, isomorphisms, Cayley's theorem

Recall: \( G \) a group, \( a \in G \) get functions

\[
L_a : G \to G \quad L_a(x) = ax
\]
\[
R_a : G \to G \quad R_a(x) = xa
\]

Proposition  \( L_a \) and \( R_a \) are bijective.

Corollary (Cancellation laws) \( G \) a group, \( a, x, y \in G \).

(i) If \( ax = ay \), then \( x = y \).

(ii) If \( xa = ya \), then \( x = y \).

Proof (i) \( ax = ay \) means \( L_a(x) = L_a(y) \). Since \( L_a \) is injective, we deduce \( x = y \).

(ii) \( xa = ya \) means \( R_a(x) = R_a(y) \). Since \( R_a \) is injective, we deduce \( x = y \).

For any set \( X \), we have a group \( \text{Sym}(X) = \{ f \mid f: X \to X \text{ is a bijective function} \} \). This is called the symmetric group of \( X \).

Now \( L_a : G \to G \) is bijective, so \( L_a \in \text{Sym}(G) \).

This actually defines a function

\[
\{ G \to \text{Sym}(G) \}
\]

\( \mapsto \{ g \mapsto L_g \} \)

This function is itself injective, for if \( L_g = L_h \), then \( L_g(e) = L_h(e) \) and \( ge = he \) and \( g = h \).

This may suggest to investigate the following.

Def  If \( G \) is a group, a subset \( H \subseteq G \) is a subgroup if the binary operation of \( G \), restricted to elements of \( H \), makes \( H \) into a group. We write \( H \leq G \).
Ex: \( G = (\mathbb{Z}, +) \), \( H = 2\mathbb{Z} \) = set of even integers.

If \( n \) and \( m \) are even, \( nm \) is even, so
+ : \( 2\mathbb{Z} \times 2\mathbb{Z} \to 2\mathbb{Z} \) makes sense as an operation.
0 \( \in 2\mathbb{Z} \) so identity exists.
If \( n \) is even, \(-n\) is, so inverses exist in \( 2\mathbb{Z} \).
So \( H = 2\mathbb{Z} \) is a subgroup of \( G = \mathbb{Z} \); \( 2\mathbb{Z} \leq \mathbb{Z} \).

Ex: \( \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq (\mathbb{C}, +) \).

Nonexample: \( (N, +) \) is NOT a subgroup of \( (\mathbb{Z}, +) \).

How to show something is a subgroup?

Proposition: Let \( G \) be a group, \( H \leq G \) a nonempty subset.
\( H \) is a subgroup of \( G \) if and only if.
(i) For all \( h_1, h_2 \in H \), we have \( h_1 \cdot h_2 \in H \).
(ii) For all \( h \in H \), we have \( h^{-1} \in H \).

[That is, \( H \) is closed under multiplication and inverses.]

Proof: Conditions (i) and (ii) are clearly necessary, as they are part of the definition of a group.

To see that they are sufficient: Observe that (ii) says that the operation of \( G \) restricts to a function
\( o: H \times H \to H \).

Associativity follows from associativity in \( G \).

Identity: take any \( h \in H \). By (ii) \( h^{-1} \in H \). By (i) \( hh^{-1} = e \in H \).
So \( H \) has the identity element of \( G \) in it (and this is also an identity element for \( H \)).

Inverses: just a restatement of (ii).
Example: \( G \) a group. \( H = \{ L_g \mid g \in G \} \subseteq \text{Sym}(G) \).

We show \( H \) is a subgroup of \( \text{Sym}(G) \):

(i) Let \( L_{g_1}, L_{g_2} \in H \). Then \( L_{g_1} \circ L_{g_2} = L_{(g_1 g_2)} \in H \). \( \checkmark \)

(ii) Let \( L_g \in H \). Then \( L_g^{-1} = L_{g^{-1}} \in H \). \( \checkmark \).

Another way two groups can be related:

Def. Let \( G \) and \( H \) be groups. A function \( \varphi: G \to H \) is called an isomorphism if:

(i) \( \varphi \) is bijective.

(ii) For all \( g_1, g_2 \in G \), \( \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) \).

More pedantically: \( \varphi(g_1 \circ g_2) = \varphi(g_1) \circ \varphi(g_2) \).

Where \( \circ \) is the binary operation in \( G \), and \( \circ \) \( H \) is the one in \( H \).

Example: \( G \) a group. \( H = \{ L_g \mid g \in G \} \subseteq \text{Sym}(G) \).

Then \( \varphi: G \to H \), \( \varphi(g) = L_g \) is an isomorphism:

(i) Already checked \( \varphi \) is injective, surjective by construction.

(ii) We showed \( L_{g_1} \circ L_{g_2} = L_{g_1 g_2} \), so

\( \varphi(g_1) \varphi(g_2) = L_{g_1} \circ L_{g_2} = L_{g_1 g_2} = \varphi(g_1 g_2) \).

Proposition: If \( \varphi: G \to H \) is an isomorphism of groups, then \( \varphi(e_G) = e_H \) and \( \varphi(g^{-1}) = \varphi(g)^{-1} \).

Proof: Pick \( h \in H \). Since \( \varphi \) is surjective, \( \varphi(g) = h \) for some \( g \in G \).

Then \( h = \varphi(g) = \varphi(e_G g) = \varphi(e_G) \varphi(g) = \varphi(e_G) h \).
Thus \( e_H \cdot h = h = \varphi(e_G) \cdot h \). By cancellation of \( h \), we deduce \( e_H = \varphi(e_G) \).

Consider \( gg^{-1} = e_G \), and apply \( \varphi \) to both sides

\[
\varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) \quad \text{so} \quad \varphi(g)\varphi(g^{-1}) = e_H \\
\varphi(e_G) = e_H
\]

By Prop 2.1.2, \( \varphi(g^{-1}) = \varphi(g)^{-1} \).

If there is an isomorphism \( \varphi : G \to H \), we say that \( G \) and \( H \) are isomorphic, written \( G \cong H \).

Ex. \( G \) is isomorphic to \( H = \{ g \in G \mid g \in G \} \leq \text{Sym}(G) \)

This proves

Cayley's Theorem: Any group \( G \) is isomorphic to a subgroup of a symmetric group.

Discussion: Originally, only "concrete" groups of transformations, such as permutations, were considered. Then the modern notion of abstract group was introduced. (This is the definition we use in this course.) There is then a question of whether every abstract group has a "concrete realization" as a collection of permutations of some set. Cayley's theorem says that the answer is yes.