Graduate Algebra, Fall 2014
Lecture 3

Andrei Jorza

2014-09-01

1 Group Theory

1.3 Subgroups (supplemental)

Example 1. Some more examples of subgroups:

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are subgroups.
2. $\mathrm{GL}(n, \mathbb{Q}) \subset \mathrm{GL}(n, \mathbb{R}) \subset \mathrm{GL}(n, \mathbb{C})$ are subgroups.
3. The following are subgroups (for $R = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$):

$$\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} | b \in R\} \subset \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | a \in R^\times, b \in R\} \subset \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a, c \in R^\times, b \in R\} \subset \mathrm{GL}(2, R)$$

Example 2. Some special subgroups:

1. $\{e\}$ and G are the non-proper subgroups of G.
2. The center $Z(G)$ of a group G is defined as $Z(G) = \{g \in G | gx = \gamma, \forall x \in G\}$. Then $Z(G)$ is a subgroup.
3. The commutator $[a, b] = aba^{-1}b^{-1}$ and $[G, G] = \langle [a, b] | a, b \in G \rangle$ is a subgroup. Indeed, $[a, b]^{-1} = [b, a]$ but a product of commutators need not be a commutator. For example $G = S_3 = \{1, (12), (13), (23), (123), (132)\}$ has center $Z(S_3) = 1$ and commutator $\langle 1, (123), (132) \rangle = \{1, (123), (132) = (123)^2\}$ which is a subgroup since (123) has order 3.
4. If $X \subset G$ then $\langle X \rangle = \{\prod a_i | a_i \text{ or } a_i^{-1} \in X\}$.

1.5 Homomorphisms

Suppose $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$ are two groups.

Definition 3. A map $f : G \to H$ is said to be a **homomorphism** if $f(x \cdot_G y) = f(x) \cdot_H f(y)$ for all $x, y \in G$.

Proposition 4. *If $f : G \to H$ is a homomorphism then:*

1. $f(e_G) = e_H$.

2. $f(x^{-1}) = f(x)^{-1}$.

Proof. $f(x) = f(e_g x) = f(e_G)f(x)$ for all $x \in G$ and so $f(e_G) = e_H$. Also $e_H = f(e_G) = f(xx^{-1}) = f(x)f(x^{-1})$ and the second property follows. □

Definition 5. Suppose $f : G \to H$ is a homomorphism of groups. The kernel is $\ker(f) = \{g \in G | f(g) = e\}$ and $\mathrm{Im}(f) = \{f(g) | g \in G\}$. The homomorphism f is said to be an isomorphism if it is bijective as a function.

Proposition 6. *Let $f : G \to H$ be a homomorphism.*

1. $\ker f \subset G$ *and* $\mathrm{Im}\, f \subset H$ *are subgroups.*
2. f *is injective iff* $\ker f = 1$ *and surjective iff* $\mathrm{Im}\, f = H$.
3. *If f is an isomorphism then $f^{-1} : H \to G$ is also a homomorphism, which is then necessarily an isomorphism.*
4. *If f is an injective homomorphism then $G \cong \mathrm{Im}\, f$.*

Proof. If $f(x) = 1$ and $f(y) = 1$ then $f(xy^{-1}) = f(x)f(y)^{-1} = 1$ and so $\ker f \subset G$ is a subgroup. Similarly, $f(x)f(y)^{-1} = f(xy^{-1}) \in \mathrm{Im}\, f$ and so $\mathrm{Im}\, f \subset H$ is a subgroup as well.

Have $f(x) = f(y)$ iff $f(x)f(y)^{-1} = 1$ iff $f(xy^{-1}) = 1$ iff $xy^{-1} \in \ker f$.

Since $f(x)f(y) = f(xy)$ it follows that $f^{-1}(f(x)f(y)) = xy = f^{-1}(f(x))f^{-1}(f(y))$ and so f^{-1} is also a homomorphism.

The last part is by definition. □

Definition 7. Two groups G and H are said to be isomorphic if there exists an isomorphism between them.

Example 8.

1. The n-roots of unity in $\mathbb{C}$ form a group μ_n wrt multiplication. The map $\mathbb{Z}/n\mathbb{Z} \to \mu_n$ given by $k \mapsto \exp(2\pi i k/n)$ is an isomorphism of groups.
2. The map $\mathbb{Z} \to n\mathbb{Z}$ given by $f(x) = nx$ is an isomorphism of infinite cyclic groups.
3. This example I did in lecture 2 but fits better here. Suppose G is a finite group with n elements. For $g \in G$ let $\sigma_g : G \to G$ given by $\sigma_g(h) = gh$. This is clearly injective and since $\sigma_g^{-1} = \sigma_{g^{-1}}$ it is also bijective. Note that $\sigma_g \circ \sigma_{g'} = \sigma_{gg'}$ and so we get a homomorphism $\sigma : G \to S_G$ from G to the set S_G of permutations of G. Since $\sigma_g = \sigma_{g'}$ if and only if $g = g'$ (evaluate at 1) we get an injective homomorphism from G into $S_n = S_G$. Thus we realized $G \cong \mathrm{Im}\, f \subset S_n$.
4. Consider the map $f : S_n \to \mathrm{GL}(n, \mathbb{Q}) \cong \mathrm{Aut}_{\mathbb{Q}-\mathrm{vs}}(\mathbb{Q}^n)$ taking the permutation $\sigma \in S_n$ to the $n \times n$ matrix with 0-s everywhere except at $(i, \sigma(i))$ for all i where there is a 1. For example

$$f(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}) = \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}$$

   What is $f(\sigma)f(\tau)$ for $\sigma, \tau \in S_n$? Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{Q}^n$. Then $f(\sigma)$ is the matrix wrt this basis of the linear map $T_\sigma : \mathbb{Q}^n \to \mathbb{Q}^n$ taking $\sum x_i e_i$ to $\sum x_i e_{\sigma(i)}$. Thus $f(\sigma)f(\tau)$ is the matrix of $T_\sigma \circ T_\tau$ which takes $\sum x_i e_i$ to $T_\sigma(\sum x_i e_{\tau(i)}) = \sum x_i e_{\sigma(\tau(i))}$ and so $T_\sigma \circ T_\tau = T_{\sigma\tau}$ and thus $f(\sigma)f(\tau) = f(\sigma\tau)$ which shows that f is a homomorphism. It's also clearly injective.

   Thus we realized S_n as a subgroup of $\mathrm{GL}(n, \mathbb{Q})$. This is the first instance of realizing a group as a subgroup of a matrix group using a "faithful linear representation", which is a very powerful tool about which we'll learn in representation theory.

1.6 The alternating group A_n

Proposition 9. *There is a homomorphism $\varepsilon : S_n \to \{-1, 1\}$ such that $\varepsilon((i_1, \ldots, i_k)) = (-1)^{k-1}$.*

Proof. Let $f : S_n \to \mathrm{GL}(n, \mathbb{Q})$ as above and take $\varepsilon(\sigma) = \det f(\sigma)$. Then ε is a homomorphism $S_n \to \mathbb{Q}^\times$. We'd like to check that $\varepsilon(\sigma) = \pm 1$ for every permutation σ.

What is $\det f(\sigma)$? It is the linear map $\wedge^n f(\sigma) : \wedge^n \mathbb{Q}^n \to \wedge^n \mathbb{Q}^n$. Explicitly, it is $\wedge^n f(\sigma) e_1 \wedge \ldots \wedge e_n = (f(\sigma)e_1) \wedge \ldots \wedge (f(\sigma)e_n) = e_{\sigma(1)} \wedge \ldots \wedge e_{\sigma(n)} = \pm e_1 \wedge \ldots \wedge e_n$ a number which is 1 if σ has an even number of inversions and -1 otherwise.

There is something more general to be said. Suppose that $f(\sigma)$ has integer entries. Then the above explanation implies that $\det f(\sigma) \in \mathbb{Z}$. Note that $f(\sigma)^{-1} = f(\sigma^{-1})$ and so $I_n = f(\sigma) f(\sigma^{-1})$ and so $1 = \varepsilon(\sigma)\varepsilon(\sigma^{-1})$ and each of the two factors is an integer. Thus again we get that $\varepsilon(\sigma) = \pm 1$ indirectly this time.

Finally $\varepsilon((ij)) = -1$ and the conclusion follows from writing the cycle as a product of transpositions. □

Definition 10. Let $A_n \subset S_n$ be the subgroup $A_n = \ker \varepsilon$ of the sign homomorphism ε.