Graduate Algebra, Fall 2014
Lecture 2

Andrei Jorza

2014-08-29

1 Group Theory

1.3 Subgroups

Recall that for a group G and $a \in G$ we defined $\mathrm{ord}(a)$ to be the smallest positive exponent of a that equals the identity element, or infinity if no such exponent exists.

Example 1. The order of 2 in the multiplicative group $(\mathbb{Z}/15\mathbb{Z})^\times$ is 4 because $2^4 \equiv 1 \pmod{15}$ but no smaller exponent is 1.

Also we wrote $\langle a \rangle = \{a^n | n \in \mathbb{Z}\} \subset G$. If $\mathrm{ord}(a) = \infty$ this was the infinite cyclic group and if $\mathrm{ord}(a) = n$ then $\langle a \rangle$ is a set of cardinality 1, consisting of $\{1, a, a^2, \ldots, a^{n-1}\}$.

Definition 2. A subgroup H of a group G is a subset of G, closed under multiplication in G, containing the identity of G and such that every element of H has an inverse in H.

Proposition 3. *Let G be a group and H a nonempty subset of G. Then H is a subgroup if and only if for all $a, b \in H$, $ab^{-1} \in H$.*

Proof. For $a \in H$, $aa^{-1} = e \in H$. For $a \in H$, $ea^{-1} = a^{-1} \in H$. For $a, b \in H$ also $b^{-1} \in H$ and so $ab = a(b^{-1})^{-1} \in H$ so H is a subgroup. □

Definition 4. If $X \subset G$ is a subset define $\langle X \rangle$ as the smallest subgroup of G containing X. For example $\langle a \rangle$ is the smallest subgroup of G containing a.

Example 5. Computing $\langle X \rangle$ is rarely easy, and most of the time relies on complicated combinatorics.

1. If $m \in \mathbb{Z}$ then $\langle m \rangle \subset (\mathbb{Z}, +)$ is the set $m\mathbb{Z} = \{km | k \in \mathbb{Z}\}$.

2. If $m, n \in \mathbb{Z}$ such that $(m, n) = 1$ then by the Euclidean algorithm one can find $p, q \in \mathbb{Z}$ such that $pm + qn = 1$. Let $H = \langle m, n \rangle$. Since $m, n \in H$ and H is a subgroup also $pm + qn = 1 \in H$. But then for all $k \in \mathbb{Z}$ also $k = k \cdot 1 \in H$ and so $H = \mathbb{Z}$.

3. Here is a complicated example based on combinatorics that has applications in complex analysis. The set $\mathrm{SL}(2, \mathbb{Z})$ of 2×2 matrices with determinant 1 and integer entries is a group (show this!). The subgroup generated by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is the entire group $\mathrm{SL}(2, \mathbb{Z})$.

4. You'll see some more examples in the second homework.

1.4 Symmetric groups and dihedral groups

1.4.1 S_n

Let S_n be the set of all bijective functions $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$. Together with composition of functions as a binary operator S_n is a group with unit the identity function. Elements of S_n are often written as

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Multiplication of matrices can be done easily visually. Here is a self-explanatory example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 4 & 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

Note that S_{n-1} is a subgroup of S_n consisting of all permutations of $\{1, 2, \dots, n-1\}$, fixing n.

On the homework you will show that S_n has cardinality $|S_n| = n!$.

1.4.2 D_{2n}

Let P be a regular n-gon, whose vertices correspond to the n roots of unity of order n in $\mathbb{C}$. Look at all symmetries of P, i.e., all operations on P that preserve P but move its vertices around. Two: examples: R is rotation counterclockwise by $2\pi/n$ and F is flip with respect to the x-axis.

Symmetries can be composed, in other words, applied sequentially. Thus F^2 is applying twice F and so $F^2 = 1$ where 1 is the identity map. Moreover R^n is rotation by 2π and again this is the identity map so $R^n = 1$. Also see that $RF = FR^{-1} = FR^{n-1}$. The group D_{2n} is generated by R and F and consists of

$$D_{2n} = \{1, R, \dots, R^{n-1}, F, FR, \dots, FR^{n-1}\}$$

Using $R^n = 1, F^2 = 1, RF = FR^{n-1}$ it is clear that any combination of rotations and flips can be written as R^k or FR^k and so D_{2n} has cardinality $|D_{2n}| = 2n$.

Note that D_{2n} is a noncommutative group (when $n \geq 3$) of order $2n$ which contains the cyclic group $\langle R \rangle$ of order n.

1.4.3 Cycles in S_n

Definition 6. A cycle $(i_1, \dots, i_k)$ is a permutation $\sigma \in S_n$ such that $\sigma(j) = j$ for $j \notin \{i_1, \dots, i_k\}$, $\sigma(i_u) = i_{u+1}$ for $u < k$ and $\sigma(i_k) = i_1$. The length of a cycle is $|(i_1, \dots, i_k)| = k$. A cycle of length 2 is (ij), only flips i and j and is called a transposition. All cycles of length 1 are equal to the identity element and instead of (i) we simply write $()$.

Two cycles $c_1 = (i_1, \dots, i_k)$ and $c_2 = (j_1, \dots, j_s)$ are said to be disjoint if $i_u \neq j_v$ for all u, v.

Proposition 7.

1. *If c_1, c_2 are disjoint cycles then $c_1c_2 = c_2c_1$.*
2. *A cycle $c = (i_1, \dots, i_k)$ of length k has order k.*
3. *$(i_1, \dots, i_k) = (i_1i_2)(i_2i_3) \cdots (i_{k-1}i_k)$.*
4. *Every $\sigma \in S_n$ can be written as a product $\sigma = c_1 \cdots c_k$ where c_i are disjoint cycles. This expression is unique up to permuting the order of the cycles.*
5. *Every $\sigma \in S_n$ can be written as a product of transpositions, but no uniquely.*

Proof. Most are straightforward, but let me show the fact that permutations are products of disjoint cycles. Here is an algorithm. Start with $a_1 = 1$ and construct the cycle $c_1 = (a_1, \sigma(a_1), \sigma^2(a_1), \ldots)$. Let a_2 be the smallest number between 1 and n that does not appear in c_1 and let $c_2 = (a_2, \sigma(a_2), \sigma^2(a_2), \ldots)$. Once you have $c_1, \ldots, c_j$ define a_{j+1} as the smallest number between 1 and n not appearing in $c_1 \cup \ldots c_j$ and construct $c_{j+1} = (a_{j+1}, \sigma(a_{j+1}), \ldots)$. This way you exhaust all the integers between 1 and n.

Lets show that c_i and c_j are disjoint for $i < j$. Suppose $\sigma^u(a_i) = \sigma^v(a_j)$. Then $\sigma^{u-v}(a_i) = a_j$ which contradicts the choice of a_j as not appearing in c_i, which contains all $\sigma^r(a_i)$ for $r \geq 0$.

It is now not difficult to show that $\sigma = c_1 c_2 \cdots c_k$. $\square$