Math 210A Lecture 11 Notes

Daniel Raban

October 22, 2018

1 Group Presentations and Automorphisms

1.1 Cyclic groups and principal ideals

Definition 1.1. A **cyclic group** is a group $G = \langle x \rangle$ that can be generated by one element.

Definition 1.2. A **principal ideal** is an ideal $(x) \subseteq R$ that can be generated by one element.

Example 1.1. In $\mathbb{Z}[x]$, $(2, x)$ is not principal. The elements are $2f + xg$ for $f, g \in \mathbb{Z}[x]$. If $h \mid 2$ and $h \mid x$, then $h = \pm 1$, but $\pm 1 \notin (2, x)$.

Example 1.2. D_{2n} is not cyclic because it is not abelian.

1.2 Presentations of groups

Suppose $X \subseteq G$ is a generating set of G. We get a surjection $\phi : F_X \to G$ given by $\phi(x) = x$ for all $x \in X$. Let $N = \ker(\phi)$, and let $R \subseteq N$ be such that $\overline{\langle R \rangle}$, the smallest normal subgroup of N containing R, equals N.

$$\overline{\langle R \rangle} = \{n_1 r_1^{\pm 1} n_1^{-1} n_2 r_2^{\pm 1} n_1^{-1} \cdots n_k r_k^{\pm 1} n_k^{-1} : n_i \in N, r_i \in R, 1 \leq i \leq k, k \geq 0\}$$

Definition 1.3. $\langle X | R \rangle$ is called a **presentation** of G.

Example 1.3. In D_n, we have the reflection s across the horizontal axis, and the rotation r by $2\pi/n$ degrees. The elements of R are relations non the generators X. So $D_n = \left\langle r, s \mid r^n, s^2, rsrs \right\rangle$ is a presentation of D_n. The elements on the right side of the presentation are things that are equal to the identity of G. So $rsrs = e$, and we get $rs = sr^{-1}$, which tells us how to commute r and s.

Example 1.4. $\mathbb{Z}^2 = \left\langle a, b \mid aba^{-1}b^{-1} \right\rangle$. Here, $a = (1, 0)$ and $b = (0, 1)$. The relation $aba^{-1}b^{-1} = e$ gives $ab = ba$; i.e. a and b commute. We may also write $\mathbb{Z}^2 = \langle a, b, \mid ab = ba \rangle$.

Definition 1.4. The **commutator** of $x, y \in G$ is $[x, y] = xyx^{-1}y^{-1}$.

Example 1.5. Let

$$H = \left\{ \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{Z} \right\} \leq \mathrm{GL}_3(\mathbb{Z})$$

be the invertible matrices with $\mathbb{Z}$-entries in $M_3(\mathbb{Z})$. This is called the **Heisenberg group**.

If

$$x = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

then

$$xy = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad x^{-1}y^{-1} = x = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} x = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$

So the commutator is

$$[x, y] = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

If we call this z, then x, y, z generate H. This matrix z commutes with everything in the group (you only need to check that $zx = xz$ and $zy = yz$. So $z \in Z(H)$, the center of G. In fact, $Z(H) = \langle z \rangle$. We get that $H = \langle x, y \mid [x, [x, y]], [y, [x, y]] \rangle$.

Definition 1.5. The **center** $Z(G)$ is the set of elements in G that commute with everything; i.e. $zg = gz$ for all $g \in G$. We can also write $H = \langle x, y, z : [x, y] = z, [x, z], [y, z] \rangle$.

The center is a subgroup of G, and it is in fact normal.

Example 1.6. The **quaternion group** of order 8 is

$$Q_8 = \left\langle i, j, k \mid ij = k, i^2 = j^2 = k^2, i^4 = e \right\rangle.$$

This can also be written as $\{\pm 1, \pm i, \pm j, \pm k\}$, where $-1 = i^2 = j^2 = k^2$.

Definition 1.6. We say a group is **finitely generated** if it has a finite set of generators. We say a group is **finitely presented** if it has a finite set of generators and has a finite set of relations on those generators.

Example 1.7. $F_2 = \langle a, b \rangle$ is the group generated by 2 elements. The **commutator subgroup**

$$[F_2, F_2] = \langle [a, b] \mid a, b \in F_2 \rangle \leq F_2,$$

is not finitely generated.

1.3 Automorphism groups

Definition 1.7. The **automorphism group** $\mathrm{Aut}(G)$ of G is the set of isomorphisms $\phi : G \to G$, with composition as the group operation.

Definition 1.8. The **inner automorphism group** of G is $\mathrm{Inn}(G) = \{\gamma_g : g \in G\} \subseteq \mathrm{Aut}(G)$, where $\gamma_g(h) = ghg^{-1}$.

Observe that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

$$\varphi\gamma_g\varphi^{-1}(x) = \varphi(g\varphi^{-1}(x)g^{-1}) = \varphi(g)\varphi(\varphi^{-1}(x))\varphi(g) = \gamma_{\varphi(g)}(x).$$

Definition 1.9. The **outer automorphism group** of G is $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

If G is abelian, then $\mathrm{Out}(G) \cong \mathrm{Aut}(G)$.

Example 1.8. $\mathrm{Out}(\mathbb{Z}^2) = \mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}_2(\mathbb{Z})$.