Graduate Algebra, Fall 2014
Lecture 7

Andrei Jorza

2014-09-09

1 Group Theory

1.13 Free groups and presentations

Definition 1. 1. A **free group** generated by a set S is the smallest group F_S containing the symbols $\{x, x^{-1}|x \in S\}$. Such a group exists and can be described in terms of words with letters in S.

2. The free group is said to have **rank** n, or be finitely generated by n generators, in which case it is denoted by F_n, if $|S| = n$.

Theorem 2. *Every subgroup of a free group is free. [This can be proven using algebraic topology, realizing free groups as homotopy groups of bouquets of circles whose covering spaces are infinite trees on which free groups act; then one proves that every group acting freely on a tree must be free.]*

Definition 3. A presentation of a group G is a pair (S, R) and a homomorphism $f : F_S \to G$ such that $\ker f$ is the normal closure in F_S of the set R. The presentation is said to be finite if S and R are finite sets. Then we write $G \cong \langle a \in S | b = 1 \text{ for } b \in R\rangle$.

Example 4. 1. $\mathbb{Z} \cong \langle a\rangle$.

2. $\mathbb{Z}/n\mathbb{Z} = \langle a|a^n = 1\rangle$.

3. $\mathbb{Z} \times \mathbb{Z} \cong \langle a, b|[a, b] = 1\rangle$.

4. $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \langle a, b|a^n = b^m = [a, b] = 1\rangle$.

5. $D_{2n} \cong \langle a, b|a^n = b^2 = 1, bab = a^{-1}\rangle$.

Remark 1. Finite presentations are extremely useful for studying homomorphisms of groups. Two important applications: finding $\mathrm{Aut}(G)$ and constructing representations. Both of these are examples of constructing homomorphisms $f : G \to H$ for some group H ($H = G$ for automorphisms, $H = \mathrm{GL}(n, \mathbb{C})$ for representations). Suppose G is finitely presented as $G \cong \langle a_1, \dots, a_n|f_1(a_i) = \dots f_k(a_i) = 1\rangle$. Then there exists a homomorphism $f : G \to H$ sending a_i to $b_i \in H$ if and only if $f_j(b_i) = 1$.

Example 5. Let's compute $\mathrm{Aut}(D_{2n}) \cong \langle a, b|a^n = b^2 = baba = 1\rangle$. A function f on D_{2n} yields a homomorphism $f : D_{2n} \to D_{2n}$ iff $f(a)^n = f(b)^2 = f(a)f(b)f(a)f(b) = 1$ and this is moreover an automorphism iff $f(a)$ has order n, $f(b)$ has order 2 and $f(a)f(b)$ has order 2. As a set $D_{2n} = \{1, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\}$ and $\mathrm{ord}(a^k) = n/(k, n)$ while $\mathrm{ord}(ba^k) = 2$. Thus the conditions on orders implies that $f(a) = a^k$ for some $(k, n) = 1$ and $f(b) = ba^r$ or $f(b) = a^{n/2}$. The latter case is not good as $f(b)f(a)$ would then not have order 2 and so $f(a) = a^k$, $f(b) = ba^r$. Any such choice is good and we denote such an automorphism $f_{k,r}$. The group $\mathrm{Aut}(D_{2n}) = \{f_{k,r}\}$ under composition satisfies $f_{k,r} \circ f_{l,s} = f_{kl,r+sk}$ and so we get

$$\mathrm{Aut}(D_{2n}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$$

from our example, consisting of matrices $\begin{pmatrix} k & r \\ 0 & 1 \end{pmatrix}$.

Proposition 6. *Let G be a group.* $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ *and the quotient group* $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ *is called the group of* **outer automorphisms**.

Proof. Check that if $f \in \mathrm{Aut}(G)$ then $f \circ \phi_g \circ f^{-1} = \phi_{f(g)}$ where $\phi_g(x) = gxg^{-1}$. □

Example 7.

1. $\mathrm{Out}(S_3) \cong 1$.
2. $Z(D_{2n})$ is trivial if n is odd, and $\{1, R^{n/2}\}$ if n is even so $|\mathrm{Out}(D_{2n})|$ has $\varphi(n)/2$ elements if n is odd and $\varphi(n)$ if n is even.
3. If G is abelian then $\mathrm{Out}(G) \cong \mathrm{Aut}(G)$.

1.14 Abelian groups

Proposition 8.

1. *If p is any prime then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic $\cong \mathbb{Z}/(p-1)\mathbb{Z}$.*
2. *If p is an odd prime and $n \geq 2$ then $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic $\cong \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}$.*
3. *If $n \geq 2$ then $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$.*

Proof. First part. Let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be an element of maximal order, which has to divide $p-1$. If h is another element such that $\mathrm{ord}(h) \nmid \mathrm{ord}(g)$ then $\mathrm{ord}(gh) = [\mathrm{ord}(g), \mathrm{ord}(h)]$ (Pset 3) has larger order than g contradicting the choice of g. Thus the order of every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ divides the order of g. Denote $n = \mathrm{ord}(g)$. Then every element of $\mathbb{Z}/p\mathbb{Z}$ except 0 satisfies $X^n - 1 = 0$ and so every element of $\mathbb{Z}/p\mathbb{Z}$ satisfies $X^{n+1} - X = 0$.

The Euclidean algorithm for polynomials with coefficients in $\mathbb{Z}/p\mathbb{Z}$ (where every nonzero element is invertible) implies that for every $h \in \mathbb{Z}/p\mathbb{Z}$, $X - h \mid X^{n+1} - X$ and so $\prod(X-h) \mid X^{n+1} - X$. Comparing degrees we deduce that $n + 1 \geq p$ and so g has order $p - 1$. Thus $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$ is cyclic $\cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Second part. Let's prove by induction that $(1+p)^{p^{n-1}} \equiv 1 + p^n \pmod{p^{n+1}}$. The base case is $n = 1$ which is trivial. Next, suppose $(1+p)^{p^{n-1}} = 1 + p^n + ap^{n+1}$. Then

$$\begin{aligned}(1+p)^{p^n} &= (1 + p^n + ap^{n+1})^p \\ &\equiv (1+p^n)^p \pmod{p^{n+2}} \\ &\equiv 1 + p^{n+1} \pmod{p^{n+2}}\end{aligned}$$

In the second line we used that $\binom{p}{i}p^{i(n+1)}$ is divisible by p^{n+2} if $i \geq 1$ and in the last line that $\binom{p}{i}p^{in}$ is divisible by p^{n+2} for $i \geq 2$.

We conclude that the order of $1 + p$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is p^{n-1}. Finally, since p^{n-1} and $p - 1$ are coprime the order of $g(1+p)$ is $p^{n-1}(p-1)$ and so $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic $\cong \langle g(1+p) \rangle \cong \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}$.

Third part: As above we prove by induction that if $n \geq 2$ then $3^{2^{n-1}} \equiv 1 + 2^{n+1} \pmod{2^{n+2}}$ (note the difference in exponents). Thus 3 has order 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. Moreover, $-1 \notin \langle 3 \rangle$ as if $-1 \equiv 3^k \pmod{2^n}$ then $3^{2k} \equiv 1$ and so $k = 2^{n-3}$ but $3^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ which is not $-1 \pmod{2^n}$ as $n \geq 2$. Thus $\langle -1, 3 \rangle$ is a group, larger than $\langle 3 \rangle$ which has index 2 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ and thus $(\mathbb{Z}/2^n\mathbb{Z})^\times = \langle -1, 3 \rangle \cong \langle -1 \rangle \times \langle 3 \rangle$. □