# Graduate Algebra, Fall 2014
# Lecture 8

Andrei Jorza

2014-09-12

## 1 Group Theory

### 1.13 Free groups and presentations

(continued)

**Definition 1.** A group $G$ is **finitely generated** if $G = \langle g_1, \dots, g_n \rangle$ for finitely many elements.

**Example 2.**
1. Every finite group is finitely generated.
2. $\mathbb{Z}$ is finitely generated.
3. $\mathbb{Q}$ is not finitely generated as if $X = \{p_i/q_i\}$ then $\langle X \rangle \subset (\prod q_i)^{-1}\mathbb{Z}$.
4. Let $G$ be the group $\langle \begin{pmatrix} 2 & \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \rangle \subset \mathrm{GL}(2, \mathbb{R})$. The the subgroup of matrices with 1-s on the diagonal is not finitely generated.
5. A free abelian group is a group $\cong \mathbb{Z}^n$ where $n$ is the rank of the group. We will later use results about modules over PIDs to obtain:
   (a) Every subgroup of a free abelian group of rank $n$ is a free abelian group of rank $m \leq n$.
   (b) Every subgroup of a finitely generated abelian group is finitely generated.

### 1.14 Abelian groups

When we study modules over PIDs we will prove the following theorem:

**Theorem 3.** *If $G$ is a finitely generated abelian group then there exist unique integers $r \geq 0$ (called the rank of $G$) and $n_i \geq 2$ such that $n_{i+1} \mid n_i$ for all $i$ and*

$$G \cong \mathbb{Z}^r \times \prod(\mathbb{Z}/n_i\mathbb{Z})$$

For now let's study $\mathbb{Z}/n\mathbb{Z}$.

**Proposition 4** (Chinese Remainder Theorem)**.** *Suppose $n_i$ are pairwise coprime integers. Then*

$$\mathbb{Z}/\prod n_i\mathbb{Z} \cong \prod \mathbb{Z}/n_i\mathbb{Z}$$

*and*

$$(\mathbb{Z}/\prod n_i\mathbb{Z})^\times \cong \prod(\mathbb{Z}/n_i\mathbb{Z})^\times$$

*In particular, if $n = \prod p_i^{a_i}$ is the prime decomposition of $n$ then*

$$\mathbb{Z}/n\mathbb{Z} \cong \prod \mathbb{Z}/p_i^{a_i}\mathbb{Z} \text{ and } (\mathbb{Z}/n\mathbb{Z}) \cong \prod(\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$$

*Proof.* By induction it suffices to show that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for coprime $m$ and $n$. Consider the natural map $\mathbb{Z}/mn \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ given by $x \mapsto (x \mod m, x \mod n)$. This is an injective homomorphism since $(m,n)=1$ and so $[m,n]=mn$.

We now show surjectivity. Suppose $a,b \in \mathbb{Z}$. Pick $p,q \in \mathbb{Z}$ such that $pm+qn=1$. Then $x = aqn + bpm$ satisfies $x \equiv a \pmod m$ and $x \equiv b \pmod n$ so the map is surjective.

The second part follows from the fact that $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$ for $G$ and $H$ of coprime orders. □

The theorem tells us that the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$ can be written as a direct product of cyclic groups. What are these groups?

**Lemma 5.** *Let $p$ be a prime number and $m,n \geq 0$ two integers. Write $m = \sum m_i p^i$ and $n = \sum n_i p^i$ in base $p$. Then*

$$\binom{m}{n} \equiv \prod \binom{m_i}{n_i} \pmod p$$

*Proof.* For $p$ prime if $i \neq 0,p$ we have $p \mid \binom{p}{i} = p(p-1)\cdots(p-i+1)/i!$. Thus $(X+Y)^p \equiv X^p + Y^p \pmod p$. The quantity $\binom{m}{n}$ is the coefficient of $X^n$ in $(1+X)^m \mod p$. We will prove by induction that if $a,b<p$ then

$$\binom{mp+a}{np+b} \equiv \binom{m}{n}\binom{a}{b} \pmod p$$

which is equivalent to showing that the coefficient of $X^{np+b}$ in $(1+X)^{mp+a} = (1+X^p)^m(1+X)^a$ is $\binom{m}{n}\binom{a}{b}$. Since $a<p$ the monomial $X^{np+b}$ appears only once in $(1+X^p)^m(1+X)^a$, namely as $(X^p)^n X^b$ and the comparison of coefficients is immediate. □

**Proposition 6.**

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 $(\mathbb{Z}/2^n\mathbb{Z})^\times = \langle -1, 3\rangle \cong \langle -1\rangle \times \langle 3\rangle$. □

What about non-finitely generated abelian groups?

**Definition 7.** Let $G$ be an abelian group. Multiplication by $n$ is a homomorphism on $G$ and we denote $G[n]$ its kernel. Denote $G[p^\infty] = \cup G[p^n]$ and $\mathrm{Tor}(G) = \cup_{n\in\mathbb{Z}} G[n]$.

**Lemma 8.** *If $G$ is abelian then $\mathrm{Tor}(G)$ is a subgroup of $G$.*

*Proof.* If $ng = 0$ and $mh = 0$ then $mn(g+h) = 0$. □

**Example 9.**

1. $G = \mathbb{Q}/\mathbb{Z}$ is not finitely generated. If $n \in \mathbb{Z}$ then $G[n] = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.
2. $\mathbb{Q}/\mathbb{Z}[p^\infty] = \mathbb{Z}[1/p] = \{\frac{m}{n} | n = p^k\}$.
3. $\mathrm{Tor}(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.
4. $\mathrm{Tor}(\mathbb{Q}) = 0$.

**Proposition 10.** *If $G$ is abelian then $G/\mathrm{Tor}(G)$ is torsion-free.*

*Proof.* Suppose $ng \in \mathrm{Tor}(G)$. Then $mng = 0$ for some $m$ and so $g \in \mathrm{Tor}(G)$. □

## 1.15 Group actions

**Definition 11.** A **group action** of a group $G$ on a set $X$ is any homomorphism from $G$ to the group of permutations of $X$. I.e., to each $g \in G$ one associates a map $x \mapsto gx$ on $X$ such that if $g, h \in G$ then $(gh)x = g(hx))$ and $1x = x$ for all $x \in X$.

**Example 12.**

1. The trivial action: $G$ acts on $X$ trivially, sending every $g$ to the identity map.
2. The left regular action of $G$ on itself is $g \mapsto (x \mapsto gx)$. The right regular action is $g \mapsto (x \mapsto xg)$.
3. Let $S$ be a set and $X$ the set of functions $G \to S$. Then $G$ acts on $X$ by $(gf)(x) = f(xg)$, also called the right regular action.
4. The conjugation action. $G$ acts on itself sending $g$ to the inner homomorphism $h \mapsto ghg^{-1}$. The conjugation action gives an action of $G$ on any normal subgroup of $G$.
5. If $X$ is the set of subgroups of $G$ then the conjugation action of $G$ on itself yields a conjugation action on $X$. Indeed, if $H$ is a subgroup then $gHg^{-1}$ is also a subgroup. The left and right regular actions of $G$ on itself also give actions on $X$.
6. The group $S_n$ acts on $\mathbb{C}^n$ by permuting coordinates.
7. For $R = \mathbb{Z}/p\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ the group $\mathrm{GL}(n, R)$ acts on $R^n$ by left matrix multiplication.
8. If $H$ is a subgroup of $G$ then the left regular action of $G$ on itself gives the action of $G$ on $G/H$ by $g \mapsto (xH \mapsto gxH)$. Similarly the right regular action of $G$ on itself gives an action of $G$ on $H\backslash G$.
9. The group $\mathrm{GL}(2, R)$ acts on $\mathbb{P}^1_R$ as follows: the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acts by sending $z \in \mathbb{R} \cup \infty$ to $\frac{az+b}{cz+d} \in R \cup \infty$.
10. The group $\mathrm{GL}(n, R)$ acts on the set of $k$-dimensional sub-vector space of $R^n$ by left matrix multiplication.
11. Let $k \geq 0$ and $V_k$ be the set of polynomials $P(X, Y) \in \mathbb{C}[X]$ homogeneous of degree $k$. Then $\mathrm{GL}(2, \mathbb{C})$ acts on $V_k$ as follows: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} P(X, Y) = P(aX + bY, cX + dY)$. This is called the $k$-th symmetric representation.