Finitely Generated Abelian Groups

Math 417: Abstract Algebra

Lecture 24

Charles Rezk

University of Illinois at Urbana-Champaign

Proof of the Classification of Finitely Generated Abelian Groups

UI

finite Abelian groups.

$G = \langle a_1, \ldots, a_n \rangle$ - finitely generated group

$N \trianglelefteq G \to G/N = \langle a_1 N, \ldots, a_n N \rangle$ → write as words

$\Rightarrow$ quotients of f.gen groups are finitely generated.

Fact: If $a_n \in N$, then $G/N = \langle a_1 N, \ldots, a_{n-1} N \rangle$

throw away the identity

$a_n N = eN$
can be generated
by other elements.

timestamp: 00:17

Proof of the Classification of Finitely Generated Abelian Groups

If $\boldsymbol{H} \leqslant \boldsymbol{G}$-f.gen

is $\boldsymbol{H}$ also f.gen?

NO it does not have to be f.gen.

Thm.

~~**Prop:**~~ = If $\boldsymbol{G}$ is f.gen and abelian, then every subgroup $\boldsymbol{H} \leqslant \boldsymbol{G}$ is also f.gen.

Thm

timestamp: 03:14

Proof of the Classification of Finitely Generated Abelian Groups

not really required

Lemma: If $\boldsymbol{H}$-(abelian) group,

$\boldsymbol{N} \trianglelefteq \boldsymbol{H}$ (normal) subgroup

If $\boldsymbol{N}$ and $\boldsymbol{H}/\boldsymbol{N}$ are f.gen $\Rightarrow$ $\boldsymbol{H}$ is f.gen.

$\langle\{x_1, \dots, x_m\}\rangle$ (just a notation)

$\Vert$

Proof: Suppose $\boldsymbol{N} = \mathbb{Z}\{x_1, \dots, x_m\}$

$$\boldsymbol{H}/\boldsymbol{N} = \mathbb{Z}\{\bar{y}_1, \dots, \bar{y}_n\}$$

cosets of N.

$$\boxed{\begin{array}{c} \pi : \boldsymbol{H} \twoheadrightarrow \boldsymbol{H}/\boldsymbol{N} \\ \pi(y_\imath) = \bar{y}_\imath \end{array}}$$

Pick. For each $\bar{y}_\imath$ pick $y_\imath \in \boldsymbol{H}$ such that $\bar{y}_\imath = y_\imath + \boldsymbol{N}$

Proof of the Classification of Finitely Generated Abelian Groups

Claim: $\boldsymbol{H} = \mathbb{Z}\{x_1, \ldots, x_m, y_1, \ldots, y_n\}$ → is finite generated

Suppose: $u \in \boldsymbol{H}$

Consider $v := \pi(u) = b_1\bar{y}_1 + \ldots + b_n\bar{y}_n \in \boldsymbol{H}/\boldsymbol{N}$ for some $b_1 \in \mathbb{Z}$

Define: $\widehat{v} := 1y_1 + \ldots + b_n y_n \in \boldsymbol{H}$; $\pi(\widehat{v}) = v$ → $\pi(b_1y_1) + \cdots + \pi(b_ny_n)$ (homo) $= b_1\bar{y}_1 + \cdots + b_n\bar{y}_n = v$

Have: $\pi(u) = v = \pi(\widehat{v}) \Dashv \pi(u - \widehat{v}) = 0 \Dashv u - \widehat{v} \in \boldsymbol{N}$

kernel !

so $u - \widehat{v} = a_1x_1 + \ldots + a_mx_m$ for some $a_1 \in \mathbb{Z}$

$\Dashv u = \underbrace{\Sigma a_i x_i + \Sigma b_j y_j}_{\text{H is a generating set !}} \Dashv$ done

timestamp: 08:51

Proving The Subgroup $\boldsymbol{H}$ Is Finitely Generated

a WTS

$\;\;\|$

Pf. of thm: $\boldsymbol{G} = \mathbb{Z}\{a_1, ..., a_n\}$, $\boldsymbol{H} \leqslant \boldsymbol{G}$

Use induction an n = size of a generating set of $\boldsymbol{G}$

Base case: $n = 0$, $\boldsymbol{G} = \mathbb{Z}\{\} = \{0\}$

$n = 1$, $\boldsymbol{G} = \mathbb{Z}\{a\}$

we shared $\Dashv$ $\boldsymbol{H}$ is cyclic (proved)

Lecture 10, 11

Basically, $G = \langle g \rangle \cong \mathbb{Z}_n$ has its subgroups to be cyclic.

timestamp: 14:49

Induction Step

Induction Step: n $\geqslant$ 2

gen by n

gen by n-1

by induction.

$$\begin{tikzcd}
 & \boldsymbol{G} \arrow[rr, two heads] & & \boldsymbol{G}/\mathbb{Z}a & \\
 & \boldsymbol{H} + \mathbb{Z}\{a\} \arrow[u] \arrow[rr, two heads, "\text{quotient}"] & & (\boldsymbol{H} + \mathbb{Z}a)/\mathbb{Z}a \arrow[u] & \\
\mathbb{Z}\{a\} \arrow[ur] & & \boldsymbol{H} \arrow[ul] \arrow[rr, two heads, "\text{quotient}"] \arrow[dr] & & \boldsymbol{H}/\boldsymbol{N} = \boldsymbol{H}/\boldsymbol{H}\cap\mathbb{Z}a \arrow[ul, "\text{iso}"'] \\
 & \boldsymbol{H}\cap\mathbb{Z}\{a\} \arrow[ul] \arrow[ur] & & \text{LEMMA} & \\
\boldsymbol{N} \arrow[ur] & & & &
\end{tikzcd}$$

(CORR THM.) correspondence theorem

f.gen (Induction)

(cyclic)

(DIAMOND ISO THM.)

iso

f.gen

f.gen

intersect

f.gen

(cyclic)

f.gen

Showed Fact

timestamp: 17:24

Consequence of Proof

Consequence. step 1 ↓

Fact: $\boldsymbol{G}$-f.gen abelian $\Rightarrow \exists\, m \geq 0, \Phi : \mathbb{Z}^m \twoheadrightarrow \boldsymbol{G}$ surj homomorphism

$N = \ker(\varphi) \trianglelefteq G$.

$\Rightarrow \boldsymbol{G} \cong \mathbb{Z}^m / \boldsymbol{N}$,

Thm: $\boldsymbol{N}$ is f.gen, so $\exists\, n \geq 0, \bar{\alpha} : \mathbb{Z}^n \twoheadrightarrow \boldsymbol{N}$ sury hom.

so i exists

image is N

Consider $\mathbb{Z}^n \xrightarrow{\bar{\alpha}} \boldsymbol{N} \overset{i}{\rightarrowtail} \mathbb{Z}^m$, $\quad \alpha = i \cdot \bar{\alpha}$

$\alpha(\mathbb{Z}^n) = \boldsymbol{N}$

$\bar{\alpha}(\mathbb{Z}^n) = N$, so

$\Rightarrow \boldsymbol{G} \simeq \mathbb{Z}^m / \cancel{\alpha(\mathbb{Z}^n)}$ $L_A(\mathbb{Z}^n)$

For some $\boldsymbol{A} \in \mathrm{Mat}_{m \times n}(\mathbb{Z})$

STEP 2 DONE!

STEP 3 in the following

timestamp: 26:02, 37:29

Studying the Homomorphism from $\mathbb{Z}^n$ to $\mathbb{Z}^m$

Observe: $\boldsymbol{A} \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$, define

$L_{\boldsymbol{A}} : \mathbb{Z}^n \to \mathbb{Z}^m$ by $\boldsymbol{A} = (a_{ij})$, $a_{ij} \in \mathbb{Z}$

$$L_{\boldsymbol{A}}\big(\underbrace{(c_1, \ldots, c_n)}_{c_i \in \mathbb{Z}}\big) := \left(\sum_{j=1}^n a_{1j}c_j, \sum_{j=1}^n a_{2j}c_j, \ldots, \sum_{j=1}^n a_{mj}c_j \right)$$

$$\text{i.e. } L_{\boldsymbol{A}}\left(\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}\right) = \boldsymbol{A}\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} \in \begin{bmatrix} d_1 \\ \vdots \\ \vdots \\ d_m \end{bmatrix} \in \mathbb{Z}^m$$

Claim: $L_{\boldsymbol{A}}$ is a homomorphism.

timestamp: 31:23

Studying the Homomorphism from $\mathbb{Z}^n$ to $\mathbb{Z}^m$

To find out what this matrix is, we can plug in the a "standard basis" to α.

Also, any homomorphism $\alpha : \mathbb{Z}^n \to \mathbb{Z}^m$

is equal to $L_{\boldsymbol{A}}$ for a unique $\boldsymbol{A} \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$

Furthermore $\quad \boldsymbol{A} \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$

$\boldsymbol{B} \in \mathrm{Mat}_{\overset{n}{m}\times p}(\mathbb{Z})$

Then: $L_{\boldsymbol{AB}} = L_{\boldsymbol{A}} \circ L_{\boldsymbol{B}}$

$$\begin{tikzcd} & \mathbb{Z}^n \arrow[dr, "L_{\boldsymbol{A}}"] & \\ \mathbb{Z}^p \arrow[ur, "L_{\boldsymbol{B}}"] \arrow[rr, "L_{\boldsymbol{AB}}"'] & \text{same} & \mathbb{Z}^m \end{tikzcd}$$

timestamp: 34:27

Studying the Homomorphism from $\mathbb{Z}^n$ to $\mathbb{Z}^m$

previously its just hom.

Rem: Suppose $L_{\boldsymbol{A}} : \mathbb{Z}^n \to \mathbb{Z}^m$ is an isomorphism $[\boldsymbol{A} \in \mathrm{Mat}_{m\times n}(\mathbb{Z})]$

Then $(L_{\boldsymbol{A}})^{-1} : \mathbb{Z}^m \to \mathbb{Z}^n$ is also an isomorphism

$$(L_{\boldsymbol{A}})^{-1} = L_{\boldsymbol{B}} \text{ for some } \boldsymbol{B} \in \mathrm{Mat}_{n\times m}(\mathbb{Z})$$

$$L_{\boldsymbol{BA}} = L_{\boldsymbol{B}} \circ L_{\boldsymbol{A}} = id_{\mathbb{Z}^n} = L_{\boldsymbol{I}} \qquad L_{\boldsymbol{A}} \circ L_{\boldsymbol{B}} = id_{\mathbb{Z}^m} = L_{\boldsymbol{I}}$$

$$\Rightarrow \boldsymbol{AB} = \boldsymbol{I}, \boldsymbol{I} = \boldsymbol{AB} \xRightarrow[\text{(over } \mathbb{R})]{\text{Lin Alg.}} m = n, \text{so } \boldsymbol{B} = \boldsymbol{A}^{-1}$$

$\boxed{\text{Corr: } \mathbb{Z}^m \cong \mathbb{Z}^m \Rightarrow \cancel{m \times n}\ m = n}$

timestamp: 38:20

Smith Normal Form

<u>Smith Normal Form</u>

[When $\boldsymbol{A} \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$], $\boldsymbol{A}$ is in Smith normal form if

$$\boldsymbol{A} = \mathrm{diag}(d_1, d_2, ..., d_s), d_1 \leqslant 0, d_\imath | d_{\imath+1}$$

$$S = min(m, n)$$

$$\text{eg. } \boldsymbol{A} = \begin{pmatrix} 1 & & & & & \\ & 3 & & \Large 0 & & \\ & & 12 & & & \\ & \Large 0 & & 0 & 0 & 0 \end{pmatrix}$$

timestamp: 43:09

Smith Normal Form

<u>Prop:</u> If $\boldsymbol{A} = diag(d_1, \ldots, d_s) \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$ [Smith Normal Form]

$$\mathbb{Z}^m / L_{\boldsymbol{A}}(\mathbb{Z}^n) \simeq \mathbb{Z}/\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}/\mathbb{Z}_{d_s} \times \mathbb{Z}^{m-s} = \boldsymbol{G}$$

<u>Proof:</u> $\mathbb{Z}^m \xrightarrow{\varphi} \boldsymbol{G}$ by

$$(x_1, \ldots, x_s, x_{s+1}, \ldots, x_m) \mapsto \left([x_1]_{d_1}, \ldots, [x_s]_{d_s}, \underline{x_{s+1}, \ldots, x_m}\right)$$

This is surjective, $\ker\varphi = L_{\boldsymbol{A}}(\mathbb{Z}^n)$ by iso, is true

means: $x_{s+1}, \ldots, x_m$ are all zero.

and $x_i | d_i$ for $i = 1, \ldots, s$.

So $\ker(\varphi)$ = linear comb of $\mathbb{Z}^n = L_A(\mathbb{Z}^n)$

timestamp: 44:32

Smith Normal Form

Prop: If $\boldsymbol{B} = \boldsymbol{PAQ}$, $\boldsymbol{A}, \boldsymbol{B} \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$

$\boldsymbol{P}, \boldsymbol{Q} \quad \mathbb{Z} -$ invertible

then $\mathbb{Z}^m / L_{\boldsymbol{A}}(\mathbb{Z}^n) \cong \mathbb{Z}^m / L_{\boldsymbol{B}}(\mathbb{Z}^n)$.

Say that $\boldsymbol{A} \backsim \boldsymbol{B}$ "equivalent".

$$\Pi_{\boldsymbol{A}} : \mathbb{Z}^m \to \mathbb{Z}^m / L_{\boldsymbol{A}}(\mathbb{Z}^n)$$

$$\Pi_{\boldsymbol{B}} : \mathbb{Z}^m \to \mathbb{Z}^m / L_{\boldsymbol{B}}(\mathbb{Z}^n)$$

timestamp: 47:25

Smith Normal Form

Pf: Consider

$$\begin{tikzcd}
\mathbb{Z}^m \arrow[r, "L_{p-1}", "\simeq"'] \arrow[rr, bend left, "\varphi = \Pi_{\boldsymbol{A}} \circ L_{p-1}"] \arrow[d] & \mathbb{Z}^m \arrow[r, tail, two heads, "\Pi_{\boldsymbol{A}}"] & \mathbb{Z}^m / L_{\boldsymbol{A}}(\mathbb{Z}^n) \\
\mathbb{Z}^m / \ker \varphi \arrow[urr, "\trianglerighteq \text{ Iso. Thm}"'] & &
\end{tikzcd}$$

Claim: $\ker \varphi = L_{\boldsymbol{B}}(\mathbb{Z}^n)$

Smith Normal Form

$$
\begin{aligned}
x \in \ker \varphi &\iff \boldsymbol{P}_x^{-1} \in \ker \Pi_{\boldsymbol{A}} \\
&\iff \boldsymbol{P}_x^{-1} = \boldsymbol{A} y \text{ for some } y \in \mathbb{Z}^n \\
&\iff \boldsymbol{P}_x^{-1} = \boldsymbol{A}\boldsymbol{Q} z, \text{ for some } z \in \mathbb{Z}^n \ [z = \boldsymbol{Q}^{-1} y] \\
&\iff x = \boldsymbol{P}\boldsymbol{A}\boldsymbol{Q} z = \boldsymbol{B} z \text{ for some } z \in \mathbb{Z}^n \\
&\iff x \in L_{\boldsymbol{B}}(\mathbb{Z}^n)
\end{aligned}
$$