20241027 MATH3301 NORE 6[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Introduction **3**

2 The Fundamental Theorem of Finite Abelian Group **3**

2.1 Preliminaries 3

2.2 Finite Abelian Group with Unique Prime Divisor 5

2.3 Finite Abelian Group with Multiple Prime Divisors 5

3 Jordan Canonical Form **6**

3.1 Preliminaries 6

3.2 Finite Complex Matrix with Unique Eigenvalue 7

3.3 Finite Complex Matrix with Multiple Eigenvalues 8

1 Introduction

This note introduces two similar systematical ways to decompose certain structures into the direct products of smaller structures.

2 The Fundamental Theorem of Finite Abelian Group

2.1 Preliminaries

First, we propose ***Cauchy's Theorem****.*

Theorem 2.1. (**Cauchy's Theorem**)
Let G be an Abelian group of order n, and p be a prime divisor of n.
There exists $g \in G$, such that $\operatorname{ord}(g) = p$.
Here, $\operatorname{ord}(g)$ is the smallest positive integer μ such that $g^\mu = e$.

Proof. We prove this theorem by the strong form of mathematical induction.
Basis Step: When $n = p$, G is cyclic, so G has a generator g with $\operatorname{ord}(g) = p$.
Inductive Hypothesis: For all $k \in \mathbb{N}$, for all $1 \leq l \leq k$, when $n = lp$, assume that there exists $g \in G$, such that $\operatorname{ord}(g) = p$.
Inductive Step: When $n = (l+1)p$, G has a nontrivial proper subgroup H.
Case 1: If p divides $|H|$, then there exists $h \in H$, such that $\operatorname{ord}(h) = p$.
There exists $h \in G$, such that $\operatorname{ord}(h) = p$.
Case 2: If p divides $|G/H|$, then there exists $gH \in G/H$, such that $\operatorname{ord}(gH) = p$.
Notice that $g^p H = (gH)^p = H$, so $h = g^p \in H$.
There exists $g' = g^{\operatorname{ord}(h)} \in G$, such that $\operatorname{ord}(g') = p$.
To conclude, the statement is true for all $n = kp$. Quod. Erat. Demonstrandum. □

Then, we reduce a finite Abelian group G with $\forall g \in G, g^p = e$.

Theorem 2.2. (**The Recognition Theorem**[2])
Let G be an Abelian group,
and H, K be two subgroups of G.
(1) HK is a subgroup of G.
(2) $\sigma : H \times K \to HK, (h,k) \mapsto hk$ is a homomorphism.
(3) σ is an isomorphism if and only if $H \cap K = \{e\}$.

Proof. We may divide our proof into three parts.
Part 1: In this part, we prove HK is a subgroup of G.

$$\begin{aligned} e &= ee \in HK \\ hkh'k' &= hh'kk' \in HK \\ k^{-1}h^{-1} &= h^{-1}k^{-1} \in HK \end{aligned}$$

Hence, HK is a subgroup of G.
Part 2: In this part, we prove $\sigma : H \times K \to HK, (h,k) \mapsto hk$ is a homomorphism.

$$\begin{aligned}(h,k) &\mapsto hk \\ (h',k') &\mapsto h'k' \\ (hh',kk') &\mapsto hh'kk' = hkh'k'\end{aligned}$$

Part 3: In this part, we prove σ is an isomorphism if and only if $H \cap K = \{e\}$.
Assume that $H \cap K$ only contains the identity e.

$$\begin{aligned}hk = h'k' &\implies h'^{-1}h = k'k^{-1} \in H \cap K = \{e\} \\ &\implies (h,h') = (k,k')\end{aligned}$$

Hence, the surjective homomorphism σ is injective, σ is an isomorphism.
Assume that $H \cap K$ contains some nonidentity element g.

$$\begin{aligned}(g,g^{-1}) &\mapsto gg^{-1} = e \\ (e,e^{-1}) &\mapsto ee^{-1} = e\end{aligned}$$

Hence, σ fails to be injective, σ is not an isomorphism.
Quod. Erat. Demonstrandum. □

Proposition 2.3. Let G be an Abelian group of order n,
and p be a prime divisor of n.
If $\forall g \in G, g^p = e$, then $\forall g \in G, \exists H \leq G, G \cong H \times \langle g \rangle$.
Here, $\langle g \rangle = \left\{ g^k \in G : k \in \mathbb{Z} \right\}$.

Proof. Assume to the contrary that for some $x \in G$, such H doesn't exist.
That is, the maximum of the following set is strictly less than n/p:

$$\mathcal{H} = \{|H| \in \mathbb{Z} : H \leq G \text{ and } x \notin H\}$$

Take a maximal H, the index $[G : H] > p$, so $G \backslash \left(\bigcup_{k=0}^{p-1} x^k H \right) \neq \emptyset$.
Take $y \in G \backslash \left(\bigcup_{k=0}^{p-1} x^k H \right)$ and construct $K = H\langle y \rangle$.
On one hand, $y \in K$ and $y \notin H$ and $K \supseteq H$, so $|K| > |H|$.
On the other hand, assume to the contrary that $x \in K$, so x is equal to some hy^μ.
Case 1: If $\mu \equiv 0 (\text{mod } p)$, then $x = h \in H$ is a contradiction.
Case 2: If $\mu \not\equiv 0 (\text{mod } p)$, then $y = x^{\mu^{-1}} h^{-\mu^{-1}} \in x^{\mu^{-1}} H$ is a contradiction.
Now $x \notin K$, so $K \in \mathcal{H}$, contradicting to the maximality of H.
Quod. Erat. Demonstrandum. □

Remark: *For this case, there exists* $(g_k)_{k=0}^{l-1}$ *in* G*, such that* $G \cong \prod_{k=0}^{l-1} \langle g_k \rangle$.

2.2 Finite Abelian Group with Unique Prime Divisor

Next, we reduce a finite Abelian group G with unique prime divisor.

Proposition 2.4. Let G be an Abelian group of order n,
and p be the unique prime divisor of n.
For all $g \in G$, g has maximal order p^{β} implies $\exists H \leq G, G \cong H \times \langle g \rangle$.

Proof. We prove this theorem by mathematical induction.
Basis Step: When $n = p$, G is cyclic, so $\exists \{e\} \leq G, G = \langle g \rangle \cong \{e\} \times \langle g \rangle$.
Inductive Hypothesis: For all $\gamma \in \mathbb{N}$, when $n = p^{\gamma}$, assume that for all $g \in G$, g has maximal order p^{β} implies $\exists H \leq G, G \cong H \times \langle g \rangle$.
Inductive Step: When $n = p^{\gamma+1}$, for all $g \in G$ with maximal order p^{β}:
Case 1: If $n = p^{\beta}$, then G is cyclic, so $\exists \{e\} \leq G, G = \langle g \rangle \cong \{e\} \times \langle g \rangle$.
Case 2: If $n > p^{\beta}$, then $G \backslash \langle g \rangle \neq \emptyset$. Take $h \in G \backslash \langle g \rangle$. WLOG, assume that $\mathrm{ord}(h) = p$.
In $G/\langle h \rangle$, as $\langle g \rangle \cap \langle h \rangle = \{e\}$, the coset $g\langle h \rangle$ must have order p^{β}.
There exists $\widetilde{H} \leq G/\langle h \rangle$, such that $G/\langle h \rangle \cong \widetilde{H} \times \langle g\langle h \rangle \rangle$.
This gives a subgroup $H = \pi^{-1}(\widetilde{H})$ of G,
where $\pi : G \to G/\langle h \rangle$ is the natural projection.
Note that $H \cap \langle g \rangle = \{e\}$, so $\exists H \leq G, G = H\langle g \rangle \cong H \times \langle g \rangle$.
Quod. Erat. Demonstrandum. □

Remark: *For this case, there exists $(g_k)_{k=0}^{l-1}$ in G, such that $G \cong \prod_{k=0}^{l-1} \langle g_k \rangle$.*
Assume that each $\mathrm{ord}(g_k) = p^{\alpha_k}$, then $G \cong \prod_{k=0}^{l-1} \mathbb{Z}_{p^{\alpha_k}}$.

2.3 Finite Abelian Group with Multiple Prime Divisors

Proposition 2.5. Let G be an Abelian group of order n,
and p, q be two distinct prime divisors of n.
For all p-subgroup H and q-subgroup K, $H \cap K = \{e\}$.
Here, p-subgroup means a subgroup with unique prime divisor p.

Proof. For all $g \in G$:

$$\begin{aligned} g \in H \cap K &\implies g \in H \text{ and } g \in K \\ &\implies \mathrm{ord}(g) = p^s \text{ and } \mathrm{ord}(g) = q^t \\ &\implies g = g^{xp^s} g^{yq^t} = e \end{aligned}$$

Quod. Erat. Demonstrandum. □

Remark: *Hence, G is the Cartesian product of p-subgroups.*

3 Jordan Canonical Form

3.1 Preliminaries

*First, we propose **Cauchy's Theorem**.*

Theorem 3.1. (**Cauchy's Theorem**)
Let A be a complex matrix of order n, and λ be an eigenvalue of A.
There exists $\mathbf{u} \in \mathbb{C}^n$, such that $\operatorname{ord}(\mathbf{u}) = 1$.
Here, $\operatorname{ord}(\mathbf{u})$ is the smallest positive integer μ such that $(\lambda I - A)^{\mu}\mathbf{u} = \mathbf{0}$.

Proof.

$$\begin{aligned}
\lambda \text{ is an eigenvalue of } \mathcal{A} &\implies A\mathbf{u} = \lambda\mathbf{u} \text{ has a nontrivial solution } \mathbf{u} \in \mathbb{C}^n \\
&\implies \text{There exists } \mathbf{u} \in \mathbb{C}^n, \text{ such that } \operatorname{ord}(\mathbf{u}) = 1
\end{aligned}$$

Quod. Erat. Demonstrandum. □

Then, we triangularize a finite complex matrix A with $\forall \mathbf{u} \in \mathbb{C}^n, (\lambda I - A)\mathbf{u} = \mathbf{0}$.

Theorem 3.2. (**The Recognition Theorem**[2])
Let A be a complex matrix of order n,
and V, W be two invariant subspaces of A.
(1) $V + W$ is an invariant subspace of A.
(2) $\sigma : V \times W \to V + W, (\mathbf{v}, \mathbf{w}) \mapsto \mathbf{v} + \mathbf{w}$ is a homomorphism.
(3) σ is an isomorphism if and only if $V \cap W = \{\mathbf{0}\}$.

Proof. We may divide our proof into three parts.
Part 1: In this part, we prove $V + W$ is an invariant subspace of A.

$$\begin{aligned}
\mathbf{0} = \mathbf{0} + \mathbf{0} &\in V + W \\
\mathbf{v} + \mathbf{w} + \mathbf{v}' + \mathbf{w}' = \mathbf{v} + \mathbf{v}' + \mathbf{w} + \mathbf{w}' &\in V + W \\
\lambda(\mathbf{v} + \mathbf{w}) = \lambda\mathbf{v} + \lambda\mathbf{w} &\in V + W \\
A(\mathbf{v} + \mathbf{w}) = A\mathbf{v} + A\mathbf{w} &\in V + W
\end{aligned}$$

Hence, $V + W$ is an invariant subspace of A.
Part 2: In this part, we prove $\sigma : V \times W \to V + W, (\mathbf{v}, \mathbf{w}) \mapsto \mathbf{v} + \mathbf{w}$ is a homomorphism.

$$\begin{aligned}
(\mathbf{v}, \mathbf{w}) &\mapsto \mathbf{v} + \mathbf{w} \\
(\mathbf{v}', \mathbf{w}') &\mapsto \mathbf{v}' + \mathbf{w}' \\
(\mathbf{v} + \mathbf{v}', \mathbf{w} + \mathbf{w}') &\mapsto \mathbf{v} + \mathbf{v}' + \mathbf{w} + \mathbf{w}' = \mathbf{v} + \mathbf{w} + \mathbf{v}' + \mathbf{w}'
\end{aligned}$$

Part 3: In this part, we prove σ is an isomorphism if and only if $V \cap W = \{\mathbf{0}\}$.
Assume that $V \cap W$ only contains the identity $\mathbf{0}$.

$$\begin{aligned}\mathbf{v} + \mathbf{w} = \mathbf{v}' + \mathbf{w}' &\implies -\mathbf{v}' + \mathbf{v} = \mathbf{w}' - \mathbf{w} \in V \cap W = \{\mathbf{0}\} \\ &\implies (\mathbf{v}, \mathbf{v}') = (\mathbf{w} + \mathbf{w}')\end{aligned}$$

Hence, the surjective homomorphism σ is injective, σ is an isomorphism.
Assume that $V \cap W$ contains some nonidentity element $\mathbf{u}$.

$$\begin{aligned}(\mathbf{u}, -\mathbf{u}) &\mapsto \mathbf{u} - \mathbf{u} = \mathbf{0} \\ (\mathbf{0}, -\mathbf{0}) &\mapsto \mathbf{0} - \mathbf{0} = \mathbf{0}\end{aligned}$$

Hence, σ fails to be injective, σ is not an isomorphism.
Quod. Erat. Demonstrandum. □

Proposition 3.3. Let A be a complex matrix of order n,
and λ be an eigenvalue of A.
If $\forall \mathbf{u} \in \mathbb{C}^n, (\lambda I - A)\mathbf{u} = \mathbf{0}$, then $\forall \mathbf{u} \in \mathbb{C}^n, \exists$ invariant $V \leq \mathbb{C}^n, \mathbb{C}^n \cong V \times \langle \mathbf{u} \rangle$.
Here, $\langle \mathbf{u} \rangle = \left\{ \sum_{l=0}^{k-1} c_l (\lambda I - A)^l \mathbf{u} \in \mathbb{C} : k \in \mathbb{Z} \text{ and } (c_l)_{l=1}^{k-1} \text{ in } \mathbb{C} \right\}$.

Proof. We may divide our proof into two cases.
Case 1: If $\mathbf{u} = \mathbf{0}$, then take $V = \mathbb{C}^n$.
Case 2: If $\mathbf{u} \neq \mathbf{0}$, then expand $\mathbf{u}$ into a basis of $\mathbb{C}^n$ and take the span of the rest as V.
Quod. Erat. Demonstrandum. □

Remark: *For this case, there exists* $(\mathbf{u}_k)_{k=0}^{l-1}$ *in* $\mathbb{C}^n$, *such that* $\mathbb{C}^n = \prod_{k=0}^{l-1} \langle \mathbf{u}_k \rangle$.

3.2 Finite Complex Matrix with Unique Eigenvalue

Next, we reduce a finite complex matrix with unique eigenvalue.

Proposition 3.4. Let A be a complex matrix of order n,
and λ be the unique eigenvalue of A.
If some $\mathbf{u} \in \mathbb{C}^n$ has maximal order β, then $\exists$ invariant $V \leq \mathbb{C}^n, \mathbb{C}^n \cong V \times \langle \mathbf{u} \rangle$.

Proof. We prove this theorem by mathematical induction.
Basis Step: When $n = 1$, $\mathbb{C}$ is cyclic, so $\exists$ invariant $\{\mathbf{0}\} \leq \mathbb{C}, \mathbb{C} \cong \{\mathbf{0}\} \times \langle \mathbf{u} \rangle$.
Inductive Hypothesis: For all $\gamma \in \mathbb{N}$, when $n = \gamma$, assume that for all $\mathbf{u} \in \mathbb{C}^n$, $\mathbf{u}$ has a maximal order β implies $\exists$ invariant $V \leq \mathbb{C}^n, \mathbb{C}^n \cong V \times \langle \mathbf{u} \rangle$.
Inductive Step: When $n = \gamma + 1$, for all $\mathbf{u} \in \mathbb{C}^n$ with maximal order β:
Case 1: If $n = \beta$, then $\mathbb{C}^n$ is cyclic, so $\exists \{\mathbf{0}\} \leq G, G \cong \{\mathbf{0}\} \times \langle \mathbf{u} \rangle$.
Case 2: If $n > \beta$, then $\mathbb{C}^n \backslash \langle \mathbf{u} \rangle \neq \emptyset$. Take $\mathbf{v} \in \mathbb{C}^n \backslash \langle \mathbf{u} \rangle$. WLOG, assume that $\text{ord}(\mathbf{v}) = 1$.
In $\mathbb{C}^n / \langle \mathbf{v} \rangle$, as $\langle \mathbf{u} \rangle \cap \langle \mathbf{v} \rangle = \{\mathbf{0}\}$, the coset $\mathbf{u} + \langle \mathbf{v} \rangle$ must have order β.

There exists $\widetilde{V} \leq \mathbb{C}^n/\langle \mathbf{u} \rangle = \{\mathbf{u}\}$, such that $\mathbb{C}^n/\langle \mathbf{u} \rangle = \widetilde{H} \times \langle \mathbf{u}\langle \mathbf{v} \rangle\rangle$.
This gives an invariant subspace $V = \pi^{-1}(\widetilde{V})$ of $\mathbb{C}^n$,
where $\pi : \mathbb{C}^n \to \mathbb{C}^n/\langle \mathbf{v} \rangle$ is the natural projection.
Note that $V \cap \langle \mathbf{u} \rangle = \{\mathbf{0}\}$, so $\exists$ invairant $V \leq \mathbb{C}^n, \mathbb{C}^n = V + \langle \mathbf{u} \rangle \cong V \times \langle \mathbf{u} \rangle$.
Quod. Erat. Demonstrandum. $\square$

Remark: *For this case, there exists* $(\mathbf{u}_k)_{k=0}^{l-1}$ *in* $\mathbb{C}^n$*, such that* $\mathbb{C}^n \cong \prod_{k=0}^{l-1} \langle \mathbf{u}_k \rangle$*.*
Assume that each $\operatorname{ord}(\mathbf{u}_k) = \alpha_k$*, then* $\mathbb{C}^n \cong \prod_{k=0}^{l-1} \mathbb{C}_\lambda^{\alpha_k}$*.*

3.3 Finite Complex Matrix with Multiple Eigenvalues

Proposition 3.5. Let A be a complex matrix of order n,
and λ, μ be two distinct eigenvalues of A.
For all λ-invariant subspace V and μ-invariant subspace W, $V \cap W = \{\mathbf{0}\}$.
Here, λ-invariant subspace V with unique eigenvalue λ.

Proof. For all $\mathbf{u} \in \mathbb{C}^n$:

$$\begin{aligned}
\mathbf{u} \in V \cap W &\implies \mathbf{u} \in V \text{ and } \mathbf{u} \in W \\
&\implies (\lambda I - A)^s \mathbf{u} = \mathbf{0} \text{ and } (\mu I - A)^t \mathbf{u} = \mathbf{0} \\
&\implies \mathbf{u} = f(A)(\lambda I - A)^s \mathbf{u} + g(A)(\mu I - A)^t \mathbf{u} = \mathbf{0}
\end{aligned}$$

Quod. Erat. Demonstrandum. $\square$

Remark: *Hence,* $\mathbb{C}^n$ *is the Cartesian product of* λ*-invariant subspaces.*

References

[1] H. Ren, “Template for math notes,” 2021.

[2] A. Piro, “The fundamental theorem for finite abelian groups: A brief history and proof.”