# IB Groups, Rings and Modules

Martin von Hodenberg (mjv43@cam.ac.uk)

January 27, 2022

These are my notes for the IB course 'Groups, Rings and Modules', which was lectured in Lent 2022 at Cambridge by Dr R.Zhou. These notes are written in LaTeX for my own revision purposes. Any suggestions or feedback is welcome.

## Contents

# §0 Introduction

This course will contain several sections:

1. Groups; this will be a continuation from IA, focusing on simple groups, $p$-groups, and $p$-subgroups. The main result in this part of the course will be the Sylow theorems.
2. Rings; these are sets where you can add, subtract and multiply (e.g $\mathbb{Z}$ or $\mathbb{C}[X]$). We will study rings of integers such as $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$. These also generalise to polynomial rings. We will also study fields, which are rings where you can divide (e.g $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$ for $p$ prime).
3. Modules; these are an analogue of vector spaces where the scalars belong to a ring instead of a field. We will classify modules over certain "nice" rings. This allows us to prove Jordan Normal Form, and classify finite abelian groups.

# §1 Groups

## §1.1 Recall of IA Groups

**Definition 1.1** (Group)

A group is a pair $(G, \cdot)$ where $G$ is a set and $\cdot : G \times G \to G$ is a binary operation satisfying:

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity)
2. $\exists e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$ (identity)
3. $\forall g \in G$, $\exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$ (inverses)

**Remark.**
- In practice, one often needs to check closure in order to check that $\cdot$ is well-defined.
- If using additive (respectively multiplicative) relations, we will often write 0 (or 1) for the identity.
- We write $|G|$ for the number of elements in $G$.

**Definition 1.2** (Subgroup)

A subset $H \subseteq G$ is a subgroup (written $H \leq G$) if $H$ is closed under $\cdot$ and $(H, \cdot)$ is a group.

**Remark.** A non-empty subset $H$ of $G$ is a subgroup if $a, b \in H \implies a \cdot b^{-1} \in H$ (see IA Groups for the proof).

**Example 1.3** (Examples of groups)

Groups we have already seen include:

- Additive groups $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.
- Cyclic and dihedral groups $C_n$ and $D_{2n}$.

- Abelian groups: those groups $G$ such that $a \cdot b = b \cdot a$ for all $a, b \in G$.
- Symmetric and alternating groups $S_n$ = group of all permutations of $\{1, \dots, n\}$ and $A_n \leq S_n$, the group of all even permutations.
- Quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ where $i, j, k$ are quaternions.
- General and special linear groups $GL_n(\mathbb{R}) = n \times n$ matrices on $\mathbb{R}$ with $\det \neq 0$, where the group operation is matrix multiplication. This contains the subgroup $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$, which is the subgroup of matrices with $\det = 1$.

**Definition 1.4** (Direct product)

The direct product of groups $G$ and $H$ is the set $G \times H$ with operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

**Theorem 1.5** (Lagrange's theorem)

Let $H \leq G$. Then the left cosets of $H$ in $G$ are the sets $gH = \{gh : h \in H\}$ for $g \in G$. These partition $G$, and each has the same cardinality as $H$. From this we can deduce Lagrange's theorem:

If $G$ is a finite group and $H \leq G$, then $|G| = |H|[G : H]$ where $[G : H]$ is the number of left cosets of $H$ in $G$ (the index of $H$ in $G$).

**Remark.** Can also carry this out with right cosets. A corollary of Lagrange's theorem is thus that the number of left cosets = number of right cosets.

**Definition 1.6** (Order of an element)

Let $g \in G$. If $\exists n \geq 1$ such that $g^n = 1$, then the least such $n$ is the order of $g$ in $G$. If no such $n$ exists, $g$ has infinite order.

**Remark.** If $g$ has order $d$, then

- $g^n = 1 \implies d | n$.
- $\{1, g, \dots, g^{d-1}\} \leq G$ and so if $G$ is finite, then $d \| G|$ (Lagrange).

**Definition 1.7** (Normal subgroup)

A subgroup $H \leq G$ is normal if $g^{-1} H g = H$ for all $g \in G$. We write $H \trianglelefteq G$.

**Proposition 1.8**

If $H \trianglelefteq G$ then the set $G/H$ of left cosets of $H$ in $G$ is a group (called the quotient group) with operation

$$g_1 H \cdot g_2 H = g_1 g_2 H.$$

*Proof.* Check $\cdot$ is well-defined:

Suppose $g_1H = g_1'H$ and $g_2H = g_2'H$ for some $g_1, g_1', g_2, g_2' \in G$. Then $g_1' = g_1h_1$ and $g_2' = g_2h_2$ for some $h_1, h_2 \in H$. Therefore

$$\begin{aligned} g_1'g_2' &= g_1h_1g_2h_2 \\ &= g_1g_2 \underbrace{({g_2}^{-1}h_1g_2)}_{\in H} \underbrace{h_2}_{\in H} \end{aligned}$$

Therefore $g_1'g_2'H = g_1g_2H$. Associativity is inherited from $G$, the identity is $H = eH$, and the inverse of $gH$ is $g^{-1}H$. □

**Definition 1.9** (Homomorphism)

If $G, H$ are groups, then a function $\phi : G \to H$ is a group homomorphism if $\phi(g_1g_2) = \phi(g_1g_2) = \phi(g_1)\phi(g_2)$. It has kernel

$$\ker \phi = \{g \in G : \ \phi(g) = e\} \leq G.$$

and image

$$\operatorname{Im} \phi = \{\phi(g) : \ g \in G\} \leq H.$$

**Remark.** If $a \in \ker \phi$ and $g \in G$, then

$$\begin{aligned} \phi(g^{-1}ag) &= \phi(g^{-1})\phi(a)\phi(g) \\ &= \phi(g^{-1})\phi(g) \\ &= \phi(g^{-1}g) = \phi(e) = e. \end{aligned}$$

So $g^{-1}ag \in \ker \phi$ and hence $\ker \phi$ is a normal subgroup of $G$.

**Definition 1.10** (Isomorphism)

An isomorphism of groups is a group homomorphism that is also a bijection. We say $G$ and $H$ are isomorphic and write $G \cong H$ if there exists an isomorphism $\phi : G \to H$. (Note it follows from the definition that $\phi^{-1}$ is also a group homomorphism)

**Theorem 1.11** (First Isomorphism Theorem)

Let $\phi : G \to H$ be a group homomorphism. Then $\ker \phi \trianglelefteq G$ and

$$G/\ker \phi \cong \operatorname{Im} \phi.$$

*Proof.* Let $K = \ker \phi$. We have already checked $K$ is normal. Now we define $\Phi : G/K \to \operatorname{Im} \phi$ by

$$gK \to \phi(g)..$$

To show $\Phi$ is well defined and injective:

$$\begin{aligned} g_1K = g_2K &\iff {g_2}^{-1}g_1 \in K \\ &\iff \phi({g_2}^{-1}g_1) = e \\ &\iff \phi(g_1) = \phi(g_2). \end{aligned}$$

To show $\Phi$ is a group hom.:

$$\begin{aligned}\Phi(g_1Kg_2K) &= \Phi(g_1g_2K) \\ &= \phi(g_1g_2) = \phi(g_1)\phi(g_2) \\ &= \Phi(g_1K)\Phi(g_2K)\end{aligned}$$

Showing $\Phi$ is surjective:

Let $x \in \operatorname{Im}\phi$, say $x = \phi(g)$ for some $g \in G$. Then $x = \phi(gR)$. $\square$

**Example 1.12**

Let $\phi : \mathbb{C} \to \mathbb{C}^x = \{x \in C : x \neq 0\}$ given by $z \mapsto e^z$.

Since $e^{z+w} = e^z e^w$, this is a group homomorphism from $(\mathbb{C}, +) \to (\mathbb{C}^x, \times)$. We have that

$$\begin{aligned}\ker\phi &= \{z \in \mathbb{C} :\ e^x = 1\} = 2\pi i\mathbb{Z} \\ \operatorname{Im}\phi &= \mathbb{C}^x \text{ by existence of log}\end{aligned}$$

Hence $\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^x$.

**Theorem 1.13** (Second Isomorphism Theorem)

Let $H \leq G$, and $K \trianglelefteq G$. Then $HK = \{hk : h \in H, k \in K\} \leq G$ and $H \cap K \trianglelefteq H$. Moreover,

$$HK/K \cong H/(H \cap K).$$

*Proof.* Let $h_1k_1, h_2k_2 \in HK$ (so $h_1h_2 \in H,\ k_1k_2 \in K$). Now

$$h_1k_1(h_2k_2)^{-1} = \underbrace{h_1{h_2}^{-1}}_{\in H}\underbrace{(h_2k_1{k_2}^{-1}{h_2}^{-1})}_{\in K} \in HK.$$

Thus $HK \leq G$ (by our previous remark). Let $\phi : H \to G/K$ be given by $h \to hK$. This is the composite of $H \to G$ and the quotient map $G \to G/K$; hence $\phi$ is a group homomorphism. Thus

$$\begin{aligned}\ker\phi &= \{h \in H : hK = K\} = H \cap K \trianglelefteq H \\ \operatorname{Im}\phi &= \{hK :\ h \in H\} = HK/K\end{aligned}$$

Now by the First Isomorphism Theorem

$$HK/K \cong H/(H \cap K).$$

$\square$

**Remark** (1.2)**.** Suppose $K \trianglelefteq G$. There is a bijection

$$\{\text{subgroups of } G/K\} \leftrightarrow \{\text{subgroups of } G \text{ containing } K\},$$

where $X \mapsto \{g \in G : gK \in X\}$ and $H/K \leftarrow H$. This further restricts to a bijection

$$\{\text{normal subgroups of } G/K\} \leftrightarrow \{\text{normal subgroups of } G \text{ containing } K\},$$

**Theorem 1.14** (Third Isomorphism Theorem)
Let $K \leq H \leq G$ be normal subgroups of $G$. Then

$$\frac{G/K}{H/K} \cong G/H.$$

*Proof.* Let $\phi : G/K \to G/K$ be defined by $gK \mapsto gH$. If $g_1K = g_2K$, then ${g_2}^{-1}g_1 \in K \leq H \implies g_1H = g_2H$. Thus $\phi$ is well-defined.

Thus $\phi$ is a surjective homomorphim with kernel $H/K$. Now just apply the First Isomorphism Theorem. □

## §1.2 Simple groups

If $K \trianglelefteq G$, then studying the groups $K$ and $G/K$ gives some information about $G$. However, this approach is not always available. This is the case when a group is simple.

**Definition 1.15** (Simple group)
A group $G$ is simple if $\{e\}$ and $G$ are its only normal subgroups.

**Remark.** It is convention to not consider the trivial group a simple group.

**Lemma 1.16**
Let $G$ be an abelian group. $G$ is simple iff $G \cong C_p$ for some prime $p$.

*Proof.* $\Longleftarrow$ **:** Let $H \leq C_p$. Lagrange's theorem says that $|H|\ ||C_p| = p$. Since $p$ is prime, $|H| = 1$ or $p$. So $H$ is the trivial group or $C_p$.

$\implies$ **:** Let $g \in G$ where $g \neq e$. Consider the subgroup generated by $g$:

$$\langle g \rangle = \left\{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\right\}.$$

This is normal in $G$ since $G$ is abelian. Since $G$ is simple, $\langle g \rangle = G$. If $G$ is infinite, $G \cong (\mathbb{Z}, +)$ and $2\mathbb{Z} \leq \mathbb{Z}$ which gives a contradiction.

Otherwise, we now know $G \cong C_n$ for some $n$. Let $g$ be a generator. If $m|n$ then $g^{n/m}$ generates a subgroup of order $m$ and so $G$ simple $\implies$ the only factors of $n$ are 1 and $n$. Therefore $n$ is prime. □

**Lemma 1.17**
If $G$ is a finite group, then $G$ has a composition series

$$e = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m = G,$$

with each quotient $G_i/G_{i-1}$ simple.

*Proof.* We induct on $|G|$. If $|G| = 1$ it's obvious. If $|G| > 1$, let $G_{m-1}$ be a normal subgroup of largest possible order that isn't $G$ itself. Remark 1.2 implies $G/G_{m-1}$ is simple. Then apply the induction hypothesis to $G_{m-1}$. □

## §1.3 Group actions

**Definition 1.18** (Permutation group)

For $X$ any set, let $\text{Sym}(X)$ be the group of all bijections $X \to X$ under composition. This clearly forms a group with $e = \text{Id}_X$.

A group $G$ is a permutation group of degree n if $G \leq \text{Sym}(X)$ with $|X| = n$.

**Example 1.19** (Examples of permutation group)

- $S_n = \text{Sym}(\{1, 2, \ldots, n\})$ is a permutation group of degree $n$, as is $A_n \leq S_n$.
- $D_{2n} =$ (symmetries of a regular $n$-gon) is a subgroup of $\text{Sym}(\{\text{vertices of n-gon}\})$.

**Definition 1.20** (Group action)

An actio of a group $G$ on a set $X$ is a function $* : G \times X \to X$ satisfying

(i) $e * x = x$ for all $x \in X$

(ii) $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G$, $x \in X$.

**Proposition 1.21**

An action of a group $G$ on a set $X$ is equivalent to specifying a group homomorphism $\phi : G \to \text{Sym}(X)$.

*Proof.* For each $g \in G$, let $\phi_g : X \to X$ send $x \mapsto g * x$.

We have $\phi_{g_1 g_2}(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = \phi_{g_1} \circ \phi_{g_2}(x)$. (†)

In particular, $\phi_g \circ \phi_{g^{-1}} = \phi_{g^{-1}} \circ \phi_g = \phi_e = \text{Id}_X$. Thus $\phi_g \in \text{Sym}(X)$. Then the map $\phi : G \to \text{Sym}(X)$ given by $g \mapsto \phi_g$ is a group homomorphism by (†).

Conversely, let $\phi : G \to \text{Sym}(X)$ be a group homomorphism. Define $* : G \times X \to X$ given by $(g, x) \mapsto \phi(g)(x)$. Then

(i) $e * x = \phi(e)(x) = \text{Id}_X(x) = x$.

(ii) $(g_1 g_2) * x = \phi(g_1 g_2)(x) = \phi(g_1)(\phi(g_2)(x)) = g_1 * (g_2 * x)$.

□

**Definition 1.22**

We say $\phi : G \to \text{Sym}(X)$ is a permutation representation of $G$.

**Definition 1.23** (Orbit and stabiliser)

Let $G$ act on a set $X$.

(i) The orbit of $x \in X$ is $\operatorname{orb}_G(x) = \{g * x : \ g \in G\} \subset X$

(ii) The stabiliser of $x \in X$ is

$$G_x = \{g \in G : \ g * x = x\} \leq G.$$

Recall the Orbit-Stabiliser Theorem from IA Groups: There is a bijection $\operatorname{orb}_G(x) \leftrightarrow$ the set of left cosets of $G_x$ in $G$. In particular if $G$ is finite, then

$$|G| = |\operatorname{orb}_G(x)||G_x|.$$

**Example 1.24** (Example of Orbit-Stabiliser)

Let $G$ be the group of all symmetries of a cube, acting on the set of veretices $X$. We can reach any vertex from any other one, so $|\operatorname{orb}_G(x)| = 8$. Some basic geometry gives $|G_x| = 6$. Therefore $|G| = 48$.

**Remark.**

- $\ker \phi = \bigcap_{x \in X} G_x$ is called the kernel of the group action.
- The orbits partition $X$. We say the action is transitive if there is only one orbit.
- $G_{g*x} = gG_xg^{-1}$, so if $x, y \in X$ belong to the same orbit, then their stabilisers are conjugate.

Later on a lot of the proofs will involve picking a nice group action. So let's look at some examples of group actions.

(i) Let $G$ act on itself by left multiplication, i.e $g * x = gx$. The kernel of this action is

$$\{g \in G : gx = x \quad \forall x \in G\} = e.$$

Thus $G$ is injective into $\operatorname{Sym}(G)$. This proves Cayley's theorem:

**Theorem 1.25** (Cayley's theorem)

Any finite group $G$ is isomorphic to a subgroup of the symmetric group $S_n$ for some $n$. (Take $n = |G|$.)

*Proof.* As above in (i). □

(ii) Let $H \leq G$; then $G$ acts on $G/H$ by left multiplication, i.e $g * xH = gxH$. This action is transitive (since $(x_2{x_1}^{-1})x_1H = x_2H$) with

$$\begin{aligned} G_{xH} &= \{g \in G : gxH = xH\} \\ &= \left\{g \in G : x^{-1}gx \in H\right\} \\ &= xHx^{-1} \end{aligned}$$

Thus $\ker(\phi) = \bigcap_{x \in G} xHx^{-1}$. This is the largest normal subgroup of $G$ that is contained in $H$.

**Theorem 1.26**

Let $G$ be a non-abelian simple group, and $H \leq G$ a subgroup of index $n > 1$. Then $n \geq (5$ and $G$ is isomorphic to a subgroup of $A_n$.

*Proof.* Let $G$ act on $X = G/H$ by left multiplication, and let $\phi : G \to \mathrm{Sym}(X)$ be the associated permutation representation. As $G$ is simple, $\ker(\phi) = e$ or $G$. If $\ker(\phi) = G$, then $\mathrm{Im}(\phi) = e$. This is a contradiction since $G$ acts transitively on $X$ and $|X| > 1$. Thus $\ker(\phi) = e$ and $G \cong \mathrm{Im}(\phi) \leq S_n$. Since $G \leq S_n$ and $A_n \trianglelefteq S_n$, the second isomorphism theorem gives $G \cap A_n \trianglelefteq G$ and $G/(G \cap A_n) \cong GA_n/A_n \leq S_n/A_n \cong C_2$. Since $G$ is simple, $G \cap A_n = e$ (this is impossible as $G \leq C_2$ but $G$ isn't abelian) or $G$. Thus $G \leq A_n$. Finally, if $n \leq 4$, then $A_n$ has no non-abelian simple subgroups. □

(iii) Let $G$ act on itself by conjugation, i.e $g * x = gxg^{-1}$. We define the conjugacy class of $x \in G$ to be

$$\mathrm{ccl}_G(x) = \mathrm{orb}_G(x) = \left\{gxg^{-1} \in G : \quad g \in G\right\}.$$

We also define the centraliser of $x$ by

$$C_G(x) = G_x = \{g \in G : \quad gx = xg\} \leq G.$$

We define the centre of $G$ by

$$Z(G) = \mathrm{Ker}(\phi) = \{g \in G : \quad gx = xg \ \forall x \in G\}.$$

Note that the $\phi(g) : G \to G$ given by $h \mapsto ghg^{-1}$ satisfies

$$\phi(g)(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \phi(g)(h_1)\phi(g)(h_2).$$

Thus $\phi(g)$ is a group homomorphism, and also a bijection i.e $\phi(g)$ is an isomorphism.

**Definition 1.27** (Automorphism)

$\mathrm{Aut}(G) = \{$ group isomorphisms $\zeta : G \to G\}$. Then $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$ and $\phi : G \to \mathrm{Sym}(G)$ has image in $\mathrm{Aut}(G)$.

(iv) Let $X$ be the set of all subgroups of $G$. Then $G$ acts on $X$ by conjugation, i.e $g * H = gHg^{-1}$. The stabiliser of $H$ is

$$\left\{g \in G : \quad gHg^{-1} = H\right\} = N_G(H).$$

This is also called the normaliser of $H$ in $G$, and is the largest subgroup of $G$ containing $H$ as a normal subgroup. In particular,

$$H \trianglelefteq G \iff N_G(H) = G.$$

## §1.4 Alternating groups

From IA Groups, we know that elements in $S_n$ are conjugate iff they have the same cycle type. For example, in $S_5$, we have the following:

| Cycle type | Number of elements | Sign |
|---|---|---|
| id | 1 | +1 |
| $(**)$ | 10 | -1 |
| $(**)(**)$ | 15 | +1 |
| $(***)$ | 20 | +1 |
| $(**)(***)$ | 20 | -1 |
| $(****)$ | 30 | -1 |
| $(*****)$ | 24 | +1 |
| Total: | $120{=}5!{=}\|S_5\|$ | |

Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$. We effectively have two cases:

- If there exists an odd permutation commuting with $g$, then $|C_{A_n}(g)| = \frac{1}{2}|C_{S_n}(g)|$ and by Orbit-Stabiliser, $|\operatorname{ccl}_{A_n}(g)| = |\operatorname{ccl}_{S_n}(g)|$.
- Otherwise, $|C_{A_n}(g)| = |C_{S_n}(g)|$ and by Orbit-Stabiliser, $|\operatorname{ccl}_{A_n}(g)| = \frac{1}{2}|\operatorname{ccl}_{S_n}(g)|$.

**Example 1.28** (Conjugacy classes of $A_5$)

If we take $n = 5$, then first consider the element $(12)(34)$, which commutes with $(12)$. Also, $(123)$ commutes with $(45)$.

But if we take $g = (12345)$, then $h \in C_{S_5}(g)$ means

$$\begin{aligned}(12345) &= h(12345)h^{-1} \\ &= (h(1)h(2)h(3)h(4)h(5)) \implies h \in \langle g \rangle \leq A_5.\end{aligned}$$

In this case, the conjugacy class does split.

Thus $A_5$ has conjugacy classes of sizes 1,15,20,12,12.

**Proposition 1.29**

$A_5$ is simple.

*Proof.* If $H \trianglelefteq A_5$, then $H$ is a union of conjugacy classes. Therefore

$$|H| = 1 + 15a + 20b + 12c \quad \text{for some } a, b \in \{0,1\} \text{ and } c \in \{0,1,2\}\,.$$

Since $H|60$, this implies $H = 1$ or 60, i.e $A_5$ is simple. □

Now we move on to a more general statement about $A_n$ being simple. Before we can do that, we will need some lemmas for the proof.

**Lemma 1.30**

$A_n$ is generated by 3-cycles.

*Proof.* Each $\sigma \in A_n$ is a product of an even number of transpositions. Thus it suffices to write the product of any two transpositions as a product of 3-cycles. For

$a, b, c, d$ distinct, we can have

$$\begin{cases} (ab)(bc) = (abc) \\ (ab)(cd) = (acb)(acd). \end{cases}$$

□

**Lemma 1.31**

If $n \geq 5$, then all 3-cycles in $A_n$ are conjugate.

*Proof.* We claim that every 3-cycle is conjugate to (123). Indeed, if $(abc)$ is a 3-cycle, then $(abc) = \sigma(abc)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \notin A_n$, then replace $\sigma$ by $\sigma(45)$ (using the fact that $n \geq 5$). □

**Theorem 1.32**

$A_n$ is simple for all $n \geq 5$.

*Proof.* Let $e \neq N \trianglelefteq A_n$. Suffices to show that $N$ contains a 3-cycle, since by 1.30 and 1.31 we then have $N = A_n$.

Take $e \neq \sigma \in N$ and write $\sigma$ in its disjoint cycle decomposition. We have three cases:

1. $\sigma$ contains a cycle of length $r \geq 4$. WLOG $\sigma = (123\ldots r)\tau$, where $\tau$ is some product of cycles that fixes $1, 2, \ldots, r$.

   Let $\delta = (123)$. Then consider the element

   $$\underbrace{\sigma^{-1}}_{\in N}\underbrace{\delta^{-1}\sigma\delta}_{\in N} = (r\ldots 21)(132)(12\ldots r)(123) = (23r) \in N.$$

   Note $\tau$ gets cancelled as it fixes 1 to $r$. Therefore $N$ contains a 3-cycle and we are done.

2. $\sigma$ contains two 3-cycles. WLOG $\sigma = (123)(456)\tau$. Let $b = (124)$. Then

   $$\sigma^{-1}\delta^{-1}\sigma\delta = (132)(465)(142)(123)(456)(124) = (12436) \in N.$$

   Then we are back to Case 1, so we are done.

3. $\sigma$ contains two 2-cycles. WLOG $\sigma = (12)(34)\tau$. Let $\delta = (123)$ and consider

   $$\sigma^{-1}\delta^{-1}\sigma\delta = (12)(34)(132)(12)(34)(123) = (14)(23) = \pi \in N.$$

   Let $\varepsilon = (235)$. Then

   $$\pi^{-1}\varepsilon^{-1}\pi\varepsilon = (14)(23)(253)(14)(23)(235) = (253).$$

   So we are done.

□