Groups, Rings, and Modules

Notes made by Finley Cooper

13th July 2025

Contents

1 Review of IA Groups

1.1 Definitions

We'll start with some simple definitions covered in IA Groups

Definition. A group is a *triple*, $(G, \circ, e)$ consisting of a set G, a binary operation $\circ : G \times G \to G$ and an identity element $e \in G$ where we have the following three properties,

- $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$
- $\forall a \in G, a \circ e = e \circ a = a$
- $\forall a \in G, \exists a^{-1} \in G, a \circ a^{-1} = a^{-1} \circ a = e$

We say that the *order* of the group $(G, \circ, e)$ is the size of the set G

Proposition. Inverses are unique.

Proof. Basic algebraic manipulation, covered in Part IA Groups.

Definition. If G is a group, then a subset $H \subseteq G$ is a subgroup if the following hold,

- $e \in H$
- If $a, b \in H$ then $a \circ b \in H$
- $(H, \circ, e)$ forms a group.

Now we'll give simple test for a subset being a subgroup

Lemma. A non-empty subset, H, of a group G is a subgroup if and only if $\forall h_1, h_2 \in H$ we have that $h_1 h_2^{-1} \in H$

Proof. Again covered in Part IA Groups

Definition. A group G is abelian if $\forall g_1, g_2 \in G$ we have that $g_1 g_2 = g_2 g_1$

Let's look at some examples of groups.

- The integers under addition, $(\mathbb{Z}, +)$
- The integers modulo n under addition $(\mathbb{Z}_n, +_n)$
- The rational numbers under addition $(\mathbb{Q}, +)$
- The set of all bijections from $\{1, \cdots, n\}$ to itself with the operation given by functional composition, S_n
- The set of all bijections from a set X to itself under functional composition is a group $\mathrm{Sym}(X)$
- The dihedral group, D_{2n} the set of symmetries of the regular n-gon
- The general linear group over $\mathbb{R}$, $\mathrm{GL}(n, \mathbb{R})$, is the set of functions from $\mathbb{R} \to \mathbb{R}$ which are linear and invertiable. Or we can think of the group as the set of $n \times n$ invertiable matrices under matrix multiplication. We can view this group as a subgroup of $\mathrm{Sym}(\mathbb{R}^n)$

- The subgroup of S_n which are even permutations, so can be written as a product of evenly many transpositions, A_n
- The subgroup of D_{2n} which are only the rotation symmetries which is denoted by C_n
- The subgroup of $\mathrm{GL}(n, \mathbb{R})$ of matrices which have determinate 1 which is $\mathrm{SL}(n, \mathbb{R})$
- The Klein four-group, which is $K_4 = C_2 \times C_2$, the symmetries of the non-square rectangle
- The quaternions, Q_8 with the elements $\{\pm 1, \pm i, \pm j, \pm k\}$ with multiplication defined with $ij = k, ji = -k$, $i^2 = j^2 = k^2 = -1$

1.2 Cosets

Definition. Let G be a group and $g \in G$. Let H be a subgroup of G. The *left coset*, written as gH is the set $\{gh : h \in H\}$

Some observations we can make are,

- Since $e \in H$ we have that $g \in gH$. So every element is in some coset
- The cosets partition, so if $gH \cap g'H \neq \emptyset$ then $gH = g'H$
- The function, $f : H \to gH$ defined by $f(h) = gh$ is a bijection, so all cosets are the same size

Theorem. (Lagrange's Theorem) If G is a finite group, then for a subgroup H of G, $|G| = |H||G : H|$, where $|G : H|$ is the number of left cosets of H in G

Proof. Obvious from the observations we've just made.

Definition. Let G be a group, and take some element $g \in G$. We define the *order* of g as the smallest positive integer n, such that $g^n = e$. If no such n exists, we say the order of g is infinite. We denote the order by ord(g).

Proposition. Let G be a group and $g \in G$. Then $\mathrm{ord}(g)$ divides $|G|$

Proof. Let $g \in G$. Consider the subset, $H = \{e, g, g^2, \cdots, g^{n-1}\}$ where n is the order of g. We claim H is a subgroup. $e \in H$ so H is non-empty. Observe that $g^r g^{-s} = g^{r-s} \in H$ so we have that $H \leq G$. Elements are distinct since if $g_i = g_j, i \neq j, 0 \leq i < j < n$ then $gj - i = e$ which contradicts the minimality of n since $0 \leq j - i \leq n$. We have that $|H| = n$, so by Lagrange, $|H|$ divides, $|G|$.

1.3 Normal subgroups

When does $gH = g'H$? Then $g \in g'H$, so we have that ${g'}^{-1} g \in H$. The converse also holds.

Lemma. For a group G with $g, g' \in G$ and subgroup H we have that $gH = g'H$ if and only if ${g'}^{-1} g \in H$

Proof. In Part IA Groups

Let $G/H = \{gH : g \in G\}$ be the set of left cosets. This partitions G. Does G/H have a natural group structure?
We propose the formula that $g_1H \cdot g_2H = (g_1g_2) \cdot H$ for a group law on G/H.
We need to check well definedness of this proposed formula.
Case 1: Suppose that $g_2H = g_2'H$. Then $g_2' = g_2h$ for some $h \in H$. $(g_1H) \cdot (g_2'H) = g_1g_2'H$ by the proposed formula. By the previous relation this is $g_1g_2hH = g_1g_2H$.

Case 2: Suppose that $g_1H = g_1'H$ we have that $g_1' = g_1h$ for some $h \in H$. We need $g_1g_2H = \underbrace{g_1h}_{g_1'}g_2H$. Equivalently we need that $(g_1g_2)^{-1}g_1hg_2 \in H$. Or equivalently still, ${g_2}^{-1}hg_2 \in H$ for all g_2 and h. This the definition of normality.

Definition. (Normality) A subgroup $H \leq G$ is *normal* if $\forall g \in G$, $h \in H$, we have that $ghg^{-1} \in H$

If $H \leq G$ is normal we write that $H \triangleleft G$.

Definition. (Quotient) Let $H \triangleleft G$. The *quotient group* is the set $(G/H, \cdot, e = eH)$ where $\cdot : G/H \times G/H \to G/H$ by $(g_1H, g_2H) \to (g_1g_2)H$.

Definition. (Homomorphism) Let G and H be groups. A *homomorphism* is a function $f : G \to H$ such that for all $g_1, g_2 \in G$ we have that $f(g_1g_2) = f(g_1)f(g_2)$

This is a very constrained condition. For example $f(e_G) = e_H$ always. To see this, observe $e_G = e_Ge_G$, so we have that $f(e_G) = f(e_G)f(e_G)$ so $f(e_G) = e_H$ by multiplying by $f(e_G)^{-1}$.

Lemma. If $f : G \to H$ is a homomorphism. Then $f(g^{-1}) = f(g)^{-1}$

Proof. Calculate $f(gg^{-1})$ in two ways.
In the first way $f(gg^{-1}) = f(e) = e$, in the second way $f(gg^{-1}) = f(g)f(g^{-1})$.
Equating gives that $f(g^{-1}) = f(g)^{-1}$.

Definition. Let $f : G \to H$ be a homomorphism. The *kernal* of f is $\ker f = \{g \in G : f(g) = e\}$. The *image* of f is $\operatorname{im} f = \{h \in H : h = f(g) \text{ for some } g \in G\}$.

Proposition. Let $f : G \to H$ be a homomorphism. Then $\ker f \triangleleft G$ and $\operatorname{im} f \leq H$.

Proof. First let's proof that $\ker f$ is a subgroup by the subgroup test. Observe by the lemma that $e \in \ker f$.. If $x, y \in \ker f$, then $f(xy^{-1}) = f(x)f(y)^{-1} = e \implies xy^{-1} \in \ker f$. For normality, let $x \in G$ and $g \in \ker f$. Calculate $f(xgx^{-1}) = f(x)f(g)f(x)^{-1}$. But $f(g) = e$. So we just get the identity. Hence we have that $xgx^{-1} \in \ker f$. So $ker f \triangleleft G$.
To check that the $\operatorname{im} f \leq H$, take $a, b \in \operatorname{im} f$, say that $a = f(x), b = f(y)$. Then $ab^{-1} =$

$f(x)f(y)^{-1} = f(xy^{-1})$. But $xy^{-1} \in G$ so $f(xy^{-1}) \in \operatorname{im} f$. Also $e \in \operatorname{im} f$, so we have that $\operatorname{im} f \leq H$.

Definition. (Isomorphism) A homomorphism $f : G \to H$ is an *isomorphism* if it is a bijection. Two groups are called *isomorphic* if there exists an isomorphism between them.

Theorem. (First isomorphism theorem) Let $f : G \to H$ be a homomorphism. Then $\ker f$ is normal, and the function $\varphi : G/\ker f \to \operatorname{im} f$, by $\varphi(g \ker f) = f(g)$, is a well-defined, isomorphism of groups.

Proof. Already shown $\ker f \lhd G$. Consider whenever φ is well-defined. Suppose that $g \ker f = g' \ker f$. Need to check $\varphi(g \ker f) = \varphi(g' \ker f)$. We know that $gg'^{-1} \in \ker f$, so $f(g'g^{-1}) = e \iff f(g') = f(g)$. To see that φ is a homomorphism: $\varphi(g \ker f g' \ker f) = \varphi(gg' \ker f) = f(gg') = f(g)f(g') = \varphi(g \ker f)\varphi(g' \ker f)$. So φ is a homomorphism.

Finally let's check φ is bijective. First for surjectivity, let $h \in \operatorname{im} f$, then $h = f(g)$ for some $g \in G$. So we have that $h = \varphi(g \ker f)$.
Now for injectivity, $\varphi(g \ker f) = \varphi(g' \ker f) \implies f(g) = f(g') \implies g'g^{-1} \in \ker f$. Hence the cosets are the same by the coset equality criterion, so we have that $g \ker f = g' \ker f$, hence we have injectivity, so φ is an isomorphism.

For an example of this theorem, consider the groups $(\mathbb{C}, +)$ and $(\mathbb{C}^*, \times)$ related by the homomorphism, $\varphi(z) = e^z$. The kernal of exp is exactly, $2\pi i\mathbb{Z} \leq \mathbb{C}$, so the first isomorphism theorem gives that $\frac{\mathbb{C}}{2\pi i \mathbb{Z}} \cong \mathbb{C}^*$. *(Try to visualise this!)*

Theorem. (Second isomorphism theorem) Let $H \leq G$ and $K \lhd G$. Then $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G, the set $H \cap K$ is normal in H, and $\frac{HK}{K} \cong \frac{H}{H \cap K}$.

Proof. We take the statements in turn. First we can see that HK is a subgroup. Clearly it contains the identity, and take some $x, y \in HK$, $x = hk, y = h'k'$. We will show that $yx^{-1} \in HK$. Observe that $yx^{-1} = h'k'k^{-1}h^{-1} = h'(h^{-1}h)(k'k^{-1})h^{-1} = (h'h^{-1})h\underbrace{(k'k^{-1})}_{k''}h^{-1}$. But we have that $hk''h^{-1} \in K$ by the normality of K, hence $yx^{-1} \in HK$. So we have that $HK \leq G$.

Now we prove that $H \cap K \lhd G$. Consider the homomorphism, $\varphi : H \to G/K$, defined as $\varphi(h) = hK$. This is a well defined homomorphism for the same reason that the group structure G/K is well-defined. The kernal of φ, is $\ker \varphi = \{h : hK = K\} = \{h : h \in K\} = H \cap K \lhd G$.

Now finally we're left to prove the isomorphism. Now apply the first isomorphism theorem to φ. This tells us that $\frac{H}{\ker \varphi} = \frac{H}{H \cap K} \cong \operatorname{im} \varphi$. The image of the φ is exactly those coests of K in G that can be represented as hK which is exactly $\frac{HK}{K}$.

Theorem. (Correspondence theorem). Consider a group G with $K \triangleleft G$, with the homomorphism $p : G \to G/K$, by $p(g) = gK$. Then there is a bijection between the subgroups of G which contain K and the subgroups of G/K.

Proof. For some subgroup L, we have $K \triangleleft L \leq G$, and we map L to L/K, so we have that $L/K \leq G/K$. In the reverse direction, for a subgroup $A \leq G/K$, we map it to $\{g \in G : gK \in A\}$.
We can think of this as taking $L \to p(L)$ and $p^{-1}(A) \leftarrow A$.

Now we will state some facts without proof. (Although the proofs are fairly straightforward).

- This is a bijection.
- This correspondence maps normal subgroups to normal subgroups.

Theorem. (Third isomorphism theorem) Let K, L be normal subgroups of G with $K \leq L \leq G$. Then we have that $\frac{G/K}{L/K} \cong \frac{G}{L}$.

Proof. Define a map $\varphi : G/K \to G/L$, by $\varphi(gK) = gL$. First we'll show that φ is a well-defined homomorphism, then we'll calculate the image and kernal, and finally apply the first isomophism theorem. To see well-definedness, if $gK = g'K$, then $g'g^{-1} \in K \subseteq L$, so $g'L = gL$, so φ is well-defined. Obviously a homomorphism.
The kernal of φ is $\ker \varphi = \{gK : gL = L\} = \{gK : g \in L\} = L/K$. φ is clearly surjective, so we conclude by the first isomorphism theorem that $\frac{G/K}{L/K} \cong \frac{G}{L}$.

Definition. (Simple groups) A group G is called *simple* if the only normal subgroups are G itself and $\{e\}$.

Proposition. Let G be an abelian group. Then G is simple if and only if $G \cong C_p$, for p prime.

Proof. If $G \cong C_p$, then any $g \in G, g \neq e$ is a generator of G by Lagrange. Conversely if G is simple and abelian, then take some non-identity, $g \in G$, then $\{g^n : n \in \mathbb{Z}\}$ is a subgroup, and because G is abelian, this subgroup is normal. Since $g \neq e$, we must have G is cyclic, generated by g. Now if G is infinitely cyclic, then $G \cong \mathbb{Z}$, which is not simple since $2\mathbb{Z} \triangleleft \mathbb{Z}$, so we can't have this. Therefore $G \cong C_m$ for some $m \in \mathbb{Z}_{>0}$. Say q divides m, then the subgroup of G generated by $g^{\frac{m}{q}}$ is a normal subgroup, so we must have that $q = m$ or $q = 1$ by simplicity, hence we have that m is prime.

Theorem. (Composition series) Let G be a finite group. Then there exists subgroups such that, $G = H_1 \triangleright H_2 \triangleright H_3 \triangleright \cdots \triangleright H_n = \{e\}$, such that $\frac{H_i}{H_{i+1}}$ is simple.

Proof. If G is simple then take $H_2 = \{e\}$ and we're done. Otherwise, let H_2 be a proper normal subgroup of maximal order in G. We claim that G/H_2 is simple. To see this, suppose not and consider $\varphi : G \to G/H_2$. By non-simplicity and correspondence between normal subgroups, we find a proper normal in G/H_2 and therefore a proper normal $K \triangleleft G$. This leads to a contradiction as K contains H_2 non-trivally, so we contradict maximality, so G/H_2 is simple. Now we continue by replacing G with H_2 and iterate the process. Either we get that H_2 simple and we're done again, or we get find a proper normal subgroup $H_3 \triangleleft H_2$ of maximal order. This process must terminate, since G is finite and the order is strictly decreasing in each step.

We know from Part IA groups that A_5 is simple. We see a series like this for S_5, namely, $S_5 \triangleright A_5 \triangleright \{e\}$.

1.4 Groups actions and permutations

Definition. Let X be a set. Let $\mathrm{Sym}(x)$ denote the symmetric group of X and $S_n = \mathrm{Sym}([n])$ where we have that $[n] = \{1, 2, \ldots, n\}$.

Reminders from IA Groups:

- We can write any $\sigma \in S_n$ as a product of disjoint cycles.
- If $\sigma \in S_n$ we can write σ as a product of transpositions. The number of transpositions needed to write σ is well-defined modulo 2. This is called the sign of the transposition, denoted by sgn, where $\mathrm{sgn} : S_n \to \{\pm 1\}$.
- sgn is a homomorphism between the groups where $\{\pm 1\}$ is given the unique group structure. When $n \geq 3$, the homomorphism is surjective.

Definition. (Alternating group) The *alternating group* A_n is the kernal of sgn.

A homomorphism $\varphi : G \to \mathrm{Sym}(X)$ is called a permutation representation of G.

Definition. (Group action) An *action* of G on a set X is a function $\tau : G \times X \to X$ sending $(g, x) \to \tau(g, x) \in X$ such that $\tau(e, x) = x, \forall x \in X$, and $\tau(g_1, \tau(g_2, x)) = \tau(g_1 g_2, x), \forall g_1 g_2 \in G, \forall x \in X$.

How are actions and permmutation representations related?
For some homomorphism, $\varphi : G \to \mathrm{Sym}(X)$ we map the homomorphism to $a(\varphi) : G \times X \to X$, where $(g, x) \to \varphi(g)(x)$.

Proposition. The funtion a above is a bijection from the set of homomorphism from $G \to \mathrm{Sym}(X)$ to the set of actions from G on X.

Proof. We'll construct an inverse of a. Given a group action $* : G \times X \to X$. Define $\varphi(*) : G \to \mathrm{Sym}(X)$ defined by sending $g \to \varphi(*)(g)$, where $\varphi(*)(g)(x) = g * x$. We aim to show that $\varphi(*)(g) : X \to X$ is a permutation. We have an inverse $\varphi(*)(g^{-1})$, and to see that it is a homomorphism $\varphi(*)(g_1)\varphi(*)(g_2)(x) = g_1 * (g_2 * x) = (g_1 g_2) * x = \varphi(*)(g_1 g_2)(x)$. This is true for all x, so the construction is a group homomorphism.

Notation: Given a group action G acting on X given by $\varphi : G \to \mathrm{Sym}(X)$, denote

$G^X = \text{im}(\varphi)$, and $G_X = \ker(\varphi)$. By the first isomorphism theorem we have that $G_X \triangleleft G$ and $G/G_X \cong G^X$.

For an example, consider the unit cube. Let G be the symmetric group it. Now let X be the set of (body) diagonals of the cube. Any element of G sends a diagonal to another diagonal, we get an action $G \to (X) \cong S_4$. The kernal $G_X = \ker(\varphi) = \{,\ \text{send each vertex to its opposite}\}$. Easy exercise to check that any diagonal can be sent to any other diagonal, so $G^X = \text{im}(\varphi) = \text{Sym}(X)$. So by the first isomorphism theorem, we have that $S_4 \cong G^X \cong G/G_X \implies \frac{|G|}{2} = 4! \implies |G| = 48$.

For the next example let's look at a group acting on itself. Let G act on itself by $G \times G \to G$, sending $(g, g_1) \to gg_1$. This gives a homomorphism $G \to \text{Sym}(G)$ (easy to check that φ is injective since the kernal is trival). By the first isomorphism theorem we get that every group is isomorphism to a subgroup of a symmetric group (Cayley's theorem).

Now let $H \leq G$ and let $X = G/H$, let G act on X by $g * g_1 H = gg_1 H$. We get $\varphi G \to \text{Sym}(X)$. Consider $G_X = \ker\varphi$. If $g \in G_X$, then $gg_1H = g_1H, \forall g_1 \in G$, so ${g_1}^{-1}gg_1H = H \implies G_X \subseteq \bigcap_{g_1 \in G} g_1 H {g_1}^{-1}$. This argument is completely reversible, so if $g \in \bigcap_{g_1} g_1 H g_1^{-1}$, then for each $g_1 \in G$, we have $\text{g}_1^{-1} gg_1 \in H, so\ \text{g} \in G_X \implies G_X = \bigcap_{g_1 \in G} g_1 H {g_1}^{-1}$. Since G_X is a kernal and is a subset of H, we've got a way of making H smaller and making it normal. This is the largest normal subgroup contained in H.

Theorem. Let G be finite and $H \leq G$ of index n. There exists a normal subgroup of G, $K \triangleleft G$, with $K \leq H$, such that G/K is isomorphic to a subgroup of S_n. Thus, $|G/K|$ divides $n!$, and $|G/K| \geq n$.

Proof. Consider G acting on G/H in the previous example. So the kernal of $\varphi : G \to \text{Sym}(G/H)$ is normal, denote it by K. We've shown it is contained by H. First isomorphism theorem gives that $G/K \cong \text{im}(\varphi) \leq Sym(X) \cong S_n$. Give that $|G/K|$ divides $n!$ by Lagrange. Since that $K \leq H$, we have that $|G/K| \geq |G/H| \implies |G/K| \geq n$.

Corollary. Let G be non-abelian and simple. Let $H \leq G$ be a proper subgroup of index $n > 1$. Then G is isomorphism to a subgroup A_n. Moreover, $n \geq 5$, i.e. no subgroup of index less than 5.

Proof. Action of G on the set $X = G/H$ gives a homomorphism $\varphi : G \to \text{Sym}(X) \cong S_n$. Since the kernal is normal, since G is simple it is either G or $\{e\}$. Since H is a proper subgroup, for some $g \in G$, $gH \neq H$, so we must have that $\ker\varphi = \{e\}$. So $G \cong \operatorname{im}\varphi \leq S_n$. Now we want to show that $\operatorname{im}\varphi \leq A_n$. To see this observe that $A_n \triangleleft S_n$. Consider $A_n \cap \operatorname{im}\varphi \leq \operatorname{im}\varphi$. By the second isomorphism theorem, $\operatorname{im}\varphi \cap A_n \triangleleft \operatorname{im}\varphi \implies \operatorname{im}\varphi \cap A_n = \{e\}$ or $\operatorname{im}\varphi$ itself. By the rest of the second isomorphism theorem, if $\operatorname{im}\varphi \cap A_n = \{e\} \implies \operatorname{im}\varphi \cong \frac{\operatorname{im}\varphi}{\operatorname{im}\varphi \cap A_n} \cong \frac{\operatorname{im}\varphi A_n}{A_n} \leq \frac{S_n}{A_n} \cong C_2$, but G is non-abelian, so $\operatorname{im}\varphi$ is non-abelian, so we have a contradiction. So we have that $\operatorname{im}\varphi \cap A_n = \operatorname{im}\varphi$, so $\operatorname{im}\varphi$ is a subgroup of A_n.
For the next part of the corollary, S_1, S_2 are abelian and S_3, S_4 have no non-abelian simple subgroups, so we must have $n \geq 5$.

Definition. (Orbits and stabiliser) Let G act on some set X. Then, the *orbit* of $x \in X$ is $G \cdot x = \operatorname{orb} x = \{gx : g \in G\} \subseteq X$. And the *stabiliser* of $x \in X$ is $G_x = \operatorname{stab}_G(x) = \{g \in G : gx = x\} \leq G$.

Theorem. (Orbit-stabiliser) For a group G acting on a set X. For all $x \in X$, there is a bijection $G \cdot x \to G/G_x$ given by $g \cdot x \to gG_x$. In particular, if G is finite, then $|G| = |G \cdot x||G_x|, \forall x \in X$.

Proof. In the IA Groups course.

1.5 Conjugacy, centralisers, and normalisers

Let G be a group. The conjugation action of G acting on itself by $G \times G \to G$, is $(g, h) \to ghg^{-1}$. This is equivilent to a homomorphism $G \to \operatorname{Sym}(G)$.

Fix $g \in G$. Then the permutation $G \to G$ given by $h \to ghg^{-1}$ is also a homomorphism.

Definition. (Automorphism) Let G be a group. A permutation $G \to G$ that is also a homomorphism is called an *automorphism* of G. The set of all automorphisms of G, $\operatorname{Aut}(G) = \{f : G \to G : f \text{ is a automorphism}\} \subseteq \operatorname{Sym}(G)$, is a subgroup, called the automorphism group of G.

Definition. (Conjugacy classes and centralisers) Fix $g \in G$. The *conjugacy class* of g is the set $\operatorname{ccl}_G(g) = \{hgh^{-1} : h \in G\}$, i.e it is the orbit under the conjugation action. The *centraliser* of $g \in G$ is $C_G(g) = \{h \in G : hgh^{-1} = g\}$, i.e the stabiliser of g under the action.

Definition. (Centre) The *centre* of G is $Z(G) = \{z \in G : hzh^{-1} = z \forall h \in G\}$, i.e. it is the kernal of the conjugation action and the intersection of the centralisers.

Corollary. Let G be a finite group. Then $|\operatorname{ccl}_G(x)| = |G : C_G(x)| = \frac{|G|}{|c_G(x)|}$.

Proof. Apply orbit-stabiliser to the conjugation action.

Definition. (Normaliser) Let $H \leq G$. The *normaliser* of H in G is $N_G(H) = \{g \in G : ghg^{-1} \in H, \forall h \in H\}$.

We can see clearly that $H \subseteq N_G(H)$ so $N_G(H)$ is non-empty, and if we pick two elements $x, y \in N_G(H)$, then we can see that $(xy)h(xy)^{-1} \in H$. So we have that $N_G(H) \leq G$.

In fact we have that $N_G(H)$ is the largest subgroup containing H in which H is normal.

1.6 Simplicity of A_n for $n \geq 5$

Recall from Part IA groups that a conjugacy class in S_n consists of the set of all elements with a fixed cycle type.

Theorem. Let $n \geq 5$. Then A_n is simple.

Proof. We will prove the statement via these three claims:

- A_n is generated by 3-cycles
- If $H \triangleleft A_n$ that contains a 3-cycle then it contains all the 3-cycles
- Any non-trival $H \triangleleft A_n$ contains a 3-cycle.

First we prove the first claim. Let $g \in A_n$, when viewed in S_n it is the product of evenly many transposition. Consider a product of two transpositions:

- $(ab)(ab) = e \in A_n$
- $(ab)(bc) = (abc) \in A_n$
- $(ab)(cd) = (acb)(acd) \in A_n$.

In each case we can write all products of transpositions as a product of 3-cycles, hence we can write all elements in A_n as a product of 3-cycles.

Now for the second claim, any two 3-cycles in A_n are conjugate when viewed in S_n. Let δ, δ' be 3-cycles and write $\delta' = \sigma\delta\sigma^{-1}$, where $\sigma \in S_n$. If σ is even, we're done since it's in A_n. If σ is odd, observe since $n \geq 5$, there exists a transposition τ disjoint from δ, now $\delta' = \sigma(\tau\tau^{-1})\delta\sigma^{-1} = (\sigma\tau)\delta(\sigma\tau)^{-1}$. Since $\sigma\tau$ is even, we're done.

$\mathbb{Z}$