Part IB — GRM

Based on lectures by Dr R Zhou and notes by thirdsgames.co.uk

Lent 2022

Contents

§0 Review of IA Groups

This section contains material covered by IA Groups.

§0.1 Definitions

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

- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- there exists $e \in G$ such that for all $g \in G$, we have $g \cdot e = e \cdot g = g$; and
- for all $g \in G$, there exists an inverse $h \in G$ such that $g \cdot h = h \cdot g = e$.

Remark 1.

1. Sometimes, such as in IA Groups, a closure axiom is also specified. However, this is implicit in the type definition of $\cdot$. In practice, this must normally be checked explicitly.
2. Additive and multiplicative notation will be used interchangeably. For additive notation, the inverse of g is denoted $-g$, and for multiplicative notation, the inverse is instead denoted g^{-1}. The identity element is sometimes denoted 0 in additive notation and 1 in multiplicative notation.

A subset $H \subseteq G$ is a *subgroup* of G, written $H \leq G$, if $h \cdot h' \in H$ for all $h, h' \in H$, and $(H, \cdot)$ is a group. The closure axiom must be checked, since we are restricting the definition of $\cdot$ to a smaller set.

Remark 2. A non-empty subset $H \subseteq G$ is a subgroup of G if and only if

$$a, b \in H \implies a \cdot b^{-1} \in H$$

An *abelian* group is a group such that $a \cdot b = b \cdot a$ for all a, b in the group. The *direct product* of two groups G, H, written $G \times H$, is the group over the Cartesian product $G \times H$ with operation $\cdot$ defined such that $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$.

§0.2 Cosets

Let $H \leq G$. Then, the *left cosets* of H in G are the sets gH for all $g \in G$. The set of left cosets partitions G. Each coset has the same cardinality as H. Lagrange's theorem states that if G is a finite group and $H \leq G$, we have $|G| = |H| \cdot [G \colon H]$, where $[G \colon H]$ is the number of left cosets of H in G. $[G \colon H]$ is known as the *index* of H in G. We can construct Lagrange's theorem analogously using right cosets. Hence, the index of a subgroup is independent of the choice of whether to use left or right cosets; the number of left cosets is equal to the number of right cosets.

§0.3 Order

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

1. $g^n = 1 \implies d \mid n$;
2. $\langle g \rangle = \left\{1, g, \dots, g^{d-1}\right\} \leq G$, and by Lagrange's theorem (if G is finite) $d \mid |G|$.

§0.4 Normality and quotients

A subgroup $H \leq G$ is *normal*, written $H \trianglelefteq G$, if $g^{-1}Hg = H$ for all $g \in G$. In other words, H is preserved under conjugation over G. If $H \trianglelefteq G$, then the set ${}^{G}\!/_{H}$ of left cosets of H in G forms the *quotient group*. The group action is defined by $g_1H \cdot g_2H = (g_1 \cdot g_2)H$. This can be shown to be well-defined.

§0.5 Homomorphisms

Let G, H be groups. A function $\varphi\colon G \to H$ is a *group homomorphism* if $\varphi(g_1 \cdot_G g_2) = \varphi(g_1) \cdot_H \varphi(g_2)$ for all $g_1, g_2 \in G$. The *kernel* of φ is defined to be $\ker \varphi = \{g \in G\colon \varphi(g) = 1\}$, and the *image* of φ is $\operatorname{Im} \varphi = \{\varphi(g)\colon g \in G\}$. The kernel is a normal subgroup of G, and the image is a subgroup of H.

§0.6 Isomorphisms

An *isomorphism* is a homomorphism that is bijective. This yields an inverse function, which is of course also an isomorphism. If $\varphi\colon G \to H$ is an isomorphism, we say that G and H are isomorphic, written $G \cong H$. Isomorphism is an equivalence relation. The isomorphism theorems are

1. if $\varphi\colon G \to H$, then ${}^{G}\!/_{\ker \varphi} \cong \operatorname{Im} \varphi$;
2. if $H \leq G$ and $N \trianglelefteq G$, then $H \cap N \trianglelefteq H$ and ${}^{H}\!/_{H \cap N} \cong {}^{HN}\!/_{N}$;
3. if $N \leq M \leq G$ such that $N \trianglelefteq G$ and $M \trianglelefteq G$, then ${}^{M}\!/_{N} \trianglelefteq {}^{G}\!/_{N}$, and ${}^{G/N}\!/_{M/N} = {}^{G}\!/_{M}$.

§1 Simple groups

§1.1 Introduction

If $K \trianglelefteq G$, then studying the groups K and ${}^{G}\!/_{K}$ give information about G itself. This approach is available only if G has nontrivial normal subgroups. It therefore makes sense to study groups with no normal subgroups, since they cannot be decomposed into simpler structures in this way.

Definition 1.1 (Simple Group)
A group G is **simple** if $\{1\}$ and G are its only normal subgroups.

By convention, we do not consider the trivial group to be a simple group. This is analogous to the fact that we do not consider one to be a prime.

Lemma 1.1
Let G be an abelian group. G is simple iff $G \cong C_p$ for some prime p.

Proof. Certainly C_p is simple by Lagrange's theorem. Conversely, since G is abelian, all subgroups are normal. Let $1 \neq g \in G$. Then $\langle g \rangle \trianglelefteq G$. Hence $\langle g \rangle = G$ by simplicity. If G is infinite, then $G \cong \mathbb{Z}$, which is not a simple group; $2\mathbb{Z} \triangleleft \mathbb{Z}$. Hence G is finite, so $G \cong C_{o(g)}$. If $o(g) = mn$ for $m, n \neq 1, p$, then $\langle g^m \rangle \leq G$, contradicting simplicity. □

Lemma 1.2
If G is a finite group, then G has a **composition series**

$$1 \cong G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

where each quotient ${}^{G_{i+1}}\!/_{G_i}$ is simple.

Remark 3. It is not the case that necessarily G_i be normal in G_{i+k} for $k \geq 2$.

Proof. We will consider an inductive step on $|G|$. If $|G| = 1$, then trivially $G = 1$. Conversely, if $|G| > 1$, let G_{n-1} be a normal subgroup of largest possible order not equal to $|G|$. Then, ${}^{G}\!/_{G_{n-1}}$ exists, and is simple by the correspondence theorem. □

§2 Group actions

§2.1 Definitions

Definition 2.1 (Symmetric Group)
Let X be a set. Then $\mathrm{Sym}(X)$ is the group of permutations of X; that is, the group of all bijections of X to itself under composition. The identity can be written id or id_X.

Definition 2.2 (Permuation Group)
A group G is a permutation group of degree n if $G \leq \mathrm{Sym}(X)$ where $|X| = n$.

Example 2.1
The symmetric group S_n is exactly equal to $\mathrm{Sym}(\{1, \dots, n\})$, so is a permutation group of order n. A_n is also a permutation group of order n, as it is a subgroup of S_n. D_{2n} is a permutation group of order n.

Definition 2.3 (Group Actions)
A **group action** of a group G on a set X is a function $\alpha\colon G \times X \to X$ satisfying

$$\alpha(e, x) = x; \quad \alpha(g_1 \cdot g_2, x) = \alpha(g_1, \alpha(g_2, x))$$

for all $g_1, g_2 \in G, x \in X$. The group action may be written $*$, defined by $g * x \equiv \alpha(g, x)$.

Proposition 2.1
An action of a group G on a set X is uniquely characterised by a group homomorphism $\varphi\colon G \to \mathrm{Sym}(X)$.

Proof. For all $g \in G$, we can define $\varphi_g\colon X \to X$ by $x \mapsto g * x$. Then, for all $x \in X$,

$$\varphi_{g_1 g_2}(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = \varphi_{g_1}(\varphi_{g_2}(x))$$

Thus $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$. In particular, $\varphi_g \circ \varphi_{g^{-1}} = \varphi_e$. We now define

$$\varphi\colon G \to \mathrm{Sym}(X); \quad \varphi(g) = \varphi_g \implies \varphi(g)(x) = g * x$$

This is a homomorphism.

Conversely, any group homomorphism $\varphi\colon G \to \mathrm{Sym}(X)$ induces a group action $*$ by $g * x = \varphi(g)$. This yields $e * x = \varphi(e)(x) = \mathrm{id}\, x = x$ and $(g_1 g_2) * x = \varphi(g_1 g_2)x = \varphi(g_1)\varphi(g_2)x = g_1 * (g_2 * x)$ as required. □

Definition 2.4 (Permutation Representation)

The homomorphism $\varphi\colon G \to \mathrm{Sym}(X)$ defined in the above proof is called a **permutation representation** of G.

Definition 2.5 (Orbit, Stabiliser)

Let G act on X. Then,

1. the **orbit** of $x \in X$ is $\mathrm{Orb}_G(x) = \{g * x : g \in G\} \subseteq X$;
2. the **stabiliser** of $x \in X$ is $G_x = \{g \in G : g * x = x\} \leq G$.

Definition 2.6 (Transitive Group Action)

If there is only orbit, i.e. $\mathrm{Orb}_G(x) = X \quad \forall\, x$ then the group action is **transitive**.

Definition 2.7 (Kernel)

The **kernel** of a permutation representation is $\bigcap_{x \in X} G_x$.

Remark 4. The kernel of the permutation representation φ is also referred to as the kernel of the group action itself.

Definition 2.8 (Faithful Group Action)

If the kernel is trivial the action is said to be **faithful**.

Theorem 2.1 (Orbit-stabiliser theorem)

The orbit $\mathrm{Orb}_G(x)$ bijects with the set ${}^{G}\!/\!{}_{G_x}$ of left cosets of G_x in G (which may not be a quotient group). In particular, if G is finite, we have

$$|G| = |\mathrm{Orb}(x)| \cdot |G_x|$$

Example 2.2

If G is the group of symmetries of a cube and we let X be the set of vertices in the cube, G acts on X. Here, for all $x \in X$, $|\mathrm{Orb}(x)| = 8$ and $|G_x| = 6$ (including reflections), hence $|G| = 48$.

Remark 5. The orbits partition X.

Note that $G_{g*x} = gG_xg^{-1}$. Hence, if x, y lie in the same orbit, their stabilisers are conjugate.

§2.2 Examples

Example 2.3

G acts on itself by left multiplication. This is known as the **left regular action**. The kernel is trivial, hence the action is faithful. The action is transitive, since for all $g_1, g_2 \in G$, the element $g_2g_1^{-1}$ maps g_1 to g_2.

Theorem 2.2 (Cayley's theorem)

Any finite group G is a permutation group of order $|G|$; it is isomorphic to a subgroup of $S_{|G|}$.

Example 2.4

Let $H \leq G$. Then G acts on ${}^{G}\!/_{H}$ by left multiplication, where ${}^{G}\!/_{H}$ is the set of left cosets of H in G. This is known as the **left coset action**. This action is transitive using the construction above for the left regular action. We have $\ker\varphi = \bigcap_{x\in G} xHx^{-1}$, which is the largest normal subgroup of G contained within H.

Theorem 2.3

Let G be a non-abelian simple group, and $H \leq G$ with 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. Let $\varphi\colon G \to \mathrm{Sym}(X)$ be the permutation representation associated to this group action.

Since G is simple, $\ker\varphi = 1$ or $\ker\varphi = G$. If $\ker\varphi = G$, then $\mathrm{Im}\,\varphi = \mathrm{id}$, which is a contradiction since G acts transitively on X and $|X| > 1$. Thus $\ker\varphi = 1$, and $G \cong \mathrm{Im}\,\varphi \leq S_n$.

Since $G \leq S_n$ and $A_n \triangleleft S_n$, the second isomorphism theorem shows that $G \cap A_n \triangleleft G$, and

$$\left. G \middle/ G \cap A_n \right. \cong \left. GA_n \middle/ A_n \right. \leq \left. S_n \middle/ A_n \right. \cong C_2$$

Since G is simple, $G \cap A_n = 1$ or G. If $G \cap A_n = 1$, then G is isomorphic to a subgroup of C_2, but this is false, since G is non-abelian. Hence $G \cap A_n = G$ so $G \leq A_n$. Finally, if $n \leq 4$ we can check manually that A_n is not simple; A_n has no non-abelian simple subgroups. □

§2.3 Conjugation actions

Example 2.5

Let G act on G by conjugation, so $g * x = gxg^{-1}$. This is known as the **conjugation action**.

Definition 2.9 (Conjugacy Class, Centraliser, Centre)

The orbit of the conjugation action is called the **conjugacy class** of a given element $x \in G$, written $\mathrm{ccl}_G(x)$. The stabiliser of the conjugation action is the set C_x of elements which commute with a given element x, called the **centraliser** of x in G. The kernel of φ is the set $Z(G)$ of elements which commute with all elements in x, which is the **centre** of G. This is always a normal subgroup.

Remark 6. $\varphi\colon G \to G$ satisfies

$$\varphi(g)(h_1h_2) = gh_1h_2g^{-1} = hh_1g^{-1}gh_2g^{-1} = \varphi(g)(h_1)\varphi(g)(h_2)$$

Hence $\varphi(g)$ is a group homomorphism for all g. It is also a bijection, hence $\varphi(g)$ is an isomorphism from $G \to G$.

Definition 2.10 (Automorphism)

An isomorphism from a group to itself is known as an **automorphism**. We define $\mathrm{Aut}(G)$ to be the set of all group automorphisms of a given group. This set is a group. Note, $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$, and the $\varphi\colon G \to \mathrm{Sym}(G)$ above has image in $\mathrm{Aut}(G)$.

Example 2.6

Let X be the set of subgroups of G. Then G acts on X by conjugation: $g * H = gHg^{-1}$. The stabiliser of a subgroup H is $\{g \in G \colon gHg^{-1} = H\} = N_G(H)$, called the **normaliser** of H in G. The normaliser of H is the largest subgroup of G that contains H as a normal subgroup. In particular, $H \triangleleft G$ if and only if $N_G(H) = G$.

§3 Alternating groups

§3.1 Conjugation in alternating groups

We know that elements in S_n are conjugate if and only if they have the same cycle type. However, elements of A_n that are conjugate in S_n are not necessarily conjugate in A_n. Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$. There are two possible cases.

- If there exists an odd permutation that commutes with g, then $2|C_{A_n}(g)| = |C_{S_n}(g)|$. By the orbit-stabiliser theorem, $|\mathrm{ccl}_{A_n}(g)| = |\mathrm{ccl}_{S_n}(g)|$.
- If there is no odd permutation that commutes with g, we have $|C_{A_n}(g)| = |C_{S_n}(g)|$. Similarly, $2|\mathrm{ccl}_{A_n}(g)| = |\mathrm{ccl}_{S_n}(g)|$.

Example 3.1

For $n = 5$, the product $(1\ 2)(3\ 4)$ commutes with $(1\ 2)$, and $(1\ 2\ 3)$ commutes with $(4\ 5)$. Both of these elements are odd. So the conjugacy classes of the above inside S_5 and A_5 are the same. However, $(1\ 2\ 3\ 4\ 5)$ does not commute with any odd permutation. Indeed, if that were true for some h, we would have

$$(1\ 2\ 3\ 4\ 5) = h(1\ 2\ 3\ 4\ 5)h^{-1} = (h(1)\ h(2)\ h(3)\ h(4)\ h(5))$$

Hence h must be a 5-cycle so $h \in \langle g \rangle \leq A_5$. So $|\mathrm{ccl}_{A_5}(g)| = \frac{1}{2}|\mathrm{ccl}_{S_5}(g)| = 12$. We can then show that A_5 has conjugacy classes of size $1, 15, 20, 12, 12$.

If $H \trianglelefteq A_5$, H is a union of conjugacy classes so $|H|$ must be a sum of the sizes of the above conjugacy classes. By Lagrange's theorem, $|H|$ must divide 60. We can check explicitly that this is not possible unless $|H| = 1$ or $|H| = 60$. Hence A_5 is simple.

§3.2 Simplicity of alternating groups

Lemma 3.1

A_n is generated by 3-cycles.

Proof. Each $\sigma \in A_n$ is a product of an even number of transpositions. It therefore suffices to show that a product of any two transpositions can be written as a product of 3-cycles. For a, b, c, d distinct,

$$(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d); \quad (a\ b)(b\ c) = (a\ b\ c)$$

□

Lemma 3.2

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

Proof. We claim that every 3-cycle is conjugate to $(1\ 2\ 3)$. If $(a\ b\ c)$ is a 3-cycle, we have $(a\ b\ c) = \sigma(1\ 2\ 3)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \in A_n$, then the proof is finished. Otherwise, $\sigma \mapsto \sigma(4\ 5) \in A_n$ suffices, since $(4\ 5)$ commutes with $(1\ 2\ 3)$. □

Theorem 3.1

A_n is simple for $n \geq 5$.

Proof. Suppose $1 \neq N \triangleleft A_n$. To disprove normality, it suffices to show that N contains a 3-cycle by the lemmas above, since the normality of N would imply N contains all 3-cycles and hence all elements of A_n.

Let $1 \neq \sigma \in N$, writing σ as a product of disjoint cycles.

1. Suppose σ contains a cycle of length $r \geq 4$. Without loss of generality, let $\sigma = (1\ 2\ 3 \dots r)\tau$ where τ fixes $1, \dots, r$. Now, let $\delta = (1\ 2\ 3)$. We have

$$\underbrace{\sigma^{-1}}_{\in N}\underbrace{\delta^{-1}\sigma\delta}_{\in N} = (r \dots 2\ 1)\tau^{-1}(1\ 3\ 2)(1\ 2 \dots r)\tau(1\ 2\ 3) = (2\ 3\ r)$$

   So N contains a 3-cycle.

2. Suppose σ contains two 3-cycles, which can be written without loss of generality as $(1\ 2\ 3)(4\ 5\ 6)\tau$. Let $\delta = (1\ 2\ 4)$, and then

$$\sigma^{-1}\delta^{-1}\sigma\delta = (1\ 3\ 2)(4\ 6\ 5)(1\ 4\ 2)(1\ 2\ 3)(4\ 5\ 6)(1\ 2\ 4) = (1\ 2\ 4\ 3\ 6)$$

   Therefore, there exists an element of N which contains a cycle of length $5 \geq 4$. This reduces the problem to case (i).

3. Finally, suppose σ contains two 2-cycles, which will be written $(1\ 2)(3\ 4)\tau$. Then let $\delta = (1\ 2\ 3)$ and

$$\sigma^{-1}\delta^{-1}\sigma\delta = \underbrace{(1\ 2)(3\ 4)(1\ 3\ 2)(1\ 2)(3\ 4)}_{(2\ 4\ 1)}(1\ 2\ 3) = (1\ 4)(2\ 3) = \pi$$

   Let $\varepsilon = (2\ 3\ 5)$. Then

$$\underbrace{\pi^{-1}}_{\in N}\underbrace{\varepsilon^{-1}\pi\varepsilon}_{\in N} = (1\ 4)(2\ 3)(2\ 5\ 3)(1\ 4)(2\ 3)(2\ 3\ 5) = (2\ 5\ 3)$$

   Thus N contains a 3-cycle.

There are now three remaining cases, where σ is a transposition, a 3-cycle, or a transposition composed with a 3-cycle. Note that the remaining cases containing transpositions cannot be elements of A_n. If σ is a 3-cycle, we already know A_n contains a 3-cycle, namely σ itself. $\square$

§4 p-groups

§4.1 p-groups

Definition 4.1 (p-group)

Let p be a prime. A finite group G is a **p-group** if $|G| = p^n$ for $n \geq 1$.

Theorem 4.1

If G is a p-group, the centre $Z(G)$ is non-trivial.

Proof. For $g \in G$, due to the orbit-stabiliser theorem, $|\mathrm{ccl}(g)||C(g)| = p^n$. In particular, $|\mathrm{ccl}(g)|$ divides p^n, and they partition G. Since G is a disjoint union of conjugacy classes, modulo p we have

$$|G| \equiv \text{number of conjugacy classes of size } 1 \equiv 0 \implies |Z(G)| \equiv 0$$

Hence $Z(G)$ has order zero modulo p so it cannot be trivial. We can check this by noting that $g \in Z(G) \iff x^{-1}gx = g$ for all x, which is true if and only if $\mathrm{ccl}_G(g) = \{g\}$. $\square$

Corollary 4.1

The only simple p-groups are the cyclic groups of order p.

Proof. Let G be a simple p-group. Since $Z(G)$ is a normal subgroup of G, we have $Z(G) = 1$ or $Z(G) = G$. But $Z(G)$ may not be trivial, so $Z(G) = G$. This implies G is abelian. The only abelian simple groups are cyclic of prime order by lemma 1.1, hence $G \cong C_p$. $\square$

Corollary 4.2

Let G be a p-group of order p^n. Then G has a subgroup of order p^r for all $r \in \{0, \dots, n\}$.

Proof. Recall from lemma 1.2 that any group G has a composition series $1 = G_1 \lhd \dots \lhd G_N = G$ where each quotient ${G_{i+1}}/{G_i}$ is simple.

Since G is a p-group, ${G_{i+1}}/{G_i}$ is also a p-group. Each successive quotient is an order p group by the previous corollary, so we have a composition series of nested subgroups of order p^r for all $r \in \{0, \dots, n\}$. $\square$

Lemma 4.1

Let G be a group. If ${}^{G}\!/_{Z(G)}$ is cyclic, then G is abelian. This then implies that $Z(G) = G$, so in particular ${}^{G}\!/_{Z(G)} = 1$.

Proof. Let $gZ(G)$ be a generator for ${}^{G}\!/_{Z(G)}$. Then, each coset of $Z(G)$ in G is of the form $g^r Z(G)$ for some $r \in \mathbb{Z}$. Thus, $G = \{g^r z \colon r \in \mathbb{Z}, z \in Z(G)\}$. Now, we multiply two elements of this group and find

$$g^{r_1} z_1 g^{r_2} z_2 = g^{r_1 + r_2} z_1 z_2 = g^{r_1 + r_2} z_2 z_1 = z_2 z_1 g^{r_1 + r_2} = g^{r_2} z_2 g^{r_1} z_1$$

So any two elements in G commute. □

Corollary 4.3

Any group of order p^2 is abelian.

Proof. Let G be a group of order p^2. Then $|Z(G)| \in \{1, p, p^2\}$. The centre cannot be trivial as proven above, since G is a p-group. If $|Z(G)| = p$, we have that ${}^{G}\!/_{Z(G)}$ is cyclic as it has order p. Applying the previous lemma, G is abelian. However, this is a contradiction since the centre of an abelian group is the group itself. If $|Z(G)| = p^2$ then $Z(G) = G$ and then G is clearly abelian. □

§4.2 Sylow theorems

Theorem 4.2 (Sylow Theorems)

Let G be a finite group of order $p^a m$ where p is a prime and p does not divide m. Then:

1. The set $\mathrm{Syl}_p(G) = \{P \leq G \colon |P| = p^a\}$ of Sylow p-subgroups is non-empty.
2. All Sylow p-subgroups are conjugate.
3. The amount of Sylow p-subgroups $n_p = \left|\mathrm{Syl}_p(G)\right|$ satisfies

$$n_p \equiv 1 \mod p; \quad n_p \mid |G| \implies n_p \mid m$$

Proof. 1. Let Ω be the set of all <u>subsets</u> of G of order p^a. We can directly find

$$|\Omega| = \binom{p^a m}{p^a} = \frac{p^a m}{p^a} \cdot \frac{p^a m - 1}{p^a - 1} \cdots \frac{p^a m - p^a + 1}{1}$$

Note that for $0 \leq k < p^a$, the numbers $p^a m - k$ and $p^a - k$ are divisible by the same power of p. In particular, $|\Omega|$ is coprime to p.

Let G act on Ω by left-multiplication, so $g * X = \{gx : x \in X\}$. For any $X \in \Omega$, the orbit-stabiliser theorem can be applied to show that

$$|G_X||\mathrm{orb}_G(X)| = |G| = p^a m$$

Since $|\Omega|$ is coprime to p, there must exist an orbit with size coprime to p, since orbits partition Ω. For such an X, $p^a \mid |G_X|$.

Conversely, note that if $g \in G$ and $x \in X$, then $g \in (gx^{-1}) * X$. Hence, we can consider

$$G = \bigcup_{g \in G} g * X = \bigcup_{Y \in \mathrm{orb}_G(X)} Y$$

Thus $|G| \leq |\mathrm{orb}_G(X)| \cdot |X|$, giving $|G_X| = \frac{|G|}{|\mathrm{orb}_G(X)|} \leq |X| = p^a$.

As $p^a \mid |G_X|$ we must have $|G_X| = p^a$. In other words, the stabiliser G_X is a Sylow p-subgroup of G.

2. We will prove a stronger result for this part of the proof. We claim that if P is a Sylow p-subgroup and $Q \leq G$ is a p-subgroup, then $Q \leq gPg^{-1}$ for some $g \in G$. Indeed, let Q act on the set of left cosets of P in G by left multiplication. By the orbit-stabiliser theorem, each orbit has size which divides $|Q| = p^k$ for some k. Hence each orbit has size p^r for some r.

   Since ${}^{G}\!/\!{}_{P}$ has size m, which is coprime to p, there must exist an orbit of size 1. Therefore there exists $g \in G$ such that $q * gP = gP$ for all $q \in Q$. Equivalently, $g^{-1}qg \in P$ for all $q \in Q$. This implies that $Q \leq gPg^{-1}$ as required. This then weakens to the second part of the Sylow theorems.

3. Let G act on $\mathrm{Syl}_p(G)$ by conjugation. Part (ii) of the Sylow theorems implies that this action is transitive. By the orbit-stabiliser theorem, $n_p = \left|\mathrm{Syl}_p(G)\right| \mid |G|$.

   Let $P \in \mathrm{Syl}_p(G)$. Then let P act on $\mathrm{Syl}_p(G)$ by conjugation. Since P is a Sylow p-subgroup, the orbits of this action have size dividing $|P| = p^a$, so the size is some power of p. To show $n_p \equiv 1 \mod p$, it suffices to show that $\{P\}$ is the unique orbit of size 1. Suppose $\{Q\}$ is another orbit of size 1, so Q is a

Sylow p-subgroup which is preserved under conjugation by P. P normalises Q, so $P \leq N_G(Q)$. Notice that P and Q are both Sylow p-subgroups of $N_G(Q)$. By (ii), P and Q are conjugate inside $N_G(Q)$. Hence $P = Q$ since $Q \trianglelefteq N_G(Q)$. Thus, $|P|$ is the unique orbit of size 1, so $n_p \equiv 1 \mod p$ as required.

□

Corollary 4.4

If $n_p = 1$, then there is only one Sylow p-subgroup, and it is normal.

Proof. Let $g \in G$ and $P \in \mathrm{Syl}_p(G)$. Then gPg^{-1} is a Sylow p-subgroup, hence $gPg^{-1} = P$. P is normal in G. □

Example 4.1

Let G be a group with $|G| = 1000 = 2^3 \cdot 5^3$. Here, $n_5 \equiv 1 \mod 5$, and $n_5 \mid 8$, hence $n_5 = 1$. Thus the unique Sylow 5-subgroup is normal. Hence no group of order 1000 is simple.

Example 4.2

Let G be a group with $|G| = 132 = 2^2 \cdot 3 \cdot 11$. n_{11} satisfies $n_{11} \equiv 1 \mod 11$ and $n_{11} \mid 12$, thus $n_{11} \in \{1, 12\}$.

Suppose G is simple.

Then $n_{11} = 12$[a]. The amount of Sylow 3-subgroups satisfies $n_3 \equiv 1 \mod 3$ and $n_3 \mid 44$ so $n_3 \in \{1, 4, 22\}$. Since G is simple, $n_3 \in \{4, 22\}$.

Suppose $n_3 = 4$. Then G acts on $\mathrm{Syl}_3(G)$ by conjugation, and this generates a group homomorphism $\varphi\colon G \to S_4$. But the kernel of this homomorphism is a normal subgroup of G, so $\ker\varphi$ is trivial or G itself as G simple. If $\ker\varphi = G$, then $\mathrm{Im}\,\varphi$ is trivial, contradicting Sylow's second theorem. If $\ker\varphi = 1$, then $\mathrm{Im}\,\varphi$ has order $132 > |S_4|$ $\lightning$.

Thus $n_3 = 22$ and recall $n_{11} = 12$. This means that G has $22 \cdot (3-1) = 44$ elements of order 3[b], and further G has $12 \cdot (11-1) = 120$ elements of order 11. However, the sum of these two totals is more than the total of 132 elements, so this is a contradiction. Hence G is not simple.

[a] If $n_{11} = 1$ then we have a normal subgroup by the previous corollary.

[b] Each group in $\mathrm{Syl}_3(G)$ intersect trivially, as if they didn't any non trivial element in the intersection would generate both groups as they're all C_3.