Proposition 49.

1. *A group G is nilpotent if and only if G appears as an element of its upper central series.*

2. *If G is nilpotent, then the upper central series and the lower central series have the same length. (That is to say, the least c such that $\gamma_{c+1}(G) = \{e\}$, is equal to the least c such that $Z_c(G) = G$.)*

Proof.
1. Suppose that G has nilpotency class c. Then the lower central series is a central series for G of length c. Now by Proposition 48 we see that $\gamma c - i + 1(G) \leq Z_i(G)$ for all i (taking the different numbering convention for the lower central series into account). In particular, $\gamma_1(G) \leq Z_c(G)$. But $\gamma_1(G) = G$, and so $Z_c(G) = G$. Suppose conversely that $Z_k(G) = G$ for some G. Then the series $\{G_i\}$, given by $G_i = Z_{k-i}(G)$ for $0 \leq i \leq k$, is a central series for G. So G is nilpotent by Corollary 47.
2. In the proof of part 1 we have seen that if $\gamma_{c+1}(G) = \{e\}$, then $Z_c(G) = G$. Suppose conversely that $Z_k(G) = G$. Let $\{G_i\}$ be the central series defined in the proof of part 1. By Proposition 46 we have $\gamma_{k+1}(G) \leq G_k = \{e\}$. It follows that the lower central series and the upper central series have the same length. □

Warning. A group G of nilpotency class c may have a central series of length greater than c. For instance, if G is abelian, then it has class 1; but any chain of subgroups

$$G = G_0 > G_1 > \cdots > G_k = \{e\}$$

constitutes a central series, and such a series can be arbitrarily long. Proposition 46 does tell us, however, that no central series can be of length *shorter* than c.

Theorem 50

Every p-group is nilpotent.

Proof. Let G be a p-group. For $i \in \mathbb{N}$, suppose that $Z_i(G) < G$. Since G is finite, there exists k such that $Z_k(G) = Z_{k+1}(G)$. Suppose that $Z_k(G) \neq G$. Then the quotient $G/Z_k(G)$ is a non-trivial p-group, and so by Proposition 21 it has a non-trivial centre. But it follows that $Z_{k+1}(G) > Z_k(G)$, and this is a contradiction. So we must have $Z_k(G) = G$, and so G is nilpotent by Proposition 49.1. □

Example. We have seen that $D_{2^{a+1}}$ is nilpotent, even though no other dihedral group is. Thus the only nilpotent dihedral groups are 2-groups.

Proposition 51. *Let G be nilpotent of class c.*

1. *Any subgroup H of G is nilpotent of class at most c.*

2. *If $N \trianglelefteq G$, then G/N is nilpotent of class at most c.*

3. *If H is nilpotent of class d then $G \times H$ is nilpotent of class* $\max(c,d)$.

Proof.

1. Let $H \leq G$. It is easy to show inductively that $\gamma_i(H) \leq \gamma_i(G)$ for all i. So $\gamma_{c+1}(H) = \{e\}$.
2. Let $\theta : G \longrightarrow G/N$ be the canonical map. It is easy to show inductively that $\theta(\gamma_i(G)) = \gamma_i(G/N)$ for all $i \in \mathbb{N}$. So $\gamma_{c+1}(G/N) = \{e_{G/N}\}$.
3. We note that

$$[(g_1,h_1),(g_2,h_2)] = ([g_1,g_2],[h_1,h_2])$$

for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$. So $\gamma_i(G \times H) = \gamma_i(G) \times \gamma_i(H)$ for all i, and the result follows. □

Example. Let $G = \langle a \rangle \rtimes_\varphi \langle b \rangle$, where a has order 12, b has order 2, and $\varphi_b(a) = a^7$. We show that G is nilpotent.

We note that $\langle a \rangle = \langle a^3 \rangle \times \langle a^4 \rangle$ (as an internal direct product), and that $\varphi_b(a^3) = a^{-3}$, while $\varphi_b(a^4) = a^4$. It follows that a^4 is central in G, and hence that

$$G = (\langle a^3 \rangle \rtimes \langle b \rangle) \times \langle a^4 \rangle \cong D_8 \times C_3.$$

Now both D_8 and C_3 are nilpotent, and so G is nilpotent.

Proposition 52. *If G is a finite nilpotent group, and H is a proper subgroup of G, then $N_G(H) \neq H$.*

Proof. Let c be the nilpotency class of G. Since $\gamma_1(G) = G$, and $\gamma_{c+1}(G) = \{e\}$, there exists j such that $\gamma_j(G) \not\leq H$, but $\gamma_{j+1}(G) \leq H$. Since $\gamma_j(G)$ is normal in G we see that $\gamma_j(G)H$ is a subgroup of G. Now $H/\gamma_{j+1}(G)$ is certainly normal in the abelian group $\gamma_j(G)/\gamma_{j+1}(G)$, and so H is normal in $\gamma_j(G)H$. So we have $H < \gamma_j(G)H \leq N_G(H)$, hence the result. □

Example. Let $G = D_{16}$. Every subgroup H of rotations is normal in G, and so $N_G(H) = G$. Let a be a rotation of order 8, and let b be a reflection. Then we see that

$$\langle b \rangle \lhd \langle a^4, b \rangle \lhd \langle a^2, b \rangle \lhd G,$$

since each of the subgroups in the chain has index 2 in the next. Every subgroup of G is either a rotation subgroup, or else one of the subgroups in the chain above (for some reflection b), and so we see that every proper subgroup of G is normalized by a strictly larger subgroup.

Lemma 53 (Frattini Argument)**.** *Let G be a finite group, and K a normal subgroup. Let P be a Sylow p-subgroup of K. Then $G = KN_G(P)$.*

Proof. Let $g \in G$. Then $()^g P \leq K$ since K is normal, and so ${}^g P \in \mathrm{Syl}_p(K)$. Since any two Sylow p-subgroups of K are conjugate in K, we have ${}^g P = {}^k P$ for some $k \in K$. But now it is clear that ${}^{k^{-1}g} P = P$, and $g = k(k^{-1}g) \in KN_G(P)$. □

Corollary 54. *Let G be a finite group, and let P be a Sylow p-subgroup of G. Then $N_G(N_G(P)) = N_G(P)$.*

Proof. Since $N_G(P)$ is a normal subgroup of $N_G(N_G(P))$, and since $P \in \mathrm{Syl}_p(N_G(P))$, the Frattini Argument tells us that $N_G(N_G(P)) = N_G(P)N_{N_G(N_G(P))}(P)$. But clearly $N_{N_G(N_G(P))}(P) \leq N_G(P)$, and the result follows. □

Theorem 55

Let G be a finite group, and let $p_1, \ldots, p_k$ be the distinct prime divisors of $|G|$. Let $P_1, \ldots, P_k$ be subgroups of G with $P_i \in \mathrm{Syl}_{p_i}(G)$ for all i. The following statements are equivalent.

1. *G is nilpotent.*
2. *$P_i \trianglelefteq G$ for all i.*
3. *$G \cong P_1 \times \cdots \times P_k$.*

Proof.

$1 \Longrightarrow 2$Let G be nilpotent. Corollary 54 tells us that $N_G(P_i) = N_G(N_G(P_i))$. But Proposition 52 tells us that no proper subgroup of G is equal to its own normalizer. Hence $N_G(P_i) = G$.

$2 \Longrightarrow 3$Suppose that $P_i \trianglelefteq G$ for all i. We argue by induction; let $\mathscr{P}(j)$ be the statement that $P_1 \cdots P_j \cong P_1 \times \cdots \times P_j$. Certainly $\mathscr{P}(1)$ is true. Suppose that $\mathscr{P}(j)$ true for a particular $j < k$. Let $N = P_1 \ldots P_j$. Since N and NP_{j+1} are both normal in G, and since their orders are coprime, we have $[N, P_{j+1}] \leq N \cap P_{j+1} = \{e\}$. So $ng = gn$ for all $n \in N$ and $g \in P_{j+1}$, and so $NP_{j+1} \cong N \times P_{j+1}$. The statement $\mathscr{P}(j+1)$ follows inductively. This is sufficient to prove the implication, since $|G| = |P_1 \cdots P_k|$.

$3 \Longrightarrow 1$Suppose that $G = P_1 \times \cdots \times P_k$. Each subgroup P_i is nilpotent by Theorem 50. Since G is the direct product of nilpotent groups, it follows from Proposition 51.3 that G is itself nilpotent. □

Corollary 56. *Let G be a finite group, and let $g, h \in G$ be elements with coprime orders. Then $gh = hg$.*

Proof. Let $P_1, \ldots, P_k$ be the Sylow subgroups of G. By Theorem 55 there exists an isomorphism $\theta G \longrightarrow P_1 \times \cdots \times P_k$. Let $\theta(g) = (g_1, \ldots, g_k)$ and $\theta(h) = (h_1, \ldots, h_k)$. Since g and h have coprime orders, one of g_i or h_i must be the identity, for all i. Hence g and h commute. □

Remark. The converse to Corollary 56 is also true. Suppose that G has the property that any two elements with coprime order commute. Let $P_1, \ldots, P_k$ be Sylow subgroups for the distinct prime divisors $p_1, \ldots, p_k$ of G. Then clearly $P_i \in N_G(P_j)$ for all i, j, since if $i \neq j$ then the elements of P_i and P_j commute. It follows that $N_G(P_i) = G$ for all i, and so the Sylow subgroups of G are all normal; hence G is nilpotent.

Definition. Let G be a group. A subgroup $M < G$ is *maximal* if $M \leq H \leq G \Longrightarrow H = M$ or $H = G$. We write $M <_{\max} G$ to indicate that M is a maximal subgroup of G.

Remark. We note that if G is a finite group, then it is clear that every proper subgroup of G is contained in some maximal subgroup of G. This is not necessarily the case in an infinite group; indeed there exist infinite groups with no maximal subgroups, for instance $(\mathbb{Q}, +)$.

Proposition 57. *If G is a finite nilpotent group, and if $M <_{\max} G$, then $M \triangleleft G$, and $|G/M|$ is prime.*

Proof. By Proposition 52 we see that $N_G(M) \neq M$. But certainly $M \leq N_G(M) \leq G$, and so $N_G(N) = G$. So $M \triangleleft G$. Since there are no proper subgroups of G strictly containing M, it follows from Proposition 2 that G/M has no proper, non-trivial subgroup. Hence G/M is cyclic of prime order. □

Proposition 58. *Let G be a finite group. If every maximal subgroup of G is normal, then G is nilpotent.*

Proof. Suppose that every maximal subgroup of G is normal. Let P be a Sylow p-subgroup of G, and suppose that $N_G(P) \neq G$. Then $N_G(P) \leq M$ for some maximal subgroup M. Now $P \in \mathrm{Syl}_p(M)$, and M is normal in G by hypothesis. So the conditions of the Frattini argument are satisfied, and we have $G = MN_G(P)$. But this is a contradiction, since $N_G(P) \leq M$. So we must have $N_G(P) = G$. Hence every Sylow subgroup of G is normal, and so G is nilpotent by Theorem 55.

We summarize our main criteria for nilpotence in the following theorem.

Theorem 59

Let G be a finite group. The following are all equivalent to the statement that G is nilpotent.

1. *The lower central series for G terminates at $\{e\}$.*
2. *The upper central series for G terminates at G.*
3. *G has a central series.*
4. *Every Sylow subgroup of G is normal.*
5. *G is a direct product of p-groups.*
6. *Any two elements of G with coprime order commute.*
7. *Each proper subgroup of G is properly contained in its normalizer.*
8. *Every maximal subgroup of G is normal.*

The first three of these conditions apply also to infinite groups.

§ 8 More on group actions

Definition. Let G and H be isomorphic groups. Let G act on a set X, and H on a set Y.

1. We say that the actions of G and H are *equivalent* if there is an isomorphism $\theta : G \longrightarrow H$ and a bijection $\alpha : X \longrightarrow Y$ such that $\alpha(gx) = \theta(g)\alpha(x)$ for all $g \in G$ and $x \in X$.

2. In the special case that $G = H$ and θ is the identity map, we have $\alpha : X \longrightarrow Y$ such that $\alpha(gx) = g\alpha(x)$ for all $g \in G$ and $x \in X$. Then we say that the actions on X and Y are *equivalent actions of* G, and that α is an *equivalence of actions*.

We revisit the Orbit-Stabilizer Theorem in the light of this definition.

Theorem 60. ✠ ***Orbit-Stabilizer Theorem Revisited***
Let G act transitively on a set X. Let $x \in X$, and let H be the stabilizer of x in G. Let Y be the set of left cosets of H in G. Then the action of G on Y by left translation, and the action of G on X, are equivalent actions of G.

Proof. Recall that for $k_1, k_2 \in G$ we have $k_1H = k_2H \Longleftrightarrow k_1x = k_2x$. So there is a well-defined map $f : Y \longrightarrow X$ given by $f(kH) = kx$ for $k \in G$. The map f is bijective (this is the substance of the proof of Theorem 10.) Now for all $g \in G$ we have $gf(kH) = gkx = f(gkH)$, and so f is an equivalence of actions. □

The significance of Theorem 60 is that the study of transitive actions of G is reduced to the study of actions of G on the left cosets of its subgroups.

Suppose that G is a group acting on a set Ω. For every $k \in \mathbb{N}$, there is an action of G on Ω^k given by

$$g(x_1, \ldots, x_k) = (gx_1, \ldots, g_{x_k}).$$

Definition. Let G act on Ω, and let $k \leq |\Omega|$. We say that the action of G on Ω is k-transitive if for any two k-tuples $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_k)$ in Ω^k, with the property that $x_i \neq x_j$ and $y_i \neq y_j$ when $i \neq j$, there exists $g \in G$ such that $gx = y$ (so $gx_i = y_i$ for $1 \leq i \leq k$).

Another way of phrasing the definition is that G is k-transitive on Ω if it acts transitively on the subset of Ω^k consisting of k-tuples of *distinct* elements of Ω.

Remark. If G acts k-transitively on Ω, then it is clear that it acts ℓ-transitively on Ω for every $\ell \leq k$.

Examples.
1. S_n acts n-transitively on $\Omega = \{1, \ldots, n\}$. For any n-tuple $x = (x_1, \ldots, x_n)$ of distinct elements of Ω we have $\{x_1, \ldots, x_n\} = \{1, \ldots, n\}$, and so the map $f_x : i \mapsto x_i$ is in S_n. Now if y is another n-tuple of distinct elements then $f_y f_x^{-1} : x \mapsto y$.
2. A_n acts only $(n-2)$-transitively on $\Omega = \{1, \ldots, n\}$. It is not $(n-1)$-transitive, since the tuples $(1, 3, \ldots, n)$ and $(2, 3, \ldots, n)$ lie in distinct orbits. Let x and y be $(k-2)$-tuple of distinct elements of Ω. Then there is an element g of S_n such that $gx = y$. Now there exist two points i, j which are not in the tuple y, and since $(i\,j)y = y$ we have $(i\,j)gx = y$. Since one of g or $(i\,j)g$ lies in A_n, we see that x and y lie in the same orbit of A_n, as we claimed.

3. If $n > 3$ then D_{2n} is only 1-transitive on the vertices of a regular n-gon. There exist vertices u, v, w such that u is adjacent to v but not to w, and it is clear that there is no $g \in D_{2n}$ such that $g(u,v) = (u,w)$ since symmetries of an n-gon preserve adjacency of vertices.

Remark. If G acts on Ω and $H = \mathrm{Stab}_G(x)$ for $x \in \Omega$, then H acts on $\Omega \setminus \{x\}$.

Proposition 61. *Let G be transitive on Ω, let $x \in \Omega$, and let $H = \mathrm{Stab}_G(x)$. Let $k \in \mathbb{N}$. Then G acts k-transitively on Ω if and only if H acts $(k-1)$-transitively on $\Omega \setminus \{x\}$.*

Proof. Suppose G is k-transitive. Let $y = (y_1, \ldots, y_{k-1})$ and $z = (z_1, \ldots, z_{k-1})$ be $(k-1)$-tuples of distinct elements of $\Omega \setminus \{x\}$. Then $y' = (y_1, \ldots, y_{k-1}, x)$ and $z' = (z_1, \ldots, z_{k-1}, x)$ are k-tuples of distinct elements of Ω, and so there exists $h \in G$ such that $hy' = z'$. Now we see that $hx = x$, and so $h \in H$. It is also clear that $hy = z$. So we have shown that H is $(k-1)$-transitive on $\Omega \setminus \{x\}$.

Conversely, suppose that H is $(k-1)$-transitive on $\Omega \setminus \{x\}$. Let $y = (y_1, \ldots, y_k)$ and $z = (z_1, \ldots, z_k)$ be distinct k-tuples of elements of Ω. Since G is transitive on Ω, there exist $f, g \in G$ such that $fy_k = x$ and $gz_k = x$. Now we see that $u = (fy_1, \ldots, fy_{k-1})$ and $v = (gz_1, \ldots, gz_{k-1})$ are $(k-1)$-tuples of distinct elements of $\Omega \setminus \{x\}$. So there exists $h \in H$ such that $hu = v$. Now it is straightforward to check that $hfy_i = gz_i$ for $1 \leq i \leq k$, and so $g^{-1}hfy = z$. We have therefore shown that G is k-transitive on Ω. □

Definition. Recall that an equivalence relation on a set Ω may be regarded as a partition of the set Ω into disjoint subsets (the parts, or equivalence classes) whose union is Ω. (If $x, y \in \Omega$, then $x \sim y$ if and only if x and y lie in the same part.

1. We say that an equivalence relation is *trivial* if it has only one part, or if all of its parts have size 1. (So either $x \sim y$ for all x, y, or else $x \sim y$ only if $x = y$.)
2. Suppose that G acts on Ω. We say that G *preserves* Ω if

$$x \sim y \Longleftrightarrow gx \sim gy, \quad \text{for } x, y \in \Omega.$$

It is clear that any group G acting on Ω preserves the trivial partitions.

Definition. Let $|\Omega| > 1$, and let G act transitively on Ω.

1. If $\sim$ is a non-trivial equivalence relation on Ω, such that G preserves $\sim$, then we say the action of G is *imprimitive*, and that $\sim$ is a *system of imprimitivity* for G. The parts of $\sim$ are called *blocks*.
2. If there is no non-trivial equivalence relation on Ω which is preserved by G, then we say that the action of G is *primitive*.

Examples.

1. Let g be the n-cycle $(1\,2\,\ldots\,n) \in S_n$, and let $\langle g \rangle$ act on $\Omega = \{1, \ldots, n\}$ in the natural way. The action is primitive if and only if n is prime. Otherwise n has some proper divisor d, and the equivalence relation on Ω given by $i \sim j \Longleftrightarrow i \equiv j \bmod d$ is a system of imprimitivity.

2. S_n is primitive on $\Omega = \{1, \ldots, n\}$ for $n > 1$. And A_n is primitive on Ω for $n > 2$.

3. D_{2n} acts primitively on the vertices of an n-gon if and only if n is prime. If $n = ab$ is a proper factorization of n, then we can inscribe b distinct a-gons inside the n-gon, and the vertices of the a-gons form the blocks of a system of imprimitivity.

Proposition 62. *Let $\mathscr{B}$ be a system of imprimitivity for the action of G on Ω. For a block B of $\mathscr{B}$, define $gB = \{gx \mid x \in B\}$. Then gB is a block of $\mathscr{B}$, and the map $B \mapsto gB$ defines a transitive action of G on the set of blocks of $\mathscr{B}$.*

Proof. If $x \in gB$ and $y \in \Omega$, then $g^{-1}x \in B$, and so $g^{-1}x \sim g^{-1}y \iff g^{-1}y \in B$. So we have $x \sim y \iff y \in gB$, and so gB is a block of $\mathscr{B}$. It is easy to see that $eB = B$ and that $g(hB) = ghB$ for $g, h \in G$, and so the map $B \mapsto gB$ gives an action of G. And since G is transitive on Ω, it is clear that it is transitive on the blocks. □

Corollary 63. *If $\mathscr{B}$ is a system of imprimitivity for the action of G on Ω, then all of the blocks of $\mathscr{B}$ have the same size.*

Proof. This is clear from the transitivity of G on the blocks; if B and C are blocks then $C = gB$ for some $g \in G$. □

Corollary 64. *If $|\Omega| = p$, where p is prime, and if G acts transitively on Ω, then the action of G is primitive.*

Proof. Let $\sim$ be an equivalence relation preserved by G. It is clear from Corollary 63 that the size of each part divides $|\Omega|$. But since p is prime, its only divisors are 1 and p. So $\sim$ must be trivial, and hence G is primitive. □

Remark. Corollary 64 establishes the claim, in the examples above, that the actions of C_p and D_{2p} on p points are primitive.

Proposition 65. *If G is 2-transitive on Ω, then it is primitive.*

Proof. Let $\sim$ be any non-trivial equivalence relation on Ω. it has distinct parts B_1 and B_2, and the part B_1 comtains distinct points x and y. Let $z \in B_2$. Then since G acts 2-transitively, there exists $g \in G$ such that $g(x, y) = (x, z)$. So we have $x \sim y$ but $gx \not\sim gy$. Hence G does not preserve $\sim$, and so G is primitive. □

Remark. Primitivity is a strictly stronger condition than transitivity, since e.g. $\langle (1\,2\,3\,4) \rangle$ is transitive but not primitive on $\{1, 2, 3, 4\}$. And 2-transitivity is strictly stronger than primitivity, since e.g. A_3 is primitive but not 2-transitive on $\{1, 2, 3\}$.

Proposition 66. *Let G act transitively on Ω. Let H be the stabilizer of a point $x \in \Omega$. Then the action of G is primitive if and only if $H <_{\max} G$.*

Proof. Suppose that $\mathscr{B}$ is a system of imprimitivity for G on Ω. Let B be the block of $\mathscr{B}$ which contains the point x. Let y be point in B distinct from x. Since G is transitive, there exists $g \in G$ with $gx = y$. Since $y \in gB$, we have $gB = B$. Let $L = \mathrm{Stab}_G(B)$, the stabilizer in the action of G on the blocks of $\mathscr{B}$. It is clear that $H \leq L$, and since $g \in L \setminus H$, we have $H < L$. But since there is more than one block of $\mathscr{B}$, and G is transitive on blocks, we see that $L < G$. We have that $H < L < G$, and so H is not maximal in G.

Conversely, suppose H is not maximal. Let L be a subgroup such that $H < L < G$. Recall from Theorem 60 that the action of G on Ω is equivalent to its action on left cosets of H. So we may suppose that Ω is this set of cosets. Now we define an equivalence relation $\sim$ on Ω by $aH \sim bH \iff aL = bL$. This relation is well defined, since if $aH = a'H$ then $aL = a'L$, and it is clear that it is an equivalence relation; it is non-trivial, since $H < L < G$. Now for $g \in G$ we have

$$aH \sim bH \iff aL = bL \iff gaL = gbL \iff gaH \sim gbH,$$

and so $\sim$ is a system of imprimitivity for G. So G is not primitive. □

Corollary 67. *If G is nilpotent and G acts primitively on Ω, then $|\Omega|$ is prime.*

Proof. Let H be the stabilizer of $x \in \Omega$. Then $H <_{\max} G$, and so $|G : H|$ is prime, by Proposition 57. But $|\Omega| = |G : H|$ by Theorem 60. □

Remark. Let G and Ω be as in Corollary 67. We have that $H \lhd G$ by Proposition 57, and it follows that H is the kernel of the action. So we have a homomorphism $G/H \longrightarrow \mathrm{Sym}(\Omega) \cong S_p$ for some prime p. Now in S_p there is no non-p-element which commutes with a p-cycle. But since G is nilpotent, any two elements of coprime order commute, and it follows that the image of G/H in S_p is cyclic of order p.

Proposition 68. *Let G act faithfully and primitively on a finite set Ω, and let N be a non-trivial normal subgroup of G. Then N is transitive on Ω.*

Proof. Let $M <_{\max} G$ be the stabilizer of $x \in \Omega$, and let $N \trianglelefteq G$. Then $M \leq MN \leq G$, and so MN is equal either to M or to G. If $MN = N$ then $N \leq M$, and since N is normal we have $N \leq {}^gM$ for every $g \in G$. But the conjugates of M are the point-stabilizers in G, and it follows that N is contained in the kernel of G. But G is faithful, and so we must have $N = \{e\}$ in this case.

We may therefore suppose that $MN = G$. Now the stabilizer of x in N is $M \cap N$, and we have

$$|\mathrm{Orb}_N(x)| = \frac{|N|}{|M \cap N|} = \frac{|MN|}{|M|} = \frac{|G|}{|M|} = |\mathrm{Orb}_G(x)|.$$

(Here we have used the Orbit-Stabilizer Theorem and the Third Isomorphism Theorem.) Since G is transitive, we have $\mathrm{Orb}_N(x) = \Omega$, and so N is transitive. □

Proposition 69. *Let G be a subgroup of S_7 of order 168. Then G is simple.*

Proof. First note that since 7 divides 168, there is a 7-cycle in G, and so G is transitive on $\{1,\ldots,7\}$. By Corollary 64 we see that G acts primitively. Suppose that N is a proper, non-trivial normal subgroup of G. Then N is transitive by Proposition 68, and so $|N|$ is divisible by 7. So N contains a Sylow 7-subgroup of G, and since it is normal, it must contain all Sylow 7-subgroups of G.

Let P be a Sylow 7-subgroup of G. We observe that S_7 contains 120 conjugates of P, and so the normalizer of P in S_7 has order 42. So G does not normalize P. The number $n_7(G)$ of Sylow 7-subgroups of G is therefore greater than 1; we have $n_7(G) \equiv 1 \bmod 7$, and $n_7(G)$ divides 168, and so we must have $n_7(G) = 8$. So the subgroup N has 8 Sylow 7-subgroups, and hence 8 divides $|N|$. Since 7 also divides $|N|$, we see that 56 divides $|N|$. It follows that $|N| = 56$, since $168 = 56 \times 3$.

Now N contains 48 elements of order 7, since each conjugate of P contains 6 such elements. It follows that N has only 8 elements whose order is not 7, and it is clear that these must form a normal Sylow 2-subgroup K. Now N acts transitively on 7 points, and so N is primitive by Corollary 64. So K is transitive by Proposition 68. So we have a subgroup of order 8 acting transitively on 7 points, and this is absurd since 7 does not divide 8. So we have a contradiction; no such subgroup N can exist, and so G is simple. □

We conclude the course by constructing a subgroup of S_7 of order 168. More precisely, we shall construct a group G with a faithful action on 7 points, which can therefore be identified with a subgroup of S_7.

Let $G = \mathrm{GL}_3(2)$, the set of invertible 3×3 matrices with entries from $\mathbb{Z}_2$, under matrix multiplication. Since $\mathbb{Z}_2$ is a field, the standard results of linear algebra apply. A 3×3 matrix is invertible if and only if it has non-zero determinant, which is the case if and only if its columns are linearly independent over $\mathbb{Z}_2$.

There is an action of G on the space ${\mathbb{Z}_2}^3$ of column vectors, with basis

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

This space has size $2^3 = 8$, and G acts transitively on the 7 non-zero vectors.

Note that if $Ae_i = c_i$ for $i = 1,2,3$, then the columns of A are c_1, c_2, c_3. It follows that the action of G is faithful, since the only element which fixes all three basis vectors is the identity.

It remains to calculate $|G|$. We consider how we can construct an element A of G, column by column. There are clearly 7 possibilities for the first column c_1 of A, since any non-zero vector will do. The columns must be linearly independent, and so the second column c_2 cannot lie in the span of the first. This rules out the choices $c_2 \in \{0, c_1\}$, and there are 6 remaining possibilities. Now we require the last column c_3 to lie outside the span of the first two; this span contains 4 vectors, and so there are 4 possible choices for c_3. So there are $7 \times 6 = 168$ possible choices for the matrix A, and so $|G| = 168$.

Proposition 70. *The group* $\mathrm{GL}_3(2)$ *constructed above is simple.*

Proof. We have shown that $\mathrm{GL}_3(2)$ acts faithfully and transitively on 7 points. So it is isomorphic with a subgroup of S_7, of order 168, and so it is simple by Proposition 69. □

Remark. The group $\mathrm{GL}_3(2)$ is one member of an infinite family of simple groups. Let $\mathrm{GL}_d(p)$ be the *general linear group*, the group of invertible $d \times d$ matrices over the field $\mathbb{Z}_p$. Define $\mathrm{SL}_d(p)$ to be the *special linear group*, the subgroup consisting of matrices with determinant 1. The centre of $SL_d(p)$ is given by

$$Z = Z(\mathrm{SL}_d(p)) = \left\{ \lambda I \mid \lambda \in \mathbb{Z}_p, \lambda^d = 1 \right\}.$$

The quotient group $\mathrm{PSL}_d(p) = \mathrm{SL}_d(p)/Z$, the *projective special linear group*, is simple except when $d = 2$ and $p = 2, 3$. It has a natural 2-transitive action on the *lines* of ${\mathbb{Z}_p}^d$.

The field $\mathbb{Z}_p$ in this construction can be replaced with any other finite field.