ALGEBRA 3 NOTES

NICHOLAS HAYEK

Lectures by Prof. Henri Darmon

CONTENTS

I Groups **1**

Axioms and First Properties **1**

I Groups

8/28/24

In Algebra 3, we will study abstract algebraic structures. Chiefly among them, we have *groups*, which are useful in representing symmetries, *rings & fields*, which help us think about number systems, and *vector spaces & modules*, which encode physical space.

AXIOMS AND FIRST PROPERTIES

DEF 1.1 A *group* is a set G endowed with a binary composition $G \times G \to G$ such that the following axioms hold:

1. $\exists e \in G$, an identity element, such that $e * a = a * e = a \ \forall a \in G$.
2. $\forall a \in G, \exists a' \in G$ such that $a * a' = a' * a = e$.
3. $a * (b * c) = (a * b) * c \ \forall a, b, c \in G$.

DEF 1.2 If $a * b = b * a \ \forall a, b \in G$, we call G *commutative*.

Why do we care about groups? If X is an object, we call a *symmetry* of X a function $X \to X$ which preserves the structure of the object.

e.g. a polygon, graphs, tilings, "crystal," "molecules," rings, vector spaces, metric spaces, manifolds

The collection of symmetries, $\text{Aut}(X) = \{f : X \to X\}$, we can structure as a group: let $* = \circ$, $e = \text{Id}$, and $f \in \text{Aut}(X)$ (note that, by axiom 2, these must be bijective).

A note on notation: for non-commutative groups, we write $a * b = ab$, $e = 1$ or $\mathbb{1}$, $a' = a^{-1}$, and $a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ times}}$. This is called *multiplicative notation*. For commutative rings, we write $a * b = a + b$, $e = 0$ or $\mathbb{0}$, $a' = -a$, and $na = \underbrace{a + \ldots + a}_{n \text{ times}}$.

The following are some examples of groups generated by sets:

1. If X is a set with no operations, $\text{Aut}(X)$ is the set of all bijections $f : X \to X$. One calls this the *permutation group*, or, if $|X| = n < \infty$, the *symmetric group*, and we write $\text{Aut}(X) = S_n$.
2. If V is a vector space over $\mathbb{F}$, $\text{Aut}(V) = \{T : V \to V\}$, the set of vector space isomorphism. If $\dim(V) = n$, recall that we assocate V with $\mathbb{F}^n$, whose set of isomorphism is given by $GL_n(\mathbb{F})$, the collection of $n \times n$ invertible matrices. This is called the *linear group*.
3. If R is a ring, then $(R, +, \mathbb{0})$ is a commutative group. Furthermore, $(R^\times, \times, \mathbb{1})$ is a non-commutative group, where $R^\times := R \setminus \{\text{non-invertible elements of } R\}$.
4. If V is Euclidean space endowed with a dot product, where $\mathbb{F} = \mathbb{R}$, with $\dim(V) < \infty$, $\text{Aut}(V) = O(V)$ is called the *orthogonal group of* V. In particular, $O(V) = \{T : V \to V : T(u) \cdot T(v) = u \cdot v\}$.

5. If X is a geometric figure (e.g. a polygon), we write $\text{Aut}(X) = D_n$, where $|\text{Aut}(X)| = n$, and call this the *dihedral group*.

8/30/23

DEF 1.3 A *homomorphism* from groups $G_1 \to G_2$ is a function $\phi : G_1 \to G_2$ satisfying $\phi(ab) = \phi(a)\phi(b)$, where $a, b \in G_1$.

PROP 1.1 $\phi(\mathbb{1}_{G_1}) = \mathbb{1}_{G_2}$ and $\phi(a^{-1}) = \phi(a)^{-1}$ $\forall a \in G_1$.

PROOF.

$$\phi(\mathbb{1}_{G_1}) = \phi(\mathbb{1}_{G_1}^2) = \phi(\mathbb{1}_{G_1})^2 \implies \phi(\mathbb{1}_{G_1}) = \phi(\mathbb{1}_{G_1}^{-1})\phi(\mathbb{1}_{G_1}) = \mathbb{1}_{G_2}.$$

$$\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(\mathbb{1}_{G_1}) = \mathbb{1}_{G_2} \implies \phi(a_{-1}) = \phi(a)^{-1}. \qquad \square$$

DEF 1.4 A homomorphism which is bijective is called an *isomorphism*. If there exists an isomorphism between two groups G_1 and G_2, we call them *isomorphic*, and write $G_1 \cong G_2$. One can thus call $\text{Aut}(G)$ the set of isomorphisms from $G \to G$.

As an example, take $G = \mathbb{Z}/n\mathbb{Z} = \{0, 1, ..., n-1\}$. Note that $\phi : G \to G$ is determined entirely by $\phi(1)$, since $\phi(i) = \phi(\underbrace{1 + ... + 1}_{i \text{ times}}) = \underbrace{\phi(1) + ... + \phi(1)}_{i \text{ times}}$. How can we find an element of $\text{Aut}(G)$? Clearly, not all mappings $\phi(1)$ are bijective: take n to be even and $\phi(1) = 2$. Then $\phi(2) = 4$, $\phi(3) = 6$, ..., $\phi(n/2) = 0$, so ϕ is not surjective. We know then that $\phi(G) = \phi(1)\mathbb{Z} \mod n$, and would like $\phi(G) = G$. If $\phi(1)$ and n are co-prime, then we can write $k\phi(1) + ln = k\phi = 1$, so every element can be reached.

We can construct a group isomorphism $\eta : \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ which sends $\phi \to \phi(1)$. Clearly $\eta(\phi_{t_1} \circ \phi_{t_2}) = \phi_{t_1} \circ \phi_{t_2}(1) = \phi_{t_1}(t_2) = t_1 t_2 = \eta(\phi_{t_1})\eta(\phi_{t_2})$, so η is a homomorphism. It is also bijective: given $\phi(1)$, we can deduce a mapping for each element.

DEF 1.5 For a group G and an object X, define an *action* to be a function from $G \times X \to X$ such that

1. $\mathbb{1} \times x = x$
2. $(g_1 g_2)x = g_1(g_2 x)$

for $x \in X$, $g_1, g_2 \in G$. One can create from this the automorphism $m_g : x \to gx$ of X: if $gx_1 = gx_2$, one can take the group inverse to conclude $x_1 = x_2$. Similarly, given $x \in X$, we know $m_g(g^{-1}x) = x$.

PROP 1.2 Given an action of G on X, the assignment $g \to m_g$ is a homomorphism between $G \to \text{Aut}(X)$.

PROOF.

$$m_{g_1 g_2}(x) = g_1 g_2 x = g_1(g_2 x) = g_1 m_{g_2}(x) = m_{g_1}(m_{g_2}(x)) = m_{g_1} \circ m_{g_2}(x) \qquad \square$$

9/4/24

In fact, given a homomorphism of this form, one can extract the group action.

DEF 1.6

A *G-set* is a set X endowed with a group action of G. If $\forall x, y \in X, \exists g \in G : gx = y$, we say that this G-set is *transitive*. Finally, a transitive G-set of a subset of X ("G-subset of X") is called an *orbit* of G on X.

PROP 1.3

Every G-set is a disjoint union of orbits.

PROOF.

We define a relation on X as follows: $x \underset{G}{\sim} y$ if $\exists g : gx = y$. This is an equivelance relation:

1. Take $g = \mathbb{1}$. Then $\mathbb{1}x = x$, so $x \underset{G}{\sim} x$.
2. If $gx = y$, then $g^{-1}y = x$, so $x \underset{G}{\sim} y \implies y \underset{G}{\sim} x$.
3. If $gx = y$ and $hy = z$, then $hgx = z$, so $x \underset{G}{\sim} y \wedge y \underset{G}{\sim} z \implies x \underset{G}{\sim} z$.

From prior theory, we know that equivalence classes of an equivalence relation on X form a partition of X. However, by definition, the equivalence classes of the above relation are exactly the orbits of the G-set on X. $\square$

We denote the set of equivalence classes defined in the proof above X/G.

E.G. 1.1

♠ *Examples* ♣

1. Let $X = \{\clubsuit\}$, G be a group, and $g\clubsuit = \clubsuit$. This is a group action. The homomorphism $m : G \to \mathrm{Aut}(X) = S_1$ sends g to the identity.
2. Let $X = G$, G be a group, and $gx = gx$ (group action on the LHS, left-multiplication on the RHS). We have the homomorphism $m : G \to \mathrm{Aut}(G)$ such that $m(g)(x) = gx = gx$. This is an injective function, since we can always take the group inverse, i.e. $m(h)(x) = m(g)(x) \implies g = h$. Thus, $G \cong m(G) \subseteq \mathrm{Aut}(G)$.
3. Let $X = G$ as before, but let $gx = xg^{-1}$. We can check that this is a group action: (1) $\mathbb{1} * x = x\mathbb{1}^{-1} = x\mathbb{1} = x$ and (2) $g * (h * x) = (h * x)g^{-1} = xh^{-1}g^{-1}$, where $(gh) * x = x(gh)^{-1} = xh^{-1}g^{-1} \implies g * (h * x) = (gh) * x$.
4. Letting $X = G \times G$, we can form a group action from both left- and right-multiplication: $(g, h) * x = gxh^{-1}$. One can check its validity.

1.1 Cayley

Every group G is isomorphic of a group of permutations (i.e. a subgroup of a symmetric group). If G is finite, then G is isomorphic to S_n, where $n = |G|$.

DEF 1.7 If X_1 and X_2 are G-sets, then an *isomorphism* from X_1 to X_2 is a bijection $\phi : X_1 \to X_2$ such that $\phi(gx) = g\phi(x)\ \forall x \in X_1, g \in G$.

9/6/24

DEF 1.8 Let $H < G$. Define G/H to be the set of orbits for right action on G, i.e $\{aH : a \in G\}$, where $aH = \{ah : h \in H\}$. We call these *left cosets*. We also have *right cosets*, $\{Ha : a \in G\}$.

For example, take $G = S_3$ and $H = \{\mathbb{1}, (12)\}$. Then $G/H = \{\{\mathbb{1}, (12)\}, \{(13), (123)\}\} = \{H, (13)H\}$ and $H \setminus G = \{\{\mathbb{1}, (12)\}, \{(13), (132)\}, \{(23), (123)\}\}$.

1.2 Size of Cosets

Let $H < G$. If H is finite, then $|H| = |aH|\ \forall a \in G$.

As proof of this fact, one may take the bijection $\phi : H \to aH : \phi(h) = ah$.

1.3 Lagrange

Let G be finite. The cardinality of any subgroup $H < G$ divides the cardinality of G. In particular, $|G| = |H| \cdot |G/H|$.

DEF 1.9 Define the *stabilizer* of an element of a G-set $x_0 \in X$ to be $\{g \in G : g \circledast x_0 = x_0\}$.

PROP 1.4 If X is a transitive G-set, then $\exists H < G$ such that $X \cong G/H$ as a G-set.

PROOF. Choose $x_0 \in X$. Define $H = \text{stab}(x_0) := \{g \in G : g \circledast x_0 = x_0\}$. One may show that H is indeed a subgroup. We then define $\phi : G/H \to X$ such that $gH \to gx_0$. Checking some properties:

1. ϕ is well defined. If $gH = g'H$, then $\exists h : gh = g'$. Then $\phi(gH) = gx_0$ and $\phi(g'H) = g'x_0 = ghx_0$. But $h \in \text{stab}(x_0)$, so this is just gx_0.
2. ϕ is surjective. This follows from the fact that X is transitive: for $x, x_0 \in X, \exists g \in G$ with $gx_0 = x$. Then $\phi(gH) = gx_0 = x$.
3. ϕ is injective. Take $g_1x_0 = g_2x_0$. Then $g_2^{-1}g_1x_0 = x_0$, so $g_2^{-1}g_1 \in H$, i.e. $g_2H = g_1H$
4. ϕ is a G-set isomorphism. $\phi(g \circledast aH) = \phi(gaH) = gax_0 = g\phi(aH)$. $\square$

1.4 Orbit-Stabilizer

If X is a transitive G-set, $x_0 \in X$, and $|G| < \infty$, then $X \cong G/\text{stab}_G(x_0)$. In particular, $|G| = |X| \cdot |\text{stab}_G(x_0)|$

Given $H < G$, we say $h_1, h_2 \in H$ are *conjugate* if $\exists g : g^{-1}h_1 g = h_2$, or, equivalently, $gh_1 g^{-1} = h_2$. Given $H_1, H_2 < G$, we say H_1 and H_2 are *conjugate equivalent* if every element in H_1 is conjugate to some element in H_2. DEF 1.10

Stabilizers of elements in a transitive G-set X are conjugate equivalent. PROP 1.5

PROOF. Let $x_1, x_2 \in X$ and consider $\text{stab}(x_1), \text{stab}(x_2)$. Since X is transitive, $\exists g : gx_1 = x_2$. Thus, if $h \in \text{stab}(x_2)$, i.e. $hx_2 = x_2$, then $hgx_1 = gx_1 \implies g^{-1}hgx_1 = x_1 \implies g^{-1}hg \in \text{stab}(x_1)$. Thus, there exists a conjugation of every element in $\text{stab}(x_2)$ which is an element in $\text{stab}(x_1)$. One shows the converse similarly to conclude that $\text{stab}(x_1)$ and $\text{stab}(x_2)$ are conjugate equivalent. $\square$

We can show a natural bijection between the "pointed G-sets" (X, x_0) with subgroups of G: send $(X, x_0) \to \text{stab}(x_0)$ and $H \to (G/H, H)$. This establishes the intuition that the number of transitive G-sets up to isomorphism is exactly the number of subgroups of G up to conjugation. PROP 1.6

PROOF. Consider an isomorphism class P of pointed G-sets, i.e. $\forall (X, x_0), (Y, y_0) \in P$, $X \cong Y$. Consider the mapping $\Phi : (X, x_0) \in P \to \text{stab}(x_0)$. The image of this mapping is a conjugation class: since $X \cong Y$, we know that there exists a unique mapping $\phi(y_0) = x_k$. Since X is transitive, $\exists g : gx_k = x_0$. Then $h \in \text{stab}(x_0) \implies hx_0 = x_0 \implies hgx_k = gx_k \implies hg\phi(y_0) = g\phi(y_0) \implies \phi(hgy_0) = \phi(gy_0) \implies hgy_0 = gy_0 \implies g^{-1}hg \in \text{stab}(y_0)$.

[8pt]Conversely, one can show that the image of the mapping $\Xi : H \to (G/H, H)$ over a conjugation class $I : \forall F, H \in I, \exists g \in G : g^{-1}Fg = H$ is an isomorphism class over G-sets.

[8pt]Thus, the set of G-sets up to isomorphism is in bijection with the set of $H < G$ up to conjugation. $\square$

♠ *Examples* ♣ E.G. 1.2

1. Let $H = G$. Then $G/H = \{H\}$. $X = \{*\} \cong G/H$. Similarly, if $H = \mathbb{1}$, then $G/H \cong G = X$.
2. Let $G = S_n$. Let $X = \{1, 2, ..., n\}$. For $n \in X$, $X \cong G/\text{stab}(n) = G/S_{n-1}$.
3. Let X be a regular tetrahedron. Let $G = \text{Aut}(X)$ (the set of rigid motions). Notate $X = \{1, 2, 3, 4\}$ (for each vertex). Then G acts transitively on X. In particular, $\text{stab}(1) = \mathbb{Z}3 \implies |G| = 4 \cdot 3 = 12$.
4. Let $G = \text{Aut}(X)$ on a tetrahedron, this time *including* reflections. Then $G = S_4$, since one can always send $a \to b$ by reflecting through a plane intersecting c, d.

5. Let X be a cube, $G = \mathrm{Aut}(X)$, the rigid motions on X. Note that there are 6 faces, 12 edges, and 8 vertices. If x_0 is a face, then $\mathrm{stab}(x_0)$ are exactly the rotations about the axis intersecting the face, i.e. $|\mathrm{stab}(x_0)| = 4$, so $|G| = 6 \cdot 4 = 24$. As $4! = 24$, it is tempting to consider that $G \cong S_4$. This turns out to be true: let G act on the cube's diagonals.

PROP 1.7 If $\phi : G \to H$ is a homomorphism, then ϕ is injective $\iff \phi(g) = \mathbb{1} \implies g = \mathbb{1} \forall g \in G$.

PROOF. Let $\phi(g) = \mathbb{1}$ and ϕ be injective. Then $\phi(g^2) = \phi(g) \implies g^2 = g \implies g = \mathbb{1}$.

[8pt]Let $\phi(g) = \mathbb{1} \implies g = \mathbb{1}$. Then $\phi(a) = \phi(b) \implies \phi(b^{-1}a) = \mathbb{1} \implies b^{-1}a = \mathbb{1} \implies a = b$, so ϕ is injective. $\square$

Define $\ker(\phi) := \{g \in G : \phi(g) = \mathbb{1}\}$. This is a subgroup.

DEF 1.11 Observe that, for $g \in G, h \in \ker(\phi)$, we have $g^{-1}hg \in \ker(\phi)$. Subgroups which obey this property are called *normal subgroups*.

PROP 1.8 If N is normal, then $G/N = N/G$, i.e. $gN = Ng\ \forall g$. One can view G/N as a group with $g_1N \cdot g_2N = g_1g_2N$, and $\mathbb{1}_{G/N} = N$.

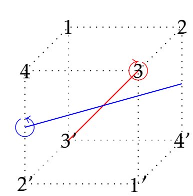
PROOF. $gN = \{gn : n \in N\} = \{gg^{-1}ng : n \in N\} = \{ng : n \in N\} = Ng$. The group operations follow immediately. $\square$

1.5 Isomorphism Theorem for Groups

If $\phi : G \to H$ is a homomorphism, $N = \ker(\phi)$, then ϕ induces an injective homomorphism $\overline{\phi} : G/N \hookrightarrow H : \overline{\phi}(aN) = \phi(a)$.

PROOF. $\overline{\phi}$ being a homomorphism follows from the fact that ϕ is a homomorphism. For injectivity, see that $\overline{\phi}(aN) = \mathbb{1} \implies \phi(a) = \mathbb{1} \implies a = \mathbb{1}$. $\square$

E.G. 1.3 ♠ *Examples* ♣



Let X be a cube, and $G = \text{Aut}(X)$ be the set of rigid motions. Consider the homomorphism $\phi : G \to S_4$ (permutations of the diagonals). Then $\ker(\phi) = \{\sigma \in \text{Aut}(X) : \sigma(\{ii'\}) = \{ii'\}\} = \cap_{j=1}^{4} \text{stab}(\{jj'\})$. Observe that $\text{stab}(\{ii'\})$ are exactly the 3 rotations about the axis ii' (red), the 2 perpendicular rotations (blue), as well as the identity. Observe that these rotations are disjoint, so $\cap_{j=1}^{4} \text{stab}(\{jj'\}) = \{\mathbb{1}\} \implies \ker(\phi) = \mathbb{1}$.

Then, we have $\overline{\phi} : G/\ker(\phi) \hookrightarrow S_4 = G/\{\mathbb{1}\} \hookrightarrow S_4 = G \hookrightarrow S_4$ is injective. Since $|G| = |S_4|$, we have that $G \cong S_4$.

Consider now $\widetilde{G} = \widetilde{\text{Aut}}(X)$, consisting of rigid motions *and* reflections. We have $\widetilde{G}/G = \{1, \tau\}$, where τ is some orientation-reversing reflection. One can conclude then that $\#\widetilde{G} = 4! \cdot 2 = 48$. One could write $\tau = -I_3$, the orientation-reversing identity. Thus $g\tau = \tau g \; \forall g \in \widetilde{G}$. *9/13/24*

It's tempting to say $\widetilde{G} \cong S_4 \times \mathbb{Z}2$, given the construction above, and that $\widetilde{G} = G \sqcup \tau G$. This is correct: take $S_4 \times \mathbb{Z}2 \to \widetilde{G} : (g, i) \mapsto g\tau^i$. We verify this is a homomorphism: $g_1 \tau^{i_1} g_2 \tau^{i_2} = g_1 g_2 \tau^{i_1 + i_2}$.

The *center* of G, notated $Z(G)$, is $\{z \in G : zg = gz \forall g \in G\}$. Elements in the center are their own conjugations. DEF 1.12

Let $\sigma \in S_n$ be decomposed into disjoint cycles $\tau_1, ..., \tau_k$. The unordered set $\{|\tau_1|, ..., |\tau_k|\}$ is called the *cycle shape* of σ. Alternatively, the cycle shape is the partition of n DEF 1.13

$$|\tau_1| + ... + |\tau_k| = n$$

where we include all identity cycles (i), with size 1.

♠ *Examples* ♣ E.G. 1.4

1. Let $\sigma \in S_n$ fix all elements. Then the cycle shape of σ is dictated by $1 + ... + 1 = n$.
2. Let $\sigma = (1\ 2\ ...\ n) \in S_n$. The cycle shape of σ is dictated by n.
3. Consider all permutations in S_4, decomposed into disjoint cycles. We have

the following cycle shapes:

partition	$\sigma \in S_4$	#
$1+1+1+1$	$\{\mathbb{1}\}$	1
$2+1+1$	$\{(12),(13),(14),(23),(24),(34)\}$	$\binom{4}{2}=6$
$3+1$	$\{(123),(124),(132),(134),(142),(143),(243),(342)\}$	$4\cdot 2=8$
$2+2$	$\{(12)(34),(13)(24),(14)(23)\}$	3
4	$\{(1234),(1243),(1324),(1342),(1423),(1432)\}$	$3!=6$

1.6 Relation Between Cycle Shape and Conjugation

Two permutations in S_n are conjugate $\iff$ they have the same cycle shape.

PROOF.

$(\implies)$ Let $g \sim g'$, i.e. $g' = hgh^{-1}$ for some $h \in G$. Let $g(i) = j$. Then $g'(h(i)) = hgh^{-1}h(i) = hg(i) = hj$. Thus, for a disjoint cycle τ of g, say $(a, b, \ldots, z)$, we have that $\tau' = (h(a), h(b), \ldots, h(z))$ is a disjoint cycle of g', i.e. they have the same cycle shape.

Let $g, g' \in S_n$ have the same cycle shape. Then consider $h \in S_n$ which permutes the elements of cycles in g to the elements of cycles in g'. Then $hgh^{-1} = g'$.

For example, $g = (123)(45)(6)$ and $g' = (615)(24)(3)$. h is then (163524). □

E.G. 1.5

♠ *Examples* ♣

We'll revisit example (3) from above:

conjugacy class	#
$\mathbb{1}$	1
(12)	$\binom{4}{2}=6$
(123)	$4\cdot 2=8$
$(13)(24)$	3
(1234)	$3!=6$

Recall that $S_4 \cong \text{Aut(cube)}$. Thus, we may associate each of these conjugacy classes with conjugacy classes of cube automorphisms:

conjugacy class	#	Aut(cube)
$\mathbb{1}$	1	Id
(12)	$\binom{4}{2} = 6$	rotations about edge diagonals by π
(123)	$4 \cdot 2 = 8$	rot'n about face centers by π
(13)(24)	3	rot'n about principal diagonals by $\frac{\pi}{3}$
(1234)	$3! = 6$	rot'n about face centers by $\frac{\pi}{2}$

Recall Lagrange's Theorem, which states that, for all $H < G$, $|H| \mid |G|$. Is the converse true? Not necessarily (try considering subgroup of order 15 of S_5).

1.7 Sylow 1

Let p be prime. If $\#G = p^t m$, $p \nmid m$, then G has a subgroup of cardinality p^t.

If $H \subseteq G$ is as in Thm 1.7, then H is called a *Sylow p-subgroup* of G. DEF 1.14

♠ *Examples* ♣ E.G. 1.6

1. $\#S_5 = 120 = 2^3 \cdot 3 \cdot 5$. We can thus find Sylow subgroups of cardinality 8, 3, and 5.

2. $\#S_6 = 720 = 2^4 \cdot 3^2 \cdot 5$. We can find Sylow subgroups of cardinality 16, 9, and 5. The subgroup with 9 elements can be constructed by taking $\langle (123), (456) \rangle$, the generator of two order 3 elements. This is isomorphic to $\mathbb{Z}3 \times \mathbb{Z}3$. What about the subgroup of 16 elements? Take $H = D_8 \times S_2$, where D_8 acts on vertices 1, 2, 3, 4, and S_2 swaps the remaining 5, 6 independently.

3. $\#S_8 = 2^7 \cdot 3^2 \cdot 5 \cdot 7$. How can we find a subgroup with $2^7 = 128$ elements? An idea would be taking $D_8 \times D_8$, and then swapping these squares via S_2, i.e. $H = D_8 \times D_8 \times S_2$.

Take this with a grain of salt, I'm not sure that it works
-Prof. Darmon

Given a prime p and a group G, the following are equivalent: PROP 1.9

1. $\exists$ a G-set of cardinality prime to p, i.e. not a multiple of p, with no orbit of size 1.

2. $\exists$ a transitive G-set of cardinality ≥ 2 and prime to p.

3. G has a proper subgroup of index prime to p.

PROOF.

($1 \implies 2$) Write $X = X_1 \sqcup X_2 \sqcup ... \sqcup X_k$ for orbits X_i. This orbits are especially transitive. Then $\exists j$ such that $|X_j|$ is prime to p. Suppose otherwise. Then $|X| = |X_1| + ... + |X_k| = mp$, so $|X|$ is not prime to p.

($2 \implies 3$). Let X be a transitive G set with $|X| \geq 2$ and $|X|$ prime to p. Then $X \cong G/\text{stab}(x_0)$ for some $x_0 \in X$. If $\text{stab}(x_0) = G \forall x_0 \in X$, then $X = \{\star\}$, i.e. does not have cardinality ≥ 2. Thus, $\text{stab}(x_0) < G$ is a strict subgroup. Finally, it is prime to p, since $|X| = \frac{|G|}{|\text{stab}(x_0|}$, i.e. we'd find that $|X|$ is not prime to p.

($3 \implies 1$). Take $H < G$, a proper subgroup of index prime to p, and consider the G-set $X = G/H$. If X had an orbit of size 1, say of x_0, then $H \sim \text{stab}(x_0) = G$, i.e. is not a proper subset. We also conclude that $|X|$ is prime to p by Lagrange. □

PROP 1.10

For a finite group G, with $\#G = p^t m$ for some prime p and $m \neq 1$, then (G, p) satisfies Prop 1.9.

PROOF.

Let $X = \{\text{set of } H \subseteq G : \#H = p^t\}$. Then if $A \subseteq X$, $gA \in X$, since $ga = gb \implies a = b$, i.e. g acts faithfully. Furthermore, unless $g = \mathbb{1}$, $A \neq gA$. Thus, X has no fixed points, and thus no orbits of size 1. X therefore (almost) satisfies (1) of Prop 1.9. It remains to show that $|X|$ is prime to p.

$$\begin{aligned}\#X = \binom{p^t m}{p^t} &= \frac{(p^m)(p^m - 1) \cdot ... \cdot (p_t m - p^t + 1)}{p^t \cdot (p^t - 1) \cdot ... \cdot 1} \\ &= \prod_{j=0}^{p^t - 1} \frac{p^t m - j}{p^t - j}\end{aligned}$$

From here, one can show that the maximal power of p dividing the numerator is the same maximal power of p which divides the denominator. Thus, p cannot divide any of the product terms. By Euler's Lemma, then, p cannot divide $\prod$. □

PROOF OF SYLOW 1

Fix a prime p. Let G be a finite group of minimal cardinality for which Sylow 1 fails (such a group exists: we have found such groups in Example 1.6). By Prop 1.10, (G, p) satisfies (3) of Prop 1.9. Thus, $\exists H < G$ such that $p \nmid [G : H]$. By strong induction, $\exists N < H$ of cardinality p^t. N is thus also a p-Sylow subgroup of G, violating minimality. $\lightning$. □