ALGEBRA III NOTES

NICHOLAS HAYEK

Lectures by Prof. Henri Darmon

CONTENTS

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

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

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. $a * (b * c) = (a * b) * c \ \forall a, b, c \in G$.

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

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, $\mathrm{Aut}(X) = \{f : X \to X\}$, we can structure as a group: let $* = \circ$, $e = \mathrm{Id}$, and $f \in \mathrm{Aut}(X)$ (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 $na = \underbrace{a + \ldots + a}_{n \text{ times}}$.

♠ *Examples* ♣ E.G. 1.1

1. If X is a set with no operations, $\mathrm{Aut}(X)$ 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 $\mathrm{Aut}(X) = S_n$.
2. If V is a vector space over $\mathbb{F}$, $\mathrm{Aut}(V) = \{T : V \to V\}$, 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*.

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

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

PROOF.

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

$$\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(\mathbb{1}_{G_1}) = \mathbb{1}_{G_2} \implies \varphi(a_{-1}) = \varphi(a)^{-1}.$$ □

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 $\varphi : G \to G$ is determined entirely by $\varphi(1)$, since $\varphi(i) = \varphi(\underbrace{1 + ... + 1}_{i \text{ times}}) = \underbrace{\varphi(1) + ... + \varphi(1)}_{i \text{ times}}$. How can we find an element of $\text{Aut}(G)$? Clearly, not all mappings $\varphi(1)$ are bijective: take n to be even and $\varphi(1) = 2$. Then $\varphi(2) = 4$, $\varphi(3) = 6$, ..., $\varphi(n/2) = 0$, so φ is not surjective. We know then that $\varphi(G) = \varphi(1)\mathbb{Z} \mod n$, and would like $\varphi(G) = G$. If $\varphi(1)$ and n are co-prime, then we can write $k\varphi(1) + ln = k\varphi = 1$, 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 $\varphi \to \varphi(1)$. Clearly $\eta(\varphi_{t_1} \circ \varphi_{t_2}) = \varphi_{t_1} \circ \varphi_{t_2}(1) = \varphi_{t_1}(t_2) = t_1 t_2 = \eta(\varphi_{t_1})\eta(\varphi_{t_2})$, so η is a homomorphism. It is also bijective: given $\varphi(1)$, 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 $m_g(g^{-1}x) = x$.

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

PROOF.

$m_{g_1g_2}(x) = g_1g_2x = g_1(g_2x) = g_1m_{g_2}(x) = m_{g_1}(m_{g_2}(x)) = m_{g_1} \circ m_{g_2}(x)$ $\square$

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.

Every G-set is a disjoint union of orbits. PROP 1.3

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.

♠ *Examples* ♣ E.G. 1.2

1. Let $X = \{♣\}$, G be a group, and $g♣ = ♣$. 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 $\varphi : X_1 \to X_2$ such that $\varphi(gx) = g\varphi(x)\ \forall x \in X_1, g \in G$.

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 $\varphi : H \to aH : \varphi(h) = ah$.

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 $\varphi : G/H \to X$ such that $gH \to gx_0$. Checking some properties:

1. φ is well defined. If $gH = g'H$, then $\exists h : gh = g'$. Then $\varphi(gH) = gx_0$ and $\varphi(g'H) = g'x_0 = ghx_0$. 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 $\varphi(gH) = gx_0 = x$.
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. $\varphi(g \circledast aH) = \varphi(gaH) = gax_0 = g\varphi(aH)$. $\square$

1.4 Orbit-Stabilizer

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

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, $gh_1g^{-1} = h_2$. 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

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

We can show a natural bijection between the "pointed G-sets" (X, x_0) with subgroups of G: send $(X, x_0) \to \mathrm{stab}(x_0)$ 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

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 $\Phi : (X, x_0) \in P \to \mathrm{stab}(x_0)$. The image of this mapping is a conjugation class: since $X \cong Y$, we know that there exists a unique mapping $\varphi(y_0) = x_k$. Since X is transitive, $\exists g : gx_k = x_0$. Then $h \in \mathrm{stab}(x_0) \implies hx_0 = x_0 \implies hgx_k = gx_k \implies hg\varphi(y_0) = g\varphi(y_0) \implies \varphi(hgy_0) = \varphi(gy_0) \implies hgy_0 = gy_0 \implies g^{-1}hg \in \mathrm{stab}(y_0)$. PROOF.

[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. 1.3

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 $n \in X$, $X \cong G/\mathrm{stab}(n) = G/S_{n-1}$.
3. Let X be a regular tetrahedron. Let $G = \mathrm{Aut}(X)$ (the set of rigid motions). Notate $X = \{1, 2, 3, 4\}$ (for each vertex). Then G acts transitively on X. In particular, $\mathrm{stab}(1) = \mathbb{Z}3 \implies |G| = 4 \cdot 3 = 12$.

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, $G = \text{Aut}(X)$, the rigid motions on X. Note that there are 6 faces, 12 edges, and 8 vertices. If x_0 is a face, then $\text{stab}(x_0)$ are exactly the rotations about the axis intersecting the face, i.e. $|\text{stab}(x_0)| = 4$, 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 $\varphi : G \to H$ is a homomorphism, then φ is injective $\iff$ $\varphi(g) = \mathbb{1} \implies g = \mathbb{1} \forall g \in G$.

PROOF.

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

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

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

DEF 1.11

Observe that, for $g \in G, h \in \ker(\varphi)$, we have $g^{-1}hg \in \ker(\varphi)$. 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 $g_1 N \cdot g_2 N = g_1 g_2 N$, 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. □

1.5 Isomorphism Theorem for Groups

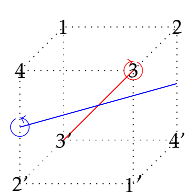
If $\varphi : G \to H$ is a homomorphism, $N = \ker(\varphi)$, then φ induces an injective homomorphism $\overline{\varphi} : G/N \hookrightarrow H : \overline{\varphi}(aN) = \varphi(a)$.

PROOF.

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

E.G. 1.4

♠ *Examples* ♣



Let X be a cube, and $G = \text{Aut}(X)$ be the set of rigid motions. Consider the homomorphism $\varphi : G \to S_4$ (permutations of the diagonals). Then $\ker(\varphi) = \{\sigma \in \text{Aut}(X) : \sigma(\{ii'\}) = \{ii'\}\} = \cap_{j=1}^{4}\text{stab}(\{jj'\})$. 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 $\cap_{j=1}^{4}\text{stab}(\{jj'\}) = \{\mathbb{1}\} \implies \ker(\varphi) = \mathbb{1}$.

Then, we have $\overline{\varphi} : G/\ker(\varphi) \hookrightarrow S_4 = G/\{\mathbb{1}\} \hookrightarrow S_4 = G \hookrightarrow S_4$ 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: $g_1\tau^{i_1}g_2\tau^{i_2} = g_1g_2\tau^{i_1+i_2}$.

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 $\tau_1, \ldots, \tau_k$. The unordered set $\{|\tau_1|, \ldots, |\tau_k|\}$ is called the *cycle shape* of σ. Alternatively, the cycle shape is the partition of n DEF 1.13

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

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

♠ *Examples* ♣ E.G. 1.5

1. Let $\sigma \in S_n$ fix all elements. Then the cycle shape of σ is dictated by $1 + \ldots + 1 = n$.
2. Let $\sigma = (1\ 2\ \ldots\ n) \in S_n$. 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 $(a, b, ..., z)$, we have that $\tau' = (h(a), h(b), ..., h(z))$ 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. 1.6

♠ *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 $S_4 \cong \mathrm{Aut(cube)}$. 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).

SYLOW THEOREMS

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. 1.7

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 $X \cong G/\mathrm{stab}(x_0)$ for some $x_0 \in X$. If $\mathrm{stab}(x_0) = G \forall x_0 \in X$, then $X = \{\star\}$, i.e. does not have cardinality ≥ 2. Thus, $\mathrm{stab}(x_0) < G$ is a proper subgroup.

($3 \implies 1$). 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 $H \sim \mathrm{stab}(x_0) = G$, i.e. is not a proper subset. □

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 1.7). By Prop 1.10, (G, p) satisfies (3) of Prop 1.9. Thus, $\exists H < G$ such that $p \nmid [G : H]$. But also, $\#H | \#G$, so $\#H = p^t m_0$ for $m_0 < m$.

By strong induction, $\exists N < H$ of cardinality p^t. N is thus also a p-Sylow subgroup of G, violating minimality $\lightning$. □

PROP 1.11

If $\#G = p^t m$, with $p \nmid m$, then G has a proper subgroup H of cardinality $p^t m_0$: $m_o < m$.

PROOF.

This is mentioned in the previous proof. By (3) of Prop 1.9, we have a proper subgroup $H < G$ with $p \nmid \frac{p^t m}{\#H}$ and $\#H | p^t m$.

Thus, $\#H = p^{t_0} m_0$ with $t_0 \leq t, m_0 \leq m$. If $t_0 < t$, then

$$p \nmid \frac{p^t m}{p^{t_0} m_0} = p^{t-t_0} \frac{m}{m_0} \lightning$$

$\implies t_0 = t$. Then, if $m_0 = m$, $H = G$, but H is proper.

$\implies \#H = p^t m_0 : m_0 < m$. □

If G is abelian and finite, with $p|\#G$ for a prime p, then G has an element of order p. Thus G has a subgroup of order p. PROP 1.12

PROOF.

Let $\#G = pm$. It is sufficient to find $g \in G$ with $p|\mathrm{ord}(g)$, since then $\mathrm{ord}(g^{\frac{\mathrm{ord}(g)}{p}}) = p$. Let $g_1, ..., g_t \in G$ be the set of generators for G. Let $n_i = \mathrm{ord}(g_i)$. Then consider the homomorphism

$$\varphi : n_1\mathbb{Z} \times ... \times n_t\mathbb{Z} \to G : (a_1, ..., a_t) \to g_1^{a_1} \cdot ... \cdot g_t^{a_t}$$

This is surjective, since we can always write $g \in G$ in terms of powers of generators. Recall that, for a homomorphism $\varphi : A \to B$, $A/\ker(\varphi) \cong \mathrm{Im}(\varphi)$. Thus, $\#G | n_1 \cdot ... \cdot n_t$. But $p|\#G \implies p|n_1 \cdot ... \cdot n_t \implies p|n_j$ for some j. Then $p|\mathrm{ord}(g_j)$. □

1.8 Sylow 2

If H_1, H_2 are Sylow$-p$ subgroups of G, then $\exists g \in G$ with $gH_1g^{-1} = H_2$.

PROOF.

Let $\#G = p^t m : p \nmid m$. Let H_1, H_2 have cardinality p^t. Consider G/H_1 as a G-set. In fact, think of G/H_1 as an H_2-set. Then we may decompose into orbits:

$$G/H_1 = X_1 \sqcup X_2 \sqcup ... \sqcup X_N$$

Then $\#X_i \#H_2$ by Orbit-Stabilizer, so $\#X_i = p^a : a \leq t \ \forall i$. Then $\exists$ an orbit of size 1, otherwise $p|G/H_1 \implies p|m \lightning$.

Let $X_j := \{gH_1\}$. Thus, $\forall h \in H_2, hgH_1 = gH_2 \implies g^{-1}hg \in H_1$, i.e. $\exists g : g^{-1}H_2 g = H_1$. Rewriting, this means $gH_1g^{-1} = H_2$. □

Given a group G and $H < G$, we call $\{g \in G : gHg^{-1} = H\}$ the *normalizer* of H. DEF 1.15

H is a subgroup of its normalizer. PROP 1.13

1.9 Sylow 3

Let N_p be the number of distinct Sylow-p subgroups of G. Then

1. $N_p | m$, where $\#G = p^t m : p \nmid m$
2. $N_p \equiv 1 \mod p$

PROOF. **(1st Claim)** Let X be the set of Sylow-p subgroups, and consider X as a G-set under conjugation. By Sylow 2, X is transitive. Thus, $X \cong G/\text{stab}(H)\ \forall H \in X$. Fix some H. Notice that stab(H) is the normalizer of H. Thus, $\#H | \#\text{stab}(H) \implies \#G/\#\text{stab}(H) | \#G/\#H = \frac{p^t m}{p^t} = m$. We conclude that $\#X | m$.

(2nd Claim) Let H be a Sylow-p subgroup. Let X be the set of all Sylow-p subgroups, viewed as an H-set by conjugation. We decompose X into orbits:

$$X = X_1 \sqcup X_2 \sqcup \ldots \sqcup X_a$$

X_i are all transitive, so $\#X_i | \#H = p^t \implies \#X_i = 1 \vee p \vee \ldots \vee p^t$. We claim that there is exactly one orbit of size 1. Let $X_j = \{H'\}$ be an orbit of size 1. Then $aH'a^{-1} = H'\ \forall h \implies H$ is a subset of the normalizer of H'. Let $H \subseteq R = \{a \in G : aH'a^{-1} = H'\}$. Then H' is a normal subgroup of R. Thus, we may consider R/H' as a group. Then $\frac{\#R}{\#H'} = \frac{\#R}{p^t} = \frac{p^t m_0}{p^t} = m_0 < m \implies p \nmid \frac{\#R}{\#H'}$.

Consider the natural map $\varphi : R \to R/H'$. Then $\#\varphi(H) | p^t$ (by First Iso. Thm.) and also $\#\varphi(H) | \frac{\#R}{\#H'}$ (by Lagrange). But $p \nmid \frac{\#R}{\#H'}$, so $\#\varphi(H) = 1$. Then $H \subseteq \ker(\varphi) = H'$, but $\#H = \#H'$, so $H = H'$. We could always have chosen H as an orbit of size 1, and find now that all other orbits of size 1 are exactly H. Thus, $|X| = N_p \equiv 1 \mod p$. $\square$

PROP 1.14 If p, q are primes with $p < q$ and $p \nmid q - 1$, then all groups of cardinality pq are cyclic.

BURNSIDE'S LEMMA

DEF 1.16 Let G be a group, and let X be a G-set. Given $g \in G$, we consider $X^g := \{x \in X : gx = x\}$. Denote by $\text{FP}_X(g) = \#X^g$.

For instance, if $G = S_4$ with $X = \{1, 2, 3, 4\}$, then $X^{(12)} = \{3, 4\}$. Thus, $\text{FP}_X((12)) = 2$. Consider also $\text{FP}_X((12)(34)) = 0$.

PROP 1.15 $\text{FP}_X(hgh^{-1}) = \text{FP}_X(g)\ \forall h \in G$.

PROOF.

Take the bijection $\varphi : X^g \to X^{hgh^{-1}}$ by $\varphi(x) = hx$. $\square$

1.10 Burnside's Lemma

$$\frac{1}{\#G}\sum_{g\in G} \mathrm{FP}_X(g) = \#(X/G) = \#\text{orbits of } X$$

PROOF. Let $\Sigma \subseteq G \times X$ be $\Sigma = \{(g,x) : gx = x\}$. We'll count Σ in two ways:

1. $\Sigma = \sum_{g\in G} \mathrm{FP}_X(g)$ by definition
2. $\Sigma = \sum_{x\in X} \#\mathrm{stab}(x) = \sum_{O\in X/G}\sum_{x\in O} \#\mathrm{stab}(x)$. By Orbit-Stabilizer, $\#\mathrm{stab}(x)\#O = \#G$, where $x \in O$. Thus, we have

$$\Sigma = \sum_{O\in X/G}\sum_{x\in O} \frac{\#G}{\#O} = \sum_{O\in X/G} \#G = \#(X/G)\#G$$

Thus, $\sum_{g\in G} \mathrm{FP}_X(g) = \#(X/G)\#G$ as desired. $\square$

PROP 1.16 If X is a transitive G-set, with $|X| > 1$, then $\exists g \in G$ such that $\mathrm{FP}_X(g) = 0$.

PROOF. If X is transitive, then, by Burnside, $\sum_{g\in G} \mathrm{FP}_X(g) = \#G$. But $\mathrm{FP}_X(\mathbb{1}) = \#X > 1$. Thus, $\sum_{g\in G\setminus \mathbb{1}} \mathrm{FP}_X(g) \leq \#G - 2$. The result follows by pigeonhole principle. $\square$

DEF 1.17 Let $C = \{1, \ldots, t\}$. A coloring of X by C is a function $X \to C$. The set of such functions we denote by C^X. Note that $|C^X| = |C|^{|X|}$.

II Rings & Fields

People developed rings by counting: 0, 1, 2, 3, ... are natural. We generalize:

DEF 2.1

A *ring* is a set R endowed with two binary operations, denoted $+$ and $\times$, such that $+, \times : R \times R \to R$. The following axioms govern rings:

1. The neutral element $\mathbb{0}$ is such that $a + \mathbb{0} = a\ \forall a \in R$.
2. The inverse of a, denoted $(-a)$, is such that $a + (-a) = \mathbb{0}$.
3. The neutral element $\mathbb{1}$ is such that $a \times \mathbb{1} = a\ \forall a \in R$.
4. R is associative over (strictly) addition and multiplication
5. We have the following two distributive laws:
   (a) $a \times (b + c) = a \times b + a \times c$.
   (b) $(b + c) \times a = b \times a + c \times a$.

PROP 2.1

Notes on rings:

1. We denote by $(R, \cdot)$ the ring R endowed only with only the operation $\cdot$. Then, $(R, +)$ is an abelian group. We call $(R, \times)$ a *monoid*.
2. Sometimes, we do not require $\mathbb{1}$ (take the ring of even numbers, which has no units). However, in this class we will always have $\mathbb{1}$.
3. $\mathbb{1} \neq \mathbb{0}$ (i.e. we do not consider the zero ring).
4. $\mathbb{0}$ is never invertible, and $\mathbb{0}a = \mathbb{0}\ \forall a$.
5. $(-a) \times (-b) = ab$

E.G. 2.1

♠ *Examples* ♣

Recall completion in the analysis sense: X is not complete if it has a Cauchy sequence which does not converge in it; then the completion of X is $X \cup \{\text{limits of Cauchy seq's}\}$

1. $\mathbb{Z}$ is a ring.
2. $\mathbb{Q} = \{\frac{a}{b} : b \neq 0\}$, with $+, \times$, is a ring. We may complete $\mathbb{Q}$ by taking $\{\text{Cauchy sequences}\}/\{\text{null sequences}\} = \mathbb{R}$
3. Given a prime p, $|x - y|_p = p^{-\mathrm{ord}_p(x-y)}$. $x - y = \Pi q^{e_q} : e_q \in \mathbb{Z}$. Then $\mathrm{ord}_p(x - y) = e_p$. Note that $|ab|_p = |a|_p|b|_p$, and $|a + b|_p \leq |a|_p + |b|_p$. The completion by this metric is denoted $\mathbb{Q}_p$ (the field of p-atic numbers).
4. $\mathbb{C} = \mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$.
5. $R[x] = \{a_0 + a_1 x + ... + a_n x^n : a_i \in \mathbb{R}\}$.

6. $R \leftrightarrow$ # line and $\mathbb{C} \leftrightarrow$ plane geometry. For the latter, we note the properties

$$a + bi = r_1 e^{i\theta_1} \qquad c_1 \cdot c_2 = r_1 r_2 e^{i(\theta_1 + \theta_2)}$$

   Q: is there a ring which may be well adopted to $\mathbb{R}^3$ geometry? **A:** No, not quite. It is possible to do so with $\mathbb{R}^4$ 👎. From this arises the Hamilton quaternions:

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\} \qquad i^2 = j^2 = k^2 = -1$$

   with $ij = -ji = k$, $jk = -kj = i$, $ik = -ki = j$.

7. Let R be some commutative ring. Then $M_n(R) = n \times n$ matrices with entries on R. $M_n(R)$ is a ring, where $\mathbb{0}$ is the matrix with all 0 entries, and $\mathbb{1}$ is the matrix with all 0 entries except on the diagonal (where they are 1).

   Showing $(AB)C = A(BC)$ is tough via brute-force, but easy when taking an isomorphism from $M_n(R)$ to linear transformations on $R \to R$, with $M_1 M_2 \to f_1 \circ f_2$.

8. We may take a ring $R \rightsquigarrow (R, +, \mathbb{0})$, an additive, commutative group. Similarly, $R \rightsquigarrow (R^\times, \times, \mathbb{1})$, which is an associative multiplicative group. We denote by $R^\times$ the set of units in R, i.e. $\{a \in R : \exists a' : aa' = a'a = \mathbb{1}\}$.

A ring R such that $r_1 r_2 = r_2 r_1 \forall r_1, r_2 \in R$ is called *commutative*. DEF 2.2

A *homomorphism* of rings, $\varphi : R_1 \to R_2$ is such that DEF 2.3

$$\varphi(a + b) = \varphi(a) + \varphi(b) \qquad \varphi(ab) = \varphi(a)\varphi(b) \qquad \forall a, b \in R_1$$

From this arises the property $\varphi(\mathbb{1}_{R_1}) = \mathbb{1}_{R_2}$. Alternatively, φ is a ring homomorphism if it is an additive group homomorphism and obeys $\varphi(ab) = \varphi(a)\varphi(b)$.

The *kernel* of φ, denoted $\ker(\varphi)$, is the set DEF 2.4

$$\{a \in R_1 : \varphi(a) = 0\}$$

It is tempting to consider elements sent to 1, as in group kernels; however, *this* kernel will not be closed under multiplication, and is hence less interesting to study.

Recall that, in groups, $\ker(\varphi)$ is normal, and every normal subgroup may be conceptualized as the kernel of some group homomorphism. We have a similar notion in rings:

$I \subseteq R$ is called an *ideal* if DEF 2.5

1. I is an additive subgroup of R
2. $\forall r \in R, ri \in I, ir \in I$

Note, if R is commutative, we only need to check one of these inclusions.

If φ is a ring homomorphism, then $\ker(\varphi)$ is an ideal. PROP 2.2

PROOF.

Condition (1) follows from the fact that φ is an additive group homomorphism. Condition (2) follows from $\varphi(ri) = \varphi(r)\varphi(i) = \varphi(r) \cdot 0 = 0$, and similarly for $\varphi(ir) = 0$. □

PROP 2.3 If $I \subseteq R_1$ is an ideal, then $\exists$ a ring R_2 and a homomorphism $\varphi : R_1 \to R_2$ such that $\ker(\varphi) = I$.

PROOF. Consider $R_2 := R_1/I = \{a + I : a \in R_1\}$. Since I is commutative as an additive ring, it is normal, and thus R_1/I is a group under addition. For multiplication, we define $(a+I)(b+I) = (ab+I)$. Then let $\varphi : R_1 \to R_1/I$ be such that $a \mapsto a+I$. $\ker(\varphi) = \{a \in R_1 : a + I = I\} = \{a \in R_1 : a \in I\} = I$. □

Note that $\mathbb{0}_{R/I} = 0 + I$ and $\mathbb{1}_{R/I} = 1 + I$.

2.1 First Isomorphism Theorem

Let R be a ring (or a group), and let φ be a surjective ring (or group) homomorphism. Then $\mathrm{Im}(\varphi) \cong R/\ker(\varphi)$.

PROOF. We may take $\mathrm{Im}(\varphi) \to R/\ker(\varphi) : a \mapsto \varphi^{-1}(a)$ and $R/\ker(\varphi) \to \mathrm{Im}(\varphi) : a + \ker(\varphi) \mapsto \varphi(a)$. One can show without too much trouble that these are homomorphisms and inverses of eachother, and thus bijective. □

DEF 2.6 An *ideal* $I \subseteq R$ is called *maximal* if it is not properly contained in any proper ideal of R, i.e. $I \subsetneq I' \implies I' = R$ for any ideal I'.

DEF 2.7 An ideal $I \subseteq R$ is called *prime* if $ab \in I \implies a \in I$ or $b \in I$.

PROP 2.4 Let $R = \mathbb{Z}$, $I = n\mathbb{Z} = (n) = \{na : a \in \mathbb{Z}\}$. Then (n) is prime $\iff$ n is prime.

PROOF. ($\impliedby$) If $ab \in (n)$, then $n|ab$. By Gauss' Lemma, $n|a$ or $n|b$. Thus, $a \in (n)$ or $b \in (n)$.

($\implies$) By contrapositive: let $n = ab$. Then $ab \in (n)$. But $a, b < n$, so $a, b \notin (n)$. □

2.2 Integers are Principal

If $I \subseteq Z$ is an ideal, then $\exists n \in \mathbb{Z}$ such that $I = (n)$.

PROOF.

Proof 1. Consider the quotient $\mathbb{Z}/I$. As an abelian group, it is cyclic, generated by $1+I$. Let $n := \#(\mathbb{Z}/I) = \operatorname{ord}(1+I)$. If $n = \infty$, then $\mathbb{Z} \to \mathbb{Z}/I$ is injective, so $I = (0)$. Otherwise, $I = (n)$.

Proof 2. Assume that $I \neq (0)$. Let $n = \min\{a \in I : a > 0\}$. Let $a \in I$. Then $a = qn + r$, where $0 \leq r \leq n$. Then $a \in I, n \in I, qn \in I$ (by sucking in), so $a - qn \in I$. Thus, $r \in I \implies r = 0$ by minimality. □

Let R be a commutative ring. An ideal of the form $aR = (a) = \{ar : r \in R\}$ is called a *principal ideal*. DEF 2.8

A ring in which every idea is principal is called a *principal ideal ring*. DEF 2.9

2.3 Polynomials are Ideal

Consider $R = \mathbb{F}[x]$, where $\mathbb{F}$ is a field. If I is an ideal of $\mathbb{F}[x]$, then I is principal

By convention, we say $\deg(0) = -\infty$ in order to satisfy $\deg f(x)g(x) = \deg f(x) + \deg g(x)$. Note that $\deg(c) = 0$ where $c \neq 0$.

PROOF.

Let $f(x)$ be a polynomial in I of minimal degree (with $I \neq (0)$). Then let $\deg f(x) = d$, where $d \leq \deg g(x)\ \forall g \in \mathbb{F}[x]$.

For $g(x) \in I$, we may write $g(x) = f(x)q(x) + r(x)$, where $\deg r(x) < d$. Then $r(x) \in I$ by the same arguments presented in Thm 2.2. Thus, $\deg r(x) = 0$, so $I = (f)$. □

♠ *Examples* ♣ E.G. 2.2

1. Let $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, and let $I = \{a + n\mathbb{Z}\}$ be some ideal of $\mathbb{Z}/n\mathbb{Z}$. Then $\varphi^{-1}(I)$ is an ideal of $\mathbb{Z}$. Hence, $\varphi^{-1}(I) = (a)$ for some $a \in \mathbb{Z}$.

2. Let $R = \mathbb{Z}[x]$. Then $I = \{f(x) : f(0) \text{ is even}\} \subsetneq \mathbb{Z}[x]$. We claim that I is an ideal. We know that I is an additive subgroup of $\mathbb{Z}[x]$. If $f(x) \in \mathbb{Z}[x]$, $g(x) \in I$, then $f(x)g(x) \in I$, since $f(0)g(0)$ is always even.

3. If I were of the form $a\mathbb{Z}[x]$, then $a|2$ and $a|x$, so $a = \pm 1$. But $I \subsetneq \mathbb{Z}[x]$, so this can't be the case. From this example we consider $I = (2, x) = 2\mathbb{Z}[x] + xZ[x]$.

4. Let $R = \mathbb{F}[x, y]$ (a polynomial ring of two variables). Consider $(x, y) = Rx + Ry$. Note that all elements in this ideal are non-constant. We may write $Rx + Ry = \{f(x, y) : f(0, 0) = 0\}$.