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

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, $\mathrm{Aut}(X) = \{f : X \to X\}$, 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 $na = \underbrace{a + \ldots + a}_{n \text{ times}}$.

E.G. 1.1

♠ *Examples* ♣

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.

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

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. □

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

♠ *Examples* ♣ E.G. 1.2

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 $\varphi : X_1 \to X_2$ 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 $H = \mathrm{stab}(x_0) := \{g \in G : g \circledast x_0 = x_0\}$. 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 $h \in \mathrm{stab}(x_0)$, 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 $\exists g : g^{-1}h_1g = h_2$, 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

PROOF. 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. $\square$

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

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 $\Phi : (X, x_0) \in P \to \mathrm{stab}(x_0)$. 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 $h \in \mathrm{stab}(x_0) \implies hx_0 = x_0 \implies hgx_k = gx_k \implies hg\varphi(y_0) = g\varphi(y_0) \implies \varphi(hgy_0) = \varphi(gy_0) \implies hgy_0 = gy_0 \implies g^{-1}hg \in \mathrm{stab}(y_0)$.

[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 $G = \mathrm{Aut}(X)$ 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 $\varphi : G \to H$ 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 $g_1N \cdot g_2N = g_1g_2N$, and $\mathbb{1}_{G/N} = N$.

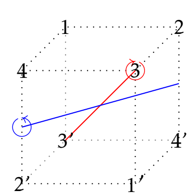
PROOF. $gN = \{gn : n \in N\} = \{gg^{-1}ng : n \in N\} = \{ng : n \in N\} = Ng$. The group operations follow immediately. □

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

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 $\widetilde{G} = \widetilde{\mathrm{Aut}}(X)$, 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. 1.5

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 $(a, b, ..., z)$, 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 $S_4 \cong \text{Aut(cube)}$. 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).

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 $X \cong G/\text{stab}(x_0)$ 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 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 $H \sim \text{stab}(x_0) = G$, 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.

$\implies \#H = p^t m_0 : m_0 < m$. □

PROP 1.12 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.

PROOF. Let $\#G = pm$. It is sufficient to find $g \in G$ with $p|\text{ord}(g)$, since then $\text{ord}(g^{\frac{\text{ord}(g)}{p}}) = p$. Let $g_1, ..., g_t \in G$ be the set of generators for G. Let $n_i = \text{ord}(g_i)$. 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 $\varphi : A \to B$, $A/\ker(\varphi) \cong \text{Im}(\varphi)$. 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 $p|\text{ord}(g_j)$. □

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 $gH_1g^{-1} = H_2$. □

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

PROP 1.13 H is a subgroup of its normalizer.

PROOF.

$\varphi : H \to H : h \mapsto ghg^{-1}$, where $g \in H$, is a bijection (check for yourself). Thus, $gHg^{-1} = H$ for a fixed $g \in H$, so $H < N$, the normalizer of H. $\square$

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, $X \cong G/\mathrm{stab}(H)\ \forall H \in X$. Fix some H. Notice that $\mathrm{stab}(H)$ is the normalizer of H. Thus, $\#H | \#\mathrm{stab}(H) \implies \#G/\#\mathrm{stab}(H) | \#G/\#H = \frac{p^t m}{p^t} = m$. 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 $\mathrm{FP}_X(g) = \#X^g$.

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

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

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, $\sum_{g\in G\setminus\mathbb{1}}\mathrm{FP}_X(g) \le \#G - 2$. 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 $|C^X| = |C|^{|X|}$.

EXCEPTIONAL OUTER AUTOMORPHISM OF S_6

All automorphisms on S_n are typically *inner*, i.e. can be written instead as a conjugation by some element. However, in S_6 there exists a unique *outer* automorphism, i.e. one which is not inner. Thus, we call it *exceptional*.

We are able to find an S_5-set of cardinality 6 (this comes from considering S_5/F_{20}, where F_{20} is the Frobenius group of 20 elements). Thus, one constructs the group action homomorphism $\varphi : S_5 \to \mathrm{Aut}(X)$, and finds the subgroup $\varphi(S_5) \cong S_5 \subseteq S_6$. We also have the typical subgroup $\mathrm{stab}(i) \cong S_5 \subseteq S_6$. Importantly, these two subgroups are not conjugate to eachother. Denote $\mathrm{stab}(i) = S_5$ and $\varphi(S_5) = \widetilde{S_5}$.

$$S_5 \subset S_6 \supset \widetilde{S_5}$$

To investigate the outer automorphism of S_6, we first consider the cycle shapes in F_{20} (i.e. conjugation classes of F_{20}). They are as follows:

$$(1234) \qquad (12)(34) \qquad (12345)$$

Similarly, in S_5, we have

Shape	Name	#	on S_5/F_{20}
$\mathbb{1}$	$1A$	1	$\mathbb{1}$
(12)	$2A$	10	(12)(34)(56)
(12)(34)	$2B$	15	(12)(34)
(123)	$3A$	20	(123)(456)
(1234)	$4A$	30	(1234)
(12345)	$5A$	24	(12345)
(12)(345)	$6A$	20	(123456)

For $2A$: Note that F_{20} has no transpositions, so $2A$ will have no fixed points. Thus, consider order 2 permutation on 6 elements with no fixed points: there is only (12)(34)(56).

For $4A$: How many fixed points does $4A$ have in S_5/F_{20}? It must have some, since the shape (1234) appears in F_{20}. Thus, we have an order 4 element in S_6 which fixes some points. This is only (1234).

For $2B$: We know that $2A = 4A^2$, so $2A$ will look like (12)(34).

For $3A$: There are no 3 cycles in F_{20}, so this has no fixed points in S_5/F_{20}. There is one such permutation on 6 elements, (123)(456)

For $5A$: There is only one order 5 cycle on 6 elements, and that is (12345).

For $6A$: Since (12)(345) is not in F_{20}, we observe no fixed points in S_5/F_{20}. There is only one such permutation on 6 elements of order 6, and that is (123456).

Thus, we conclude that $\widetilde{S_5} \subseteq S_6$, which is constructed via the action of S_5 on S_5/F_{20}, has exactly the cycle shapes expressed in the right-most column.

Now we investigate the cycle shapes in S_6:

Shape	Name	#	on $S_6/\widetilde{S_5}$
$\mathbb{1}$	$1A$	1	$\mathbb{1}$
(12)	$2A$	15	(12)(34)(56)
(12)(34)	$2B$	45	(12)(34)
(12)(34)(56)	$2C$	15	(12)
(123)	$3A$	40	(123)(456)
(123)(456)	$3B$	40	(123)
(1234)	$4A$	90	(1234)
(1234)(56)	$4B$	90	(1234)(56)
(12345)	$5A$	144	(12345)
(123456)	$6A$	120	(123)(45)
(123)(45)	$6B$	120	(123456)

For $2A$: Since $\widetilde{S_5}$ contains no single transpositions, $2A$ on $S_6/\widetilde{S_5}$ will have no fixed points. There is one such permutation of order 2, then, which is (12)(34)(56).

An automorphism $\varphi : G_1 \to G_2$ will send conjugacy classes of G_1 to conjugacy classes of G_2. Thus, for a conjugacy classes C_1 of G_1, $\varphi(C_1)$ is a conjugacy class of G_2 of equal cardinality. PROP 1.17

For $2B$: We map to a conjugacy class of order 2 elements of size 45 to another of size 45. Thus, there is only (12)(34).

For $2C$: By pigeonhole, we can map only to the remaining conjugacy class of order 2 elements, (12).

For $3A$: We do not have (123) in $\widetilde{S_5}$, so we have no fixed points on $S_6/\widetilde{S_5}$. The only order 3 cycle satisfying this is (123)(456).

For $3B$: By pigeonhole, we map to (123).

For $4A$: We have fixed points on $S_6/\widetilde{S_5}$, since $(1234) \in \widetilde{S_5}$. Thus, we map to (1234).

For $4B$:By pigeonhole, we map to (1234)(56).

For $5A$: We have only one order 5 cycle to choose from, and that is (12345).

For $6A$:The cycle (123456) is in $\widetilde{S_5}$, so we act on $S_6/\widetilde{S_5}$ with some fixed points. The only order 6 cycle satisfying this is (123)(45).

For $6B$: By pigeonhole, we map to (123456).

IDENTIFYING NORMAL SUBGROUPS

Given G, how might we identify its normal subgroups? We'll proceed by example. $G = A_5$, with $\#A_5 = 60$. We know that A_5 has no non-trivial normal subgroups. How can we show this?

One computes the conjugacy classes their sizes of G:

Shape	Name	#
$\mathbb{1}$	$1A$	$\mathbb{1}$
(12)(34)	$2A$	15
(123)	$3A$	20
(12345)	$5A$	24

However, in A_5, $24 \nmid 60$, so $5A$ is *not* in fact a conjugacy class. Consider $X = (12345)^{A_5}$, all conjugations of $5A$. This is, by definition, a transitive A_5-set. Invoking Orbit Stabilizer, $|X| = \frac{\#A_5}{\#\text{stab}(12345)}$. Then, the stabilizer of (12345) is

$$H := \{g \in A_5 : g(12345)g^{-1} = (12345)\} = \{g \in A_5 : g(12345) = (12345)g\}$$

Clearly any power $(12345)^j$ is in H for $j = 1, 2, 3, 4, 5$. We can further identify $\{1, 2, 3, 4, 5\}$ with $\mathbb{Z}5$, and observe that $\delta(x) = (12345)(x) = x + 1 \mod 5$. So we'd like $g\delta(j) = \delta(j)g \implies g(j + 1) = g(j) + 1$. Thus, if $g(1) = a$, then $g(2) = a + 2$, etc., etc. Thus, we can find only 5 such δ, so indeed $H = \{(12345)^j : j \in [1, 5]\}$, and $\#X = \frac{60}{5} = 12$.

Thus, we correct our prior statement and write that $\#5A = 12$. But (12345) is not conjugate to (12354) in A_5 (a transposition runs between them), so in fact we have two conjugacy classes of 5 cycles.

Shape	Name	#
$\mathbb{1}$	$1A$	$\mathbb{1}$
(12)(34)	$2A$	15
(123)	$3A$	20
(12345)	$5A$	12
(12354)	$5B$	12

PROP 1.18 A normal subgroup is a union of conjugacy classes.

The divisors of 60 are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30. We can rule out 1, ..., 12, since no conjugacy class is small enough to contain these. We must include the identity, so 15 is too small as well. For 20 and 30, by considering combinations, we cannot partition with the classes above.

MIDTERM 2023 Q4

Let n be odd. Let P be a Sylow-2 subgroup of S_{n-1}. Then P acts on $\{1, ..., n-1\}$ without fixed points (else, P would be isomorphic to a subgroup of S_{n-2}—but $2 \nmid n-2$). Thus P lies in S_n by fixing exactly one element. We may choose n such elements, and thus n such copies of $S_{n-1} \subset S_n$.

II Rings & Fields

FIRST PROPERTIES

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

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: DEF 2.1

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) $(b + c) \times a = b \times a + c \times a$.

Notes on rings: PROP 2.1

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. $(-a) \times (-b) = ab$

♠ *Examples* ♣ E.G. 2.1

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 {Cauchy sequences}/{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. $\mathbb{C} = \mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$.

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 $X \cup$ {limits of Cauchy seq's}

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. $\{a \in R : \exists a' : aa' = a'a = \mathbb{1}\}$.

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

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

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

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 $\varphi(ab) = \varphi(a)\varphi(b)$.

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

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

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:

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

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.

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

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 $\varphi(ir) = 0$. $\square$

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 $a \mapsto a+I$. $\ker(\varphi) = \{a \in R_1 : a + I = I\} = \{a \in R_1 : a \in I\} = I$. $\square$

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. $\square$

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 $a, b \notin (n)$. $\square$

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 $n := \#(\mathbb{Z}/I) = \mathrm{ord}(1+I)$. 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. □

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

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

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 $I = (f)$. □

E.G. 2.2 ♠ *Examples* ♣

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 $I = (2, x) = 2\mathbb{Z}[x] + xZ[x]$. This is not principal.
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 $Rx + Ry = \{f(x, y) : f(0, 0) = 0\}$.

PROP 2.5 I is a prime ideal of R if and only if R/I has no zero divisors (i.e. $\exists x, y \neq 0 : xy = 0$).

DEF 2.10 A ring which satisfies this is called an *integral domain*.

PROOF.

($\implies$). Given $a+I, b+I \in R/I$, let $(a+I)(b+I)=0$. Then $ab+I=0$, so $ab \in I$. Then $a \in I$ or $b \in I$, i.e. $a+I=0$ or $b+I=0$. Thus, R/I has no zero divisor. □

REMARK

If R is an integral domain, then it satisfies the cancellation law:

$$\forall a \neq 0, ax = ay \implies x = y$$

I is a maximal ideal $\iff$ R/i is a field. PROP 2.6

PROOF.

($\implies$)$a+I \in R/I$. If $a+I \neq 0$, then $Ra+I \supsetneq I$. By maximality, $Ra+I=R$. Then, let $b \in R, i \in I$. We have $1 = ba+i \implies 1+I = (b+I)(a+I) \implies (b+I) = (a+I)^{-1}$.

($\impliedby$) Given an ideal $J \supsetneq I$, let $a \in J - I$. Then $a+I \neq 0$. Thus, $\exists b$ such that $ba+I = 1+I$ in R/I, since it is a field. Thus, $1 \in J \implies R = J$. (By absorption property). □

I is prime $\iff$ R/I is an integral domain. PROP 2.7

QUOTIENTS

R/I, $a+I=b+I \iff a-b \in I$. If $I=(d)$, then $a+I=b+I \iff d|(b-a)$. PROP 2.8

♠ *Examples* ♣ E.G. 2.3

1. $R=\mathbb{Z}, I=(n)$. Then $\mathbb{Z}/n\mathbb{Z} = \{a+n\mathbb{Z} : a \in \mathbb{Z}\} = \{0,1,2,\ldots,n-1\}$†
2. $R=\mathbb{F}[x], I=(f(x))$. Then $\mathbb{F}[x]/(f(x)) = \{p(x)+f(x)\mathbb{F}[x]\} = \{p(x) : \deg(p(x)) \leq d-1\}$, where $d = \deg(f(x))$†

   † as representatives
3. $R=\mathbb{Z}[x], I=(2,x)=\{f(x) : f(0) \text{ even}\}$. Then $\mathbb{Z}[x]/(2,x)$ has two elements: functions where $f(0)$ is even, and functions where $f(0)$ is odd. Thus, $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}/2\mathbb{Z}$.

   PROOF.

   Consider the homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ such that $f(x) \mapsto f(0) \bmod 2$. This is clearly surjective. Then $\ker(\varphi) = \{f(x) : f(0) \text{ even}\} = (2,x)$. By Thm 2.1, $\mathbb{Z}[x]/\ker(\varphi) \cong \mathbb{Z}/2\mathbb{Z}$, so $\mathbb{Z}[x] \cong \mathbb{Z}/2\mathbb{Z}$. □
4. $R=\mathbb{F}[x,y], I=(x,y)=x\mathbb{F}[x,y]+y\mathbb{F}[x,y]=\{f(x,y) : f(0,0)=0\}$. Then $R/I \cong \mathbb{F}$, with cosets classifying exactly $f(0,0)$.

   PROOF.

   Consider $\varphi : f(x,y)+I \mapsto f(0,0)$, as before. □

5. $R = \mathbb{F}[x_1, ..., x_n]$, $I = (f_1, ..., f_t)$, where $f_i(x_1, ..., x_n)$ are polynomials of n variables. Finding R/I is difficult. We are touching on algebraic geometry here. Let

$$V(I) = \left\{ (x_1, ..., x_n) \text{ s.t. } \begin{cases} f_1(x_1, ..., x_n) = 0 \\ f_2(x_1, ..., x_n) = 0 \\ \vdots \\ f_t(x_1, ..., x_n) = 0 \end{cases} \right\} \in (\overline{\mathbb{F}})^n$$

The algebraic closure of $\mathbb{F}$.

PROP 2.9

Given a ring R, $p(x) \in R[x]$, there exists a ring $S \supset R$ containing a root of $p(x)$.

PROOF.

Let $S = R[x]/((p(x)))$. Then consider $R \to S$ by $a \mapsto a + (p(x))$. Let $\alpha = x + (p(x))$. Then $p(\alpha) = p(x) + (p(x)) = 0 + (p(x))$. □

For example, $R = \mathbb{R}$, $p(x) = x^2 + 1$. $R[x]/(x^2 + 1) = \mathbb{C}$.

2.4 Adjustment of Elements

Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$ be irreducible. Then $\exists$ a field $K \supset F$ such that K contains a root of $f(x)$.

PROOF.

We let $K = \mathbb{F}[x]/\langle f(x)\rangle$. We wish to show that $\langle f(x)\rangle$ is maximal. Assume otherwise. Then $\langle f(x)\rangle \subsetneq I$. But $\mathbb{F}[x]$ is principle, so $\exists g$ with $I = \langle g(x)\rangle$. Then $f(x) = g(x)q(x)$ for some $q(x) \in \mathbb{F}[x]$. But $f(x)$ is irreducible, so $g(x) = \alpha \vee \alpha f(x)$. In the former, we have that $I = \mathbb{F}[x]$. In the latter, we have that $I = \langle f(x)\rangle$. Thus, we conclude that $\langle f(x)\rangle$ is maximal.

Thus, $\mathbb{F}[x]/\langle f(x)\rangle$ is a field. We also need to show that $K \supset \mathbb{F}$, i.e. find an injection between the two. Let $\varphi : \mathbb{F} \hookrightarrow K : \lambda \to \lambda + \langle f(x)\rangle$.

Lastly, we need to show that $f(t)$ has a root in K. We have $f(t) \in \mathbb{F}[t] \subset K[t]$. Let $\alpha \in K := x + \langle f(x)\rangle$. Then $f(\alpha) = f(x + \langle f(x)\rangle) = f(x) + \langle f(x)\rangle = 0$ in K. □

Generally, for R/I, $f(x) \in \mathbb{R}[x]$, and $a + I \in R/I$, we have $f(a + I) = f(a) + I$. One may show this by induction.

E.G. 2.4

♠ *Examples* ♣

1. Consider $F = \mathbb{R}$, $x^2 + 1$. Let $\mathbb{C} = \mathbb{R}[x]/\left\langle x^2 + 1\right\rangle$. Concretely, this is $\{a + bx : a, b \in \mathbb{R}\}$ and $x^2 \cong -1 \mod x^2 + 1$.

2. Consider $F = \mathbb{Q}$, $x^2 - 2$. Then $K = \mathbb{Q}[x]/\left\langle x^2 - 2 \right\rangle := \mathbb{Q}[\sqrt{2}] = \left\langle a + b\sqrt{2} : a, b \in \mathbb{Q} \right\rangle$.

If F is a finite field, then $\#F = p^t$ with p a prime number. PROP 2.10

PROOF. If R is any ring, then there is a unique homomorphism $\varphi : \mathbb{Z} \to \mathbb{R}$ which sends $\mathbb{0}_{\mathbb{Z}} \to \mathbb{0}_{\mathbb{R}}$ and $\mathbb{1}_{\mathbb{Z}} \to \mathbb{1}_{\mathbb{R}}$. This same homomorphism applied to F, i.e. $\varphi : \mathbb{Z} \to F$, is not injective, since F is finite.

Let $\ker(\varphi) = I$. Then, by the isomorphism theorem, $\overline{\varphi} : \mathbb{Z}/I \to F$ which sends $a + I \to \varphi(a)$ is an injection. Thus, we may view $\mathbb{Z}/I$ as a subring of F. Hence, $\mathbb{Z}/I$ contains no zero divisors, so it is an integral domain. Hence, by Prop 2.7, I is a prime ideal. In $\mathbb{Z}$, this means $I = p\mathbb{Z}$ for some p.

Thus, F contains $\mathbb{Z}/p\mathbb{Z}$. Then F may be viewed as a vector space over $\mathbb{Z}/p\mathbb{Z}$, necessarily finite dimensional. Thus, let $t = \dim(F)$. Hence, $F \cong (\mathbb{Z}/p\mathbb{Z})^t$ as a vector space isomorphism, so $\#F = p^t$. □

Given a prime p and some t, is there a field of cardinality p^t? If so, how many are there? If $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ is irreducible of degree t, then we have a candidate for $\mathbb{Z}/p\mathbb{Z}[x]/\langle f(x) \rangle$ has cardinality p^t.