MAT347 Lecture Notes

Arky!! :3c

'25 Fall & '26 Winter Semester

Contents

§1 Day 1: Rubik's Cube (Sept. 3, 2025)

The first semester of this class will be taught by Dror Bar-Natan instead of Joe Repka. Since this was a last minute change, the Quercus, tutorials, textbook, homework policy, etc. are all unknown for now (until the rest of the week probably).

This will be today's handout. Let $G = \langle g_1, \dots, g_\alpha \rangle$, i.e., the group generated by $g_1, \dots, g_\alpha$, be a subgroup of S_n, with $n = O(100)$. To understand G, let us start by computing $|G|$. *insert long digression about Rubik's cubes that can be read elsewhere.*

Definition 1.1. A *group* is a set G along with a binary multiplication $m : G \times G \to G$ usually written as $(g_1, g_2) \mapsto g_1 \cdot g_2 = m(g_1, g_2)$ such that

(i) m is associative, i.e., for all $g_1, g_2, g_3 \in G$, we have that $(g_1 g_2) g_3 = g_1 (g_2 g_3)$,

(ii) m has an identity, i.e., there exists some $e \in G$ such that $g \cdot e = e \cdot g = g$ for all $g \in G$,

(iii) m has an inverse, i.e., for all $g \in G$, there exists some $h \in G$ such that $g \cdot h = e = h \cdot g$,

We present a few examples of groups for intuition.

(a) $(\mathbb{Z}, m = +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(F, +)$ are naturally all groups. We also have that $(2\mathbb{Z}, +)$ is a group, even though it is not a field, because it does not admit inverses.

(b) $(\mathbb{Q} \setminus \{0\}, \times)$ has identity given by 1 and naturally admits inverses because all reciprocals are contained within $\mathbb{Q} \setminus \{0\}$ itself. We commonly write the rationals without zero as $\mathbb{Q}^\times$.

(c) If $n \in \mathbb{Z}_{\geq 0}$, then let $S_n := \{\sigma : \underline{n} \to \underline{n} \mid \sigma \text{ is bijective}\}$, where we define $\underline{n} = \{1, \dots, n\}$.[1] Let the group operation on S_n be given by composition. Here, Dror goes into a big digression on how composition should be written, and he suggests the following,[2]

$$\sigma \cdot \mu = \mu \circ \sigma = \sigma /\!\!/ \mu.$$

Indeed, S_n is a group, where its identity element e is given by the identity function on $\underline{n}$. We have that $|S_n| = n!$.

As a substantive example, consider $S_2 = \{[1,2], [2,1]\}$, where $[1,2]$ represents the identity function and $[2,1]$ represents the function mapping 1 to 2 and 2 to 1. Then we obtain the following possible compositions,

$$\begin{aligned} [1,2][1,2] &= [1,2], \\ [1,2][2,1] &= [2,1], \\ [2,1][1,2] &= [2,1], \\ [2,1][2,1] &= [1,2]. \end{aligned}$$

As for S_3, we have that S_3 contains 6 functions, comprised of all the possible permutations possible on $\{1,2,3\}$. One such composition is given as follows,

$$[1,3,2][2,1,3] = [2,3,1], \qquad [2,1,3][1,3,2] = [3,1,2],$$

[1] angry yapping incoming i am so used to seeing $[n]$ when i saw that on the board i was like, watefak!!!
[2] also, plus one angry footnote for using $/\!\!/$ as a composition symbol

which confirms that S_3 is indeed not abelian (i.e., non-commutative).

In the opposite direction, S_1 consists of an identity function only; clearly, $|S_1| = 1! = 1$. S_0 is the set of all permutations on $\underline{0}$, which is clearly the empty set, meaning the "empty function" on the empty set is the only function in S_0; similarly, $|S_0| = 0! = 1$.

(d) There are 24 rotational symmetries of a cube.

(e) The orthogonal transformations $o(3) = \{A \in M_{3\times 3}(\mathbb{R}) \mid A \cdot A^\top = I\}$ form a group.

Theorem 1.2. The identity element of a group is unique. If G is a group and e, e' are both identity elements, then for all $g \in G$, we have that $eg = ge = g$ and $e'g = ge' = g$, and $e = e'$.

Proof. Observe that $e' = e' \cdot e = e$. □

Theorem 1.3. The inverse of an element in a group is unique. Let G be a group and $g \in G$; if h, h' satisfy $gh = hg = e = gh' = h'g$, then $h = h'$.

Proof. Observe that $h' = h' \cdot e = h'(gh) = (h'g)h = eh = h$. □

From here on, the inverse of g will be denoted g^{-1}, i.e., g^{-1} is the unique inverse of g.

Theorem 1.4. If $ac = bc$ in a group then $a = b$.

Proof. Given that $ac = bc$, we have $acc^{-1} = bcc^{-1}$, implying $a = b$. □

Theorem 1.5. $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. Observe that $(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. □

Definition 1.6. A subset $H \subset G$ of a group G is called a subgroup if H is closed under multiplication, $e \in H$, and admits inverses (i.e., H is a group itself with the multiplication operation from G). We write $H < G$.

As an example, $(2\mathbb{Z}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$. The Rubik's cube group is also a subgroup of S_{54}.

§2 Day 2: More Non-commutative Gaussian Elimination (Sep. 5, 2025)

The syllabus is not yet public, but you should check this link next Wednesday for more information. Our TAs are Jacob and Matt. The course code for this class is "MAT347", and it carries the iconic '7', meaning this class will be "hard as shit".

The permutation product is the usual composition $\sigma \cdot \tau = \sigma \circ \tau$.[3] Today's goal is to understand $G = \langle g_1, \dots, g_\alpha \rangle \in S_n$, where we wish to answer the questions: (i) what size is $|G|$? (ii) what does it mean to say $\sigma \in G$? (iii) if $\sigma \in G$, how do we write it in terms of the g_i's? (iv) what does a random $\sigma \in G$ look like?

Let us construct a lower-triangular table of size $n \times n$, where each box (i, j) describes an operation on how to move the ith sticker to the jth sticker. In particular, we have that if $i = j$, the operation is simply the identity. We start with an empty such table, and we will proceed to fill it in with permutations. For any $\sigma \in S_n$, we have that σ can be represented as a permutation of the form $[1, 2, \dots, i-1, j, *, \dots, *]$, i.e., σ fixes the first $i-1$ entries, and the ith entry contains j. We label such a permutation as $\sigma_{i,j} \in S_n$, and we call i the *pivot*.

We proceed to "feed $g_1, \dots, g_\alpha$" in order; to feed a non-identity σ, let the pivotal position be i and let j be given by $\sigma(i)$. If the box (i, j) is empty, let us place σ there; otherwise, if it already contains some $\sigma_{i,j}$, let us place $\sigma' := \sigma_{i,j}^{-1}\sigma$ in there instead. Notice that this makes it so that σ' is indeed the identity for the first i entries, instead of the first $i-1$ entries, meaning we have fixed an additional sticker. After this step, for each pair of occupied boxes (i, j) and (k, l), let us feed $\sigma_{i,j}\sigma_{k,l}$ and perform the steps above again, until the table no longer changes for any such pair of $(i, j), (k, l)$.

Claim 2.1. This process stops in $O(n^6)$ time; call the resulting table T.

We obtain n^6 from observing that there is approximately n operations per permutation, and hence n per inverse permutation; since computing $\sigma' = \sigma_{i,j}^{-1}\sigma$ potentially requires n inverses, we note that each feeding operation takes at worst n^2 operations. For the (i, j), (k, l) pairs, the table is of $O(n^2)$ size, meaning there are a total of $O(n^4)$ possible foods. Combining these figures we have $O(n^6)$, which is much less than $O(n!)$.

Claim 2.2. Every $\sigma_{i,j} \in T$ is indeed in G.

[3] so we're going to be changing the notation conventions every lecture from now on.

§3 Day 3: NCGE, Pt. 3 (Sep. 10, 2025)

Before we return to the discussion on the Rubik's cube, we have another property of inverses to discuss;

Theorem 3.1. Let $a \in G$. Then $(a^{-1})^{-1} = a$.

Proof. $(a^{-1})^{-1} = (a^{-1})^{-1} \cdot (a^{-1} \cdot a) = a$. □

The point of the twist is that we want to fill every box of our table that can be filled by the group; assuming that the twist hits everything, we would be able to work nicely with the group by just unfurling each permutation progressively. As an example, given $(\dot{z_1}, \dot{z_2}, \dots)$, we wish to find the index k such that $\dot{z_k} = 1$. We may then apply $\sigma_{1,k}^{-1}$ to $(\dot{z_1}, \dot{z_2}, \dots)$ to obtain $(1, \dots)$, on which we may then recursively proceed. Inventing this gives us $(\dot{z_1}, \dot{z_2}, \dots)$ in terms of the generators.

Lemma 3.2. Every box (i, j) of the table T is in G.

Proof. We fed generators or elements of the table into the table, but each feed only performs group operations, which means inductively, we are done here. □

Lemma 3.3. Any $\sigma \in S_n$ fed into the table is a monotone product of elements of T. We have that $\sigma = \sigma_{1,j_1} \cdot \sigma_{2,\cdot j_2} \cdot \dots \cdot \sigma_{n,j_n}$, where our σ_{i,j_i}s are drawn from the table, and the box in the index (i, j_i) is nonempty.

Proof. There are three possibilities;

(i) If $\sigma = e$, then it's just $\sigma_{1,1}\sigma_{2,2}\sigma_{3,3} \dots$.

(ii) If σ is in the table, suppose its $\sigma_{i,j}$; then $\sigma = \sigma_{1,1} \dots \sigma_{i,j} \dots \sigma_{n,n}$.

(iii) If σ is neither of these, then suppose σ has pivot i, $\sigma(i) = j$, and $\sigma_{i,j}$ is full; then we just feed $\sigma' = \sigma_{i,j}^{-1}\sigma$. In other words, $\sigma = \sigma_{i,j}\sigma'$, and since you can only repeat this finitely many times, this is eventually $\sigma = \sigma_{1,1} \dots \sigma_{i,j} \dots \sigma_{n,j_n}$. □

The before holds for $\sigma \in S_n$ fed into the table, but we don't necessarily have that the table T generates the group just yet[4]. If we feed in a generator g_i, we have that g_i is in $\langle T \rangle$, meaning that by feeding our generators, we indeed have that $\langle T \rangle = G$. Therefore, feeding products of elements is to get everything in G as a monotone product.

Lemma 3.4. Two monotone products are equal if and only if they are the same.

Proof. If they are the same, they are equal, so it suffices to check that if two monotone products are equal, they are the same. Suppose that $\sigma_{1,j_1} \dots \sigma_{n,j_n} = \sigma_{1,j_1'} \dots \sigma_{n,j_n'}$. Then

$$\sigma_{i,j_1} \dots \sigma_{n,j_n} = (\sigma_{i,j_1}^{-1}\sigma_{1,j_1'})\sigma_{2,j_2'} \dots \sigma_{n,j_n'},$$

meaning that

$$\sigma = \sigma_{n,j_n}^{-1}(\sigma_{n-1,j_{n-1}}^{-1}(\dots(\sigma_{1,j_1}^{-1}\sigma_{1,j_1})\dots)\sigma_{n-1,j_{n-1}'})\sigma_{n,j_n'} = e,$$

but then we have $\sigma(1) = 1$, so, since all but the middle are the identity on 1, we have that $\sigma(1) = \sigma_{1,j_1}^{-1}\sigma_{i,j_i}(1)$, meaning $j_1 = j_1'$, and so

$$\sigma = \sigma_{n,j_n}^{-1}(\dots(\sigma_{2,j_2}^{-1}\sigma_{2,j_2})\dots)\sigma_{n,j_n'} = e,$$

and so by an inductive process, we are done. □

[4] if we feed $\sigma \in G$, then we are essentially going to apply #2 until we reach the identity permutation; if we feed in $\sigma \notin G$, then we will arrive at an empty square in the table T

Lemma 3.5. $M = \{\sigma_{1,j_1}, \dots \sigma_{n,j_n} \mid j_i \in [n]; \sigma_{i,j_i} \in T\}$ is a group.

Lemma 3.6. $M_k = \{\sigma_{k,j_k} \dots \sigma_{n,j_n} \mid j_i \in [n]; \sigma_{i,j_i} \in T\}$ is a group.

Proof. M_n is a group, because M_n is just the identity. The proof is to be continued. □

Personal note; claims 3 and 4 from Dror's handout is used to establish a bijection between valid Rubik's cubes moves (i.e., elements of G), and elements in M (monotone products of red boxes in T).

If we have $M_1 = G$, then we can solve the questions set out at the beginning of our course, namely,

(i) Compute $|G|$; we have that $|G| = |M_1|$.

(ii) Given $\sigma \in S_n$, decide if $\sigma \in G$; suppose we feed σ into T. If it would change the table, then σ is not in G.

(iii) Write a $\sigma \in G$ in terms of the generators g_i; by keeping track of the elements we feed in, we can find each of the boxes of T in terms of the generators, so we can write each element as a monotone product in terms of the generators.

(iv) Product random elements $\sigma \in G$; for each $i \in [n]$, pick some j_i randomly such that $\sigma_{i,j_i} \in T$. Then we may take the product of all such σ_{i,j_i} to produce a random element of G.

In a random tangent, we now proceed to define cycle notation. Suppose

$$G = \langle (1\,2\,3), (1\,2)(3\,4) \rangle ;$$

we now proceed to fill in a 4×4 lower-triangular T, which Dror spent a lot of time trying to do. It also taught me that I am never going to even bother solving a Rubik's cube with this algorithm; this goes without saying but there is no chance in hell I'm typing all that shit down.

§4 Day 4: NCGE, Pt. 4 (Sep. 12, 2025)

We do a review of the non-commutative Gaussian elimination process.

(i) We have that $T \subset G$. Recall the definition that

$$M_k = \{\sigma_{k,j_k} \dots \sigma_{n,j_n} \mid \sigma_{i,j_i} \in T\}.$$

(ii) Anything fed into the table is in M_1.

(iii) If two monotone products are equal as elements of S_n, then they are the same.

Theorem 4.1. For all k, $M_k \cdot M_k \subset M_k$; we note that in general, $A \cdot B = \{ab \mid a \in A, b \in B\}$.

Corollary 4.2. $M_1 \cdot M_1 \subset M_1$, meaning that $M_1 = G$.

Proof. To see this, $M_1 \subset G$ per its construction, as all the generators of G, $g_1, \dots, g_\alpha$, have been fed into M_1. Observe that by our previous claims, we have that products of elements in M_1 are in M_1. To check that M_1 is in fact a group (which requires M_1 to be closed under inverses and the group operation), we may first note that it is closed under multiplication, and observe the following;

$$e = g^0, g = g^1, g^2, g^3, \dots$$

is an infinite sequence, where each of the elements in said sequence are in G. However, G is a finite group, meaning that there must be some sort of periodicity in the sequence. Without loss of generality, for all $n < m$ such that $g^n = g^m$, let us write $m = n + k$, where $k > 0$. Since $g^n = g^n g^k$, we must have that $e = g^k$, meaning that g^{k-1} is indeed the inverse of g. Thus, we establish that if G is finite and M_1 is a subset closed under multiplication, then M_1 is a subgroup of G. Thus, we conclude that $G = M_1$ by double inclusion. □

Definition 4.3. We define the *order* of $g \in G$ to be $\mathrm{ord}_G(g) = |g|$, i.e., the smallest possible k such that $g^k = e$.

We now prove the theorem with backwards induction (from the maximum value of k to the minimum value, i.e., $k = n$ to $k = 1$).

Proof. We start with the base case; $M_n \cdot M_n \subset M_n$ is trivially true, because M_n contains only the identity, so $\{\mathrm{id}\}\{\mathrm{id}\} \subset \{\mathrm{id}\}$ is obviously true.

Since Dror doesn't want to work with some random k, we're going to assume $M_5 \cdot M_5 \subset M_5$, and show that $M_4 \cdot M_4 \subset M_4$ as a consequence.[5] Again, Dror doesn't like indices, so he's going to start by showing that $\sigma_{8,j} \cdot M_4 \subset M_4$. Observe that the set of all $\sigma_{8,j} M_4 \subset \bigcup_{j_4 \geq 4} \sigma_{8,j} (\sigma_{4,j_4} \cdot M_5)$; by associativity, we have that

$$\bigcup_{j_4 \geq 4} \sigma_{8,j} (\sigma_{4,j_4} \cdot M_5) = \bigcup_{j_4 \geq 4} (\sigma_{8,j} \sigma_{4,j_4}) M_5.$$

We have that $\sigma_{8,j}\sigma_{4,j_4}$ is a monotone product in M_4, meaning that the above is a subset of $M_4 \cdot M_5$, which is equal to $\bigcup_j \sigma_{4,j}(M_5 \cdot M_5)$, which, by our inductive hypothesis, we have that

$$\bigcup_j \sigma_{4,j}(M_5 \cdot M_5) \subset \bigcup_j \sigma_{4,j} M_5 \subset M_4,$$

[5] damn!!!! i hate indices!!!! rah!!!! grrr snarll growllll.... (bongos) BOMBS OVER BAGHDADDDdddd

since all $\sigma_{4,j}M_5$ is a monotone product in M_4. Moreover, observe that using our process above, we obtain

$$\sigma_{4,j_4} \dots \sigma_{n,j_n} M_4 \subset \sigma_{4,j_4} \dots \sigma_{n-1,j_{n-1}} M_4,$$

and so on, since we may note that σ_{i,j_i} for $i \geq 4$ still fixes the pivot at 4. In the end, we have that any $\sigma \in M_4$ must satisfy $\sigma M_4 \subset M_4$, and so we are done with the inductive step. □

Recall that in math so far, we've seen linear functions $L : V \to W$ and continuous functions $F : X \to Y$. We now discuss maps between groups.

Definition 4.4. Let G, H be groups. $\varphi : G \to H$ is called a *group homomorphism* (morphism) if its a set map and $\varphi(xy) = \varphi(x)\varphi(y)$, $\varphi(e_G) = e_H$, and $\varphi(x^{-1}) = \varphi(x)^{-1}$.

§5 Day 5: Group Homomorphisms, Normal Subgroup (Sep. 17, 2025)

Recall the definition of a group homomorphism,

Definition 5.1. $\varphi : G \to H$ is said to be a group homomorphism (where G, H are groups) if it is a structure-perserving group transformation, i.e.,

(i) $\varphi(xy) = \varphi(x)\varphi(y)$,

(ii) $\varphi(e_G) = e_H$,

(iii) $\varphi(x^{-1}) = \varphi(x)^{-1}$

for all $x, y \in G$.

In particular, the three properties above are equivalent to $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1}$; they are also equivalent to the implication that (i) implies (ii), (iii). Below are some examples of group homomorphisms,

(a) Let $\mathbb{Z}, \mathbb{R}$ both be equipped with addition; then the inclusion map $\mathbb{Z} \to \mathbb{R}$ is a group homomorphism.

(b) The function $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ is a group homomorphism ($e^{x+y} = e^x e^y$).

(c) $\mathbb{R} \ni t \mapsto e^{2\pi i t} \in \{z \in \mathbb{C} \mid |z| = 1\} = S^1 \subset \mathbb{C}$ is a group homomorphism.

(d) $\varphi : S_4 \to S_3$ given by mapping the faces of a tetrahedron to the three pairs arising from identifying its opposite edges is also a homomorphism.

As an aside, groups, together with their homomorphisms, form a category. In category theory terms, objects (groups) and maps (group homomorphisms) are seen as points and morphisms.

(i) The identity map $I : G \to G$ is a homomorphism.

(ii) If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms, then $\psi \circ \phi$ is a homomorphism.

A morphism is called an *isomorphism* if it has an inverse that is also a morphism, i.e., $\varphi : G \to H$ is an isomorphism if and only if it is bijective with $\varphi^{-1} : H \to G$ being a group homomorphism.

Definition 5.2. $\operatorname{Aut} G = \{\varphi : G \to G \mid G \text{ is an isomorphism}\}$; i.e., $\operatorname{Aut} G$ is the set of all group isomorphisms.

As an example, $\operatorname{Aut} \mathbb{Z}$ consists of the identity morphism and the "multiplication by -1" morphism, both of which we may readily check to satisfy isomorphism properties.

Claim 5.3. $\operatorname{Aut} G$ is a group under composition.

Given any group G, there is a map $C : G \to \operatorname{Aut} G$ called "conjugation", where $G \ni h \mapsto C_h \in \operatorname{Aut} G$; we have that $C_h(g) := h^{-1}gh = g^h$, i.e., "conjugation of g by h", where $C_h : G \to G$.

(i) C_h is a morphism, since $C_h(g_1 \cdot g_2) = C_h(g_1) \cdot C_h(g_2)$, since $(g_1 \cdot g_2)^h = g_1^h \cdot g_2^h$, i.e.,

$$g_1^h g_2^h = h^{-1}g_1 h h^{-1} g_2 h = h^{-1} g_2 g_2 h = (g_1 g_2)^h.$$

(ii) C_h is an invertible map; in fact, $C_h \circ C_{h^{-1}} = I$. We see this by considering that $(g^{h_1})^{h_2} = g^{h_1 \circ h_2}$. In this way, $g \mapsto (g^{h^{-1}})^h = g^{h^{-1}h} = g^e = g$, and the same holds when we consider $g \mapsto (g^h)^{h^{-1}}$.

Claim 5.4. C is an anti-homomorphism, i.e. $\varphi(ab) = \varphi(b)\varphi(a)$. Specifically, $C_{h_1 \circ h_2}(g) = C_{h_2} \circ C_{h_1}(g)$, which we see from expanding both sides to obtain $g^{h_1 \cdot h_2} = (g^{h_1})^{h_2}$.

Claim 5.5. Let $\varphi : G \to H$ is a morphism. Then $\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}$ is a subgroup of G. We write $\ker \varphi < G$. Also, $\operatorname{im} \varphi = \{\varphi(g) \mid g \in G\} < H$, meaning that $\operatorname{im} \varphi$ is a subgroup too.

As an example, let $t \mapsto e^{2\pi i t}$ from $\mathbb{R} \to S^1$; we have that

$$\ker t = \{t \mid e^{2\pi i t} = 1\} = \{t \mid \cos 2\pi t + i \sin 2\pi t = 1\} = \mathbb{Z}.$$

We also have that if $\varphi : S_4 \to S_3$, then $\ker \varphi = \{I, (12)(34), (14)(23), (13)(24)\}$, and $\operatorname{im} \varphi = S_3$. In general, if $H < G$, then H is always in the image of φ for some φ; we may immediately see this to be true by considering the inclusion $H \hookrightarrow G$.

Claim 5.6. If $\varphi : G \to S^1$ and $g \in \ker \varphi$, then for any $h \in G$, $g^h \in \ker \varphi$.

Proof. $\varphi(g^h) = \varphi(h^{-1}gh) = \varphi(h^{-1})\varphi(g)\varphi(h) = \varphi(h^{-1})\varphi(h) = e$, meaning that $g^h \in \ker \varphi$. □

Yet, if we consider the example where $S_3 < S_4$, is there $\varphi : S_3 \to S_n$ such that $\ker \varphi = S_3$? We observe that $(23) \in S_3$, and $(23)^{3\,4} = (34)(23)(34) = [1432] \notin S_3$, meaning that S_3 is not a kernel in S_n.

Definition 5.7. $N < G$ is called *normal* in G and denoted $N \lhd G$ if $n \in N$, $h \in G$, then $n^h \in N$ if and only if $h^{-1}Nh \subset N$.[6]

Claim 5.8. $\varphi : G \to H$ has $\ker \varphi \lhd G$.

Suppose $N \lhd G$. Is there a morphism $\varphi : G \to H$ such that $N = \ker \varphi$?

[6] we're going to use lhd for normal subgroup and see if it works, like "left hand delta" ig

§6 Day 6: Normal Subgroup as Kernel of Homomorphism (Sep. 19, 2025)

Term test 1 has been moved a week earlier to Nov. 4; homework 1 is due at 11:59pm today, and homework 2 is online now.

We now recap last class' definitions,

Definition 6.1. We say that $N \lhd G$ if $N < G$ and for all $h \in G$, we have that $N^h = h^{-1}Nh = N$. We say that N is *normal.*

Claim 6.2. If $\varphi : G \to H$, then $\ker \varphi \lhd G$.

Given $N \lhd G$, there exists a unique $\varphi : G \twoheadrightarrow H$ (we denote surjections with double headed arrows, $\twoheadrightarrow$) with $\ker \varphi = N$. As an aside, surjections are the same as equivalence relations. This is a general set theoretic fact, and we should be aware of it.

Let us discuss in terms of sets, for now. We say that a relation $\sim: X \times X \to \{T, F\}$ (i.e., true or false) on a set X is called an *equivalence relation*, where $a \sim b$ if $\sim(a, b) = T$, if it satisfies the following axioms,

(i) (*Reflexivity*) For all $x \in X$, we have that $x \sim x$.

(ii) (*Symmetry*) For all $x, y \in X$, we have that $x \sim y$ if and only if $y \sim x$.

(iii) (*Transitivity*) For all $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

As an example of an equivalence relation, let $f : X \to Y$ be a function, and define $a \sim b$ for $a, b \in X$ if $f(a) = f(b)$.

Definition 6.3. Let $(X, \sim)$ be a set equipped with an equivalence relation $\sim$; given some $x \in X$, we say $[x]_\sim = \{y \in X \mid x \sim y\}$. The subscript $\sim$ denoting which equivalence class it belongs to is dropped if it is evident from context.

Claim 6.4. Equivalence classes are either equal or disjoint, i.e., let $[x], [y]$ be equivalence classes; we have that $[x] \cap [y]$ is either $\varnothing$ or $[x] = [y]$. The former occurs if $x \not\sim y$, and the latter occurs if $x \sim y$.

Definition 6.5. We say that $X/\sim = \{[x] \mid x \in X\}$ is the set of equivalence classes on X.

Definition 6.6. $\phi : X \to X/\sim$ is the quotient map $\phi : X \ni x \mapsto [x]$. We have that ϕ is surjective. Specifically, $\phi : X \twoheadrightarrow Y \implies a \sim b$ if $\phi(a) = \phi(b)$, and $\sim$ induces the $\phi : X \to X/\sim$ map.

We now look to construct the surjection $\varphi : G \twoheadrightarrow H$ with $\ker \varphi = N \lhd G$. Given $N \lhd G$, we define $g_1 \sim g_2$ if and only if $g_1^{-1}g_2 \in N$. This comes from the train of thought where we want $\varphi(g_1) = \varphi(g_2) \implies \varphi(g_1)^{-1}\varphi(g_2) = \varphi(g_1^{-1}g_2) = e$, i.e., we're constructing φ such that N is the kernel of φ. Clearly, we can see that $\sim$ is an equivalence relation when defined as earlier; reflexivity and symmetry are immediate, and for transitivity, we see that if $a, b, c \in G$ are such that $a^{-1}b, b^{-1}c \in N$, then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in N$, since N is a subgroup and is closed.

In this manner, let us write $G/\sim = \{[g] \mid g \in G\}$. We write this group as $G/N = \{gN \mid g \in G\}$, and $[g] = g \cdot N = \{g \cdot n \mid n \in N\}$. Indeed, we have that $\phi : G \to G/N$ by $\varphi(g) = g \cdot N$. It remains to check that ϕ is a group homomorphism and $\ker \phi = N$. Let us define a group structure on G/N by including the operation $[g_1] \cdot [g_2] = [g_1 g_2]$. To check

that $\cdot$ is well-defined, observe that for any $g_1 \sim g_1'$ and $g_2 \sim g_2'$, we have that $g_1 g_2 \sim g_1' g_2'$, since by definition, there exists $n_1, n_2 \in N$ where $g_1' = g_1 \cdot n_1$, and $g_2' = g_2 \cdot n_2$, so

$$g_1' g_2' = g_1 n_1 g_2 n_2 = g_1 g_2 g_2^{-1} n_1 g_2 n_2 = g_1 g_2 n_1^{g_2} n_2 \in g_1 g_2 N,$$

where we use the fact that N is normal to see that $n_1^{g_2} \in N$. We note that this is the only place that we've used the fact that N is normal.

Theorem 6.7. Let G/N be a group, and let $\phi : G \to G/N$ be a morphism (recall that we let $g \mapsto gN$). Then $\ker \phi = N$.[7]

Proof. Since we already established that ϕ is a well-defined morphism, we have that $\ker \phi = \{g \in G \mid \phi(g) = gN = N\} = N$, since $gN = N$ if and only if $g \in N$ (which is true in general for any subgroup, not just normal N). □

[7] we call this the natural homomorphism iirc? and its surj

§7 Day 7: First and Second Isomorphism Theorems (Sep. 24, 2025)

Recall from last lecture that we define $G/N := \{gN \mid g \in G\}$, where if $N \lhd G$, then $(g_1N)(g_2N) = g_1g_2N$, making it a group.

Example 7.1. Let $N = n\mathbb{Z}$ and $G = \mathbb{Z}$ (where $n \in \mathbb{Z}$, and we regard $n\mathbb{Z}$ as the group of all integers divisible by n). We write the "lazy notation" $\mathbb{Z}/n$ for $\mathbb{Z}/n\mathbb{Z}$,[8] which is a group as $n\mathbb{Z}$ is normal as $\mathbb{Z}$ is abelian. We have that $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$, i.e., the equivalence classes of integers modulo n, where $[a] + [b] = [a + b]$.

As an aside, $H < G$ implies that $|G| = |H| \cdot |G/H|$, which should be regarded as the statement that "every coset has size H", and that there are $|G/H|$ cosets (given by the equivalence classes). In turn, we obtain

Theorem 7.2 (Lagrange's Theorem)**.** If $H < G$, then $|H|$ divides into $|G|$.

As a quick check, take $|S_4| = 24$, and $|S_3| = 6$. Clearly, $6 \mid 24$.

We now proceed to introduce the isomorphism theorems. Recall the rank-nullity theorem; let $L : V \to W$ be a linear map between vector spaces. Then

$$\dim L = \dim \ker L + \dim \operatorname{im} L.$$

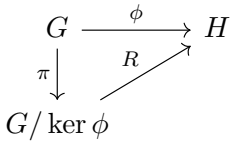
Specifically, we have that $V/\ker L \cong \operatorname{im} L$. We may generalize this notion to groups as well.

Theorem 7.3 (First Isomorphism Theorem)**.** Given a morphism $\phi : G \to H$, then $G/\ker\phi \cong \operatorname{im}\phi$.

Proof. The proof of this theorem is you "read the definition and do the only reasonable thing". Let $R : [g]_{\ker\phi} \mapsto \phi(g)$; we wish to show that R is well-defined and multiplicative. Let $L : \phi(g) \mapsto [g]$; clearly, we have that $L \circ R$ and $R \circ L$ are both the identity, so it remains to check that both maps are well-defined (we skip the proof of multiplicativity).

If g, g' are such that $[g] = [g']$, then $g^{-1}g' \in \ker\phi$, meaning that $\phi(g^{-1})\phi(g') = e$, i.e., $\phi(g) = \phi(g')$. In the other direction, let $h \in \operatorname{im}\phi$ be such that $\phi(g) = h = \phi(g')$; we check that $[g] = [g']$. We have that $\phi(g^{-1}g') = \phi(g)^{-1}\phi(g') = h^{-1}h = e$, and so g, g' belong to the same equivalence class.

A personal note; this proof is better seen by considering



and that we are checking R is a well-defined map. Note that even though π wasn't defined in the proof, just see it as part of the factorization sending to cosets. □

We now give a preview of the second isomorphism theorem; let $H, K < G$ be such that $H \cap K$ is a subgroup of both H and K. Then $H/(H \cap K) \cong HK/K$.

[8] i am one million trillion percent he will backtrack this notation after backlash

We start with some intuition. In terms of vector spaces, if we let $V, U \subset W$, then $V/(V \cap U) \cong (V+U)/U$, which we may quickly verify by checking dimensions as follows;

$$\dim \frac{V}{V \cap U} = \dim V - \dim V \cap U = \dim(V+U) - \dim U = \dim \frac{V+U}{U},$$

since

$$\dim U + \dim V = \dim(U+V) + \dim(U \cap V).$$

We now discuss the group analogue of this fact. The intersection of two groups is a group, so we see that $H \cap K$ is a group; moreover,

Claim 7.4. Given $H, K < G$, we have that $HK = \{hk \mid h \in H, k \in K\} < G$ if and only if $HK = KH$.

Proof. We check the reverse implication first, i.e., we want to show that HK is a group. For any $h_1k_1, h_2k_2 \in HK$, we have that $(h_1k_1) \cdot (h_2k_2) = h_1(k_1h_2)k_2$; we may let $k_1h_1 = h'k'$ since $KH = HK$, so we obtain $h_1h'k'k_2 = (h_1h')(k'k_2) \in HK$. Clearly, the identity is in HK since $e_{HK} = e_He_K \in HK$, and HK admits inverses since $(hk)^{-1} = k^{-1}h^{-1} = h'k' \in HK$ for some h', k'.

For the forwards direction, assume that $HK < G$; to see $KH \subset HK$, observe that $(kh)^{-1} = h^{-1}k^{-1} \in HK$; so $((kh)^{-1})^{-1} = kh \in HK$. To see $HK \subset KH$, observe that for any $hk \in HK$, we have that $(hk)^{-1} = k^{-1}h^{-1} \in KH$, and so by the same process, $((hk)^{-1})^{-1} = hk \in KH$. □

Definition 7.5. Let $X \subset G$ be a subset of a group. Then

(i) $N_G(X) = \{g \in G \mid X^g = X\}$ is called the *normalizer* of X in G. In the case $X = G$, we have that $N_G(G) = G$.

(ii) $C_G(X) = \{g \in G \mid x^g = x \text{ for all } x \in X\}$ is called the *centralizer* of X in G.

(iii) $z(G) = C_G(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$ is called the *center* of G.

In particular, we may check that all three are groups, and we have $z(G) < C_G(X) < N_G(X) < G$.

Example 7.6. Let $G_0 = \{\pm 1, \pm i\} \subset \mathbb{C}$ where $G_0 \cong \mathbb{Z}/4\mathbb{Z}$, induced by mapping $G_0 \ni i \mapsto [1] \in \mathbb{Z}/4\mathbb{Z}$ and $1 \mapsto [0]$. In this manner, we may define $G = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}$ (where we regard $\mathbb{H}$ as the quaternions). Clearly, $|G| = 8$, and i, j, k are defined to satisfy $i^2 = j^2 = k^2 = -1$. By definition of the quaternions, $ij = k$, $jk = i$, $ki = j$, with $ji = -k$, $kj = -i$, $ik = -j$, so we see $z(G) = \{1, -1\}$ and the centralizer of G_0 in G is given by $C_G(G_0) = G_0$. To compute the normalizer of G_0 in G, observe that

$$j^{-1}G_0j = G_0, \quad (-j)G_0j = G_0, \quad (-j)ij = -i \in G_0,$$

showing that $N_G(G_0) = \{\pm 1, \pm i, \pm j\}$.

Theorem 7.7 (Second Isomorphism Theorem)**.** Let $H, K < G$ and $H < N_G(K)$. Then $HK = KH$, $H \cap K \lhd H$, $K \lhd KH$ and

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$

Proof. $H < N_G(K)$, so for all $h \in H$, we have $hK = kH$, i.e., $HK = KH$ and HK is a group as seen previously. We continue the proof next lecture. □

§8 Day 8: Third Isomorphism Theorem (Sep. 26, 2025)

Dror strongly suggests starting problem set 3 early. Recall the second isomorphism theorem from last class; if $H, K < G$ and $H < N_G(K)$, then $HK = KH$, $K \lhd HK$, $H \cap K \lhd H$, and $HK/K \cong H/(H \cap K)$.

Proof. We prove each property one by one.

(i) $HK = KH$ because $hK = Kh$, as $K = h^{-1}Kh$ as $h \in N_G(k)$.

(ii) $K \lhd HK$ by construction, i.e., $K^{hk} = (K^h)^k = K^k = K$.

(iii) $H \cap K \lhd H$; we want to show that if $g \in H \cap K$ and $h \in H$, then $g^h \in H \cap K$. This is true from observing $g^h \in H$ as both $g, h \in H$, and $g^h \in K$ as $g \in K$ and $h \in N_G(K)$.

(iv) To see the isomorphism, let $R : HK/K \to H/(H \cap K)$, and $L : H/(H \cap K) \to HK/K$. R maps $hkK \mapsto h(H \cap K)$, and L maps $[hk]_k \mapsto [h]_{H\cap K}$; clearly, L is well-defined from observing $[h]_{H\cap K} = [h]_K$, since if

$$[h_1]_{H\cap K} = [h_2]_{H\cap K},$$

then $h_1^{-1}h_2 \in H \cap K \subset K$ and so $[h_1]_K = [h_2]_K$. We also see that R is well-defined by taking $[h_1k_1]_K = [h_2k_2]_K$, for which we want to show that $[h_1]_{H\cap K} = [h_2]_{K\cap K}$. We may observe that

$$(h_1k_1)^{-1}(h_2k_2) = k_1^{-1}h_1^{-1}h_2k_2 = k' \in K,$$

meaning $h_1^{-1}h_2 \in H \cap K$, since $h_1^{-1}h_2 \in H$ trivially and

$$k_1(k_1^{-1}h_1^{-1}h_2k_2)k_2^{-1} = k_1k'k_2' \in K. \qquad \square$$

Theorem 8.1 (Third Isomorphism Theorem)**.** If $K, H \lhd G$ with $K < H$ (K is a normal subgroup of H per $K \lhd G$), then $\frac{G/K}{H/K} = G/H$.

Proof. Let $R : [[g]_K]_{H/K} \mapsto [g]_H$ and $L : [g]_H \mapsto [[g]_K]_{H/K}$. We check that R is well-defined. For R, observe that if g_1, g_2 are such that

$$[[g_1]_K]_{H/K} = [[g_2]_K]_{H/K},$$

then $[g_1]_K^{-1}[g_2]_K = [h]_K$ for some h, i.e., $g^{-1}g_2 = hk$ for some $k \in K$. We want to show that $[g_1]_H = [g_2]_H$, namely, $g_1, g_2 \in H$; but this is already true because $g_1^{-1}g_2 = hk \in HK \subset H$. $\square$

§9 Day 9: Lattice Theorem and Simple Groups (Oct. 1, 2025)

Recall the first three isomorphism theorems;

(i) If $\phi : G \to H$ is a morphism, then $\ker\phi \cong \operatorname{im}\phi$

(ii) If $H, K < G$ with $K^H = K$, then $H/(H \cap K) \cong HK/K$.

(iii) If $B, C \lhd A$ and $C \lhd B$, then $(A/C)/(B/C) \cong A/B$.

We now present the fourth isomorphism theorem.

Theorem 9.1 (Lattice Theorem)**.** If $N \lhd G$, then $\pi : G \to G/N$ induces a "faithful" bijection between $\{H \mid N < H < G\}$ and the subgroups of G/N. Specifically, for all A, B such that $N < A < B < G$, we have that $\{1\} < \pi(A) < \pi(B) < G/N$, and if $N < A \lhd B < G$, we have that $\{1\} < \pi(A) \lhd \pi(B) < G/N$, and vice versa. Moreover, $\pi(A \cap B) = \pi(A) \cap \pi(B)$.

Proof. Left as an exercise. □

Definition 9.2. A group is said to be *simple* if it admits no normal subgroups aside from $\{e\}$ and itself.

Observe that $\mathbb{Z}/n\mathbb{Z}$ is simple if and only if n is prime. We claim that if $A < \mathbb{Z}$, then A is given by $m\mathbb{Z}$ for some unique m.

Proof. Let $A < \mathbb{Z}$, and observe that if $A = \{0\}$, then $m = 0$; otherwise, let $k = \min\{k \in A \mid k > 0\}$. This means that $m\mathbb{Z} \subset A$. Now, suppose $k \in A$, and write $k = m \cdot q + r$ with $0 \le r < m$. We have that $r = k - mq \in A$, and by minimality of m, we must have $r = 0$, and so $k = mq$, i.e., $k \in m\mathbb{Z}$. □

In this manner, we see that $m\mathbb{Z} > n\mathbb{Z}$ if and only if $\frac{n}{m}$ is an integer. As an example, observe that $2\mathbb{Z} > 4\mathbb{Z}$, and $\frac{4}{2} = 2 \in \mathbb{Z}$. This means that the set of nontrivial subgroups of $\mathbb{Z}/n\mathbb{Z}$ if equivalent to the set of integers $\{m\mathbb{Z} \mid m \mid n\}$, and the smallest set containing nothing other than $n\mathbb{Z}$ and $\mathbb{Z}$ occurs if and only if n itself is prime.

Example 9.3. Is S_n simple?

No, but it is *nearly*. Let us define the sign function $\operatorname{sign} : S_n \to \{\pm 1\}$, for which we may regard $\{\pm 1\}$ as a group with two elements. Let $S_n \ni \sigma \mapsto \operatorname{sign}(\sigma) := (-1)^\sigma$, which we will call the *parity* of σ, where if it is even, $\operatorname{sign}(\sigma) = 1$, and odd yields -1.[9] It remains to check if sign is a well-defined function.

Let us associate to each $\sigma \in S_n$ a matrix $M_\sigma \in M_{n\times n}$, where $M_\sigma = (\delta_{i,\sigma(i)})_{ij}$, i.e., one such matrix might look like

$$M_{[1,3,2]} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

In this manner, we have that $\operatorname{sign}\sigma = \det M_\sigma$.

Definition 9.4. A *transposition* is a permutation given by (ij); i.e., it admits a single 2-cycle while fixing all other elements.

[9] dror has a pretty confusing explanation of parity, but see this link for better intuition about it. combinatorics type stuff.

Claim 9.5. Every permutation $\sigma \in S_n$ can be written as a product of transpositions (obviously, such a product is not necessarily unique).

An informal proof of this is to simply observe the bubble sort algorithm. We have that $\operatorname{sign}(\sigma)$ is equal to (-1) to the power of however many transpositions are in the transposition decomposition of σ; the question is, is this well-defined? We may formally define sign as

$$\operatorname{sign}(\sigma) = \prod_{i=1}^{n} (-1)^{(\sigma_i)-1}, \qquad (\sigma_i = \sigma(i))$$

for which we may write down equivalent formulations

$$\operatorname{sign}(\sigma) = \prod_{i<j} \operatorname{sign}(\sigma_j - \sigma_i) = \prod_{i \neq j} \frac{\operatorname{sign}(\sigma_j - \sigma_i)}{\operatorname{sign}(j-i)} = \prod_{\substack{\{i,j\} \subset [n] \\ i \neq j}} \operatorname{sign}\left(\frac{\sigma_j - \sigma_i}{j-i}\right),$$

where each successive expression is "gooder" than the rest.[10]

Theorem 9.6. sign is a morphism.

Proof. Directly write as follows for any $\sigma, \tau \in S_n$,

$$\begin{aligned}
(-1)^{\sigma\tau} &= \prod_{i \neq j} \operatorname{sign}\left(\frac{\sigma\tau_j - \sigma\tau_i}{\tau_j - \tau_i}\right) \operatorname{sign}\left(\frac{\tau_j - \tau_i}{j-i}\right) \\
&= \prod_{i \neq j} \operatorname{sign}\left(\frac{\sigma\tau_j - \sigma\tau_i}{\tau_j - \tau_i}\right) \prod_{i \neq j} \operatorname{sign}\left(\frac{\tau_j - \tau_i}{j-i}\right) \\
&= (-1)^{\sigma} \cdot (-1)^{\tau},
\end{aligned}$$

since τ is a bijection. □

Definition 9.7. We define the *alternating group* $A_n \subset S_n$ as $\ker \operatorname{sign}$, i.e., the set of even permutations in S_n.

By the first isomorphism theorem, we have that

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}, \quad n \geq 2,$$

by the first isomorphism theorem. For example, $|A_3| = 3$, $|A_4| = 12$, $|A_5| = 60$.

Theorem 9.8. The alternating group A_n is simple for $n \neq 4$. See this handout.

[10] dror-ism

§10 Day 10: Jordan–Hölder Decomposition (Oct. 3, 2025)

Recall from last class that if $N \trianglelefteq G$, then N, G/N are simple. $\mathbb{Z}/n$ is simple if and only if n is prime. The sign function $\operatorname{sign} : S_n \to \{\pm 1\}$ tells you the parity of a permutation, where $\operatorname{sign}\sigma = 1$ if σ is even and -1 if it is odd. Finally, $A_n = \ker \operatorname{sign}$ is the "alternating" group, i.e., the set of even permutations in S_n.

Per the handout from last time, we have a proof of why A_n is simple for all but $n = 4$; the proof is just casework bash, so I will not elaborate here.

We now move onto Jordan–Hölder.

Definition 10.1. A Jordan-Hölder decomposition for a group G is a sequence

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{0\}$$

such that for all i, $H_i = G_i/G_{i+1}$ is simple.

We give a few motivating examples. Let us consider $\mathbb{Z}/n\mathbb{Z}$, where $n = p_1 \dots p_k$. Then we have that

$$\mathbb{Z} \trianglerighteq p_1\mathbb{Z} \trianglerighteq p_1p_2\mathbb{Z} \trianglerighteq \cdots \trianglerighteq n\mathbb{Z}.$$

By modding out the entire sequence by $n\mathbb{Z}$, we have

$$\mathbb{Z}/n\mathbb{Z} \trianglerighteq \frac{p_1\mathbb{Z}}{n\mathbb{Z}} \trianglerighteq \frac{p_1p_2\mathbb{Z}}{n\mathbb{Z}} \trianglerighteq \cdots \trianglerighteq \frac{n\mathbb{Z}}{n\mathbb{Z}} = \{e\};$$

let the elements of the sequence be named $G_0, G_1, \dots, G_k$ in order; observe that we have (where we pick a random index because Dror does that),

$$H_2 = \frac{G_2}{G_3} = \frac{p_1p_2\mathbb{Z}/n\mathbb{Z}}{p_1p_2p_3\mathbb{Z}/n\mathbb{Z}} = \frac{p_1p_2\mathbb{Z}}{p_1p_2p_3\mathbb{Z}}$$

by the third isomorphism theorem, and we may factor out p_1, p_2 to obtain $\mathbb{Z}/p_3\mathbb{Z}$, which we know is simple. We may follow the same computation to demonstrate that the above sequence is indeed a Jordan-Hölder decomposition. Note that the decomposition itself is not necessarily unique with respect to the group, however, because as seen above, we may take $p_1, \dots, p_k$ in any order to obtain a sequence with the same property.

For another example, consider $G = S_n$ with $n \geq 5$. We have that

$$G = G_0 \trianglerighteq G_1 = A_1 \trianglerighteq G_2 = \{e\}.$$

We have that $H_0 = S_n/A_n = \operatorname{im}(\operatorname{sign}) = \{\pm 1\} = \mathbb{Z}/2\mathbb{Z}$ which we know is simple, and $H_1 = A_n/\{e\} = A_n$ is simple.

For a third example, consider $G = S_4$ (which has 24 elements). Since A_4 is the only non-simple alternating group, we may write

$$G_0 = S_4 \trianglerighteq A_4 \trianglerighteq \ker\phi = \{e, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \trianglerighteq \{e\}.$$

where $\phi : A_4 \to A_3$ and $H_0 = S_4/A_4 = \mathbb{Z}/2\mathbb{Z}$, $H_1 = \operatorname{im}\phi = A_3 = \mathbb{Z}/3\mathbb{Z}$.

§11 Day 11: Jordan–Hölder Theorem and Group Actions (Oct. 8, 2025)

We start by giving some examples of Jordan–Hölder decompositions.

Example 11.1. Let n admit a prime decomposition of $p_1 \dots p_k$; then

$$\mathbb{Z}/n \overset{\mathbb{Z}/p_1}{\trianglerighteq} p_1\mathbb{Z}/n \overset{\mathbb{Z}/p_2}{\trianglerighteq} p_1p_2\mathbb{Z}/n \overset{\mathbb{Z}/p_3}{\trianglerighteq} \dots \overset{\mathbb{Z}/p_n}{\trianglerighteq} \{e\},$$

for which we note that the quotient of any term with its successor is abelian, as denoted on top of the $\trianglerighteq$ symbols.

Example 11.2. Using the fact that A_4 is not simple, we have that

$$S_4 \overset{\mathbb{Z}/2}{\trianglerighteq} A_4 \overset{\mathbb{Z}/3}{\trianglerighteq} (\mathbb{Z}/2)^2 \overset{\mathbb{Z}/2}{\trianglerighteq} \mathbb{Z}/2 \overset{\mathbb{Z}/2}{\trianglerighteq} \{e\}.$$

For A_n where $n \neq 4$, we have the decomposition

$$S_n \overset{\mathbb{Z}/2}{\trianglerighteq} A_n \overset{A_n}{\trianglerighteq} \{e\}.$$

Theorem 11.3 (Jordan–Hölder decomposition theorem)**.** If G is a finite group, then there exists a sequence

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{e\},$$

such that $H_i = G_i/G_{i+1}$ is simple. We call $(H_0, H_1, \dots)$ the *composition series of* G, and it is unique up to a permutation.

Proof. By induction on $|G|$, assume that the theorem is true for all groups with order under $|G|$; then take a proper maximal normal subgroup $G_1 \trianglelefteq G$, and decompose $G \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}$. G/G_1 is simple, because if there exists a nontrivial normal subgroup $N \trianglelefteq G/G_1$, then by the fourth isomorphism theorem, we have $G \trianglerighteq N' \trianglerighteq G_1$, contradicting the maximality of G_1.

We can also demonstrate uniqueness; suppose G admits two decompositions

$$G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \dots,$$
$$G \trianglerighteq G_1' \trianglerighteq G_2' \trianglerighteq \dots,$$

where $G_1 \neq G_1'$; then we claim that $G_1G_1' = G$, and G_1G_1' is indeed a normal subgroup of G, which is strictly bigger than each of G_1, G_1' individually. Choose a decomposition series $G_1 \cap G_1' \trianglerighteq G_3'' \trianglerighteq G_4'' \trianglerighteq \dots$, where

$$G = G_1G_1' \overset{H_0}{\trianglerighteq} G_1 \overset{H_0'}{\trianglerighteq} G_1 \cap G_1', \quad G_1G_1' \overset{H_0'}{\trianglerighteq} G_1' \overset{H_0}{\trianglerighteq} G_1 \cap G_1'.$$

By the second isomorphism theorem, we have that

$$G/G_1 \cong H_0 \cong G_1'/G_1 \cap G_1',$$
$$G/G_1' \cong H_0' \cong G_1/G_1 \cap G_1',$$

and so the two decomposition sequences $G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \dots$ and $G \trianglerighteq G_1' \trianglerighteq G_1 \cap G_1' \trianglerighteq G_3'' \trianglerighteq \dots$ are equivalent by induction, where, by inspection, $G \trianglerighteq G_1' \trianglerighteq G_2' \trianglerighteq \dots$ is also equivalent by induction.[11] □

[11] reference here

Up to this point, we've considered groups by what they do (for example, the tetrahedron); it is time to formalize that notion.

Definition 11.4 (G-sets)**.** A G-set (specifically left G-sets) is a set X with $G \times X \to X$, mapping $(g, x) \mapsto gx$, such that (i) $ex = x$, (ii) $(g_1 g_2)x = g_1(g_2 x)$, which we call the "action axiom".

If G acts on X, we write $G \curvearrowright X$; i.e., G-sets are equivalent to a homomorphism $\alpha : G \to S(X)$, where $S(X)$ is the group of all bijections from X to itself.

Definition 11.5. A right G-set satisfies $X \times G \to X$ where $(x, g) \mapsto xg$ such that $xe = x$ and $(xg_1)g_2 = x(g_1 g_2)$. Note that this is basically the definition from earlier but we've swapped everything to the right.

Similarly, right G-sets are equivalent to an anti-homomorphism $\beta : G \to S(X)$.

Example 11.6. Any singleton is a G-set, left or right.

Example 11.7. Any G-set acts on itself $G \curvearrowright G$ by left multiplication. In particular, this means that $\alpha : G \to S(G)$ is a morphism of groups, and in this case, α is injective. Supposing $\alpha(G) = I$, then $g' = I(g') = \alpha(g)(g') = gg'$; by cancellation, $g = e$. This means that every group is a subgroup of a permutation group.

Example 11.8. G acts on itself by conjugation, which is a right action. We have that $\beta(h)(g) = g^h = h^{-1}gh$. G right acts on its subgroups by conjugation as well; for all $g \in G$, we have that $\beta(g)N = N$ if and only if N is normal.

Example 11.9. If $G > H$, then G/H is a left G-set (even if it isn't normal). We have that $G \curvearrowright G/H : g(g'H) = gg'H$, whcih is well-defined and is also an action. As a quick subexample, let $G = S_n > H = S_{n-1} = \{\sigma \in S_n \mid \sigma n = n\}$. Then $|G/H| = n$, and $G/H = \{\tau_1 S_{n-1}, \tau_2 S_{n-1}, \dots\}$, where $(\sigma \cdot S_{n-1})n = \sigma n$ and we take τ_j to be a permutation $\tau_j(n) = j$ for all $1 \le j \le n$. We have that

$$\sigma\tau_j s_{n-1} = \tau_{\sigma(j)} s_{n-1}, \quad S_n/S_{n-1} \cong \mathbb{Z}/n.$$

Claim 11.10. The collection of all G-sets forms a category, for which the objects are group actions $G \curvearrowright X$, and morphisms $(G \curvearrowright X) \to (G \curvearrowright Y)$ are maps $f : X \to Y$, where $f(gx) = gf(x)$ for all $g \in G$ and $x \in X$. Note that if $G \curvearrowright X_1$ and $G \curvearrowright X_2$, then $G \curvearrowright X_1 \sqcup X_2$.

Theorem 11.11. Every G-set is the disjoint union (possibly infinite) of "transitive G-sets". If $G \curvearrowright X$ is transitive, then $X \cong G/\operatorname{stab}_X(x_0)$, for some $x_0 \in X$.

Definition 11.12. We say a G-set is transitive if, for any two elements $x_1, x_2 \in X$, there exists some $g \in G$ such that $gx_1 = x_2$. Transitive G-sets are essentially the "primes" of G-sets.

Definition 11.13. Given $G \curvearrowright X \ni x_0$, the *stabilizer* $\operatorname{stab}_X(x_0)$ is given by the set of all $g \in G$ such that $gx_0 = x_0$.

§12 Day 12: Group Actions, First Sylow Theorem (Oct. 10, 2025)

Recall the definitions from last class; we write the left action $G \curvearrowright X$ denoting a morphism $G \to S(X)$, where $(g, x) \mapsto gx$ such that $ex = x$ and $(g_1 g_2 x) = g_1(g_2 x)$; similarly, the right action $X \curvearrowleft G$ means an anti-morphism $G \to S(X)$ where $(x, g) \mapsto xg$, $x = xe$, and $x(g_1, g_2) = (xg_1)g_2$. Both left and right actions make a category. We say that a G-set is transitive if, for all x_1, x_2, there exists g such that $gx_1 = x_2$. Recall the theorem from last class,

Theorem 12.1. Every G-set is a disjoint union of transitive G-sets, and if $G \subset X$ is transitive and $x_0 \in X$, then[12]

$$X \cong G/[\mathrm{stab}(x_0) := \{g \mid gx_0 = x_0\}] \cong G/H,$$

where the latter isomorphism is given by $(g', (gH)) \mapsto g'gH$.

Proof. Define the equivalence relation $\sim$ on X by $x_1 \sim x_2$ if and only if there exists an element $g \in G$ such that $gx_1 = x_2$. We see that $\sim$ is well-defined, as (i) $ex = x$, (ii) $gx_1 = x_2$ implies $g^{-1}x_2 = x_1$, (iii) if $g_1 x_1 = x_2$ and $g_2 x_2 = x_3$, then $g_2 g_1 x_1 = x_3$.

From this, we have that $X/\sim$ is given by the set of orbits of X, i.e., $\{gx_0 \mid x_0 \in X\}$. Each equivalence class is called a G-orbit, and is always of the form Gx_0 for some $x_0 \in X$; clearly, each orbit is transitive, since $x_1 = g_1 x_0$ and $x_2 = g_2 x_0$ implies $x_1, x_2 \in Gx_0$, with $g_2 g_1^{-1} x_1 = x_2$. The disjointness for the first part of the theorem comes from the fact that equivalence classes are always disjoint.

For the second part of the theorem, given $x_1 \in X$, by transitivity, there exists $g \in G$ such that $gx_0 = x_1$. We will construct maps $L : G/H \to X$ and $R : X \to G/H$ (where H is the stabilizer) to demonstrate the isomorphism between X and G/H. Let $R(x_1) = gH$; observe this map is well defined because for any other $g' \in G$ satisfying $g'x_0 = x_1$, we have $g'H = gH$, since $gx_0 = x_1$, $g'x_0 = x_1$ imply $gx_0 = g'x_0$, so $x_0 = g^{-1}g'x_0$ implies $g^{-1}g' \in \mathrm{stab}_X(x_0) = H$. Now, let $L : gH \mapsto gx_0$; then L is well-defined as we may check per earlier, so L, R are morphisms of G-sets, meaning we have $L \circ R = I$, $R \circ L = I$. □

Theorem 12.2 (Orbit-Stabilizer)**.** If $G \curvearrowright X$ and $\{x_i\}$ are representatives from each orbit, then

$$|X| = \sum_i \frac{|G|}{|\mathrm{stab}_X(x_i)|}$$

Proof. The proof is obvious from the above construction. □

We now introduce the class equation. Let $G \curvearrowleft G$ (where conjugation is a right action). Pick one y_i from each nontrivial orbit (each orbit contains at least one element, but some orbits contain nothing else, so nontrivial means non-singleton), i.e., one e y_i from each non-trivial "conjugacy class of G". Then $|G|$ is given by the the number of 1-element orbits and the sum $\sum_i \frac{|G|}{\mathrm{stab}_G(y_i)}$. Specifically, this is written

$$|G| = |Z(G)| + \sum_i [G : C_G(y_i)]$$

[12] personal note: link

§13 Day 13: Sylow Theorem, Pt. 1 (Oct. 15, 2025)

Today we introduce the Sylow theorem. Pick one y_i from each of the non-singleton conjugacy classes of G_i, where

$$|G| = |Z(G)| + \sum_i (G : C_G(y_i)),$$

where $G \curvearrowright G$ by conjugation.

Corollary 13.1. If G is a p-group (a group whose order is a power of a prime p), it has a non-trivial center, i.e., $Z(G) \neq \{e\}$.

Proof. Since $p \mid |G|$, we have that each $(G : C_G(y_i))$ is divisible by p, meaning that p into $|Z(G)|$, and so $|Z(G)| > 1$. □

In particular, let $|G| < \infty$, and $|G| = p^\alpha \cdot m$ such that α is chosen maximally ($p \nmid m$); we may define the Sylow p-subgroups as follows,

Definition 13.2. The set of all Sylow p-subgroups is given by $\mathrm{Syl}_p(G) = \{\underline{P} < G \mid |\underline{P}| = P\}$, where the number of them is written $n_p(G) = \left|\mathrm{Syl}_p(G)\right|$. Here, $\underline{P}$ denotes a subgroup of G, and is specifically a Sylow p-subgroup.

Theorem 13.3 (Sylow)**.** (i) The Sylow p-subgroups exist, and $n_p(G) > 0$, (ii) Every p-subgroup of G is contained in a Sylow p-subgroup, (iii) All Sylow p-subgroups of G are conjugate, and (iv) $n_p(G) = 1 \bmod p$, and $n_p(G) \mid |G|$.

As a quick example, consider

Example 13.4. $|G| = 21 = 3 \cdot 7$; we have that $n_3(G)$ divides 21, and $n_3(G) = 1 \bmod 3$.

We ask; what are all the groups of order 15? As a preliminary, observe that any group of order p is isomorphic to $\mathbb{Z}/p$;

Proof. Let $|G| = p$; as seen previously, we have that $G = \langle x \rangle$, so $G = \{x^0 = e, x^1 = x, \ldots, x^{p-1}\}$, which is indeed isomorphic to $\mathbb{Z}/p = \{[0], [1], \ldots, [p-1]\}$. □

We now figure out the groups of order 15. Let $|G| = 15 = 3 \cdot 5$; by Sylow, there exists $P_3 < G$ and $P_5 < G$ such that they are of orders 3 and 5 respectively. Furthermore, we have that $n_3(G) = 1$ and $n_5(G) = 1$, so $P_3 \lhd G$ and $P_5 \lhd G$. Writing

$$P_3 = \langle x \rangle = \{x^i \mid 0 \leq i \leq 4\},$$
$$P_5 = \langle y \rangle = \{y^j \mid 0 \leq j \leq 2\},$$

we see that y commutes with $P_5 : C_y \in \operatorname{Aut} P_5$ (where C_y denotes conjugation by y). As an aside, what is $\operatorname{Aut}(\mathbb{Z}/p)$? We see that $\phi : \operatorname{Aut}(\mathbb{Z}/p)$ is given by $\phi : x \mapsto x^k$ for some $k = 1, \ldots, p-1$, and so $x^i \mapsto x^{ik}$ with $x^p = e \mapsto e$ obviously. Thus, $\operatorname{Aut}(\mathbb{Z}/p) = \{1, \ldots, p-1\}$. We now continue to answer the question. $|C_y|$ is equal to 1 mod 3¡ but there are no elements of order 3 in $\operatorname{Aut} P_5$, so $|C_y| = 1$ and $C_y = I$, meaning y commutes with P_5. Thus, $G = P_5 \times P_3$, and we see that $\mathbb{Z}/15 \cong \mathbb{Z}/5 \times \mathbb{Z}/3$. Note that this argument doesn't hold for $|G| = 21 = 3 \cdot 7$ because the divisibility doesn't work out.

Theorem 13.5. If $(a, b) = 1$, then $\mathbb{Z}/a \times \mathbb{Z}/b \cong \mathbb{Z}/ab$.

Proof. Find $s, t \in \mathbb{Z}$ such that $as = bt = 1$, per Bezout's identity. Then let $R : \mathbb{Z}/ab \to \mathbb{Z}/a \times \mathbb{Z}/b$ be given by multiplication by (s, t) and $L : \mathbb{Z}/a \times \mathbb{Z}/b \to \mathbb{Z}/ab$ be given by $(x, y) \mapsto bx + ay$. We claim that R, L are well-defined and inverses of each other. Observe that we have

$$(L \circ R)(h) = L(th, sh) = bth + ash = (bt + as)h = h;$$

we may also prove this by simply doing matrix products. □

From this, we see that we indeed have $\mathbb{Z}/21 = \mathbb{Z}/3 \times \mathbb{Z}/7$. We now prove the Sylow theorem. To see that $\mathrm{Syl}_p(G) \neq \varnothing$, observe that by induction on $|G|$, write

$$|G| = |Z(G)| + \sum_i (G : C_G(y_i))$$

as before; without loss of generality, let $p^2 \mid |G|$; then p must divide both or neither of the terms of the class equation. Suppose that p divides into neither of them; then $p \nmid \sum_i (G : C_G(y_i))$, and so there exists y_i such that $p \nmid (G : C_g/y_i)$, which is equal to $|G| \,/\, |C_G/y_i|$. THus, $p^2 \mid |C_G(y_i)|$, and by induction, $C_G(y_i)$ has a subgroup of order p^2, and so that's also true for G. In the case that p divides into both, we have that $p \mid |Z(G)|$, and so we may find $x \in Z(G)$ such that $|x| = p$. Consider $G' = G/\langle x \rangle$; we may use induction to find a Sylow p-subgroup of $G/\langle x \rangle$. We may use the fourth isomorphism theorem to lift it to a subgroup $\underline{P}$ of G.

Lemma 13.6 (Cauchy's Theorem)**.** If G is abelian, p prime, and $p \mid |G|$, there exists $x \in G$ with $|x| = p$.

Proof. It is enough to find $z \in G$ with $p \mid |z|$; indeed, if $|z| = pn$, take $x = z^n$ and $|x| = p$; pick $e \neq z \in G$. If $p \mid |z|$, we are done, so assume $p \nmid |z|$. We have that $p \mid |G/\langle z \rangle|$. By induction, find $y \in G$ such that $\left|[y]_{\langle z \rangle}\right| = p$. Then $|y| \mid |[y]| = p$ implies $|y| = p$, and indeed, $[y]^{[y]} = [y^{|y|}] = [e] = e$. Thus, $p \mid |y|$. □

§14 Day 14: Sylow Theorem, Pt. 2 (Oct. 17, 2025)

Let $|G| = p^\alpha m$ for some maximal α such that $p \nmid m$ (and so $p^\alpha \mid |G|$). We define $\mathrm{Syl}_p(G) := \{\underline{P} < G \mid |\underline{P}| = p^\alpha\}$[13], and $n_p(G) := \left|\mathrm{Syl}_p(G)\right|$. Recall the Sylow theorems,

Theorem 14.1 (Sylow)**.** (i) $\mathrm{Syl}_p(G) \neq \varnothing$, (ii) Every p-subgroup is contained in a Sylow p-subgroup, (iii) All Sylow p-subgroups are conjugate. (iv) $n_p(G) = 1 \bmod p$, and $n_p(G) \mid |G|$.

Lemma 14.2. (i) If $\underline{P} \in \mathrm{Syl}_p$ (we drop the G when the group is obvious) and $H < G$ is a p-subgroup of G such that $H < N_G(\underline{P})$, then $H < \underline{P}$. (ii) If $\underline{P} \in \mathrm{Syl}_p$, $|x| = p^\beta$ with $\beta \geq 1$, $x^{-1}\underline{P}x = \underline{P}$, then $x \in \underline{P}$.

Specifically, both the conditions in the lemma are equivalent to saying that you can't extend a Sylow p-subgroup by "anything with p in it". We may reformulate the lemma as follows,

Lemma. Let $\underline{P} \in \mathrm{Syl}_p(G)$, $|H| = p^\beta$, then $N_H(\underline{P}) = H \cap \underline{P}$.

Proof. For (i), we have that $\underline{P}H$ is a group, so $\underline{P} \lhd PH$ and

$$\left|\frac{\underline{P}H}{\underline{P}}\right| = \left|\frac{H}{H \cap \underline{P}}\right|$$

is a power p^γ of p. This means $|PH| = |\underline{P}| \cdot |PH/\underline{P}| = p^{\alpha+\gamma}$, and $\gamma = 0$, i.e., $|PH/\underline{P}| = 1$, so $H = H \cap \underline{P}$, and so $H \subset \underline{P}$. For (ii), take $H = \langle x \rangle$ as a p-group $H < N_G(\underline{P})$. This means $H < \underline{P}$, so $x \in \underline{P}$. □

Claim 14.3. If $\underline{P} \in \mathrm{Syl}_p$, the number of conjugates of $\underline{P}$ is equivalent to 1 mod p. We denote the set of all conjugates of $\underline{P}$ as $\mathcal{C}$, where $|\mathcal{C}| = n_{\underline{p}}$.

We claim that this is obviously true from the fact that $n_{\underline{p}} \mid |G|$.

Proof. Consider the action $\mathcal{C} \curvearrowleft G$; since $n_{\underline{p}} \mid |G|$ and $\mathcal{C} \curvearrowleft G$ is transitive, we have that $|\mathcal{C}| \mid |G|$. Now, consider $\mathcal{C} \curvearrowleft \underline{P}$, and suppose $\underline{P}' \in \mathcal{C}$. We have that $\mathrm{orb}_{\mathbb{C}}(\underline{P}') \cong \underline{P}/\operatorname{stab}_{\mathcal{C}}(\underline{P}')$, where the stabilizer of $\underline{P}'$ is $N_{\underline{P}}(\underline{P}')$, so

$$\left|\mathrm{orb}_{\mathcal{C}}(\underline{P}')\right| = \frac{|\underline{P}|}{|\underline{P} \cap \underline{P}'|},$$

which is equal to 1 if $\underline{P} = \underline{P}'$, and p^β with $\beta \geq 1$ otherwise. This means $\mathcal{C}$ has 1 singleton orbit and the rest have sizes divisible by p, so $|\mathcal{C}| = 1 \bmod p$. □

Claim 14.4. If $H < G$ is a p-group and $\underline{P} \in \mathrm{Syl}_p$, then H is contained in some conjugate of $\underline{P}$. In particular, all Sylow subgroups are conjugate to each other, and the theorem is proven.

Proof. Let $\mathcal{C}$ be the set of all conjugates of $\underline{P}$ as before, and consider the action $\mathcal{C} \curvearrowleft H$ by conjugation. Per our previous claim, we see that $|\mathcal{C}| = 1 \bmod p$, so $\mathcal{C}$ must have at least one singleton orbit, namely $\underline{P}'$, which is a conjugate of $\underline{P}$ such that $H < N_G(\underline{P}')$, implying $H < \underline{P}'$. □

[13] please, read this as "the set of subgroups of G with order p^α... $\underline{P}$ denotes 'subgroup' in dror fuckin bar natan notation"

§15 Day 15: Semidirect Products (Oct. 22, 2025)

Recall the Sylow theorem(s)[14];

(i) $\mathrm{Syl}_p(G) \neq \varnothing$;

(ii) If $H < G$ is a p-group, then H is contained in a Sylow p-group.

(iii) $n_p(G) \equiv 1 \bmod p$ and $n_p(G)$ divides into $|G|$.

Let us go over an example. Consider the groups of order 21; let G be such that $|G| = 21$, and take $P_3, P_7 < G$ to be Sylow-3 and Sylow-7 respectively. We see that $n_7 = 1$ by the above theorem, so $P_7 \lhd G$ (as it is the unique Sylow-7 group), and n_3 is equal to 1 or 7 by checking the factors of 21. If $n_3 = 1$, then $P_3 \lhd G$.

As an aside, if $K, H \lhd G$, $KH = G$, and $K \cap H = \{e\}$, then $G = K \times H$.

Claim 15.1. Recall the commutator notation, where we denote $[a, b] = aba^{-1}b^{-1}$. We claim that $[K, H] = \{e\}$.

Proof. $khk^{-1}h^{-1}$ can be seen as the product of k and $hk^{-1}h^{-1}$ (of which both are in K per normality) and the product of khk^{-1} and h^{-1} (for which both are in H). This means $khk^{-1}h^{-1} \in [K, H]$, of which is equal to $\{e\}$ per the fact that $H, K \lhd G$ and $H \cap K = \{e\}$. □

We may use this to prove the aside. Consider $\mu : K \times H \mapsto KH = G$, where $\mu(k, h) = kh$. This is clearly an isomorphism; and so we indeed see $G = K \times H$.

Returning to our example of order 21 groups, observe that, in this manner, we may pick $K = P_3$, $H = P_7$, to get $G = P_3 \times P_7 \cong \mathbb{Z}_3 \times \mathbb{Z}_7 \cong \mathbb{Z}_{21}$ as they are coprime. This concludes the $n_3 = 1$ case. In the $n_3 = 7$ case, however, we have that P_3 is not normal in G. Consider $P_7 = \langle x \rangle$ and $P_3 = \langle y \rangle$. Per normality of P_7, we see that $yxy^{-1} = x^q \in P_7$ for some q (regarded as an element of the cyclic group). Now, observe that the operation of conjugation by y yields the sequence

$$x \to yxy^{-1} \to y^2x(y^{-1})^2 \to y^3x(y^{-1})^3 = x,$$

and $x \to x^q \to x^{q^2} \to x^{q^3} = x$ simultaneously, for which we see $q^3 \equiv 1 \bmod 7$, and so $q \in \{1, 2, 4\}$. Fixing a particular such q, we see that

$$x^a y^b x^c y^d = x^a y^b x^c y^{-b} y^{b+d} = x^a x^{c \cdot q^b} y^{b+d} = x^{a + c \cdot q^b} y^{b+d}$$

fixes the multiplication table of G. If $q = 1$ as before, we have that $G \cong \mathbb{Z}_{21}$. If $q = 2$ or 4, they follow the above, but they are isomorphic, i.e., there are 2 groups of order 21. To show this, we need to introduce semidirect products. Let $N, H < G$, and consider $N \times H$ and NH.

$\mu : N \times H \to NH$ given by $\mu(n, h) = nh$ always exists as a surjective map, but it is not a homomorphism in general. If $N \cap H = \{e\}$, then μ is injective, but still not necessarily a homomorphism, and $N \cdot H$ may not even be a group. If $N, H \lhd G$ with $N \cap H = \{e\}$, then $[N, H] = \{e\}$, and μ is an isomorphism, so we have $N \times H \cong NH$. If $N \lhd G$, $H < G$, we have an interesting case. Take $\phi : H \to \mathrm{Aut}\, N$ by $\phi(h)(n) = hnh^{-1}$ (alternatively written $\phi_h(n)$).

[14] at this point i'll just say whatever man

Claim 15.2. If you know ϕ, you know NH.

Consider $n_1h_1 \cdot n_2h_2 = n_1h_1n_2h_1^{-1}h_1h_2 = n_1\phi_{h_1}(n_2)h_1h_2$. We have that $(nh)^{-1} = h^{-1}n^{-1} = h^{-1}n^{-1}hh^{-1} = \phi_{h^{-1}}(n^{-1})h^{-1}$.

Definition 15.3. Given groups N, H and a morphism $\phi : H \to \operatorname{Aut} N$, define a new group $N \rtimes_\phi H = N \rtimes H$ "the semidirect product of N and H relative to ϕ", where $N \rtimes_\phi H = N \times H$ as a set (but different as a group), with multiplication given by $(n_1, h_1)(n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2)$.

Proposition 15.4. (i) $N \rtimes H$ is a group.

(ii) $N \lhd (N \rtimes H)$, $H < N \rtimes H$, and $N \rtimes H/N \cong H$.

(iii) If $N \lhd G$, $H < G$, and $N \cap H = \{e\}$, we have $\mu : N \rtimes H \to NH$ is an isomorphism with our defined multiplication.

Proof. (i) We have that $e_{N\rtimes H} = (e_N, e_H)$, which is obviously true, and everything else is also clear enough.

(ii) $N \cong (N, e_H)$, which is clearly a subgroup as $(n_1, e)(n_2, e) = (n_1n_2, e)$ as $\phi_e(n_2) = n_2$. Checking that it is normal is left as an exercise, and the last part is also left as an exercise with the observatino that $H \cong (e_N, H)$ is obviously a subgroup too.

(iii) This is true by design. □

Example 15.5. Consider the group $ax + b$, where $(ax + b) \circ (cx + d) = acx + ad + b$. Then $\{ax + b\} \cong \mathbb{R}_b^+ \rtimes_\phi \mathbb{R}_a^\times$, where $\phi_a(b) = a \cdot b$.

§16 Day 16: Semidirect Products, Pt. 2 (Oct. 24, 2025)

Recall the definition of the semidirect product. Let N, H be groups and consider

$$\begin{aligned}\phi : H &\to \operatorname{Aut} N,\\ h &\mapsto (\phi_n : N \to N);\end{aligned}$$

we have $N \rtimes_\phi H = N \times H$ as a set, with $(n_1, h_1) \cdot (n_2, h_2) = (n_1\phi_{n_1}(n_2), h_1h_2)$ and $(n, h)^{-1} = (\phi_{h^{-1}}(n^{-1}), h^{-1})$.

Theorem 16.1. $N \rtimes_\phi H$ is a group. $(N \rtimes H)/N \cong H$, $N \lhd N \rtimes_\phi H$, and $H < N \rtimes H$.

We can identify $n \sim (n, e_H)$ and $h \sim (e_N, h)$; from this, we have $(n, h) = (n, e) \cdot (e, h)$.

Example 16.2. We have that $\{ax + b\} \cong \mathbb{R}^+ \rtimes \mathbb{R}^\times$.

Example 16.3. Consider a vector space V of dimension n, and consider $\{Ax + b\}$ where A is a linear automorphism of V and $b \in V$. We have that this is isomorphic to $V_b \rtimes_\phi \operatorname{Aut}(V)_A$, where $x \mapsto Ax + b$ is a map from V to V. We can identify

$$V_b \rtimes_\phi \operatorname{Aut}(V)_A \cong R^n_b \rtimes_\phi \{A \mid A \in \mathrm{GL}_n(V)\},$$

where $\phi_A(b) = A \cdot b$.

Example 16.4. The Poincarè group $\mathbb{R}_+ \rtimes O(3, 1)$ is the set of "Lorentz transforms" $\sum_{i=1}^3 x_i^2 - t^2$.

Example 16.5. Suppose $\phi_n = \mathrm{id}$ for all $h \in H$; we have that $N \rtimes_\phi H \cong N \times H$ as a group.

Example 16.6. Let $N = \mathbb{Z}/n$ and $H = \{0, 1\}$. Then taking $\phi_h(k) = h \cdot k$, we have $\mathbb{Z}/n \rtimes_\phi H \cong D_{2n}$. Note that $\mathbb{Z} \bmod n$ can be viewed as the rotations of a polygon with n sides, with "one extra thing" being reflections.

Example 16.7. $N = \mathbb{Z}/7 = \langle x \rangle / x^7 = e$ and $H = \mathbb{Z}/3 = \langle y \rangle / y^3 = e$. Consider $\phi_1(x) = x$, $\phi_2(x) = x^2$, and $\phi_3(x) = x^4$. Let $G_i = N \rtimes_{\phi_i} H$, where $i = 1, 2, 3$; we have $|G| = 21$, and $G_1 = \mathbb{Z}/21$, and $G_2 = G_3$. These are the two groups of order 21 (of which one is abelian and the other is not)

§17 Day 17: Semidirect Products, Pt. 3 (Nov. 5, 2025)

Recall the semidirect product definition from last class. Let G be a group of order 12, where $|G| = 12 = 2^2 \cdot 3$, and pick $P_2, P_3 \in G$ to be Sylow-p subgroups; we see that $P_3 \cong \mathbb{Z}/3$ and $|P_2| = 4$, so P_2 is either isomorphic to $\mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$.

As a quick proof, observe that $e \neq a \in P_2$ is either of order 2 or 4; if $|a| = 4$, then $P_2 \cong \mathbb{Z}/4$; if all elements are of order two, though, then all elements square to e, and so the multiplication is forced to be that of $V_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. We will see later that $|G| = p^2$ is forced to be either $G \cong \mathbb{Z}/p^2$ or $\mathbb{Z}/p \times \mathbb{Z}/p$.

Assume neither is normal; then $n_3(G) = 4$ gives $(3-1) \cdot 4 = 8$ elements of order 3. $n_2(G) = 3$, so by the same argument, there are at least 7 elements of order 2, which is too many elements, meaning either P_2 or P_3 must be normal.[15] We may now consider a semidirect product.

(i) For the first case, suppose $P_2 = \mathbb{Z}/2 \times \mathbb{Z}/2$. We have two subcases to consider first. If $P_2, P_3 \triangleleft G$, we have that $G = P_2 \times P_3 \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \cong \mathbb{Z}/2 \times \mathbb{Z}/6$. If $P_3 \triangleleft G$, then $G = \mathbb{Z}_3 \rtimes_\phi (\mathbb{Z}/2 \times \mathbb{Z}/2)$, where any such automorphism is either the identity, or switches 1 and 2. This means $\phi : \mathbb{Z}/2 \times \mathbb{Z}/2 \to \{\pm\}$ has three choices, and is "essentially" $\phi : \{\pm\} \times \{\pm\} \to \{\pm\}$. In any case, we get the group $(\mathbb{Z}/3 \rtimes_{-1} \mathbb{Z}/2) \times \mathbb{Z}/2 \cong D_6 \times \mathbb{Z}/2$, where $\mathbb{Z}/3, \mathbb{Z}/2$ in the former are regarded as rotation and reflection.

One such example of this multiplication is $\mathbb{Z}/3 \rtimes_{(-1)} \mathbb{Z}/2$, where $\mathbb{Z}/3 = \{1, r, r^2\}$ and $\mathbb{Z}/2 = \{1, s\}$; we have that the group multiplication is given by $r_1 s_1 \cdot r_2 s_2 = r_1 r_2^{-1} \cdot s_1 s_2$, where $s_1 = 1$ and $s_2 = s$ denotes '+' and '−' respectively. This is clearly the rule given in the definition of $D_n = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

For the third subcase, we have that $G = (\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/3$, where the sets are $\{e, a_1, a_2, a_3\}$ and $\{0, 1, 2\}$ respectively, where $\mathbb{Z}/3$ acts as a cyclic permutation of a_1, a_2, a_3. We let $\phi_b(a_i) = a_{i+b \bmod 3}$ for $b \in \{0, 1, 2\}$.

Claim 17.1. $G \cong A_4 = \{e, (12)(34), (13)(24), (14)(23)\} \rtimes \langle (432) \rangle$.

This is immediate from checking conjugation by $(432)^{-1}$ is the action above, and hence shows the claim.

(ii) For the second case, consider $P_2 \cong \mathbb{Z}/4$; for the first subcase, we have that $G = P_2 \times P_3 \cong \mathbb{Z}/4 \times \mathbb{Z}/3 \cong \mathbb{Z}/12$; for the second subcase, let $G = \mathbb{Z}/3 \rtimes_\phi \mathbb{Z}/4$, where $\phi : \mathbb{Z}/4 \to \mathrm{Aut}(\mathbb{Z}/3) = \mathbb{Z}/2$. The only such ϕ maps $\{0, 2\}$ to 0 and $\{1, 3\}$ to 1, and there is no better name for this group. For the third subcase, consider $G = \mathbb{Z}/4 \rtimes_\phi \mathbb{Z}/3$, where $\mathrm{Aut}(\mathbb{Z}/4) \cong \mathbb{Z}/2$. We have that $\phi : \mathbb{Z}/3 \to \mathbb{Z}/2$ is the identity, meaning the semidirect product in this case really is the direct product, which doesn't exist.

Thus, we establish that there are 5 groups of order 12. Specifically, they are $\{\mathbb{Z}/12, \mathbb{Z}/6 \times \mathbb{Z}/2, D_6 \times \mathbb{Z}/2, A_4, \mathbb{Z}/3 \rtimes_\phi \mathbb{Z}/4\}$.

We now begin an informal discussion of braid groups, but we discuss free groups and fundamental groups π first.

Definition 17.2. A free group $F_n = \langle x_1, \ldots, x_n \rangle$ is the set of all "words" of x_i's and x_i^{-1}'s of finite length. We sasume that $x_i x_i^{-1} = x_i^{-1} x_i = ()$ is an empty word.

[15] i may be counting order two elements incorrectly.. the point being that maybe the Sylow-2 subgroups may intersect, so $3 + 2 + 2 = 7$. read here

This is a group under concatenation of words as multiplication. As an example, $(bar)(natan) = barnatan$ in the English alphabet. Naturally, id is the empty word. Showing multiplication is associative is annoying and uninteresting.

Those who have taken a Dror 327 will know that the picture of $F_2 = \langle a, b\rangle$ is the Mexican cross. Elements of F_2 are thus walks along said Mexican cross.

Definition 17.3. A fundamental group $\pi_1(X, x_0)$ is just the set of all paths or walks in a space such that each path cannot be deformed to any other in the set. In other words, $\{[\gamma] \mid \gamma : [0,1] \to X, \gamma(0) = \gamma(1) = x_0\}$, with the equivalence classes given by homotopy.

For a donut $\pi_1(\mathbb{T}) = \mathbb{Z} \times \mathbb{Z}$, which we see from just counting the number of times we go around the holes and the number of times we go through the hole. For an annulus, we have that its fundamental group is $\mathbb{Z}$.

What is $\pi_1(\mathbb{D} \setminus \{a_1, a_2, a_3\})$, where $a_1, a_2, a_3 \in \mathbb{D}$ are isolated points? We see that we can loop around any of the a_i's or clockwise or counterclockwise, so $\pi_1(\mathbb{D} \setminus \{a_1, a_2, a_3\}) = F_3$, where unlike the torus, order matters, so we actually get the free group instead of just $\mathbb{Z}^3$. We may now discuss the braid groups.

The braid group PB_3 is a group on vertical connections;[16] it is a given by the set of crossinsg on 3 braids, for which to get an inverse, we simply flip all crossings. Let $\mathcal{P} : \mathrm{PB}_n \to \mathrm{PB}_{n-1}$ be the function deleting the last strand. We can think of $\mathrm{PB}_{n-1} < \mathrm{PB}_n$, where the last strand is straight with no crossings with the first $n-1$ strands. What is $N = \ker \mathcal{P}$? The set of braids that are only "tangled" by strand n; if we count passing under a strand to the left as i and under the strand i to the right as i^{-1}, we see that $\ker P = F_{n-1}$. We now have $F_{n-1} = N \lhd \mathrm{PB}_n > \mathrm{PB}_{n-1} = H$.

Claim 17.4. $H \cap N = \{e\}$ and $G = N \cdot H$.

Proof. The former is easy; since we count crossing of n in N, and there are no crossings of n in H, $N \cap H$ is simply the empty word, i.e., $\{e\}$.

If we push the nth strand to the bottom of the braid, we see that this revelas an element of H, and a crossing of n, or an element of N. Thus, $G = NH$ implies $\mathrm{PB}_n \cong F_{n-1} \rtimes \mathrm{PB}_{n-1}$. By recursion, we have that

$$F_{n-1} \rtimes \mathrm{PB}_{n-1} \cong F_{n-1} \rtimes (F_{n-2} \rtimes (F_{n-3} \rtimes (\dots (F_1)))),$$

where $F_1 = \mathbb{Z}$. In knot theory, "braids are easy", as they are just semidirect products of words, and we just pick conjugation to be the action. □

[16] please, just read about it here.

§18 Day 18: Finitely Generated Abelian Groups (Nov. 7, 2025)

If M is a finitely generated abelian group, we want to show that there exists r, p_i, s_i where $1 \leq i \leq k$ such that p_i is prime with[17]

$$M \cong \mathbb{Z}^r \times \prod_{i=1}^{k} \mathbb{Z}/p_i^{s_i}.$$

Furthermore, r is determined uniquely, as are the primes and their powers, up to permutation. Recall that if a group G is finitely generated, we have that $G = \langle g_1, \ldots, g_n \rangle$ (write X to be the set $\{g_1, \ldots, g_n\}$); we can consider the free group $F(X)$, and consider the "interpretation" group action $F(X) \to G$ as taking a word and applying the group operations in G to the word.[18] Let us provide a proof sketch of the above claim.[19]

Proof sketch. We will prove the claim by "Gaussian elimination on something". We start with the finite case for intuition; for any matrix $A \in M_{m\times n}(\mathbb{Z})$, let us construct a finitely generated abelian group M_A (then we shall show all finitely generated abelian groups are of this form) as follows,

$$A \mapsto (\phi_A : \mathbb{Z}^n \to \mathbb{Z}^m) \mapsto M_A := \frac{\mathbb{Z}^m}{\operatorname{Im} \phi_A}.$$

For some examples of this process, observe that

(i) If $A = 0$, then $\phi_A : \mathbb{Z} \to \mathbb{Z}$, so $M_{(0)} = \mathbb{Z}/0 = \mathbb{Z}$.

(ii) If $A = I_n$, then $\phi_A : \mathbb{Z}^n \to \mathbb{Z}^n$, where $M_{I_n} = \mathbb{Z}^n/\mathbb{Z}^n = \{e\}$.

(iii) If $A \in M_{1\times 1}(\mathbb{Z})$, write $A = \ell$; then $\phi_A : \mathbb{Z} \to \mathbb{Z}$ is simply given by multiplication by ℓ, so $M_\ell = \mathbb{Z}/\ell$.

This can be generalized $A \in M_{G\times X}(\mathbb{Z})$, where G is a finite set, and X not necessarily finite to also yield finitely generated abelian groups M_A. In particular, the operation would go as

$$A \mapsto (\phi_A : \mathbb{Z}^X \to \mathbb{Z}^G) \mapsto M_A = \frac{\mathbb{Z}^G}{\operatorname{Im} \phi_A}.$$

We may note that $\mathbb{Z}^X$ is the set of $f : X \to \mathbb{Z}$ with finite support (similarly, all functions $G \to \mathbb{Z}$ already have finite support), which is a group under addition, and M_A is finitely generated because $\mathbb{Z}^G$ is finitely generated. □

Claim 18.1. Every finitely generated abelian group M has a finite G, a not necessarily finite X, and $A \in M_{G\times X}$ such that $M \cong M_A$.[20]

Proof. Since M is a finitely generated abelian group, let $M = \langle g_1, \ldots, g_n \rangle$, for which we will let $G = \{g_1, \ldots, g_n\}$. Since M is abelian, we may reorder any word of G as $g_1^{a_1} \ldots g_n^{a_n}$; define $\pi : \mathbb{Z}^G \to M$ by $\pi((a_1, \ldots, a_n)^\top) = g_1^{a_1} \ldots g_n^{a_n}$; by the first isomorphism theorem, we obtain

$$\pi(\mathbb{Z}^G) \cong \mathbb{Z}^G/\ker \pi \implies M \cong \mathbb{Z}^G/\ker \pi,$$

[17] i'm just going to link this

[18] since the structure of the free group differs from that of G; think of it as a restriction on the words, perhaps.

[19] note that this G and X are unrelated to what's to come later.

[20] we omit the $\mathbb{Z}$ from $M_{G\times X}$ from now on for conciseness. damn dror is getting footnoted hard

for which we know $\ker \pi$ is abelian as it is a subgroup of $\mathbb{Z}^G$. Let X be the generators of $\ker \pi$ (note that this is not necessarily finite), and observe that the interpretation $\tilde{\pi}$ on $\mathbb{Z}^X$ sends to $\ker \pi$, for which we have

$$\mathbb{Z}^X \xrightarrow{\tilde{\pi}} \ker \pi \hookrightarrow \mathbb{Z}^G \xrightarrow{\pi} M, \qquad \mathbb{Z}^X \xrightarrow{\phi} \mathbb{Z}^G$$

As seen in the diagram above, we may define $\phi : \mathbb{Z}^X \to \mathbb{Z}^G$ and represent it by some matrix

$$A = \left(\cdots \;\middle|\; \phi(x_\alpha) \;\middle|\; \cdots \right),$$

where each column is given by $\phi(x_\alpha)$ for each $x_\alpha \in X$ (which can be thought of as each $e_\alpha \in \mathbb{Z}^X$). *Note: the intuition for A is that each column describes which words vanish in M.* □

§19 Day 19: Finitely Generated Abelian Groups, Pt. 2 (Nov. 12, 2025)

Claim 19.1. If $A = A_1 \oplus A_2$, i.e.,

$$A = \left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right) \in M_{G\times X}$$

with $A_1 \in M_{G_1\times X_1}$, $A_2 \in M_{G_2\times X_2}$ such that $G = G_1 \cup G_2$ and $X = X_1 \cup X_2$, then $M_A \cong M_{A_1} \times M_{A_2}$.

Theorem 19.2. By iterating this claim, we see that

$$A = \left(\begin{array}{c|c} \begin{matrix} 0 & & \\ & \ddots & \\ & & 0 \end{matrix} & \\ \hline & \begin{matrix} p_1^{s_1} & & \\ & \ddots & \\ & & p_n^{s_n} \end{matrix} \end{array}\right),$$

for which the top left block is of size $r \times r$.

Proof. To see this, we will construct a map $M_{A_1} \times M_{A_2} \to M_A$. Indeed, M_{A_1} is defined as $\mathbb{Z}^{G_1}/\operatorname{im}\phi_{A_1}$ and M_{A_2} is defined as $\mathbb{Z}^{G_2}/\operatorname{im}\phi_{A_2}$, so we may let the map be given by

$$\left(\left[\sum_{g\in G_1} a_g e_g\right], \left[\sum_{g\in G_2} a_g e_g\right]\right) \mapsto \left[\sum_{g\in G} a_g e_g\right].$$

Verifying that this is indeed a well-defined bijection is left as homework. □

Proposition 19.3. If $A' = PAQ$, where $P \in M_{G\times G}(\mathbb{Z})$ is invertible, $Q \in M_{X\times X}(\mathbb{Z})$ is invertible (whose columns have finite support and finite inverses), then $M_A = M_{A'}$, i.e.,[21]

$$\begin{array}{ccc} \mathbb{Z}^X & \xrightarrow{A} & \mathbb{Z}^G \\ {\scriptstyle Q}\uparrow & & \downarrow{\scriptstyle P} \\ \mathbb{Z}^X & \xrightarrow{A'} & \mathbb{Z}^G \end{array}$$

Before we provide a proof, we will show that the conditions actually work. Since A' maps from $\mathbb{Z}^X \to \mathbb{Z}^G$, where $\mathbb{Z}^X$ is the additive group of finitely supported functions $f : X \to \mathbb{Z}$, consider Qv, where v is a column vector that admits finitely many nonzero components (which, without loss of generality, we will call $v_1, \ldots, v_n$). Since the respective columns $Q_{v_1}, \ldots, Q_{v_n}$ in Q also have finite support, we see that there can only be finitely many nonzero entries in Qv, so we see that the proposition indeed yields restricted row and column operations on A without changing M_A.[22]

Proof. Observe the following diagram,

$$\begin{array}{ccccc} \mathbb{Z}^X & \xrightarrow{A} & \mathbb{Z}^G & \xrightarrow{\pi} & M_A \\ {\scriptstyle Q}\uparrow & & \downarrow{\scriptstyle P} & & \downarrow{\scriptstyle \overline{P}} \\ \mathbb{Z}^X & \xrightarrow{A'} & \mathbb{Z}^G & \xrightarrow{\pi'} & M_{A'} \end{array}$$

[21] throughout the rest of today's notes i will omit the f.s. from $\mathbb{Z}^X_{f.s.}$, since it is clear that elements of $\mathbb{Z}^X$ are finitely supported

[22] alteration of dror's proof where he thinks 3 is a big enough number (read: $n = 3$)

where $M_A = \mathbb{Z}^G/\operatorname{im} A$ and $M_{A'} = \mathbb{Z}^G/\operatorname{im} A'$. We define $\overline{P}$ by $\overline{P}([\alpha]) = [P_\alpha]$ and $\overline{P}^{-1}([\alpha']) = [P^{-1}\alpha']$. Indeed, to see that $\overline{P}$ is well-defined, it is enough to diagram chase. Suppose $[\alpha_1] = [\alpha_2]$; we immediately obtain that $\alpha_1 - \alpha_2 \in \operatorname{im} A = \ker \pi$. Now, pick $\beta \in \mathbb{Z}^X$ such that $\alpha_1 - \alpha_2 = A\beta$. We obtain

$$P\alpha_1 - P\alpha_2 = P(\alpha_1 - \alpha_2) = PA\beta = PAQQ^{-1}\beta = A'Q^{-1}\beta = A'\beta',$$

meaning that $P\alpha_1 - P\alpha_2 \in \operatorname{im} A'$, and is hence in the kernel of π again. Thus, $\overline{P}$ is well-defined. □

Proposition 19.4. If A' is obtained from A by adding or removing columns of zeroes, then $M_A = M_{A'}$, and $(A') = (A \mid 0)$.

Proof. This is immediate from our discussion before the previous proof. □

Claim 19.5. With our operations, we can diagonalize A.

Proof. Of all the presentation matrices of M (of the form PAQ) of all entries, let a_{11} be the smallest positive entry. Without loss of generality, we may assume that

(i) All entries in the row and column associated to a_{11} must be zero except a_{11} itself, since all entries in said row and column must be divisible by a_{11} (if not, we may perform row and column operations to contradict minimality).

(ii) All other entries are divisible by a_{11} for the same reason.

In this manner, we see that A can be transformed into

$$\left(\begin{array}{c|ccc} a_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{array}\right),$$

for which we may repeat the operation on A_1 and subsequent matrices to obtain

$$\left(\begin{array}{ccc|c} a_{11} & & & \\ & \ddots & & 0 \\ & & a_{nn} & \end{array}\right), \qquad (G = \{g_1, \dots, g_n\})$$

for which we may note that the the latter columns are all zeroes. Moreover, if there exists an entry in the diagonal that is zero, we see that all latter entries must vanish as well (let r denote the number of zeroes on said diagonal). If we denote D as the square diagonal matrix with entries $a_{11}, \dots, a_{nn}$, we obtain that $M = M_D$ (as all we did was apply row and column operations, so we may apply propositions 19.3 and 19.4), where we may write

$$M = M_D \cong \mathbb{Z}^r \times \prod_{a_{ii} \neq 0,1} \mathbb{Z}/a_{ii} \cong \mathbb{Z}^r \times \prod \mathbb{Z}/p_i^{s_i}.$$

Indeed, we may decompose each $\mathbb{Z}/a_{ii}$ into their prime factors using the fact that $\mathbb{Z}/ab = \mathbb{Z}/a \times \mathbb{Z}/b$ if $(a, b) = 1$. We also have that if $a_{ii} = 1$, we may factor out $\mathbb{Z}/\mathbb{Z} = \{e\}$, and if $a_{ii} = 0$, then it is simply $\mathbb{Z}$. □

§20 Day 20: Rings (Nov. 14, 2025)

Definition 20.1. A ring $(R, +, \cdot)$ is a set equipped with an addition and multiplication operation such that the additive and multiplicative identities are distinct. It must also satisfy the below,

(i) $(R, +, 0)$ is an abelian group with respect to its addition operation.

(ii) $(ab)c = a(bc)$, associative law.

(iii) For all a, $1a = a1 = a$, multiplicative identity.

(iv) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$, distributive law.

Note that there are such things as "rings without unit" and "commutative rings".

Lemma 20.2. In a ring, $0 \cdot a = 0$.

Proof. $0 = (0 + 0)$, so $0a = (0 + 0)a = 0a + 0a$ implies $0a = 0$. □

Lemma 20.3. $(-a) \cdot b = a(-b) = -(ab)$ and $(-a)(-b) = ab$.

Proof. This is true by applying the distributive law. □

Here are some examples of rings.

(a) $R = \{0, 1\}$, i.e., it has its additive and multiplicative identity only. Isomorphism is exactly what you would expect, $R \cong \mathbb{Z}/2$.

(b) $\mathbb{Z}$

(c) $\mathbb{Z}/n$

(d) $M_{n\times n}(R)$, where R is a ring.

As an aside, $M_{n\times n}(M_{m\times m}(R)) \cong M_{mn\times m}(R)$. Given any set X, $M_{X\times X}(R)$ is the set of $X \times X$ matrices with entries in R and finitely many nonzero entries in each column.

(e) Polynomials: given a ring R, we have $R[x] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in R\}$. Similarly, $\mathbb{Z}[x]$ and $\mathbb{R}[y]$ are rings too. Let $f = \sum a_i x_i$ and $g = \sum b_i x_i$; we have

$$f \cdot g = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k.$$

(f) Power series: given any R, we have $R[\![x]\!] = \left\{\sum_{i=0}^{\infty} a_i x^i\right\}$. As some examples, we have that

$$\sum_{n=0}^{\infty} \frac{1}{n!} x^n \in R[\![x]\!], \quad \sum_{n=0}^{\infty} n! x^n \in R[\![x]\!].$$

(g) If G is a group and R is a commutative ring, the group-ring of G with coefficients in R is

$$RG = \left\{ \sum_{\text{finite} i} a_i g_i \mid g_i \in G, a_i \in R \right\},$$

where $(\sum_i a_i g_i)(\sum_j b_j h_j) = \sum_{i,j} a_i b_j g_i h_j$. We denote $\underline{0} = \sum_{\varnothing}$ and $\underline{1} = 1_R \cdot e_G$.

We also have that

$$\mathbb{Z}_{\text{ring}}\mathbb{Z}_{\text{group}} \cong \mathbb{Z}\langle x \rangle = \left\{ \sum_{i\in\mathbb{Z}} a_i x^i \mid a_i \in \mathbb{Z} \right\},$$

which are the Laurent polynomials with integer coefficients.

§21 Day 21: Ring Morphisms, Cayley–Hamilton, Ideals (Nov. 19, 2025)

Definition 21.1. A ring R is formally defined as $(R, +, \cdot, 0 \neq 1)$, where $(R, +, 0)$ is an Abelian group. $(R, +, 1)$ is a monoid (group without inverses). Note the distributive laws, commutative rings, and rings without identities.

Definition 21.2. Let R, S be rings, and let $\varphi : R \to S$; we say φ is a morphism if it preserves structure, i.e., $\varphi(x + y) = \varphi(x) + \varphi(y)$, and $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

In this sense, the collection of rings is a category. We now give examples.

(i) $\mathbb{Z} \to \mathbb{Z}/n$ is a ring morphism; as an aside, the kernel is a ring.

(ii) $R \to M_{2\times 2}(R)$, where x maps to the diagonal matrix with entries x on its diagonal, is a morphism.

(iii) $R \to R[t]$ by $a \mapsto at^0 + 0t^1 + \dots$.

(iv) $\mathrm{ev}_u : R[x] \to R$ for $u \in R$; this only makes sense if R is commutative, or if u is central.

(v) Fix commutative R and let $\varphi : G \to H$ be a morphism of groups; we get a morphism $\varphi_* : RG \to RH$, i.e., $\sum a_i g_i \to \sum a_i \varphi(g_i)$. The "group ring construction with fixed R" is a functor. Fixing a group G, let $\varphi : R \to S$ be a morphism of commutative rings $\varphi_* : RG \to SG$ by $\sum a_i g_i \mapsto \sum \varphi(a_i) g_i$. The group ring construction is a bifunctor, where the product of commutative rings with groups is taken into rings.

(vi) $M_{n\times n}(R[x])$ and $M_{n\times n}(R)[x]$ are isomorphic.

As an aside, let us discuss the Cayley–Hamilton theorem.

Theorem 21.3 (Cayley–Hamilton)**.** A matrix annihilates its characteristic polynomial; i.e., let R be a commutative ring, and let $A \in M_{n\times n}(R)$. Let $\chi_A(t) = \det(tI - A) \in R[t]$. Then $\chi_A(A) = 0$.

Proof. For any matrix M over any commutative ring, the adjugate matrix $\operatorname{adj} M$ of M is defined using the minors of M, which satisfy $\det(M) I_n = (\operatorname{adj} M) M$. We will use this with $M = tI - A$ over the ring $R[t]$ and find that in the ring $M_{n\times n}(R[t])$, we have[23]

$$\chi_A(t) I_n = \det(tI - A) I_n = (\operatorname{adj}(tI - A))(tI - A),$$

where, since $M_{n\times n}(R[t]) \cong M_{n\times n}(R)[t]$, on the latter, there exist sa linear evaluation at $t = A$ map $\mathrm{ev}_A : M_{n\times n}(R)[t] \to M_{n\times n}(R)$ defined by $\sum B_k t^k \mapsto \sum B_k A^k$ by putting A to the right of all the coefficients. This evaluation map is not multiplicative, but annihilates anything that has a right factor of $(tI - A)$. Hence, under ev_A the above equality becomes $\chi_A(A) I_n = 0$. □

Claim 21.4. If $\varphi : R \to S$ is a morphism of rings, then $\operatorname{im} \varphi$ is a subring of S.

However, $\ker \varphi$ isn't a ring as $1 \notin \ker \varphi$. Yet, it is a rng (ring without identity). Namely, $0 \in \ker \varphi$, and $\ker \varphi$ is additively and multiplicatively closed; indeed, we have that $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = 0 \cdot 0 = 0$. We can prove a stronger theorem; in fact, if $x \in \ker \varphi$ and $a \in R$, then $ax \in \ker \varphi$ and $xa \in \ker \varphi$, since

$$\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0.$$

[23] ik i'm inconsistent with using I_n and I, i'm just leaving it in when necessary to determine indices

Definition 21.5. An *ideal* I in a ring R is a subset $I \subset R$ such that I is a subrng[24] and, for all $a \in R$, we have $aI \subset I$ and $Ia \subset I$, which is equivalent to $RI = I = IR$.

We ask; if $I \subset R$ is an ideal, does there exist $\varphi : R \to S$ such that $I = \ker \varphi$? Indeed, the answer is yes, since, given $I \subset R$ an ideal in a ring R¡ we can define $x \sim y$ if $x - y \in I$, where $\sim$ is an equivalence relation by group theory. Define $R/I = \{[x] \mid x \in R\}$, and $0_{R/I} := [0] = I$, $1_{R/I} := [1] = 1 + I$. More generally, we write

$$[x] = \{y \mid x - y \in I\} = x + I,$$

so $[x] + [y] = [x + y]$, which is well-defined as checked in Abelian group theory. We have that $[x][y] := [xy]$, so we can claim well-definedness. In particular, let $x' \sim x$ and $y' \sim y$; is it true that $[x'y'] = [xy]$? We see this from writing

$$xy - x'y' = xy - xy' + xy' - x'y' = x(y - y') + (x - x')y' = x(0) + (0)y' = 0.$$

[24] yes, subrng, not subring

§22 Day 22: Isomorphism Theorems for Rings (Nov. 21, 2025)

We define a ring modulo an ideal by the quotient

$$\pi : R \to R/I = \{[x]_I \mid x \in R\},$$

where $[x]_I = x + I$; R/I inherits identities (0 and 1) and the addition and multiplication from R, where $IR = RI = I$.

Theorem 22.1. R/I is a ring, and π is a ring morphism with $\ker \pi = I$.

As an example, we have that $\mathbb{Z}/n\mathbb{Z}$ is a ring, for which $\mathbb{Z}$ is a ring, and $n\mathbb{Z}$ is a rng. Let $R = \mathbb{R}[x]$ be the ring of polynomials in the reals, and consider the ideal $I = \langle x^2 + 1 \rangle$ (this notation denotes the smallest ideal containing $x^2 + 1$). We have that R/I is indeed the complex numbers, but we will prove this later. As an aside, in a general commutative ring $\mathbb{R}$, we have that $I = \langle x_1, \ldots, x_n \rangle$ with $x_i \in R$ is given by

$$I = \langle x_1, \ldots, x_n \rangle = Rx_1 + \cdots + Rx_n.$$

Indeed, the above is closed by addition and multiplication. We now discuss the isomorphism theorems.

Theorem 22.2 (Iso. 1)**.** Let $\varphi : R \to S$ be a morphism; then $R/\ker \varphi \cong \operatorname{im} \varphi$.

From the first isomorphism theorem of groups, we see that there is an isomorphism between the additive abelian groups $(R, +)$ and $(S, +)$; we just need to check that φ preserves the multiplication group defined on R and S as well. Recall, that the second isomorphism theorem for groups G is given by $HK/K \cong H/(H \cap K)$ when $H < G$ and $K \lhd G$. We obtain something similar for rings, i.e.,

Theorem 22.3 (Iso. 2)**.** Let R be a ring, and let S be a subring and I be an ideal. Then

$$\frac{S + I}{I} \cong \frac{S}{S \cap I},$$

where we may regard $S + I$ as another subring, and $S \cap I$ as an ideal of S.

In this case, we also have the established isomorphism on the additive group, so it suffices to check that the isomorphism holds for the multiplicative parts too.

Theorem 22.4 (Iso. 3)**.** Let R be a ring, and let I, J be ideals of R; if $I \subset J$, then

$$\frac{R/I}{J/I} \cong \frac{R}{J}.$$

Theorem 22.5 (Iso. 4)**.** Let R be a ring; fix an ideal $I \subset R$; there is an inclusion-preserving bijection between ideals J such that $I \subset J \subset R$ and ideals in R/I, given by $I \subset J \iff J/I \subset R/I$.

As an example in the context of rings, consider $\varphi : R_1 \to \mathbb{C}$ given by $R_1 = \mathbb{R}[x]/\langle x^2 + 1 \rangle$. If φ is given by $x \mapsto i$, then $\varphi(x^2 + 1) = i^2 + 1 = 0$, meaning that the ideal $\langle x^2 + 1 \rangle$ vanishes under φ. Moreover, φ is a surjective map, since we may readily check that any polynomial $f \in \mathbb{R}[x]$ reduces to $a + bx$ by adding and subtracting multiples of $x^2 + 1$; indeed, $a + bx \mapsto a + bi$, so $R_1 = \{[f]_{\langle x^2+1 \rangle}\} = \{[a + bx]\}$ over all $a, b \in \mathbb{R}$, from which we observe φ has trivial kernel. Per the first isomorphism theorem of rings, $R_1/\ker \varphi \cong \operatorname{im} \varphi = \mathbb{C}$, proving our example from the beginning of this lecture.

In preparation for next lecture, let us define fields.

Definition 22.6. A field is a commutative ring F such that $F \setminus \{0\}$ is a group under multiplication. All techniques from linear algebra work in any such field F.

§23 Day 23: Integral Domains, Maximal and Prime Ideals (Nov. 26, 2025)

We discuss "better rings and ideals" today, but we will start with an aside.

Definition 23.1. A division ring is a field in which $\cdot$ isn't necessarily commutative. More formally, it's a ring R in which, if $x = 0$, then there exists y such that $xy = yx = 1$.

As an example, consider the quaternions $\mathbb{H} = \{a\ell + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, modded out by $i^2 = j^2 = h^2 = -1$, and that $jk = i$, $ki = j$, and $ij = k$. The quaternions encode a lot of 3-dimensional geometry, of which they are non-commutative and the division ring $a + bi + cj + dk$ has an inverse unless $a = b = c = d = 0$. Indeed, the inverse is given by

$$\frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

We make the following definition,

Definition 23.2. $\overline{a + bi + cj + dk} := a - bi - cj - dk$.

If $z = a + bi + cj + dk$, then $z \cdot \overline{z} = |z|^2$. If $|z|^2 \neq 0$, then $(z\overline{z})/|z|^2 = 1$. From this point onwards, all rings are assumed to be commutative unless mentioned otherwise.

Theorem 23.3. If I is an ideal in R, then R/I is a field if and only if I is maximal (i.e., if $J \supset I$ is also an ideal, then $J = I$).

Proof. We proceed by checking both implications.

($\Leftarrow$) Assume I is maximal; we need to show that R/I is a field. Indeed, R/I is commutative, and if $[x] \neq 0$, then there exists y such that $[x][y] = [1]$. Let $J = Rx + I$; we may see that $J + J \subset J$ and $RJ = JR = J$; if $1 \notin J$, we would have that J is an ideal strictly containing I, since $x \in J \setminus I$, but I was assumed to be maximal. Thus, we see that $1 \in J$, and so there exists y such that $1 = yx + i$ for some $i \in I$. Thus, $[yx] = [1]$, and we have $[y][x] = 1$, so $[x]$ is invertbile.

($\Rightarrow$) Now, assume J is an ideal in R and $J \supsetneq I$. Let $x \in J \setminus I$ such that $[x]_I$ is invertible, as R/I is a field, and $[x]_I \neq 0$; this means there exists y such that $[xy] = 1$, so $xy^{-1} \in I$, and equivalently, $-1 \in -xy + I$. However, this means $1 \in xy + I$, which is a contradiction. □

We now give some examples. $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$ if p is prime, so $\mathbb{Z}/p\mathbb{Z}$ is a field. If $R = \ell^\infty$, i.e., the set of bounded sequences of real numbers, then $I_n = \{(a_i) : a_n = 0\}$ is a maximal ideal too. We have that $\ell^\infty/I_n \cong \mathbb{R}$, and $\pi_n : \ell^\infty \to \ell^\infty/I_n$ by $\pi(\{a_i\}) = a_n$; we may define $I_\infty = \{(a_i) : a_i \to 0\}$.

Notice, however, that I_∞ is not maximal. Indeed, $J = \{(a_i) : a_{2i} \to 0\} \supsetneq I$.

Theorem 23.4. Every ideal is contained in a maximal ideal.

Proof. Use Zorn's lemma or the axiom of choice. □

Take $J \supset I_\infty$; there are 2^{2^ω} because $|\beta\mathbb{N}| = 2^{2^\omega}$ (the set of ultrafilters on $\mathbb{N}$ coincides with the Stone–Čech compactification of $\mathbb{N}$). We claim that $\ell^\infty/J \cong \mathbb{R}$.

Proof. Consider the map $\mathbb{R} \to \ell^\infty/J$, $x \mapsto (x)_{n\in\mathbb{N}}$. We have that $\lim_j : \ell^\infty \to \ell^\infty/J = \mathbb{R}$, where $\lim_j(a_n) = \pi_J(a_n)$. Then the limit w.r.t. the index j of the infinite sequence (a_i) with each $a_i \equiv c$ is given by c, $\lim_j(a_i) = 0$ if (a_i) is such that $a_i \to 0$, and $\lim_j(a_i) = \lim_{i\to\infty}(a_i)$ if the conventional limit exists. $\lim_j$ is additive and multiplicative, so ℓ^∞/J is a field. Moreover, we see that every sequence in ℓ^∞ converges in J, so I_∞ cannot be a maximal ideal, as it is contained in J. □

Note that the set of commutative rings contains the set of integral domains, which also contains the set of fields.

Definition 23.5. An integral domain is a commutative ring with no zero divisors, i.e., $ab = 0$ implies $a = 0$ or $b = 0$.

We give some examples of integral domains. $R = \{0, 1\}$ is a domain. Any field, including $\mathbb{Z}$ is a domain; $\mathbb{Z}[x]$ is a domain. For non-examples, consider $\mathbb{Z}/6$ (where $2 \cdot 3 = 0$) and $M_{2\times2}(\mathbb{Z})$ are not domains.

Lemma 23.6 (Cancellation Law)**.** In a domain, if $ab = ac$ and $a \neq 0$, then $b = c$.

Proof. $ab = ac$ implies $a(b - c) = 0$, but $a \neq 0$, so $b - c = 0$, and therefore $b = c$. □

Theorem 23.7. If $I \subset R$ is called "prime" if it satisfies the property that $a \cdot b \in I$ implies $a \in I$ or $b \in I$.

Proof. Assume that R/I is a domain; if $ab \in I$, then $[ab] = [0]$ in R/I, i.e., $[a][b] = 0$, so $[a]$ or $[b] = 0$, so a or b is in I. This means I is prime. In the other direction, if $[a][b] = 0$, then $[ab] = 0$, so $ab \in I$. This means a or $b \in I$ implies $[a]$ or $[b] \in I$. □

Claim 23.8. A maximal ideal is prime.

Proof. If I is a maximal ideal, then R/I is a field, which is a domain, so I is a prime ideal. □

§24 Day 24: Primes and Irreducibles (Nov. 28, 2025)

From here on, we assume that all rings are commutative. Recall that R/I is a field if and only if I is a maximal ideal, and R/I is a domain (it admits no zero divisors) if and only if I is prime ($ab \in I$ implies $a \in I$ or $b \in I$). All rings are assumed to be domains!

Definition 24.1. We write $a \mid b$ (i.e., a divides into b) if $a \neq 0$ and there exists q such that $qa = b$.

Definition 24.2. If $a \mid b$ and $b \mid a$, we say that "a and b are associates" and write $a \sim b$.

As a quick lemma, $a \mid b$ and $b \mid c$ implies $a \mid c$, and the other direction holds. a and b being associates is equivalent to the existence of u, v such that $au = b$, $bv = a$, and $uv = 1$.

Definition 24.3. R^* is the set of invertible elements in R; we call such elements *units*, and R^* is always a group.

For examples, consider $\mathbb{Z}^* = \{\pm 1\}$ and $\mathbb{Q}[x]^* = \mathbb{Q} \setminus \{0\}$. The moral is that $a \sim b$ if and only if there exists $u \in R^*$ such that $au = b$, where the equivalence relation comes from the group action $R \setminus \{0\} \curvearrowleft R^*$, We may regard $R \setminus \{0\}/R^*$ as the classes of associativity.

A nonzero nonunit $x \in R$ is called *irreducible* if $x = ab$ implies $a \in R^*$ or $b \in R^*$, and a nonzero nonunit $x \in R$ is called *prime* if $x \mid ab$ implies $x \mid a$ or $x \mid b$.

Claim 24.4. Prime implies irreducible.

Proof. Suppose p is a prime and $p = ab$. Then $p \mid ab$ implies $p \mid a$ or $p \mid b$; without loss of generality, we will assume the former. This means that there exists some u such that $a = pu$, and $a = abu$ implies $1 = bu$, so $b \in R^*$. □

The converse need not hold; indeed, consider the classic example $\mathbb{Z}[\sqrt{-5}]$, where 2 is irreducible but not prime. We may write

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[x]/\left\langle x^2 + 5 \right\rangle;$$

2 is not prime, since 2 divides into $6 = (1+\sqrt{-5})(1-\sqrt{-5})$, but 2 does not divide into either of $1 \pm \sqrt{-5}$. Let us give some background; recall that $\|a + bi\|^2 = a^2 + b^2 = (a+bi)\overline{a+bi}$, so $\left\|a + b\sqrt{-5}\right\|^2 = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2 \in \mathbb{Z}$; for $z_1, z_2 \in \mathbb{Z}[\sqrt{-5}]$, we have that $\|z_1 z_2\|^2 = \|z_1\|^2 \cdot \|z_2\|^2$ and $\|2\|^2 = 4$. Since $2 = z_1 \cdot z_2$ in R, $\|2\|^2 = \|z_1\|^2 \|z_2\|^2 = 4$ in $\mathbb{Z}$, it must be that $|z_1|^2$ is given by 1, 2, or 4, so one of the factors must be trivial.

Claim 24.5. $p \in R$ is prime if and only if $\langle p \rangle = pR$ is a prime ideal, i.e., $p \mid ab$ implies $p \mid a$ or $p \mid b$ if and only if $ab \in I$ implies $a \in I$ or $b \in I$.

§25 Day 25: Rings like $\mathbb{Z}$ (Jan. 7, 2025)

Recall that, for commutative rings, R/I is a field if and only if I is maximal, and R/I is a domain (admits no zero divisors) if and only if I is prime, i.e., $ab \in I$ implies $a \in I$ or $b \in I$.

Now, we assume that our rings are not commutative domains. If p is prime, then $p \mid ab$ implies $p \mid a$ or $p \mid b$; equivalently, $\langle p \rangle$ is prime. If x is irreducible, then x is *not* 0, not a unit, and $x = ab$ implies $a \in R^*$ or $b \in R^*$. In general, prime implies irreducible but the converse is not necessarily true.

Recall that the properties of the integers are as follows,

(i) Unique factorization, i.e., any integer n can be written as $p_1 \dots p_n$. Equivalently, if a ring R possesses this property, we call it a unique factorization domain (UFD).

(ii) $\langle 4, 6 \rangle = \langle 2 \rangle$, i.e., even numbers. This property means R is a principal ideal domain (PID).

(iii) There exists $|\cdot|$, i.e., $347 = 37 \cdot 9 + 14$, where $|14| > |37|$. We say that R is an Euclidean domain here.

Definition 25.1. R is a *unique factorization domain* if any $x \neq 0$ can be written as $x = up_1p_2 \dots p_k$, where $u \in R^*$ and each p_i is prime.

Definition 25.2. R is a *principal ideal domain* if every ideal in it is "principal", meaning generated by a single element.

Definition 25.3. R is a *Euclidean domain* if there exists $e : R \setminus \{0\} \to \mathbb{N}$ such that $e(ab) \geq e(a)$ and, for all $a, b \neq 0$, there exists q, r such that $a = b \cdot q + r$, and $r = 0$ or $e(r) < e(b)$.

Theorem 25.4. Every Euclidean domain is a principal ideal domain, and every principal ideal domain is a unique factorization domain.

As an example, $\mathbb{Q}[t]$ is a Euclidean domain and a PID, but $\mathbb{Z}[t]$ and $\mathbb{Q}[s, t]$ is a UFD but not a PID.

Theorem 25.5. If R is a UFD and $x = up_1 \dots p_n$ and $x = vq_1 \dots q_m$, where u, v are units and each p_i, q_i are primes, then $(p_1, \dots, p_n)$ and $(q_1, \dots, q_m)$ are the same up to units and a permutation.

Proof. We konw that $p_1 \mid q_1 \dots q_m$, so by definition of p_1 being prime, $p_1 \mid q_j$ for some j. Without loss of generality, $p_1 \mid q_1$, so $p_1 \sim q_1$. We may induct on this process to obtain our desired result. □

Claim 25.6. $p_1 \mid q_1$ and q_1 being prime means $p_1 = q_1$ up to multiplication by a unit.

Proof. Indeed, $q_1 = p_1 \cdot a$, but q_1 is irreducible, so either p_1 is a unit or a is a unit (with only the latter being possible). □

Theorem. Euclidean domains are PIDs.

We start with some examples.

(i) $\mathbb{Z}$. Let $e : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ and $e(k) = |k|$.

(ii) $\mathbb{Q}[t]$ or $F[t]$, where F is a field. LEt $f = \sum_{i=1}^{n} a_i t^i$, where $a_n \neq 0$ and $e(f) = \deg f = n$.

Claim 25.7. e is a Euclidean domain.

This is clear from $e(gf) \geq e(f)$ assuming $f, g \neq 0$; the latter is clear from long divison. We now prove the theorem.

Proof. Suppose R is a Euclidean domain with norm e. Suppose $I \subset R$ is an ideal. Let $x \neq 0$ be an element of I with the least possible e. We claim that $I = \langle x \rangle$; indeed, suppose $y \in I$, write $y = q \cdot x + r$, where $e(r) < e(x)$ or $r = 0$. Then $r = y - qx \in I$, implying $r = 0$ or $y \in \langle x \rangle$. □

Theorem. PIDs are UFDs.

Lemma 25.8. If R is a PID, then R is *Noetherian*, meaning you cannot find a sequence $I_1, I_2, \ldots$ of ideals in R such that $I_1 \subsetneq I_2 \subsetneq I_3 \ldots$.

Proof. Suppose such a sequence existed. Then take J to be their union; it is clear that J is an ideal, as R is a PID, meaning $J = \langle x \rangle$ for some x, so $x \in \bigcup I_i$, so there exists N such that $x \in I_n \subset I_{n+1} \ldots$. Thus, $I_n \supset \langle x \rangle = J$ and $I_{n+1} \supset \langle x \rangle = J$, whence $I_n = I_{n+1} = \cdots = J$. □

Lemma 25.9. If R is a PID, and $x \in R$ with $x \neq 0$, then x is either a unit or a product of irreducibles.

Proof. Suppose not; then there exists $x \in R$ that is not a unit, not irreducible, and not a product of irreducibles. Since x is not irreducible, $x = x_1 \cdot x_1'$ such that $x_1, x_1' \notin R^*$; at leasto ne of x_1 and x_1' are not a product of irreducibles. Without loss of generality, x_1 isn't a product of irreducibiles; continue in the same fashion, and we get two seqeunces; x_k and x_k' such that $x_k, x_k' \notin R^*$, where $x_k = x_{k+1} x_{(k+1)'}$. Now, consider that

$$\langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq \ldots.$$

This contradicts the previous lemma, meaning that for some index (we will pick that index to be 2 for now) $x_2 \in \langle x_1 \rangle$, then $x_2 = ax_1 = a \cdot x_2 \cdot x_2'$, implying x_2' is a unit. □

§26 Day 26: PIDs, UFDs, and Greatest Common Divisors (Jan. 9, 2026)

Recall that a principal ideal domain (PID) states that all ideals are generated by a single element. A unique factorization domain (UFD) admits unique factorization of all nonzero x into $up_1 \dots p_n$, where u is a unit and $p_1, \dots, p_n$ are primes, up to uniqueness of unit and reordering of primes. A euclidean domain admits a function $e : R \setminus \{0\} \to \mathbb{N}$ such that $e(ab) \geq e(a)e(b)$ where, for all $a, b \neq 0$, there exists $a = b \cdot q + r$, where either $r = 0$ or $e(r) < e(b)$. It was shown that if R is a PID and $x \neq 0$, then x can be written as a product of irreducibles. It remains to check the following proposition.

Proposition 26.1. In a PID, irreducible elements are prime.

Proof. If x is irreducible, $\langle x \rangle$ is maximal; indeed, suppose $\langle x \rangle \subset J \subset R$ where J is an ideal, then by virtue of being in a PID, there exists a such that $J = \langle a \rangle$. Since $x \in J$, there exists b such that $x = a \cdot b$, but x is irreducible, so either $a \in R^*$, which is contradictory as now $J = \langle a \rangle = R$, or $b \in R^*$, meaning $\langle x \rangle = \langle a \rangle$ as $a = xb^{-1}$. Thus, $\langle x \rangle$ is maximal, so $\langle x \rangle$ is prime, and x is prime. □

As an aside, in a UFD, irreducible elements are prime as well.

Definition 26.2. If $a, b \in R$, g is a *greatest common divisor* of a and b if $g \mid a$, $g \mid b$, and $g' \mid a$, $g' \mid b$ implies $g' \mid g$.

Claim 26.3. If g, g' are both gcds of a, b, then $g' = ug$ where $u \in R^*$, i.e., gcds are unique up to multiplying by a unit.

Proof. By the proposition and the fact that x can be written as a product of irreducibles in PIDs, we see that $g' \mid g$ by symmetry and $g \mid g'$ as well, whence we often call this the "gcd". □

In UFDs, gcds are "easy", since if $g \mid a$, we can write

$$a = u \prod_\alpha p_\alpha^{n_\alpha}, g = v \prod_\alpha p_\alpha^{k_\alpha} \iff k_a \leq n_\alpha$$

for all α. Note that all but finitely many of the n_α and k_α are zero. In this manner, if $b = w \prod_\alpha p_\alpha^{m_\alpha}$, we obtain

$$\gcd(a, b) = \prod p_\alpha^{\min(m_\alpha, n_\alpha)}.$$

As an example, $\gcd(30, 18) = 6$ and $\gcd(x^2 - 2x + 1, x^2 - 1)$ in $\mathbb{Q}[x]$ is $x - 1$ by factorizing the former as $(x - 1)^2$ and the latter as $(x - 1)(x + 1)$.

Theorem 26.4. If R is a PID and $a, b \in R$, then $\langle a, b \rangle = \langle \gcd(a, b) \rangle$.

Proof. By PID, there exists y such that $\langle y \rangle = \langle a, b \rangle$, implying $y \mid a$ and $y \mid b$, so $y \mid g$, whence $g \in \langle y \rangle$, which gives the $\supset$ direction. We will discuss the other direction next time. □

Corollary 26.5. In a PID, $a, b \in R$, $g = \gcd(a, b)$, there exists s, t such that $g = sa + tb$.