Perry Hart
MATH 602
Fall 2018

Abstract

These notes are based on Tony Pantev's "Algebra I" lectures given at UPenn. Any mistake in what follows is my own.

(Lecture 1)

Definition. A *(left) action of a group G on a set S* is a homomorphism $\theta : G \to \mathrm{Aut}(S)$. Equivalently, a group action is a function $\alpha : G \times S \to S$ such that

- $\alpha(g, \alpha(g', x)) = \alpha(gg', x)$ and
- $\alpha(e, x) = x$

for any $g, g' \in G$ and $x \in S$.

Definition. A *right group action* is a function $\beta : S \times G \to S$ such that

- $\beta(\beta(x, g), g') = \beta(x, gg')$ and
- $\beta(x, e) = x$

for any $x \in S$ and $g, g' \in G$.

Exercise 1. Find a homomorphism representing a right group action $a : S \times G \to S$.

Proof. Given a, define $f : G^{\mathrm{op}} \to \mathrm{Aut}(S)$ by $g \mapsto (x \mapsto a(x, g))$. This is a homomorphism. Conversely, given a homomorphism $f : G^{\mathrm{op}} \to \mathrm{Aut}(S)$, define $a(x, g) = f(g)(x)$. This is a right action. $\square$

Remark 1. Every group action $\theta : G \to \mathrm{Aut}(S)$ factors through a *tautological action* $H \leq \mathrm{Aut}(S)$.

$$\begin{tikzcd} G \arrow[r, "q"] \arrow[dr, "\theta"'] & G/\ker(\theta) \arrow[d, "\cong"] \\ & \theta(G) \end{tikzcd}$$

Definition. Given a group action $\theta : G \to \mathrm{Aut}(S)$, we say that θ is *faithful* or *effective* if it is injective.

Definition. Let $\theta : G \to \mathrm{Aut}(S)$ be a group action and $x \in S$.

1. Define the *stabilizer subgroup of x* as $\mathrm{Stab}_\theta(x) = \{g \in G \mid g \cdot x = x\}$.
2. Define the *orbit of x* as $\mathrm{Orb}_\theta = \{y \in S \mid \exists g \in G \text{ s.t. } g \cdot x = y\}$.

Note 1. Note that the orbits of an action behave as equivalence classes.

Exercise 2.

1. Given an action $a : G \times S \to S$, show that the equivalence relation $R_a \subset S \times S$ is the projection of $\mathrm{Graph}(a) \subset G \times S \times S$ onto $S \times S$.
2. If $\theta : G \to \mathrm{Aut}(S)$ is a group action and $x \in S$, then show that the function $G/\mathrm{Stab}_\theta(x) \to \mathrm{Orb}_\theta(x)$ given by $[x] \mapsto g \cdot x$ is well-defined and bijective. Thus, if G is finite, then $|\mathrm{Orb}_\theta(x)| = \frac{|G|}{|\mathrm{Stab}_\theta(x)|}$.

Proof. Notice that $R_a = \{(s, gs) : s \in S,\, g \in G\}$. $\square$

Remark 2. There is a set bijection $G/\mathrm{Stab}\, x \longleftrightarrow \mathrm{Orb}(x)$ given by $[g] \mapsto gx$ for any $x \in S$, even if S is infinite.

Example 1. Any action $\theta : G \to \mathrm{Aut}(S)$ induces the following group actions.

1. $\mathcal{P}(\theta) : G \to \mathrm{Aut}(\mathcal{P}(S))$ given by $g \mapsto (T \mapsto \theta(G)(T))$.
2. For a subset $T \subset S$ that is stable under θ, $\theta_T : G \to \mathrm{Aut}(T)$ given by $g \mapsto \theta(g) \restriction_T$.
3. For a set X, $\theta^* : G \to \mathrm{Aut}(X^S)$ given by $g \mapsto (f \mapsto f \circ \theta(g^{-1}))$.
4. $\theta_* : G \to \mathrm{Aut}(S^X)$ given by $g \mapsto (f \mapsto \theta(g) \circ f)$.
5. $\theta^{\times n} : G \to \mathrm{Aut}(S^n)$ given by $g \mapsto ((x_1, \ldots, x_n) \to (gx_1, \ldots, gx_n))$

Example 2. Let $R \subset S \times S$ be an equivalence relation such that $\theta^{\times 2}(g)(R) = R$ for each $g \in G$. Then ${}^{G}\!/\!_{R} : G \to \mathrm{Aut}({}^{S}\!/\!_{R})$ given by $g \mapsto ([s] \mapsto [gs])$ is an action.

Example 3. Let $a : G \times S \to G$ be an action. If $S = G$, then we have the

- *left regular action* given by $a(g, x) = gx$,
- the *right regular action* given by $a(g, x) = xg^{-1}$, and
- the *conjugation action.* given by $a(g, x) = gxg^{-1}$

In general, only the last of these maps elements to automorphisms of G.

Example 4. If θ denotes conjugation, then we call ${}^{G}\!/\!_{Z(G)} \cong \mathrm{im}(\theta) := \mathrm{Inn}(G)$ the subgroup of *inner automorphisms of* G, which is a normal subgroup. We call the quotient ${}^{\mathrm{Aut}(G)}\!/\!_{\mathrm{Inn}(G)}$ the group of *outer automorphisms of* G, denoted by $\mathrm{Out}(G)$.

Remark 3. Let $\mathrm{Aut}_\phi(S) \leq \mathrm{Aut}(S)$ preserve the structure ϕ of S. Then

$$\begin{tikzcd} G \arrow[r, "\theta"] \arrow[dr] & \mathrm{Aut}(S) \arrow[d] \\ & \mathrm{Aut}_\phi(S) \end{tikzcd}$$

(Lecture 2)

Definition.

1. If $(S, +)$ is an abelian group and $\theta : G \to \mathrm{Aut}_+(S)$ an action, then we call S a *left G-module.*
2. If S is also a vector space over k and G is k-linear, then the action is called a *k-linear representation of G.*

Example 5. (The permutation representation) Set $S = \{1, \ldots, n\}$ and $G = S_n$. Then $\theta^*(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$, where $x_i \in X$ for a fixed set X. If X is a field, then $X^S \cong X^n$ is an n-dimensional vector space and θ^* is an X-linear representation of S_n.

$$\begin{tikzcd} G \arrow[r, "\theta^*"] \arrow[dr] & \mathrm{Aut}(X^n) \\ & \mathrm{GL}_n(X) \arrow[u, hook] \end{tikzcd}$$

Remark 4. Our previous example holds for any action $\theta : F \to \mathrm{Aut}(S^k)$ where k is a field. This is called the *regular representation of* G.

Example 6. Given an action $\theta : G \to \mathrm{Aut}(S)$, we get an action $\mathcal{P}(\theta) : G \to \mathrm{Aut}(\mathcal{P}(S))$ given by $g \mapsto (X \mapsto \theta(g)(X))$. Since $\mathcal{P}(S) \sim (\mathbb{Z}_2)^S$, we see that $\mathcal{P}(\theta)$ is a $\mathbb{Z}_2$-linear representation of G. Therefore, any action of G on S induces a representation of G.

Example 7. (Galois theory) Let $f(x) = a_n x^n + \cdots + a_0$ over $\mathbb{Q}$ where $a_n \neq 0$. We know $f(x) = a_n(x-\beta_1)\cdots(x-\beta_n)$ for some $(\beta_1, \ldots, \beta_n) \in \mathbb{C}^n$. It's true that each $\beta_i = f(a_0, \ldots, a_n)$ for some algebraic function f if and only if a certain symmetry group of $\{B_i\}$ has a special property (to be covered next semester).

Let $\mathbb{Q}[\tilde{\beta}] \coloneqq \mathbb{Q}[\beta_1, \ldots, \beta_n] = \{F(\beta_1, \ldots, \beta_n) : F \in \mathbb{Q}[x_1, \ldots, x_n]\}$. Let the Galois group of f

$\mathrm{Gal}(f) \coloneqq \{\sigma \in S_n : \exists g(\sigma) : \mathbb{Q}[\tilde{\beta}] \to \mathbb{Q}[\tilde{\beta}]$ bijection with $g(F(\beta_1, \ldots, \beta_n)) = F(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)})$ for $F \in \mathbb{Q}[x_1, \ldots, x_n]\}$.

Exercise 3. Show that $g : G \to \mathrm{Aut}(\mathbb{Q}[\tilde{\beta}])$ is a homomorphism where $G \coloneqq \{g(\sigma) : \sigma \in \mathrm{Gal}(f)\}$.

In fact, G is a representation of $\mathbb{Q}[\tilde{\beta}]$, giving

$$\begin{tikzcd} G \arrow[r] \arrow[dr] & \mathrm{Aut}(\mathbb{Q}[\tilde{\beta}]) \\ & \mathrm{GL}_{\mathbb{Q}}(\mathbb{Q}[\tilde{\beta}]). \arrow[u, hook] \end{tikzcd}$$

Now, consider $f(x) = (x^2-3)(x^2-5)$, which has roots $\{\pm\sqrt{3}, \pm\sqrt{5}\}$. Then $\mathrm{Gal}(f) \subset S_4$. Note that $g \cdot q = q$ for each $g \in \mathrm{Gal}(f)$ and $q \in \mathbb{Q}$. If $\sigma(1) = 3$, then $g(\sigma)(\beta_1^2) = g(\sigma)(3) = \beta_3^2 = 5$, which is impossible. By similar reasoning, it follows that $\mathrm{Gal}(f) = \{(1), (12), (34), (12)(34)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(Lecture 3)

Notation. Let $\{\text{Orbits}\} \coloneqq G \diagdown S$.

Definition. Let $\theta : G \to \mathrm{Aut}(S)$ be an action.

1. We say that θ is *transitive* if for any $s, s' \in S$, there is some $g \in G$ such that $g(s) = s'$.
2. We say that θ is *simple* if $\mathrm{Stab}_\theta(x) = \{e\}$ for any $x \in S$.
3. If θ is both simple and transitive, then it's called a *G-torsor*. In this case, if $x \in S$, then $f : G \to S$ given by $g \mapsto \theta(g)(x)$ is a bijection.

Example 8.

1. Consider the action $\rho : S^1 \to \mathrm{Aut}(\mathbb{C})$ given by
$$\theta \mapsto \rho_\theta \coloneqq (z \mapsto e^{i\theta} z).$$
Then $\rho_\theta = \begin{bmatrix} \cos(\theta) & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ for each θ. Note that $\mathrm{Orb}_\rho(0) = \{0\}$ and $\mathrm{Orb}_\theta(z) = \{w \mid |w| = |z|\}$. Therefore, $S^1 \diagdown \mathbb{R}^2 = \mathbb{R}_{\geq 0}$, which induces a map $\mathbb{C} \to \mathbb{R}_{\geq 0}$ given by $z \mapsto |z|$.
2. Let $H \leq G$. Consider the restriction $l\restriction_H : H \to \mathrm{Aut}(G)$ of the *left translation* action of G on itself. Then $H \diagdown G$ equals the set of right cosets of H in G.
3. The orbits of the conjugation action of G on itself are precisely the conjugacy classes of G.

Exercise 4.

1. Show that if $\sigma, \tau \in S_n$, then they are conjugate in S_n if and only if σ and τ have the same type of cyclic decomposition.
2. Show that there is a natural bijection between $S_n \diagdown_{\text{conj.}} S_n$ and the set of unordered partitions of $\{1, \ldots, n\}$.

Definition. Let $\theta : G \to \mathrm{Aut}(S)$ and $\psi : G \to \mathrm{Aut}(T)$ be actions. A function $f : S \to T$ is called *equivariant* or *an intertwiner for θ and ψ* if for each $g \in G$, the following commutes.

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[d, "\theta(g)"'] & G \arrow[d, "\psi(g)"] \\ S \arrow[r, "f"] & T \end{tikzcd}$$

Definition. We say that θ and ψ are *isomorphic*, written as$\theta \cong \psi$, if there is an equivariant bijection for θ and ψ.

Note 2. We have that $\theta \cong \psi$ if and only if there exist intertwiners $f_1 : S \to T$ and $f_2 : T \to S$ such that $f_1 \circ f_2 = \mathrm{id}_T$ and $f_2 \circ f_1 = \mathrm{id}_S$.

Remark 5.

1. If $\theta : G \to \mathrm{Aut}(S)$ is simply transitive and $x \in S$, then $f_x : G \to S$ with $g \mapsto \theta(g)(x)$ intertwines θ and left-translation on G. Therefore, every G-torsor action is non-canonically isomorphic to left-translation on G.

2. Moreover, if $H \leq G$, then left-translation by G on the coset space $\{gH\}$ is well-defined and is transitive. We can extend this to prove that left-translations by G on a coset space characterize transitive actions up to isomorphism.

Theorem 1. Let $\theta : G \to \mathrm{Aut}(S)$ be an action and $K \subset S$ be an orbit. Then $\theta \restriction_K$ is a transitive action. If $x \in K$, then $f_x : {}^{G}\!/_{\mathrm{Stab}_\theta(x)} \to K$ given by $[g] \mapsto \theta(g)(x)$ is well-defined and an equivariant bijection for $\theta \restriction_K$ and left-translation by G on ${}^{G}\!/_{\mathrm{Stab}_\theta(x)}$.

Proof. Let $[g] = [h]$. Then $g = hs$ for some $s \in \mathrm{Stab}(x)$. Hence $\theta(g)(x) = \theta(hs)(x) = \theta(h)(\theta(s)(x)) = \theta(h)(x)$, proving that f_x is well-defined.

Define the map $F : K \to \mathrm{Stab}_\theta(x)$ by $F(y) = S_y := \{g \in G : \theta(g)(x) = y\} = [s_0]$ for fixed $s_0 \in S_y$. It's easy to check that this is the inverse of f_x.

Finally, let $g, g' \in G$. Then

$$\begin{aligned} f_x \circ l(g)(g') &= f_x(l(g)) \\ &= f_x(g[g']) \\ &= \theta(gg')(x) \\ &= \theta(g)(\theta(g')(x)) \\ &= \theta(g) \circ f_x(g'). \end{aligned}$$

□

Corollary 1. If $\theta : G \to \mathrm{Aut}(S)$ is a transitive action, then θ is isomorphic to the left translation action of G on G/H where $H = \mathrm{Stab}_\theta(x)$ for any chosen $x \in S$.

Corollary 2. If $\theta : G \to \mathrm{Aut}(S)$ is an action, then $S = \coprod_{O \in G \setminus S} O$ and $\theta = \coprod_{O \in G \setminus S} \theta_O$ where each θ_O is isomorphic to the left translation action of G on $G/\,\mathrm{Stab}_\theta(x)$ for any chosen $x \in S$.

Corollary 3. (Orbit-stabilizer theorem) Let G be a finite group and $\theta : G \to \mathrm{Aut}(S)$ an action. Then

$$|\mathrm{Orb}_\theta(x)| = \frac{|G|}{|\mathrm{Stab}_\theta(x)|}$$

for any $x \in S$.

Corollary 4. (Class equation) If G is finite, then

$$|G| = |Z(G)| + \sum_{\substack{C \text{ conj. class} \\ |C|>1}} |C|.$$

Exercise 5. Suppose that $H \leq G$.

1. Compute the kernel of the left-trans. action by G on ${}^{G}\!/_{H}$
2. Show that $H \trianglelefteq G$ if and only if the kernel the above action restricted to H is trivial.

(Lecture 4)

Corollary 5. If G is finite and $H \leq G$ with $[G : H] = p$ where p is the least prime dividing $|G|$, then $H \trianglelefteq G$.

Proof. Consider the left translation action $l : G \to \mathrm{Aut}(G/H)$. Let O be any orbit of the restricted action $l\restriction_H$, so that $|O| = \frac{|H|}{|\mathrm{Stab}|}$. Since $|O| \mid |H|$, it follows that $|O| = 1$ or $|O| \geq p$. But $[G : H] = p$, and there is already an orbit of size 1. This implies that there are exactly p orbits of size 1. Thus, $l\restriction_H$ is trivial, and $H \trianglelefteq G$. □

Exercise 6. (Burnside's lemma) If G and S are finite and $\theta : G \to \mathrm{Aut}(S)$ is an action, then for each $g \in G$, consider $\mathrm{Fix}(g) \subset S$. Check that

$$|G\diagdown S| = \frac{1}{|G|} \sum_{g} |\,\mathrm{Fix}(g)|.$$

Hint: Consider $\{(g, x) : g \cdot x = x\} \subset G \times S$.

Definition. Let p be a prime. A finite group G is called a *p-group* if $|G| = p^k$ for some $k \geq 0$.

Proposition 1.

1. If $|G| = p$, then G is isomorphic to the cyclic group C_p of order p.
2. Every p-group has nontrivial center.

Proof.

1. This is obvious,
2. The class equation implies that $|Z(G)| \equiv 0 \mod p$. Since $|Z(G)| > 0$, it follows that $|Z(G)| \geq p$.

□

Definition. Let G be any group.

1. We say that a sequence of subgroup

$$G = G_0 \supset G_1 \supset \cdots \supset G_s \supset \cdots$$

   is a *subnormal series* if $G_i \trianglelefteq G_{i-1}$ for each $i \geq 1$. We say that it is a *normal series* if $G_i \trianglelefteq G_0$ for each $i \geq 0$.

2. Set $\Delta^{(0)}G = G$ and $\Delta^{(k+1)}G = \Delta(\Delta^{(k)}G)$, where $\Delta G := \Delta^{(1)}G$ is the *commutator* or *derived* subgroup of G.

Remark 6. ΔG is the smallest subgroup H such that ${}^{G}\!/_{H}$ is abelian, so that

$$G = \Delta^{(0)}G \trianglerighteq \Delta^{(1)}G \trianglerighteq \Delta^{(2)}G \trianglerighteq \cdots$$

is a normal abelian series, called the *derived series of G*.

Definition. We call $G^{\mathrm{ab}} := {}^{G}\!/\!_{\Delta G}$ the *abelianization of* G.

Remark 7. If $f : G \to \underset{\text{abelian}}{A}$, then f factors uniquely as follows.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dr, "g"'] & A \\ & G^{\mathrm{ab}}. \arrow[u, "\tilde{f}"'] \end{tikzcd}$$

where $\tilde{f} : G^{\mathrm{ab}} \to A$ has $x \mapsto f(x)$. In other words, the map g is universal for maps from G to abelian groups.

Definition. We say that the derived series of G *terminates* if $\Delta^{(t+1)}G = \Delta^{(t)}G$ for some t. If this $\Delta^{(t)}G = \{e\}$, then we say that the series terminates at $\{e\}$.

Definition. We say that G is *solvable* if its derived series terminates at $\{e\}$. The least t for which $\Delta^{(t)}$ is trivial is called the solvable length of G.

Exercise 7. Prove the following assertions.

1. Any subgroup or quotient of a solvable group is solvable.
2. If $H \trianglelefteq G$ and ${}^{G}\!/\!_{H}$ are solvable, then so is G.
3. G is solvable if and only if it admits a finite abelian subnormal series.

Definition. Let G be a group.

1. G is called *polycyclic* if it has a finite subnormal series with cyclic factors.
2. G is called *nilpotent* if it has a finite normal series $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}$ where ${}^{G_{i-1}}\!/\!_{G_i} \subset Z({}^{G}\!/\!_{G_i})$ for each $1 \leq i \leq n$.

Remark 8. Every quotient and subgroup of a nilpotent group is nilpotent.

Remark 9. Every p-group G is nilpotent.

Proof. Set $G_0 = \{e\}$, $G_1 = Z(G)$, and, for $i > 1$, G_i such that $G \geq G_i \geq G_{i-1}$ and ${}^{G_i}\!/\!_{G_{i-1}} = Z({}^{G}\!/\!_{G_{i-1}})$. Since any quotient of G is a p-group, it has nontrivial center unless it equals G. Thus, the G_i form a strictly increasing sequence bounded above by G. Since G is finite, $G = G_k$ for some k. Note that each G_i is the pullback of a normal subgroup under the natural projection and thus itself normal in G, completing the proof. $\square$

(Lecture 5)

Example 9.

1. Every abelian group is nilpotent and thus solvable.
2. There are abelian groups which are not polycyclic, e.g., $G := {}^{\mathbb{Q}}\!/\!_{\mathbb{Z}} \cong \mu_\infty$ where μ_∞ denotes the group of all roots of unity. Recall that this is not finitely generated. But if G is polycyclic, then it admits a cyclic subnormal series $G = G_0 \trianglerighteq G_1 \cdots \trianglerighteq G_n$. Choose x_i that generates each factor ${}^{G_{i-1}}\!/\!_{G_i}$ for $1 \leq i \leq n$. This implies $\langle x_i \rangle = G$, a contradiction.
3. The dihedral group D_n is polycyclic (hence solvable) since the subgroup $\langle r \rangle$ has index 2.
4. $S_3 \cong D_3$ is not nilpotent. The only normal subgroup is $\langle (123) \rangle$, which is nontrivial and thus cannot be contained in $Z(D_3)$.

Exercise 8. Determine the nilpotent dihedral groups.

Proof. We claim that D_n is nilpotent if and only if n equals a power of 2. We know that any p-group is nilpotent. Conversely, if n is odd, then D_n has trivial center, hence is not nilpotent. Further, if $n = 2^k m$ for m odd and $k \geq 1$, then $Z(D_n) = \{e, m2^{k-1}\}$, so that ${}^{D_n}\!/_{Z(D_n)} \cong D_{m2^{k-1}}$, which by induction we can assume is not nilpotent. Since every quotient of a nilpotent group is nilpotent, D_n cannot be nilpotent when $n = 2^k m$ for any $k \geq 0$. This proves the claim. $\square$

Remark 10. We have the following two chains of strict implications for certain classes of groups.

1. Cyclic $\subsetneq$ Abelian $\subsetneq$ Nilpotent $\subsetneq$ Solvable.
2. Cyclic $\subsetneq$ Polycyclic $\subsetneq$ Solvable.

To complete the proof that each implication is strict, it suffices to produce a nilpotent group which is not abelian.

Example 10. Let V be a finite-dimensional vector space over $\mathbb{R}$. Let $\omega : V \times V \to \mathbb{R}$ be a bilinear map on V such that

(a) ω is skew-symmetric, i.e., $\omega(x, y) = -\omega(y, x)$

(b) If $\omega(x, y) = 0$ for every $y \in V$, then $x = 0$.

Here ω is called a *symplectic form on* V, and V is called a *symplectic vector space.* Build a group $H(V, \omega)$ on the set $V \times \mathbb{R}$ by the operation $(x, a) \cdot (y, b) = (x + y, a + b + \omega(x, y))$. This is called the Heisenberg group of H. It is the group of symmetries of the observables in a simple quantum mechanical system.

Exercise 9. Check that $Z(H(V, \omega)) \cong \mathbb{R}$ and that ${}^{H(V,\omega)}\!/_{Z(H(V,\omega))} \cong (V, +)$, which is abelian as a vector space, so that $H(V, \omega)$ is nilpotent yet not abelian.

Example 11. Let k be a field and $B_n(k)$ denote all $n \times n$ matrices of the form

$$\begin{bmatrix} a_1 & & & \\ & a_2 & & * \\ & & \ddots & \\ & 0 & & a_n \end{bmatrix}$$

with entries in k such that each $a_i \neq 0$. Then $B_n(k)$ is called the standard Borel subgroup of $\mathrm{GL}_n(k)$. Note that it is not abelian for $n > 1$.

We prove by induction that it is solvable. For $n = 1$, it is abelian, hence solvable. Now suppose it's solvable for $n - 1$ where $n > 1$ is fixed. Define a surjective homomorphism $f : B_n(k) \to B_{n-1}(k)$ by mapping each matrix M to the upper left $n - 1 \times n - 1$ included in M. Then $\ker f$ consists of matrices of the form

$$\begin{bmatrix} 1 & & & c_1 \\ & 1 & 0 & \vdots \\ & & \ddots & \vdots \\ & 0 & & c_n \end{bmatrix}$$

where $c_n \neq 0$. Hence there is a surjective homomorphism $g : \ker f \to k^\times$ given by sending this matrix to c_n. Then $\ker g$ consists of matrices of the form

$$\begin{bmatrix} 1 & & & c_1 \\ & 1 & 0 & \vdots \\ & & \ddots & c_{n-1} \\ & 0 & & 1 \end{bmatrix}$$

so that $\ker g \cong (k^{n-1}, +)$, which is abelian. Two applications of Exercise 7(2) show that $B_n(k)$ is solvable, completing the proof.

Example 12. S_n is solvable if and only if $n \leq 4$.

Proof. Recall the surjective homomorphism $\text{sgn} : S_n \to \{\pm 1\}$ given by $\sigma \mapsto \det(P_\sigma)$ where P_σ is the permutation matrix. Note that if $\sigma = (i_1, \ldots, i_k)$, then $\text{sgn}(\sigma) = (-1)^{k-1}$. Then $\ker(\text{sgn}) = A_n$, and we see that S_n is solvable if and only if A_n is solvable. $\square$

Lemma 1. A_n is generated by 3-cycles. Moreover, if $n \geq 5$, then it is generated by products of pairs of independent transpositions.

Proof. We know that A_n is generated by products of even numbers of transpositions. Now observe that

$$(i\ j)(j\ k) = (i\ j\ k) \tag{1}$$
$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l) \tag{2}$$
$$(i\ j)(j\ l) = (i\ j)(l\ m)(k\ j)(l\ m). \tag{3}$$

$\square$

Lemma 2. $\Delta S_n = A_n$.

Proof. Clearly $A_n \supset \Delta S_n$. When $n = 3$, $S_n \cong C_3$ and ΔS_n is nontrivial, giving $A_n = \Delta S_n$. For $n > 3$, we have $S_3 \subset S_n$, so that $A_3 = \Delta S_3 \subset \Delta S_n$. Thus $(1\ 2\ 3) \in \Delta S_n$. But every 3-cycle is conjugate to this one. Since ΔS_n is normal, it follows that $\Delta S_n = A_n$. $\square$

Lemma 3. We have $\Delta^{(2)} S_4 = \Delta A_4 \cong C_2 \times C_2$. Also, $\Delta^{(2)} S_n = \Delta A_n = A_n$ for $n \geq 5$.

Proof. Recall that $A_4 \trianglerighteq \{(1), (1\ \ 2), (3\ \ 4), (1\ \ 2)(3\ \ 4)\} \cong C_2 \times C_2$. Since ${}^{A_4}\!/\!_{C_2 \times C_2}$ is abelian, we see $C_2 \times C_2 \supset \Delta A_4 \neq \{e\}$. Since ΔA_4 is normal, it must equal $C_2 \times C_2$.

Next, note that $\Delta A_4 \subset \Delta A_n$ for $n \geq 5$. Thus $(1\ 2)(3\ 4) \in \Delta A_n = \Delta^{(2)} S_n \subset S_n$ for $n \geq 4$. This implies that $\Delta A_n \trianglelefteq S_n$ so that ΔA_n contains all conjugates of $(1\ 2)(3\ 4)$. But since two permutations are conjugate exactly when they have the same cycle type, it follows for $n \geq 5$ that $\Delta A_n = A_n$. (Hence A_n is not solvable when $n \geq 5$.) $\square$

(Lecture 6)

Remark 11. In Galois theory, one finds that a polynomial $f(x)$ over $\mathbb{Q}$ is solvable in radicals if and only if the group $\text{Gal}(f)$ is solvable.

Remark 12. For finite groups, we can add information to our chain of implications in Remark 12 as follows.

1. Cyclic $\subsetneq$ Abelian $\subsetneq$ Nilpotent $\subsetneq$ Solvable.
2. Cyclic $\subsetneq$ **Abelian** $\subsetneq$ Polycyclic $=$ Solvable.

Remark 13. Symmetry groups of polynomials are similar to freely acting symmetry groups of homeomorphisms on topological spaces, giving a correspondence $\text{Gal}(f) \longleftrightarrow \pi_1(X)$.

Moreover, if the space X has interesting underlying geometry, then the possibilities of $\pi_1(X)$ belonging to one of the classes of groups listed in Remark 12 are constrained. For example, a compact complex submanifold of $\mathbb{C}P^n$ is known as a Kahler manifold. It is known that any finite group is realizable as $\pi_1(X)$ for some Kahler manifold X.

Definition. If Γ is a group and P a property of groups, then we say that Γ is *virtually* P if there exist a finite subgroup $F \trianglelefteq \Gamma$ and a subgroup $I \leq \Gamma$ of finite index so that if $q : \Gamma \to {}^{\Gamma}\!/\!_{F}$ is the natural projection, then $q(I)$ has P.

For $\pi_1(X)$ with X a Kahler manifold, we have the following chains of implications due to Arapura-Nuri (2005).

1. v. Cyclic $\subsetneq$ v. Abelian $\subsetneq$ v. Nilpotent $=$ v. Solvable.

2. v. Cyclic $\subsetneq$ v. Abelian $\subsetneq$ v. Polycyclic $=$ v. Solvable.

Example 13. If $|G| = p^2$ for p prime, then G is abelian.

Proof. This follows from the fact that G has nontrivial center as a result of the class equation. $\square$

Exercise 10. Show that G from our last example is isomorphic to either $C_p \times C_p$ or C_{p^2}.

Definition. Let G be a group with $|G| = p^k m$ for p prime, $k \geq 1$, $m \geq 1$, and $(p, m) = 1$. Then $H \leq G$ is called a *p-Sylow subgroup of* G if $|H| = p^k$.

Theorem 2. (Weak Sylow-I) Every finite group G with $|G| = p^\beta m$ contains a p-Sylow subgroup.

Proof. We use induction on $|G|$. Write $G = Z(G) \coprod_{x \notin Z(G)} C(x)$ as the union of conjugacy classes.

Case 1: Let $x \in G$ such that $|C(x)| > 1$ and $p \nmid |C(x)|$. But since $|C(x)||Z_G(x)| = |G|$, we see that $|C(x)| \mid m$ and $p^\beta \mid |Z_G(x)| < |G|$. By induction $Z_G(x)$ and thus G contain a p-Sylow subgroup.

Case 2: Suppose that for any $x \in G$, if $|C(x)| > 1$, then $p \mid |C(x)|$. Then $p \mid Z(G)$. Write $|Z(G)| = p^\alpha n$ with $1 \leq \alpha \leq \beta$ and $(n, p) = 1$. If $\alpha = \beta$, then we're done by induction, so assume that $\alpha < \beta$. Since $|Z(G)| < G$, by induction we have some $H \leq Z(G)$ with $|H| = p^\alpha$. This is normal in G, and $|{}^{G}\!/_{H}| = p^{\beta - \alpha}\frac{m}{n} < |G|$. Thus there is some p-Sylow subgroup $S \leq {}^{G}\!/_{H}$. Let $S' \coloneqq q^{-1}(S)$ be the pullback of S. Then ${}^{S'}\!/_{H} = S$, implying that $p^\beta = |S'|$.

Case 3: Assume that $Z(G) = G$. Then we can apply the FTFAG (see below) and induction to get a direct product of p-Sylow subgroups of G's invariant factors, which will be a p-Sylow subgroup of G. $\square$

Note 3. We have another proof of Weak Sylow-I. Let $|G| = p^\beta m$ with $(p, m) = 1$. Define

$$S = \{A \subset G : |A| = p^\beta\}.$$

We see that G acts on S by left translation and that $|S| = \binom{p^\beta m}{p^\beta}$, which is coprime to p. Therefore, there is some orbit Ω_x such that $p \nmid |\Omega_x|$. Since $|\Omega_x||\operatorname{Stab}_G(x)| = |G|$, we must have that $p^\beta \mid |\operatorname{Stab}_G(x)|$. Note that $\operatorname{Stab}_G(x)$ acts on A by left translation. As this action is free, each orbit must have cardinality equal to $|\operatorname{Stab}_G(x)|$ and thus be divisible by $p^\beta = |A|$. This implies that A is the only orbit, and $|A| = \operatorname{Stab}_G(x)$.

Exercise 11. (Strong Sylow-I) Use the fact that every p-group is nilpotent to prove that a finite group contains a p-subgroup of every possible order.

(Lecture 7)

Theorem 3. (Sylow-II) Let G have $|G| = p^\beta m$ as before. Then the following hold.

1. Every p-subgroup of G is contained in some p-Sylow subgroup.
2. Any two p-Sylow subgroups of G are conjugate.

Proof.

1. Let $H \leq G$ be a p-subgroup and $S \leq G$ a p-Sylow subgroup. Let H act by left translation on the coset space ${}^{G}\!/_{S}$. We have ${}^{G}\!/_{S} = \coprod$ (H-orbits), where each H-orbit has cardinality dividing $|H|$. If $\mathbb{O}$ is a nontrivial orbit, then $p \mid |\mathbb{O}|$, so that if every orbit is nontrivial, then $p \mid |{}^{G}\!/_{S}| = m$, a contradiction. Thus there is some orbit $\mathbb{O} = \{gS\}$. Since $hgS = gS$ for every $h \in H$, we have $g^{-1}Hg \subset S$, i.e., $H \leq gSg^{-1}$. Note that $|gSg^{-1}| = |S|$.
2. We just showed that $H \leq gSg^{-1}$ for some $g \in G$. Hence if $|H| = p^\beta$, then $H = gSg^{-1}$.

$\square$

Corollary 6. If $n_p(G) = 1$, then the p-Sylow subgroup is normal in G.

Corollary 7. Let $S \in \mathrm{Syl}_p(G)$. Then $N_G(N_G(S)) = N_G(S)$.

Proof. We know $N_G(S) \subset N_G(N_G(S))$. Since $N_G(S)$ is the maximal subgroup H of G such that $S \trianglelefteq H$, it suffices to show that $S \trianglelefteq N_G(N_G(S))$.

Pick H a p-Sylow subgroup of $N_G(N_G(S))$. If $h \in H$, then $|h| = p^K$ for some $K \geq 0$. Consider $\bar{h} \in {N_G(N_G(S))}/{N_G(S)}$. The $|\bar{h}|$ is also a p-power. Observe that

$$[N_G(N_G(S)) : N_G(S)] \mid [G : N_G(S)] \mid [G : S] = m.$$

Therefore, $|\bar{h}| = 1$, so that $h \in N_G(S)$. It follows that $H \subset N_G(S)$. Since H and S are both p-Sylow subgroups of $N_G(S)$, we know that $H = nSn^{-1} = S$ for some $n \in N_G(S)$. Thus, S is the unique p-Sylow subgroup of $N_G(N_G(S))$, hence is normal in $N_G(N_G(S))$. ☐

Exercise 12. Let G have $|G| = p^\beta$ and $H \leq G$ have $|H| = p^\alpha$ where $\alpha < \beta$.

1. Let H act by left translation on ${G}/{H}$. Prove that there is a fixed point other than eH.
2. Show that $H \leq N_G(H)$.
3. Show that there is some $\tilde{H} \leq G$ such that $|\tilde{H}| = p^{\alpha+1}$ and $H \leq \tilde{H} \leq G$.

Theorem 4. (Sylow-III) Suppose $|G| = p^\beta m$ as before. Let $\mathrm{Syl}_p(G)$ denote the set of p-Sylow subgroups of G. Let $n_p(G)$ and $\mathrm{syl}_p(G)$ denote $\#\,\mathrm{Syl}_p(G)$. Then

1. $n_p(G) \mid m$.
2. $n_p(G) \equiv 1 \mod p$.

Proof.

1. Notice that G acts transitively on $\mathrm{Syl}_p(G)$ by conjugation, hence $n_p(G) \mid |G|$. But below we show that $n_p(G)$ and p are coprime. Therefore, $n_p(G) \mid m$.
2. The conjugation action of G on itself induces a transitive action of G on $\mathrm{Syl}_p(G)$. If $H \in \mathrm{Syl}_p(G)$, consider $\mathrm{Stab}_H(G) = N_G(H)$. Now restrict the action to some p-Sylow subgroup S. We have that $\mathrm{Syl}_p(G) = \coprod$ (S-orbits). This implies that if there is exactly one fixed point, then $n_p(G) \cong 1 \mod p$. Suppose that H is a fixed point. Call it H. Then H and S are p-Sylow subgroups of $N_G(H)$. Thus, they are conjugate. Hence $H = S$.

☐

Note 4. The number of p-Sylow subgroups of G is equal to $[G : N_G(S)]$ where $S \in \mathrm{Syl}_p(G)$.

Corollary 8. If $|G| = pq$ for primes $p < q$ such that $q \not\equiv 1 \mod p$, then $G \cong C_{pq}$.

Example 14. Every group of order 45 is abelian.

(Lecture 8)

Theorem 5. (Fundamental theorem of finite abelian groups) If G is a finite abelian group, then

$$G \cong \mathbb{Z}/u_1 \times \cdots \times \mathbb{Z}/u_n$$

such that each $u_i \in \mathbb{Z}_{>0}$ and $u_i \mid u_{i+1}$ for each $i = 1, \ldots, n-1$.

Proof. Choose finitely many generators $g_1, \ldots, g_n$ for G with n minimal. We have a surjective homomorphism $\phi : \mathbb{Z}^n \to G$ given by $e_i \mapsto g_i$. Set $N = \ker \phi$.

Claim 1. N is free. In particular, $N \cong \mathbb{Z}^n$.

Proof. Induct on $n \geq 1$. For the base case, notice that $N = d\mathbb{Z}$ for some integer $d \neq 0$, so that $N \cong \mathbb{Z}$. For the induction step, suppose that the claim holds for any subgroup $M \leq \mathbb{Z}^m$ of finite index where $m < n$. Set $M = \langle e_1, \ldots, e_{n-1}\rangle \cap N$. Then ${}^{\langle e_1, \ldots, e_{n-1}\rangle}\!/_{M} \leq {}^{\mathbb{Z}^n}\!/_{N}$, which is finite. By our induction hypothesis, it follows that $M \cong \langle e_1, \ldots, e_{n-1}\rangle$. Find a basis $(f_1, \ldots, f_{n-1})$ for M and define the surjective group map $p : \mathbb{Z}^n \to \mathbb{Z}$ by $(x_1, \ldots, x_n) \mapsto x_n$. Then $\ker p = \langle e_1, \ldots, e_{n-1}\rangle$. We also see that $p(N) \neq 0$ for otherwise N would have infinite index. Hence $p(N) = k\mathbb{Z}$ for some nonzero integer k. Define $f_n = (0, \ldots, 0, k) \in \mathbb{Z}^n$, so that $p(f_n) = k$. Then $(f_1, \ldots, f_n)$ is a basis for N. Indeed, if $\xi \in N$, then $p(\xi) = zk$ for some $z \in \mathbb{Z}$. Then $\xi - zf_n \in \ker p \cap N = M$. Hence $\xi \in \langle f_1, \ldots, f_n\rangle$. Moreover, given the equation $0 = a_1f_1 + \cdots + a_nf_n$, we see that $0 = p(0) = a_nk$. Since $f_1, \ldots, f_{n-1}$ are linearly independent, it follows that $a_i = 0$ for each $i = 1, \ldots, n$. Thus, $f_1, \ldots, f_n$ are linearly independent as well. □

Let $i : N \to \mathbb{Z}^n$ denote inclusion. As this is $\mathbb{Z}$-linear, it may be represented by some $C \in \mathrm{Mat}_n(\mathbb{Z})$. But $\mathbb{Z}$-linearity entails $\mathbb{Q}$-linearity. Hence C also defines a $\mathbb{Q}$-linear map $i_{\mathbb{Q}} : \mathbb{Q}^n \to \mathbb{Q}^n$. Note that if $\ker i_{\mathbb{Q}} \neq 0$, then $\ker i \neq 0$, which is impossible. By linear algebra, we thus know that $\det(C) \neq 0$.

One can show that by elementary row and column operations, C is equivalent to a diagonal matrix $(u_1, \ldots, u_n)$ such that each $u_i \in \mathbb{Z}_{>0}$ and $u_i \mid u_{i+1}$ for each $i = 1, \ldots, n-1$. In particular, we can find bases $(\tilde{f}_i)$ and $(\tilde{e}_i)$ of N and $\mathbb{Z}^n$, respectively, such that $\tilde{f}_i = u_i\tilde{e}_i$ for each i. Therefore, we may write $G \cong {}^{\mathbb{Z}^n}\!/_{N} \cong \mathbb{Z}/u_1 \times \cdots \times \mathbb{Z}/u_n$. □

Remark 14. We may adapt this proof to show that if A is a finitely generated abelian group, then

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/u_1 \times \cdots \times \mathbb{Z}/u_n$$

for some integer $r \geq 0$.

(Lecture 9)

Definition. A group G is *simple* if it has no nontrivial proper normal subgroup.

Example 15.

1. An abelian group is simple if and only if it has order p prime.
2. A p-group is simple if and only if it has order p.
3. If $|G| = pq$, then G is not simple.

Definition. A *composition series for* G is a subnormal series $G = G_0 > G_1 > \cdots > G_k = \{e\}$ where each ${}^{G_i}\!/_{G_{i+1}}$ is simple.

Example 16.

1. Any finitely generated group G has a composition series.

   Proof. If G is simple, then we're done. So assume otherwise. Let $n \in \mathbb{N}$ be maximal so that there is some proper $H \lhd G$ that contains n generators of G. Let S denote the set of such H. Note that S satisfies the hypotheses of Zorn, giving a maximal element H'. Then ${}^{G}\!/_{H'}$ is simple. [[How do we proceed if H' is not simple or finitely generated? If G is abelian, then we're good, but not otherwise.]] □

2. $\mathbb{Z}$ has no composition series, since no nontrivial subgroup of $\mathbb{Z}$ is simple.
3. Any p-group admits a composition series where each factor is ${}^{\mathbb{Z}}\!/_{p}$.
4. If $|G| = pq$, then $G > G_1 > \{e\}$ where G_1 is the unique q-Sylow subgroup is a composition series.

Proposition 2. A_5 is simple.

Proof. Suppose $N \trianglelefteq A_5$ is nontrivial. Let $\sigma \in N$ be nontrivial. We may assume that $|\sigma| = p$ for some prime p. Then σ can be decomposed into disjoint cycles each of length p.

Lemma 4. If $\sigma \in A_n \subset S_n$ and in the decomposition of σ we have one of

1. two even cycles of equal length
2. an odd cycle,

then the conjugacy class of σ in A_n equals its conjugacy class in S_n.

Proof. If the first condition holds so that $\sigma = (i_1 \cdots i_r)(j_1 \cdots j_r)\cdots$ with r odd, then construct odd $\tau = (i_1\ j_1)(i_2\ j_2)\cdots(i_r\ j_r)$. Note that

$$\tau(i_1 \cdots i_r)\tau^{-1} = (j_1 \cdots j_r)$$

and

$$\tau(j_1 \cdots j_r)\tau^{-1} = (i_1 \cdots i_r).$$

This implies that $\tau \in Z_{S_n}(\sigma)$. It's easy to see as well that there is an odd permutation in the centralizer when the second condition holds. Now, let $\phi \in \mathrm{conj}_{S_n}(\sigma)$. Write $\phi = \alpha\phi\alpha^{-1}$. Assume α is odd. Then there is some odd $\tau \in Z_{S_n}(\sigma)$. Noe that $(\alpha\tau)\sigma(\alpha\tau)^{-1} = \alpha\tau\sigma\tau^{-1}\alpha^{-1} = \alpha\sigma\alpha^{-1} = \phi$. But $\alpha\tau$ is even, completing the lemma. $\square$

We have three cases to consider. If $p = 2$, then σ is the product of two independent transpositions. By the lemma, it follows that $N = A_5$. If $p = 3$, then N contains all 3-cycles because any two 3-cycles are conjugate in A_5. Finally, suppose $p = 5$. Write $\sigma = (i_1 \cdots i_5)$ and $\tau = (i_1\ i_2\ i_3)\sigma(i_1\ i_2\ i_3)^{-1} = (i_2\ i_3\ i_1\ i_4\ i_5)$. Then $\tau\sigma^{-1} = (i_1\ i_2\ i_3) \in N$, implying that N contains all 3-cycles. In conclusion, N cannot be proper. [[Why did we need that whole lemma?]] $\square$

Example 17. If $|G| = pq$, then $\mathbb{Z}/q \overset{i}{\hookrightarrow} F \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/p$ where $\mathrm{im}(i) = \ker\pi$. What data do we need to reconstruct G from $\mathbb{Z}/p$ and $\mathbb{Z}/q$?

Definition. A sequence of groups with homomorphisms $S \overset{\phi}{\to} G \overset{\pi}{\to} Q$ is called a *short exact sequence* if ϕ is injective, π is surjective, and $\ker\pi = \mathrm{im}(i)$. In this case, we say that G is an *extension of Q by S*. If $\phi(S) \le Z(G)$, then we say this is a *central extension*.

Definition. In general, a sequence $G_1 \overset{\phi_1}{\to} G_2 \overset{\phi_2}{\to} \cdots \overset{\phi_k}{\to} G_k$ is called *exact at the term G_i* if $\ker\phi_i = \mathrm{im}(\phi_{i-1})$ and is called *exact* if it is exact at all terms where this makes sense.

Remark 15. If G has subnormal series $G = G_0 > G_1 > \cdots > G_k = \{e\}$, then for each $0 \le i \le k-1$, we get an extension $\eta_i : 1 \to G_{i+1} \to G_i \to G_i/G_{i+1} \to 1$. Thus G can be built successively from the G_i/G_{i+1} and η_i.

This reduces the classification problem for groups admitting decomposition series to two smaller classification problems.

1. Understand all possible simple groups
2. Understand ways of extending simple groups by a subgroup.

Definition. A group extension $1 \to H \overset{i}{\to} G \overset{q}{\to} K \to 1$ is called *split* if we can find a homomorphism $s : K \to G$ such that $q \circ s = \mathrm{id}_K$. In symbols,

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "i"] & G \arrow[r, "q"] & K \arrow[l, bend left, "s"] \arrow[r] & 1. \end{tikzcd}$$

Example 18. Suppose $|G| = pq$. Then $1 \to Z/q \to G \to Z/p$ is split.

Remark 16. If

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "i"] & G \arrow[r, "q"] & K \arrow[l, bend left, "s"] \arrow[r] & 1. \end{tikzcd}$$

is a split exact sequence, then we say G is essentially a product of H and K by way of the inclusions $H \overset{i}{\hookrightarrow} G$ and $K \overset{s}{\hookrightarrow} G$. Further, we have $HS \cong G$ and $H \trianglelefteq G$ where $S := s(K) \cong K$. To see that $G = HS$, note if $g \in G$, then $q(g) \in K$ and $x := s(q(g)) = g \in S$ with $q(gx^{-1}) = q(g)q(x)^{-1} = e$, implying that $gx^{-1} \in \ker q = H$.

(Lecture 10)

Remark 17. Recall that G decomposes as the (direct) product of $G_1, \ldots, G_k$, i.e., the map

$$\phi : G_1 \times \cdots \times G_k \to G, \quad (g_1, \cdots, g_k) \mapsto g_1 \cdots g_k$$

is an isomorphism, if and only if

1. Each $g \in G$ can be written uniquely as $g_1 g_2 \cdots g_k$, i..e, ϕ is bijective.
2. We have $xy = yx$ for any $x \in G_i$ and $y \in G_j$, i.e., ϕ is a morphism.

Exercise 13. Check that condition (1) is equivalent to saying $G_1 \cdots G_k = G$ and $G_i \cap (G_1 \cdots \widehat{G_i} \cdots G_k) = \{e\}$ and that condition (2) is equivalent to saying $G_i \trianglelefteq G$ for each i.

Example 19.

1. $\mathbb{C}^* \cong S^1 \times \mathbb{R}$ via $z \mapsto (e^{i\theta}, r)$. Note also the extension

$$1 \longrightarrow S^1 \xrightarrow{i} \mathbb{C}^* \xrightarrow{|\cdot|} \mathbb{R}_{>0} \longrightarrow 1.$$

2. $\mathrm{GL}_n^+(\mathbb{R}) \cong \mathrm{SL}_n(\mathbb{R}) \times \mathbb{R}_{>0}$ via $A \mapsto (\frac{A}{\sqrt[n]{\det A}}, \det A)$. We have a short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{SL}_n \arrow[r, "i"] & \mathrm{GL}_n^+(\mathbb{R}) \arrow[r, "\det"] & \mathbb{R}_{>0} \arrow[l, bend left, "s"] \arrow[r] & 1, \end{tikzcd}$$

where $s(x) = \frac{1}{\sqrt[n]{a}} I_n$. Note that $s(\mathbb{R}_{>0}) = Z(\mathrm{GL}_n^+(\mathbb{R}))$, which of course commutes with $\mathrm{SL}_n(\mathbb{R})$.

3. Let Diag_n be the group of diagonal matrices over k. Then $\mathsf{Diag}_n \cong \underbrace{k^* \times \cdots \times k^*}_{n}$.

4. If p is prime, then $\mathbb{Z}/p^2$ is not a product of any nontrivial subgroups. For if $\mathbb{Z}/p^2 \cong H \times K$, then $H \trianglelefteq \mathbb{Z}/p^2$ is nontrivial, so that $H = \langle x^p \rangle$ where $\langle x \rangle = \mathbb{Z}/p$. Similarly, $K \cong C_p$. But $K \neq H$, while there is a unique subgroup of order p.

   In fact, this shows that $1 \to H \to \mathbb{Z}/p \to K \to 1$ cannot be split.

5. If $a, b > 0$ are coprime, then $\mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b$. However, $S_3 \not\cong \mathbb{Z}/2 \times \mathbb{Z}/3$, as $s(\mathbb{Z}/2)$ below is not normal.

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Z}/3 \arrow[r, "i"] & S_3(\mathbb{R}) \arrow[r, "\mathrm{sgn}"] & \mathbb{Z}/2 \arrow[l, bend left, "s"] \arrow[r] & 1, \end{tikzcd}$$

Definition. Suppose $H, K \leq G$ with H normal and $G = HK$. Then if $H \cap K$ is trivial, we call G the *semidirect product of H and K*, denoted by $H \rtimes K$.

Remark 18. Recall that if $H \trianglelefteq G$ and $K \leq G$, then $HK = KH$ is a subgroup.

Proposition 3. Suppose $G = HK$ with $H \trianglelefteq G$ and $H \cap K = \{e\}$. Let $\alpha : K \to \mathrm{Aut}_{\mathsf{grp}}(H)$ be the inner automorphism of H, which depends on the group law $*_G$. Then $*_G$ can be recovered from $*_H$, $*_K$, and α.

Proof. Let $g_1, g_2 \in G$. Then decompose $g_1 = h_1k_1$ and $g_2 = h_2k_2$ uniquely. Thus $g_1g_1 = (h_1\alpha_{k_1}(h_2))k_1k_2$. $\square$

Definition. Let K and H be groups and $\alpha : K \to \mathrm{Aut}(H)$ be a structure-preserving action. Then the *semidirect product of K with H along α*, denoted by $H \rtimes_\alpha K$, is the group with underlying set $H \times K$ and group law $(h_1, k_1)(h_2, k_2) \coloneqq (h_1\alpha_{k_1}(h_2), k_1k_2)$.

Remark 19. Every semidirect product is naturally a split extension of K by H. Indeed, if $K \ltimes_\alpha H$, then $i_H : H \to K \ltimes_\alpha H$ is normal and $p_K : K \ltimes_\alpha H \to K$ is a surjective homomorphism with kernel H. Thus

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "i_H"] & K \ltimes_\alpha H \arrow[r, "p_K"] & K \arrow[r] \arrow[l, bend left, "i_K"] & 1 \end{tikzcd}$$

is split, and $i_K(K)$ is normal if and only if α is trivial if and only if $K \ltimes_\alpha H \cong H \times K$.

Conversely, if

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "i"] & G \arrow[r, "q"] & K \arrow[r] \arrow[l, bend left, "s"] & 1 \end{tikzcd}$$

is a split extension, then we get an inner automorphism $\alpha : s(K) \to \mathrm{Aut}(H)$. Note that $s(K)$ is normal if and only if α is trivial. The map $\phi : \ltimes_\alpha H \to G$ given by $(h, x) \mapsto hx$ is an isomorphism.

Definition. Let

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "i_1"] & G_1 \arrow[r, "q_1"] & K \arrow[r] & 1 \end{tikzcd}$$

and

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r, "i_2"] & G_2 \arrow[r, "q_2"] & K \arrow[r] & 1 \end{tikzcd}$$

be extensions. Then they are *equivalent* or *isomorphic* if there is some map $\phi : G_1 \xrightarrow{\cong} G_2$ such that

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r] \arrow[d, dashed, "\mathrm{id}"] & G_1 \arrow[r] \arrow[d, dashed, "\phi"] & K \arrow[r] \arrow[d, dashed, "\mathrm{id}"] & 1 \\ 1 \arrow[r] & H \arrow[r] & G_2 \arrow[r] & K \arrow[r] & 1 \end{tikzcd}$$

commutes.

Example 20.

1. $S_n \cong C_2 \ltimes_\alpha A_n$ where $\alpha(1) = \mathrm{conj}_{(1\ 2)}$.
2. If $|G| = pq$ with $q > p$, then $G \cong \mathbb{Z}/p \ltimes_\alpha \mathbb{Z}/q$. Note that by Sylow if $q \not\equiv 1 \mod p$, then α must be trivial.

Exercise 14. Let $H(V, W)$ denote the Heisenberg group. Show that $0 \to \mathbb{R} \to H(V, W) \to V \to 0$ cannot be split.

(Lecture 11)

Definition. A group G is *indecomposable* if it cannot be written as the direct product of two nontrivial subgroups. By convention, the trivial group is not indecomposable.

Remark 20. Once we answer the question of existence, we ask in how many ways can we break a group into (a) simple groups or (b) indecomposable groups. We've shown that the existence of a composition series ensures that a group can be broken into simple groups. We now turn to the existence question for (b).

Definition. We say that G has

1. the *ascending chain condition (ACC)* if any ascending normal series of subgroups stabilizes.

2. the *descending chain condition (DCC)* if any descending normal series of subgroups stabilizes.

Example 21. Any scenario can happen.

1. Finite G has both ACC and DCC.

2. $\mathbb{Z}$ has ACC but not DCC.

3. Given p prime, let $G_p \coloneqq \{z \in \mathbb{C}^* : z^{p^k} = 1 \text{ for some } k\}$. This has DCC but not ACC. [[Why?]]

4. $\mathbb{Q}$ has neither property.

Exercise 15.

1. Given the exact sequence $1 \to H \to G \to K \to 1$, if both H and K have ACC and DCC, then so does G.

2. If $G = H \times K$ and G has ACC and DCC, then so do H and K.

Proof.

1.

2. H and K are normal in G, and any normal subgroup of either is normal in G.

□

Proposition 4. If G has either ACC or DCC, then it can be written as the product of indecomposables.

Proof. Let D denote the class of groups that can be written as the product of indecomposables. Note that D is closed under direct products and that it contains any indecomposable group.

Assume, for contradiction, that G has DCC but $G \notin D$. Set $H_0 = G$ so that $H_0 = H_1 \times K_1$ with $H_1 \notin D$ and $K_1 \neq \{e\}$. Proceeding in this way, we can construct $H_n = H_{n+1} \times K_{n+1}$ with $H_{n+1} \notin D$ and K_{n+1} nontrivial. Thus we get a normal series $G = H_0 > H_1 > H_2 > \cdots$. But there must be some i such that $H_i = H_{i+1}$, a contradiction.

Next, assume that G has ACC but $G \notin D$. By the same process as above, we can construct a normal series $K_1 < K_1 \times K_2 < K_1 \times K_2 \times K_3 < \cdots < \cdots < G$. But this must stabilize as well, a contradiction. □

Theorem 6. (Krull-Schmidt) Suppose G has ACC and DCC, so that G is a product of indecomposables

$$G = A_1 \times \cdots \times A_s$$

$$G = B_1 \times \cdots \times B_t.$$

Then $s = t$, and $A_i = B_i$ up to reindexing the B_j.

Proof. Recall that $\mathrm{End}(G) = \{\phi : G \to G \mid \phi \text{ is a homomorphism}\}$. This is a monoid under composition.

Definition. An endomorphism ϕ of G is *normal* if $\phi \circ \mathrm{conj}_x = \mathrm{conj}_x \circ \phi$ for any $x \in G$.

Lemma 5. Basic properties of normal endomorphisms.

1. The set of normal endomorphisms is closed under composition.
2. The inverse of a normal automorphism is also normal.
3. Normal endomorphisms preserve normal subgroups.
4. If ϕ and ψ are normal, then $\phi + \psi$ is normal, where $\phi + \psi$ is given by $g \mapsto \phi(g)\psi(g)$.
5. If $G = G_1 \times \cdots \times G_k$ and p_i and f_i denote projection and inclusion, respectively, then each each $f_i p_i$ is normal. Moreover, for any $\{a_1, \ldots, a_r\} \subset \{1, \ldots, k\}$, we have that $\sum_{j=1}^{r} f_{a_j} p_{a_j}$ is normal.

Proposition 5. If G has ACC and DCC and ϕ is normal, then ϕ is injective if and only if it's surjective.

Proof. Suppose first that $\ker\phi$ is trivial. Suppose there is some $g \in G \setminus \phi(G)$. Then $\phi^n(g) \notin \phi^{n+1}(G)$ for any $n \geq 1$. Hence $G > \phi(G) > \phi^2(G) > \cdots$ is a normal series that fails to terminate, a contradiction.

Now suppose that ϕ is not injective. Find nontrivial $g_1 \in \ker\phi$. Suppose, for contradiction, that $\phi(g_2) = g_1$ for some g_2. Then $g_2 \notin \ker\phi$ but $g_2 \in \ker\phi^2$. Continue to get the chain $\ker\phi < \ker\phi^2 < \cdots$, which fails to stabilize, a contradiction. □

Definition. An endomorphism ϕ is *nilpotent* if $\phi^n = (g \mapsto e)$ for some $n \geq 1$.

Lemma 6. (Fitting) If G has ACC and DCC and $\phi : G \to G$ is normal, then $G = K \times H$ where

$$\phi(K) \subset K$$

$$\phi(H) \subset H$$

$$\phi\restriction_K \text{ is nilpotent}$$

$$\phi\restriction_H \text{ is an automorphism.}$$

Proof. For each $n \in \mathbb{N}$, set $K_n = \ker\phi^n$ and $H_n = \operatorname{im}\phi^n$. This gives the normal series

$$G = H_0 \geq H_1 \geq \cdots$$

$$K_1 \leq K_2 \leq \cdots \leq G.$$

Find $a \in \mathbb{N}$ where both stabilize. Set $H = H_a$ and $K = K_a$. Then $\phi(H) = \phi(\phi^a(H)) = \phi^{a+1}(H) = H_{a+1} = H_a = H$. Further, $\phi(K) = \phi(K_a) = \{\phi(x) : x \in \ker\phi^a\}$. implying $\phi^a\phi(x) = \phi(\phi^a(x)) = e$. Hence both H and K are stable under ϕ. Note that we've shown $\phi\restriction_H$ is surjective. By our last proposition, $\phi\restriction_H$ is an isomorphism provided that H has ACC and DCC. But we can show $G = K \times H$ as follows.

(a) Let $x \in K \cap H$. Then $x \in H = H_a = \phi^a(G) \implies \phi^a(G) = x$ for some $g \implies \phi^a(\phi^a(g)) = \phi^a(x) = 0 \implies g \in K_{2a} = K_a = K \implies \phi^a(g) = e \implies x = e$.

(b) Let $g \in G$. Then $\phi^a(g) \in H = H_a = H_{2a} \implies \phi^a(g) = \phi^{2a}(x)$ for some $x \in G \implies \phi^a(g\phi^a(x^{-1})) = e \implies g\phi^a(x) \implies g\phi^a(x^{-1}) \in K_a = K \implies g = kh$ for some $k \in K$ and $h \in H$.

(c) $H, K \trianglelefteq G$,

It remains to show that $\phi\restriction_K$ is nilpotent. But it's clear that $(\phi\restriction_K)^a = e$. □

(Lecture 12)

Corollary 9. Suppose G is indecomposable and has ACC + DCC, then any normal $\phi : G \to G$ is either nilpotent or an automorphism.

Lemma 7. Suppose G is indecomposable and has ACC + DCC and that ϕ and ψ are endomorphisms such that $\phi + \psi$ is an endomorphism. Then if ϕ and ψ are nilpotent, so is $\phi + \psi$.

Proof. By our previous corollary, assuming that $\phi + \psi$ is not nilpotent, it must be an automorphism. Set $\gamma = (\phi+\psi)^{-1}$. Then $\underbrace{\phi \circ \gamma}_{U} + \underbrace{\psi \circ \gamma}_{V} = (\phi+\psi)\circ\gamma = \mathrm{id}_G$. Hence $U + V = \mathrm{id}_G$. We call U and V a *normal decomposition* of id_G. We see that $V + U$ is also a normal decomposition of id_G by applying $(-)^{-1}$ to $U(x)V(x) = x$ for any $x \in G$. Now, $U^2 + UV = U(U+V) = U = (U+V)U = U^2 + VU$. This implies that $UV = VU$. Hence we can apply the binomial theorem to get

$$(U+V)^n = \sum_{a=0}^{n} \binom{n}{a} U^a V^{n-a}.$$

But since $U = \phi \circ \gamma$, we know that $\ker U \geq \gamma^{-1}(\ker\phi) \cup \{e\} > \{e\}$. Likewise, $\ker V > \{e\}$. Thus, U and V must be nilpotent. There are minimal $k, l \in \mathbb{N}$ such that $U^k = 0 = V^l$. Set $n = k + l - 1 \geq 1$. Then each $U^a V^{n-a}$ has either $a \geq k$ or $n - a \geq l$, so that $\mathrm{id}_G = (U+V)^n = 0$, implying that G is trivial. This contradicts that G is indecomposable. □

We finally return to the proof of Krull-Schmidt. Suppose $r = 1$. Let $p_i : G \to A_i$ and $q_j : G \to B_j$ be projections and $f_i : A_i \hookrightarrow G$ and $g_j : B_j \hookrightarrow G$ be inclusions. Note that each $g_j \circ q_j$ is normal and that $\sum_{j=1}^{t} g_j \circ q_j = \mathrm{id}_G$. Note also that $p_i \circ f_i = \mathrm{id}_{A_i}$ and $q_j \circ g_j = \mathrm{id}_{B_j}$. This gives $\mathrm{id}_{A_1} = p_1 \circ \mathrm{id}_G \circ f_1 = p_1 \circ (\sum_{j=1}^{t} g_j \circ g_j) \circ f_1 = \sum_{j=1}^{t}(p_1 \circ g_j \circ q_j \circ f_1)$. Each $p_1 \circ g_j \circ q_j \circ f_1$ is normal, and each sub-sum of $\sum_{j=1}^{t}(p_1 \circ g_j \circ q_j \circ f_1)$ is normal. Hence if each sub-sum is nilpotent, then our previous lemma implies that A_1 is trivial, contrary to the fact that A_1 is indecomposable. Hence $p_1 \circ g_j \circ q_j \circ f_1$ for some $1 \leq j \leq t$. Reindex the B_i's so that $B_j = B_1$.

Thus, $G = A_1 \times \cdots \times A_r$ and $G = B_j \times \cdots \times B_t$. Further, $\phi \coloneqq p_1 \circ g_1 \circ q_1 \circ f_1$ is an automorphism. Let $\gamma \coloneqq \phi^{-1}$. This implies $(\gamma \circ p_1 \circ g_1) \circ (q_1 \circ f_1) = \mathrm{id}_{A_1}$, so that $q_1 f_1$ has a left inverse. We check that this is also a right inverse of $q_1 f_1$, giving $B_1 \cong A_1$.

Let $\theta \coloneqq (q_1 f_1)(\gamma p_1 g_1) : B_1 \to B_1$, which is normal. We want to check that this is the identity map. It's easy to compute $\theta^2 = \theta$. By Fitting, θ is either an automorphism or nilpotent. If θ is an automorphism, then $\theta^2 = \theta \implies \theta = \mathrm{id}_{B_1}$, and we're done. Suppose that it is nilpotent with n minimal such that $\theta^n = 0$. Then $0 = \theta^n = \theta^2 \circ \theta^{n-2} = \theta \circ \theta^{n-2} = \theta^{n-1}$. Hence $n = 1$, so that $\theta = 0$. This implies that $\mathrm{id}_{A_1}^2 = (\gamma p_1 g_1)(q_1 f_1)(\gamma p_1 g_1)(q_1 f_1) = (\gamma p_1 g_1)\theta(q_1 f_1) = 0$, forcing $A_1 = \{e\}$, a contradiction.

Now, $\ker q_1 = B_2 \times \cdots \times B_t$ [[even after reindexing?]], while $\ker q_1 \circ f_1 = \{e\}$. Hence

$$H \coloneqq A_1 \cdot (B_2 \times \cdots \times B_t) \cong A_1 \times B_2 \times \cdots \times B_t.$$

Define $\psi : G \to G$ by

$$b_1 b_2 \cdots b_t \mapsto \gamma f_1 p_1(b_1) b_2 b_3 \cdots b_t = (q_1 f_1)^{-1}(b_1) b_2 \cdots b_t = f_1 (q_1 f_1)^{-1} q_1 + g_2 q_2 + \cdots + g_t q_t,$$

which is a normal endomorphism with image equal to H. Moreover, since $A_1 \cap (B_2 \times \cdots \times B_t) = \{e\}$, we have $\ker\psi = \{e\}$. Therefore, ψ is an isomorphism by Fitting, which forces $H = G$.

In summary, $A_2 \times \cdots \times A_s \cong G/A_1 \cong B_2 \times \cdots \times B_t$. We can repeat our above argument to see that $s = t$ and that $A_i \cong B_i$ up to reindexing. □

Corollary 10. Suppose G is finite abelian, so that $G \cong C_{p_1^{k_1}} \times \cdots \times C_{p_n^{k_n}}$. Then the (p_i, k_i) are uniquely determined up to reordering.

Corollary 11. Suppose that G is finite and that

$$G = F^0 G \geq F^1 G \geq \cdots \geq F^s G = \{e\}$$

and

$$G = T^0 G \geq T^1 G \geq \cdots \geq T^t G = \{e\}$$

are two composition series of G. Define the *graded groups* $\mathsf{gr}_F(G) = \prod {}^{F^i}\!/_{F^{i+1}}$ and $\mathsf{gr}_T(G) = \prod {}^{T^i}\!/_{T^{i+1}}$. If $\mathsf{gr}_F(G) \cong \mathsf{gr}_T(G)$, then each pair of factors of F and T are isomorphic up to reordering.

Definition. If $F^\bullet G$ and $T^\bullet G$ are two composition series for G, then they are *equivalent* or *isomorphic* if $\mathsf{gr}_F(G) \cong \mathsf{gr}_T(G)$.

(Lecture 13)

Definition. Let G be a group. A *filtration $F^\bullet G$ on G* is a subnormal series

$$\cdots \trianglelefteq F^{i+1}G \trianglelefteq F^iG \trianglelefteq F^{i-1}G \trianglelefteq \cdots \trianglelefteq F^0G = G.$$

Remark 21. Suppose that $F^\bullet G$ is a filtration on G.

1. If $i : H \hookrightarrow G$, then we get an induced filtration on H given by

$$F^aH := i^{-1}(F^aG) = H \cap F^aG.$$

2. Similarly, if $q : G \to K$ is a quotient map, then we get an induced filtration on K given by

$$F^aK := q(F^aG) = {}^{F^aG}\!/_{F^aG \cap \ker q}.$$

[[How does this define a series of subgroups?]]

Remark 22. Suppose that $F^\bullet G$ and $T^\bullet G$ are two filtrations on G. Define the *graded i-th piece* as

$$\mathsf{gr}^i_F(G) = {}^{F^iG}\!/_{F^{i+1}G}.$$

By our previous remark, there is an induced filtration $T^\bullet \, \mathsf{gr}^i_F(G)$. Similarly, there is an induced filtration $F^\bullet \, \mathsf{gr}^j_T(G)$. Then we get graded pieces $\mathsf{gr}^j_T \, \mathsf{gr}^i_F \, G$ and $\mathsf{gr}^i_F \, \mathsf{gr}^j_T \, G$. These produce two *bigraded* groups $\mathsf{gr}_F \, \mathsf{gr}_T \, G$ and $\mathsf{gr}_T \, \mathsf{gr}_F \, G$.

Lemma 8. (Zassenhaus or butterfly) Suppose G is a group with $A \trianglelefteq \widetilde{A} \le G \ge \widetilde{B} \trianglerighteq B$. Then we have a group isomorphism

$${}^{A \cdot (\widetilde{A} \cap \widetilde{B})}\!/_{A \cdot (\widetilde{A} \cap B)} \cong {}^{B \cdot (\widetilde{A} \cap \widetilde{B})}\!/_{B \cdot (A \cap \widetilde{B})}.$$

Proof. We know that

$$A \trianglelefteq \widetilde{A} \implies A \cap \widetilde{B} \trianglelefteq \widetilde{A} \cap \widetilde{B} \qquad B \trianglelefteq \widetilde{B} \implies \widetilde{A} \cap B \trianglelefteq \widetilde{A} \cap \widetilde{B}.$$

Then $D := (A \cap \widetilde{B}) \cdot (\widetilde{A} \cap B) \cong (\widetilde{A} \cap B) \cdot (A \cap \widetilde{B})$ is normal in $\widetilde{A} \cap \widetilde{B}$. Let $x \in B \cdot (\widetilde{A} \cap \widetilde{B})$ and write $x = bc$. Take $cD \in {}^{\widetilde{A} \cap \widetilde{B}}\!/_D$. The map $f : x \mapsto cD$ is well-defined. Indeed, if $x = b_1c_2 = b_2c_2$, then $b_2^{-1}b_1 = c_2c_1^{-1}$, so that $c_2c_1^{-1} \in B \cap \widetilde{A} \cap \widetilde{B} = \widetilde{A} \cap B \le D$, i.e., $c_2D = c_1D$.

It's clear that f is surjective. We show that f is a homomorphism. Let $x_1 = b_1c_1$ and $x_2 = b_2c_2$. Then $x_1x_2 = b_1(c_1b_2c_1^{-1})c_1c_2$. Thus, $f(x_1x_2) = c_1c_2D = (c_1D)(c_2D)$.

Moreover, we compute

$$\begin{aligned}
\ker f &= \{x = bc : c \in D\} \\
&= \{x = bc_1c_2 : c_1 \in A \cap \widetilde{B},\ c_2 \in \widetilde{A} \cap B\} \\
&= \{x = bc_1c_2 : c_2 \in A \cap \widetilde{B},\ c_1 \in \widetilde{A} \cap B\} \\
&= \{x = bc : c \in A \cap \widetilde{B}\} = B \cdot (A \cap \widetilde{B}).
\end{aligned}$$

Therefore, ${}^{B \cdot (\widetilde{A} \cap \widetilde{B})}\!/_{B \cdot (A \cap \widetilde{B})} \cong {}^{\widetilde{A} \cap \widetilde{B}}\!/_D$.

The other isomorphism with ${}^{\widetilde{A} \cap \widetilde{B}}\!/_D$ is obtained by swapping $A \longleftrightarrow B$ and $\widetilde{A} \longleftrightarrow \widetilde{B}$. $\square$

Corollary 12. $\mathsf{gr}_T^j \mathsf{gr}_F^i G \cong \mathsf{gr}_F^i \mathsf{gr}_T^j G$.

Proof. Note that $\mathsf{gr}_F^i \mathsf{gr}_T^j G = \frac{F^i(\mathsf{gr}_T^j G)}{F^{i+1}(\mathsf{gr}_T^j G)}$. Using the second isomorphism theorem, we see that

$$F^i(\mathsf{gr}_T^j G) = \frac{F^i(T^jG)}{F^i(T^jG) \cap T^{j+1}G} = \frac{T^jG \cap F^iG}{(T^jG \cap F^iG) \cap T^{j+1}G} \cong \frac{T^{j+1}G \cdot (T^jG \cap F^iG)}{T^{j+1}G}.$$

Similarly, $F^{i+1}(\mathsf{gr}_T^j G) \cong \frac{T^{j+1}G\cdot(T^jG \cap F^{i+1}G)}{T^{j+1}G}$. It follows that

$$\mathsf{gr}_F^i \mathsf{gr}_T^j G = \frac{T^{j+1}G \cdot (T^jG \cap F^iG)}{T^{j+1}G \cdot (T^jG \cap F^{i+1}G)}.$$

Likewise, we can show that

$$\mathsf{gr}_T^j \mathsf{gr}_F^i G = \frac{F^{i+1}G \cdot (F^iG \cap T^jG)}{F^{i+1}G \cdot (F^iG \cap T^{j+1}G)}.$$

Thus, the assertion that $\mathsf{gr}_T^j \mathsf{gr}_F^i G \cong \mathsf{gr}_F^i \mathsf{gr}_T^j G$ is a special instance of the butterfly lemma. □

Definition. A filtration $F^\bullet G$ is called *non-repetitious* if $F^i \neq F^{i+1}G$ for any i.

Definition. We say $\{R^iG\}_{i=1}^t$ is a *refinement* of $\{F^iG\}_{i=1}^s$ if there is a non-decreasing map $j : [s] \to [t]$ such that $F^aG = R^{j(a)}G$ for every $a \in [s]$.

Theorem 7. (Schreier refinement theorem) Suppose $\{F^iG\}_{i=0}^s$ and $\{T^jG\}_{j=0}^t$ are filtrations on G. Then we can find respective refinements $\widetilde{F}^\bullet G$ and $\widetilde{T}^\bullet G$ which are equivalent to our original filtrations. Further, if the two original filtrations are non-repetitious, then we can choose the refinements to be non-repetitious as well.

Proof. Suppose $F^\bullet$ and $T^\bullet$ are non-repetitious. Let $\widetilde{F}_{i-1}^{(j)} = (F^{i-1} \cap T^j) \cdot F^i$. Then for any $q \leq i \leq s$, we get a filtration

$$F^{i-1} = F^{i-1} \cdot F^i = \widetilde{F}_{i-1}^{(0)} \geq \widetilde{F}_{i-1}^{(1)} \geq \cdots \geq \widetilde{F}_{i-1}^{(t)} = F^i.$$

Thus, the $\widetilde{F}_{i-1}^{(j)}$ define a refinement of $F^\bullet G$.

Likewise, $\widetilde{T}_{j-1}^{(i)} := (T^{j-1} \cap F^i) \cdot T^j$ defines a refinement of $T^\bullet G$.

Finally, apply Zassenhaus to the system $F^i \trianglelefteq F^{i-1} \leq G \geq T^{j-1} \trianglerighteq T^j$ to get

$$\begin{aligned}
\widetilde{F}_{i-1}^{(j-1)} \big/ \widetilde{F}_{i-1}^{(j)} &\cong F^i \cdot (F^{i-1} \cap T^{j-1}) \big/ F^i \cdot (F^{i-1} \cap T^j) \\
&\cong T^j \cdot (F^{i-1} \cap T^{j-1}) \big/ T^j \cdot (F^i \cap T^{j-1}) \\
&\cong \widetilde{T}_{j-1}^{(i-1)} \big/ \widetilde{T}_{j-1}^{(i)}.
\end{aligned}$$

□

Corollary 13. (Jordan-Holder) Any two composition series of G are equivalent.

Proof. Since each intermediate term in a composition series is a maximal normal subgroup, neither series admits a proper refinement. Hence any refinement must be identical to the original series. Hence Schreier completes the proof. □

(Lectures 14 and 15)

Remark 23. Suppose that

$$(\xi) : 1 \longrightarrow H \xrightarrow{i} G \xrightarrow{q} K \longrightarrow 1$$

is an extension. If $x \in G$, then lift it via q^{-1} to $\tilde{x}$. Now $\mathrm{conj}_{\tilde{x}} : G \to G$ is a (group) automorphism. Since $H \trianglelefteq G$, we thus have an automorphism $\mathrm{conj}_{\tilde{x}} \restriction_H$. Hence we get a map $K \ni x \mapsto \mathrm{conj}_{\tilde{x}} \restriction_H \in \mathrm{Aut}(H)$. It turns out that distinct lifts of x give distinct automorphisms whose difference is an inner automorphism.

Indeed, consider the map $\alpha^\xi : K \to \mathrm{Out}(H)$ defined by $x \mapsto \mathrm{conj}_{\tilde{x}} \cdot \mathrm{Inn}(H)$. This is well-defined. If $\tilde{x}$ and $\tilde{\tilde{x}}$ are distinct lifts of x, then $q(\tilde{x}) = x = q(\tilde{\tilde{x}}) \implies q(\tilde{x}^{-1}\tilde{\tilde{x}}) = e \implies \tilde{\tilde{x}} = \tilde{x}h$ for some $h \in H \implies \mathrm{conj}_{\tilde{\tilde{x}}} \restriction_H = \mathrm{conj}_{\tilde{x}} \restriction_H \circ \mathrm{conj}_h \implies \mathrm{conj}_{\tilde{\tilde{x}}} \restriction_H \sim \mathrm{conj}_{\tilde{x}} \restriction_H$.

Moreover, α^ξ is a homomorphism. If $x, y \in K$, then $\tilde{x}\tilde{y}$ is a lift of xy since q is a homomorphism. Thus, $\mathrm{conj}_{\tilde{x}\tilde{y}} \restriction_H = \mathrm{conj}_{\tilde{x}} \restriction_H \circ \mathrm{conj}_{\tilde{y}} \restriction_H \implies \alpha^\xi(xy) = \alpha^\xi(x)\alpha^\xi(y)$.

Now, if ξ is split via $s : K \to G$, then we get a homomorphism $\alpha^{\xi,s} : K \to \mathrm{Aut}(H)$ given by $x \mapsto \mathrm{conj}_{s(x)} \restriction_H$. Notice that $\alpha^{\xi,s}(x) \cdot \mathrm{Inn}(H) = \alpha^\xi(x)$. It follows that

$$\begin{tikzcd}
K \arrow[r, "\alpha^{\xi,s}"] \arrow[dr, "\alpha^\xi"'] & \mathrm{Aut}(H) \arrow[d, "\pi"] \\
& \mathrm{Out}(H)
\end{tikzcd}$$

commutes.

Given $\alpha : K \to \mathrm{Out}(H)$ homomorphism, we can now reduce the problem of classifying all extensions of K by H to the problem of classifying all extensions ξ such that $\alpha^\xi = \alpha$. Let $\mathrm{Ext}(K, (H, \alpha))$ denote the set of all isomorphism classes of extensions of K by H with invariant α.

Example 22.

1. Since $Z(S_3) = \{e\}$, we have that $\mathrm{Inn}(S_3) = S_3$. Recall that $S_3 \cong D_6$, so that

   $$S_3 = \langle a, b \mid a^2 = b^3 = e,\ b^2 a = ab \rangle.$$

   Let ϕ be an automorphism of S^3. Then $\phi(a) \in \{a, ab, ab^2\}$ and $\phi(b) \in \{b, b^2\}$. Hence $|\mathrm{Aut}(S_3)| \leq 6$. But $S_3 \leq \mathrm{Aut}(S_3)$, forcing $\mathrm{Aut}(S_3) = S_3$.

2. If G is abelian, then $\mathrm{Aut}(G) = \mathrm{Out}(G)$.

3. Let $f : G \to H$ be a surjective map and $\phi \in \mathrm{Aut}(G)$ such that $\phi(\ker f) = \ker f$. This induces an automorphism $\phi^f : H \to H$ given by $h = f(g) \mapsto f(\phi(g))$. [[Is this well-defined?]] Note that if $x \in G$, then $\mathrm{conj}_x : G \to G$ preserves any normal subgroup. Hence we get $(\mathrm{conj}_x)^f : H \to H$ given by $h \mapsto \mathrm{conj}_{f(x)}(h)$. In general, we have a group map $\mathrm{Inn}(G) \to \mathrm{Inn}(H)$, which in turn induces a group map $(-)^f : {\{\phi \in \mathrm{Aut}(G) : \phi(\ker f) = \ker f\}}\big/{\mathrm{Inn}(G)} \to \mathrm{Out}(H)$. [[Why?]]

   For example, consider the quotient $q : G \to G^{\mathrm{ab}}$. Since $[G, G]$ is a characteristic subgroup, we get $(-)^{\mathrm{ab}} : \mathrm{Out}(G) \to \mathrm{Out}(G^{\mathrm{ab}}) \cong \mathrm{Aut}(G^{\mathrm{ab}})$.

Example 23. Let Σ_g denote a surface of genus g. We can draw Σ_g as an oriented $4g$-gon with pairs of sides identified as follows.

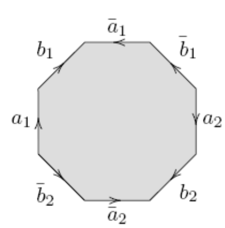

Figure 1: copied from the Manifold Atlas

For example, $a_1 \sim \bar{a}_1$. Then

$$\pi_1(\Sigma_g) = \langle a_1, \dots, a_g, b_1, \dots, b_g \mid \prod_{i=1}^{g} [a_i, b_i] = 1 \rangle.$$

We have $H_1(\Sigma_g) = \pi_1(\Sigma_g)^{\text{ab}} = \bigoplus_{i=1}^{g} (\mathbb{Z}a_i \oplus \mathbb{Z}b_i) \cong \mathbb{Z}^{2g}$. This induces the following diagram.

$$\begin{tikzcd}
\mathrm{Out}(\pi_1(\Sigma_g)) \arrow[r, "(-)^{\text{ab}}"] \arrow[drr, dashed, "G"'] & \mathrm{Aut}(H_1(\Sigma_g)) \arrow[r, "\cong"] & \mathrm{GL}_{2g}(\mathbb{Z}) \arrow[d, "\det"] \\
 & & \{\pm 1\}
\end{tikzcd}$$

Let $\mathrm{Map}(\Sigma_g) \coloneqq \ker G$. In fact, $\mathrm{Map}(\Sigma_g) \cong {}^{\mathrm{Diff}^+(\Sigma_g)}\!/\!_{\mathrm{Diff}_0(\Sigma_g)}$, where Diff^+ denotes the diffeomorphisms preserving orientation and Diff_0 denotes the diffeomorphisms isotopic to id_{Σ_g}.

Remark 24. We assume for the remainder of the classification problem that the subgroup of G is abelian. Thus, any $\alpha : K \to \mathrm{Out}(H) \cong \mathrm{Aut}(H)$ is an action.

Definition. A *K-module* is a pair (A, α) such that A is an abelian group and $\alpha : K \to \mathrm{Aut}(A)$ is a group map.

Definition. We work to define an operation on $\mathrm{Ext}(K, (A, \alpha))$.

1. Let $\phi : L \to K$ be a group map and $(\xi) : 1 \to A \to G \to K \to 1$ be an extension. We can use ϕ to produce an extension of L by A. Define the *fiber product* $G \times_K L = \{(g, l) \in G \times L : q(g) = \phi(l)\}$, which is a subgroup of $G \times L$.

   There is a natural map $p : G \times_K L \twoheadrightarrow L$ given by $(g, l) \mapsto l$. Also, $\ker p = \{(g, e) : q(g) = \phi(e) = e\} = \{(g, e) : g \in A\} \cong A$. This induces

$$\begin{tikzcd}
(\xi) : 1 \arrow[r] & A \arrow[r] \arrow[d, equal] & G \arrow[r, "q"] & K \arrow[r] & 1 \\
(\phi^*\xi) : 1 \arrow[r] & A \arrow[r] & G \times_K L \arrow[r, "p"] \arrow[u] & L \arrow[r] \arrow[u, "\phi"] & 1
\end{tikzcd}.$$

   We call $G_{\phi^*\xi} \coloneqq G \times_K L$ together with the induced map $\phi^* : G \times_K L \to G$ the *pullback* of q and ϕ. By construction, $\alpha^{\phi^*\xi} : L \to \mathrm{Aut}(A)$. is given by $\alpha^{\xi} \circ \phi$. We have defined a function $\phi^* : \mathrm{Ext}(K, (A, \alpha)) \to \mathrm{Ext}(L, (L, \alpha \circ \phi))$.

2. Let A and B be K modules and ξ be as above. Let $\psi : (A, \alpha) \to (B, \beta)$ be an equivariant map. We construct the *pushout* $G \cup_A B$ of i and ψ.'

   Consider the action $\beta \circ q : G \to \mathrm{Aut}(B)$. This induces the group map $i \times \psi : A \to G \ltimes_{\beta \circ q} B$ given by $a \mapsto (a, \psi(a))$.

   Lemma 9. The map $i \times \psi$ is injective with $\mathrm{im}(i \times \psi) \coloneqq A \trianglelefteq G \ltimes_{\beta \circ q} B$. Moreover $A \leq \ker(G \ltimes_{\beta \circ q} B \twoheadrightarrow K)$.

   Proof. Injectivity follows from the fact that i is injective. Recall the group law on $G \ltimes_{\beta \circ q} B$ is given by $(g_1, b_1)(g_2, b_2) = (g_1 g_2, b_1(\beta \circ q(g_1)(b_2)))$. To see that A is normal, we compute

$$(g, b)(a, \psi(a)()g, b)^{-1} = (g, b)(a, \psi(a))(g^{-1}, \beta \circ q(g^{-1})(b^{-1})) = (ga, b\beta \circ q(g)(\psi(a)))(g^{-1}, \beta \circ q(g^{-1})(b^{-1}))$$
$$= (gag^{-1}, b\beta \circ q(g)(\psi(a))\beta \circ q(ga)\beta \circ q(g^{-1})(b^{-1})) = (gag^{-1}, b\beta \circ q(g)(\psi(a))\beta(q(g)\underbrace{q(a)}_{=1}q(g^{-1}))(b^{-1}))$$
$$= (gag^{-1}, b\beta \circ q(g)(\psi(a))b^{-1}) = (gag^{-1}, \beta \circ q(g)(\psi(a))) = (gag^{-1}, \psi(\alpha \circ q(g)(a)))$$
$$= (\alpha \circ q(g)(a), \psi(\alpha \circ q(g)(a))) \in \mathrm{im}(i \times \psi).$$

   [[Why does $\alpha \circ q(g)(a) = gag^{-1}$ hold?]]

   Finally, observe that $\ker(G \ltimes_{\beta \circ q} B \twoheadrightarrow K) = \{(g, b) : q(g) = e\} = \{(g, b) : g \in A\} \geq A \times \{e\} \cong A$. ☐

Now, we define $G_{\psi_*\xi} := G \cup_A B = {}^{G \ltimes_{\beta \circ q} B}\!\big/_{(i \times \psi)(A)}$.

We have obtained the commutative diagram.

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, hook] & G \arrow[r] \arrow[d, hook] & K \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & A \times B \arrow[r, "i"] \arrow[d, two heads] & G \ltimes_{\beta \circ q} B \arrow[r, "q"] \arrow[d, two heads] & K \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & B \cong {}^{A \times B}\!\big/_{(i \times \psi)(A)} \arrow[r] & G_{\psi_*\xi} \arrow[r] & K \arrow[r] & 1
\end{tikzcd},$$

where $B \cong {}^{A \times B}\!\big/_{(i \times \psi)(A)}$ is via $b \mapsto [(e, b)]$. Let ψ_* denote the induced map $G \to G_{\psi_*\xi}$. Define the extension $\psi_*\xi$ as the bottom row.

3. Given $\xi, \eta \in \mathrm{Ext}(K, (A, \alpha))$, we can take $\xi \times \eta \in \mathrm{Ext}(K \times K, (A \times A, \alpha \times \alpha))$. The diagonal map $\Delta : K \to K \times K$ is a homomorphism. The function $\mathrm{mult} : A \times A \to A$ is as well since A abelian. It is also equivariant for $\alpha \times \alpha$ and α.

   Therefore, we can construct the following commutative diagram.

$$\begin{tikzcd}
1 \arrow[r] & A \times A \arrow[r] & G_\xi \times G_\eta \arrow[r] & K \times K \arrow[r] & 1 \\
1 \arrow[r] & A \times A \arrow[r] \arrow[u, equal] \arrow[d, "\mathrm{mult}"'] & (G_\xi \times G_\eta) \times_{K \times K} K \arrow[r] \arrow[u] \arrow[d] & K \arrow[r] \arrow[u, "\Delta"] \arrow[d, equal] & 1 \\
1 \arrow[r] & A \arrow[r] & ((G_\xi \times G_\eta) \times_{K \times K} K) \cup_{A \times A} A \arrow[r] & K \arrow[r] & 1
\end{tikzcd}$$

   Then define $\xi + \eta$ as the bottom row.

Exercise 16. Show that

$$\xi + \eta = \mathrm{mult}_* \Delta^*(\xi \times \eta) = \mathrm{mult} \circ ((\xi \times \eta) \circ \Delta) = (\mathrm{mult} \circ (\xi \times \eta)) \circ \Delta.$$

This implies that we could have taken the pushout first and then the pullback.

Exercise 17.

1. Verify that $(\mathrm{Ext}(K, (A, \alpha)), +)$ is an abelian group with identity $K \ltimes_\alpha A$.

2. Verify that ϕ^* and ψ_* are homomorphisms.

Remark 25. Suppose that $(\xi) : 1 \to A \to G \to K \to 1$ is an extension. If it is not split, then by the axiom of choice there is some set-theoretic section $s : K \to G$ of q.

Define $f : K \times K \to G$ by $(x, y) \mapsto s(x)s(y)s(xy)^{-1}$. This is a homomorphism if and only if it is constant at e_G. Notice that $q(f(x, y)) = e$ for any $x, y \in K$. Then $\mathrm{im}\, f \subset A$, giving $f : K \times K \to A$.

Definition. We say that f is *normalized* if $f(e, y) = f(x, e) = e$ for any $x, y \in K$. Note that if s is *normalized*, i.e., preserves the identity, then f is automatically normalized.

(Lecture 16)

Lemma 10. Let ξ be as before with s and hence f normalized. Then the data $(K, (A, \alpha), f)$ determines ξ up to isomorphism.

Proof. Let G_f be the group with underlying set $K \times A$ and group law given by $(x,a)(y,b) = (xy, a\alpha_x(b)f(x,y))$. The following diagram commutes.

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "i_f"] \arrow[d] & G_f \arrow[r, "q_f"] \arrow[d, "s\times i"] & K \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & A \arrow[r, "i"] & G \arrow[r, "q"] & K \arrow[r] \arrow[l, bend left, "s"] & 1 \end{tikzcd},$$

where $(s \times i)(x,a) = s(x)a$. ☐

Remark 26. In general, given $(K,(A,\alpha))$ and a normalized function $f : K \times K \to A$, then the formula $(x,a)(y,b) = (xy, a\alpha_x(b)f(x,y))$ defines a group law if and only if $f(x,y)f(xy,z) = \alpha_x(f(y,z))f(x,yz)$ for any $x,y,z \in K$. As A is abelian, this happens if and only if

$$\alpha_x(f(y,z))f(xy,z)^{-1}f(x,yz)f(x,y)^{-1} = e. \tag{$*$}$$

Definition.

1. We call $C^2(K,(A,\alpha)) \coloneqq \{f \mid f : K \times K \to A\}$ the set of *second Hochschild cochains of K with coefficients in (A,α)*.
2. We call $C^2(K,(A,\alpha))_0 \coloneqq \{f \mid f(x,e) = f(e,y) = e\}$ the set of *second normalized cochains*.
3. We call $Z^2(K,(A,\alpha)) \coloneqq \{f \in C^2 : (*) \text{ holds }\}$ the set of *second cocycles of K with coefficients in (A,α)*.

Remark 27. Our last remark implies that there is a one-to-one correspondence

$$\{(\xi,s) : \xi \in \mathrm{Ext}(K,(A,\alpha)),\ s \text{ a normalized section}\} \longleftrightarrow Z^2(K,(A,\alpha))_0 = Z^2 \cap C^2_0.$$

Remark 28. If $\tilde{s}$ and s are both normalized sections, then $c(x) \coloneqq \tilde{s}(x)s(x)^{-1}$ is a map $c : K \to A$ such that $c(e) = e$. Let $\tilde{f}$ be the second cochain obtained from $\tilde{s}$. Then $\tilde{f}(x,y) = \tilde{s}(x)\tilde{s}(y)\tilde{s}(xy)^{-1} = c(x)s(x)c(y)s(y)(c(xy)s(xy))^{-1}$. Thus,

$$\begin{aligned} \tilde{f}(x,y)f(x,y)^{-1} &= c(x)s(x)c(y)s(y)(c(xy)s(xy))^{-1}s(xy)s(y)^{-1}s(x)^{-1} \\ &= c(x)(s(x)c(y)s(x)^{-1})(s(x)s(y)s(xy)^{-1})c(xy)^{-1}s(xy)s(y)^{-1}s(x)^{-1} \\ &= c(x)\alpha_x(c(y))c(xy)^{-1}f(x,y)f(x,y)^{-1} = c(x)\alpha_x(c(y))c(xy)^{-1}. \end{aligned}$$

This gives a map $\delta : C^1_0 \to Z^2_0$ defined by $c \mapsto (\delta_c : (x,y) \mapsto c(x)\alpha_x(c(y))c(xy)^{-1})$, which we call the *first Hochschild differential of K with coefficients in (A,α)*. [[How do we know any first normalized cochain can be written in that form?]] We in turn obtain a natural map $\delta' : \mathrm{Ext}(K,(A,\alpha)) \to HH^2(K,(A,\alpha)) \coloneqq Z^2_0/\mathrm{im}\,\delta$ given by $(\xi,f) \mapsto [f]$. We call $HH^2(K,(A,\alpha))$ the *second cohomology group of K with coefficients in (A,α)*.

Exercise 18. Show that δ' is an isomorphism of abelian groups.

Example 24. Find all extensions of $\mathbb{Z}/2 \cong \mathbb{M}_2 \coloneqq \{\pm 1\}$ by $\mathbb{Z}$. That is, we classify all s.e.s. of the form

$$1 \longrightarrow \mathbb{Z} \longrightarrow G \longrightarrow \mathbb{M}_2 \longrightarrow 1$$

<u>Case 1:</u> $\mathbb{M}_2$ acts trivially on $\mathbb{Z}$. Then $C^2_0 = \{f : \mathbb{M}_2 \times \mathbb{M}_2 \to \mathbb{Z} \mid f(1,y) = f(x,1) = 0 \text{ for any } x,y \in \mathbb{M}_2\}$. Each $f \in C^2_0$ is thus determined by $f(-1,-1)$, giving $C^2_0 \cong \mathbb{Z}$ via $f \mapsto f(-1,1)$.

Note that $f \in Z^2_0 \iff f(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0$ for any $x,y,z \in \mathbb{M}_2$. It's easy to check this is always satisfied. Hence $Z^2_0 \cong \mathbb{Z}$ as well.

Moreover, $C^1_0 = \{c : \mathbb{M}_2 \to \mathbb{Z} : c(1) = 0\} \cong \mathbb{Z}$, giving the correspondence $\mathbb{Z} \ni b \longleftrightarrow (c : -1 \mapsto b)$. Then the differential $\delta : C_0^1 \to Z_0^2 \cong \mathbb{Z}$ is given by $\delta_c(x,y) = c(x)+c(y)-c(xy) \implies \delta_c(-1,-1) = c(-1)+c(-1) = 2b$. That is, $\delta : \mathbb{Z} \to \mathbb{Z}$ is given by $b \mapsto 2b$. This implies that $HH^2 = \mathbb{Z}/2$, so that the only nontrivial extension is

$$1 \longrightarrow \mathbb{Z} \xrightarrow{\text{mult}_2} \mathbb{Z} \longrightarrow Z/2 \longrightarrow 1 \ .$$

<u>Case 2:</u> The action is nontrivial with $-1 \mapsto (n \mapsto -n)$. Again we get $C_0^2 \cong \mathbb{Z}$. Moreover, if $f \in Z_2^0$ and $y = z = -1$, then

$$\begin{aligned} 0 &= \alpha_x(f(-1,-1)) - f(-x,-1) + f(x,1) - f(x,-1) \\ &= \alpha_x(\underbrace{f(-1,-1)}_{a}) - f(-x,-1) - f(x,-1) = \end{aligned}$$

$$\begin{cases} 0 & x = 1 \\ -2a & x = -1 \end{cases} .$$

Hence $a = 0$, and $f = 0$. This implies that $HH^2 = 0$ with $\mathbb{Z} \rtimes_\alpha \mathbb{M}_2$ being the unique extension.

(Lecture 17)

Definition. A *category* $\mathscr{C}$ consists of

- a class of *objects* $\operatorname{ob}\mathscr{C}$,
- a class of*morphisms* $\operatorname{mor}\mathscr{C}$,
- a set $\operatorname{Hom}_{\mathscr{C}}(x,y)$ of morphisms with *source* x and *target* y for each $x, y \in \operatorname{ob}\mathscr{C}$, and
- a *composition* partial function $\circ : \operatorname{Hom}_{\mathscr{C}}(x,y) \times \operatorname{Hom}_{\mathscr{C}}(y,z) \to \operatorname{Hom}_{\mathscr{C}}(x,z)$ where $(f,g) \mapsto g \circ f$.

These data must satisfy the following properties.

- $\operatorname{mor}\mathscr{C} = \coprod_{x,y \in \operatorname{ob}\mathscr{C}} \operatorname{Hom}_{\mathscr{C}}(x,y)$.
- Composition is associative.
- For each $x \in \operatorname{ob}\mathscr{C}$, there is an *identity morphism* $\mathrm{id}_x : x \to x$ such that $f \circ \mathrm{id}_x = f$ and $\mathrm{id}_x \circ g = g$ for any $f : x \to y$ and $g : z \to x$.

Definition. A morphism $\varphi : A \to B$ in $\mathscr{C}$ is an *isomorphism* if $\psi \circ \varphi = \mathrm{id}_A$ and $\varphi \circ \psi = \mathrm{id}_B$ for some morphism $\psi : B \to A$.

Note 5. if $\mathscr{C}$ is small, then $(\operatorname{mor}\mathscr{C}, \circ)$ is a partially-defined monoid.

Example 25. The following are examples of categories.

1. Recall the category $\mathbf{sSet} = \mathbf{Fun}(\Delta^{\mathrm{op}}, \mathbf{Set})$ of simplicial sets. Also recall the standard n-simplex

   $$\Delta^n = \{(t_0, \ldots, t_n) \in \mathbb{R}^{n+1} : t_i \geq 0, \ \sum_i t_i = 1\}.$$

   In this case, we send a morphism $f : [m] \to [n]$ to

   $$\Delta_f : \mathbb{R}^{m+1} \to \mathbb{R}^{n+1} \qquad e_i \mapsto e_{f(i)},$$

   which is linear over $\mathbb{R}$. Note that Δ is a covariant functor, hence not a simplicial set in the strict sense. Given a simplicial set $X_\bullet$, define its *geometric realization*

   $$|X_\bullet| = \coprod_{m \geq 0} (X_m \times \Delta^m)/\sim$$

   where $X_n \times \Delta^n \ni (x,y) \sim (x',y') \in X_m \times \Delta^m$ if $X(f)(y') = y$ and $\Delta_f(x) = x'$ for some $f : [n] \to [m]$.

2. Let **Corr** denote the *category of correspondences* with objects sets and morphisms binary relations. Given relations $u \subset X \times Y$ and $v \subset Y \times Z$, we define

   $v \circ u = \{(x, y) \in X \times Z : (\exists b \in Y)((x, b) \in u \text{ and } (b, y) \in v)\}$. Then the identity morphisms are precisely the diagonals.

3. Let $\mathbf{Ouv_X}$ denote the category of open sets of the topological space X with inclusion maps as morphisms.

   Aside. This is an order category associated to the poset $\subseteq$.

4. Let G be a group. Then the *classifying space BG of G* is a category with a single object $*$ and $BG(*, *) = G$. Composition is given by the group law.

Definition. Let $\mathscr{C}$ and $\mathscr{D}$ be categories. A *(covariant) functor $F : \mathscr{C} \to \mathscr{D}$ from $\mathscr{C}$ to $\mathscr{D}$* consists of two functions $F : \operatorname{ob}\mathscr{C} \to \operatorname{ob}\mathscr{D}$ and $F : \operatorname{mor}\mathscr{C} \to \operatorname{mor}\mathscr{D}$ such that

- $F(f) : F(x) \to F(y)$ in $\mathscr{D}$ whenever $f : x \to y$ in $\mathscr{C}$ and
- F respects both composition and identity.

We call F *contravariant* is it is a covariant functor $F : \mathscr{C}^{\mathrm{op}} \to \mathscr{D}$.

Definition. We call a contravariant functor $\mathscr{C} \to \mathscr{D}$ a *presheaf of $\mathscr{C}$ with values in $\mathscr{D}$*.

(Lecture 18)

Example 26. The following are examples of functors.

1. The forgetful functor $\mathbb{G}_A : \mathbf{Ring} \to \mathbf{Ab}$ is called the *additive group functor*.

2. Let $f : X \to Y$ be a map of spaces. Define the *section functor*

$$\Gamma_f : \mathbf{Ouv_Y}^{\mathrm{op}} \to \mathbf{Set}$$

$$\mho \mapsto \{s : \mho \to X \mid f \circ s = \mathrm{id}_\mho\}$$

$$\Gamma_f(\mho \subset V) : (s : V \to X) \to (s \restriction_\mho : \mho \to X).$$

   We also denote this by $\Gamma_{X/Y}$.

3. Let $n \geq 0$. We have the *homology functor* $H_n(-, \mathbb{Z}) : \mathbf{Top} \to \mathbf{Ab}$ sending each space X to $H_n(X, \mathbb{Z})$, the *n-th singular homology of X*.

4. Recall the homotopy functor $\pi_i : \mathbf{Top}_*^{(\text{conn, lc})} \to \begin{cases} \mathbf{Grp} & i = 1 \\ \mathbf{Ab} & i > 1 \end{cases}$.

5. Define $(-)_\bullet : \mathbf{Set} \to \mathbf{sSet}$ by $S \mapsto \underset{constant/discrete}{(S)_\bullet}$ where $S_n = S$ for every $n \geq 0$.

   Alternatively, say that an element $x \in X_n$ is *nondegenerate* if it is not of the form $x = s_i(y)$ for any $1 \leq i \leq n-1$ and $y \in X_{n-1}$ and define $(S)_\bullet$ as the unique simplicial set such that $S_n^{\mathrm{nd}} = \begin{cases} S & n = 0 \\ \emptyset & n > 0 \end{cases}$.

   Remark 29. Note that $|(S)_\bullet|$ is homotopy equivalent to S equipped with the discrete topology.

6. The geometric realization functor $|\cdot| : \mathbf{sSet} \to \mathbf{Top}$.

7. Define $\mathrm{Sing}_\bullet : \mathbf{Top} \to \mathbf{sSet}$ by

$$\mathrm{Sing}_n(\underset{\text{space}}{X}) = \{\phi \mid \phi : \Delta^n \to X\} \qquad (f : [m] \to [n]) \mapsto (\mathrm{Sing}_f(X) : \phi \mapsto \phi \circ \Delta_f)$$

$$\mathrm{Sing}_n(\underset{\text{continuous}}{u : X \to Y}) : \mathrm{Sing}_n(X) \to \mathrm{Sing}_n(Y), \quad \phi \mapsto u \circ \phi.$$

Aside. This is right adjoint to the geometric realization functor.

8. If $n = 1, 2$, then we have $HH^n(G, -) : {}_G\mathbf{Mod} \to \mathbf{Ab}$.

Example 27. The following are examples of natural transformations.

1. $\det : \mathrm{GL}_n \to \mathrm{GL}_1$.
2. The *Hurewicz map* $\mathrm{Hur} : \pi_1 \to H_1$.
3. The universal property of $(-)^{\mathrm{ab}}$ induces a commutative diagram of functors

$$\begin{tikzcd} \pi_1 \arrow[r, "\mathrm{Hur}"] \arrow[d, "(-)^{\mathrm{ab}}"'] & H_1 \\ (\pi_1)^{\mathrm{ab}} \arrow[ur, dashed, "q"'] & \end{tikzcd}.$$

Hurewicz's theorem states that q is actually an isomorphism.

Exercise 19. The *double dualization* functor $(-)^{**} : \mathbf{Vect}_k \to \mathbf{Vect}_k$ induces a map of functors $\mathrm{id}_{\mathbf{Vect}_k} \to (-)^{**}$ given by $\epsilon_V : x \mapsto (\phi \mapsto \phi(x))$.

1. Show that this map is not a natural isomorphism by showing that if V is an infinite-dimensional $\mathbb{R}$-space with a countable basis, then V^* and hence V^{**} have uncountable bases.
2. Show, however, that it is an isomorphism for finite-dimensional spaces.

Definition.

1. We say that a category $\mathscr{C}$ is *small* if $\operatorname{ob}\mathscr{C}$ is a set.
2. Let $\pi_0(\mathscr{C}) \coloneqq {}^{\operatorname{ob}\mathscr{C}}\!/_{\cong}$. We say that $\mathscr{C}$ is *essentially small* if $\pi_0(\mathscr{C})$ is a set.

Exercise 20. Show that $\mathscr{C}$ is essentially small if and only if it is equivalent to a small category.

(Lectures 19 and 20)

Example 28. Let $\mathscr{C} \coloneqq \mathbf{Vector}_k^n$ and $\mathscr{D} \coloneqq B\,\mathrm{Mat}_n(k)$. There is a functor $F : \mathscr{D} \to \mathscr{C}$ given by $* \mapsto k^n$ and $A \mapsto (v \mapsto Av)$. Construct an inverse $G : \mathscr{C} \to \mathscr{D}$ via the axiom of choice by choosing a basis for each $V \in \mathscr{C}$ and mapping each linear map f to the matrix of f in the chosen bases. Then $\mathscr{C}$ and $\mathscr{D}$ are equivalent via F and G.

Remark 30. Any functor $F : \mathscr{C} \to \mathscr{D}$ induces a map $\pi_0(F) : \pi_0(\mathscr{C}) \to \pi_0(\mathscr{D})$. If F is an equivalence with quasi-inverse G, then this is a bijection with $\pi_0(G)$ as inverse. Therefore, two equivalent categories have the same collection of isomorphism classes of objects.

Definition. If $\mathscr{C}$ is a category, then we call $\mathscr{A}$ a subcategory of $\mathscr{C}$ if

- $\operatorname{ob}\mathscr{A}$ is a subclass of $\operatorname{ob}\mathscr{C}$,
- $\mathrm{Hom}_{\mathscr{A}}(x, y) \subset \mathrm{Hom}_{\mathscr{C}}(x, y)$ for any $x, y \in \operatorname{ob}\mathscr{A}$, and
- composition and identity in $\mathscr{A}$ are exactly as they are in $\mathscr{C}$.

Definition. Let $F : \mathscr{C} \to \mathscr{D}$ be a functor. Consider the set map $F(-) : \mathrm{Hom}_{\mathscr{C}}(x, y) \to \mathrm{Hom}_{\mathscr{D}}(F(x), F(y))$.

1. We say that F is *faithful* if $F(-)$ is injective.
2. We say that F is *full* if $F(-)$ is surjective.

Example 29. The inclusion functor $i : \mathscr{A} \to \mathscr{C}$ is faithful.

Remark 31. Notice that $\mathrm{Hom}_{\mathbf{Set}}(*, x) \xrightarrow{\sim} x$ for any set x. In general, we make the following definition.

Definition. Given $x \in \mathrm{ob}\,\mathscr{C}$, a *y-point/probe* is the set $\mathrm{Hom}_{\mathscr{C}}(y, x)$ for any $y \in \mathrm{ob}\,\mathscr{C}$.

The class $\{\mathrm{Hom}_{\mathscr{C}}(y,x)\}_{y \in \mathrm{ob}\,\mathscr{C}}$ of y-points reconstructs x as an object in $\mathscr{C}$. To see this, let $\widehat{\mathscr{C}} \coloneqq \mathbf{Fun}(\mathscr{C}^{\mathrm{op}}, \mathbf{Set})$ and $x \in \mathrm{ob}\,\mathscr{C}$. Define the functor $h_x : \mathscr{C}^{\mathrm{op}} \to \mathbf{Set}$ by

$$y \mapsto \mathrm{Hom}_{\mathscr{C}}(y,x) \qquad h_x(f) : u \mapsto u \circ f.$$

Definition. A presheaf $F \in \widehat{\mathscr{C}}$ is *representable* if $F \cong h_x$ for some x. We say that x *represents* F in this case.

The assignment $h : \mathscr{C} \to \widehat{\mathscr{C}}$ given by $x \mapsto h_x$ is a functor where $h(\phi : x \to x')$ is given by

$$h(\phi)_y : \mathrm{Hom}_{\mathscr{C}}(y,x) \to \mathrm{Hom}_{\mathscr{C}}(y,x'), \quad u \mapsto \phi \circ u.$$

This is called the *Yoneda functor.* Then the essential image of h is precisely the representable presheaves of $\mathscr{C}$.

Lemma 11. (Yoneda) Let $\mathscr{C}$ be a category.

1. For any $x, y \in \mathrm{ob}\,\mathscr{C}$, the map $\mathrm{Hom}_{\mathscr{C}}(x,y) \to \mathrm{Hom}_{\widehat{\mathscr{C}}}(h_x, h_y)$ given by $\phi \mapsto h(\phi)$ is bijective.
2. There is a natural isomorphism

$$\mathrm{Hom}_{\mathscr{C}}(-,-) \cong \mathrm{Hom}_{\widehat{\mathscr{C}}}(h_{(-)}, h_{(-)})$$

of functors $\mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \mathbf{Set}$, so that $h : \mathscr{C} \to \widehat{\mathscr{C}}$ is fully faithful. Thus, we can treat objects in $\mathscr{C}$ as set-valued presheaves of $\mathscr{C}$.

Proof. We prove just the first statement as the second follows formally from the first. Specifically, we define an inverse to the given map. If $\alpha : h_x \to h_y$ is a morphism in $\widehat{\mathscr{C}}$, then define

$$i : \alpha \mapsto \alpha_x(\mathrm{id}_x).$$

Note that $\alpha_x(\mathrm{id}_x) \in h_y(x) = \mathrm{Hom}_{\mathscr{C}}(x,y)$. We must verify that $h \circ i = \mathrm{id} = i \circ h$.

If $f : x \to y$ in $\mathscr{C}$, then $h(f) : h_x \to h_y$ and $h(f)_z : \mathrm{Hom}_{\widehat{\mathscr{C}}}(z,x) \to \mathrm{Hom}_{\widehat{\mathscr{C}}}(z,y)$ is given by $(-) \mapsto f \circ (-)$ for any $z \in \mathrm{ob}\,\mathscr{C}$. But then $h(f)_x(\mathrm{id}_x) = f \circ \mathrm{id}_x = f$.

It remains to show that $h \circ i = \mathrm{id}$. Let $\alpha : h_x \to h_y$. We have that $i(\alpha) = \alpha_x(\mathrm{id}_x) \in h_y(x)$, so that $i(\alpha) : x \to y$ in $\mathscr{C}$. Note that the component map $h(i(\alpha))_z : \mathrm{Hom}_{\mathscr{C}}(z,x) \to \mathrm{Hom}_{\mathscr{C}}(z,y)$ is given by $\phi \mapsto i(\alpha) \circ \phi$. We must check that this agrees with α_z. For any $x, y, z \in \mathrm{ob}\,\mathscr{C}$ and $\phi : z \to x$, we have

$$\begin{tikzcd}
h_x(x) \arrow[r, "\alpha_x"] \arrow[d, "h_x(\phi)"'] & h_y(x) \arrow[d, "h_y(\phi)"] \\
h_x(z) \arrow[r, "\alpha_z"'] & h_y(z)
\end{tikzcd}$$

because α is a natural transformation. By evaluating this at the morphism id_x, we see that $\alpha_z(\phi) = i(\alpha) \circ \phi$. $\square$

Corollary 14. Let $F \in \widehat{\mathscr{C}}$. Recall that F is representable by x if there is some isomorphism of functors $h_x \cong F$. By the proof of Yoneda, this is completely determined by $\xi \coloneqq h_x(\mathrm{id}_x) \in F(x)$. Given $\xi \in F(x)$, we get a natural map

$$h_x(y) \to F(y)$$
$$f \mapsto F(f)(\xi).$$

This defines a map of functors $\eta^{\xi} : h_x \to F$ where $\eta^{\xi}_y(f) = F(f)(\xi)$ for any $y \in \mathrm{ob}\,\mathscr{C}$.

By the Yoneda lemma, F is representable by x if and only if there is some $\xi \in F(x)$ such that η^{ξ} is an isomorphism.

Example 30.

1. Define the presheaf $\mathcal{P} : \mathbf{Set}^{\mathrm{op}} \to \mathbf{Set}$ by $S \mapsto \mathcal{P}(S)$ and $\mathcal{P}(f : S \to T) : A \mapsto f^{-1}(A)$. To see whether $\mathcal{P}$ is representable, we need to find some set Q and $\xi \subset Q$ such that $\mathrm{Hom}(S, Q) \to \mathcal{P}(S)$ given by $u \mapsto u^{-1}(\xi)$ is a bijection for every set S. We can do so by setting $Q = \{0, 1\}$ and $\xi = \{1\}$ as $\mathrm{Hom}(S, \{0, 1\}) \cong \mathcal{P}(S)$ via the characteristic function on S.

2. Consider the forgetful presheaf $F : \mathbf{Ring}^{\mathrm{op}} \to \mathbf{Set}$. Note that for any unital ring R, the map $\mathrm{Hom}(R, \rho) \to R$ given by $u \mapsto F(u)(\xi)$ is bijective where $\rho = \mathbb{Z}[t]$ and $\xi = t$ because any ring map $\phi : \mathbb{Z}[t] \to R$ is determined by the value $\phi(t)$. Hence F is represented by $\mathbb{Z}[t]$.

3. Let $V, W \in \operatorname{ob} \mathbf{Vect}_k$ and define the presheaf $B : (\mathbf{Vect}_k)^{\mathrm{op}} \to \mathbf{Set}$ by $L \mapsto \{\phi : V \times W \to L \mid \phi$ bilinear$\}$. We want to find some k-space T and some bilinear map $\xi \in B(T)$ such that the map $\mathrm{Hom}(L, T) \to B(L)$ given by $u \mapsto B(u) \circ \xi$ is bijective for any space L.

$$\begin{tikzcd} V \times W \arrow[r, "\xi"] \arrow[dr] & T \arrow[d, "B(u)"] \\ & L \end{tikzcd}$$

We construct such a pair (T, ξ) as follows. Let $\mathcal{F}$ denote the vector space of set functions $f : V \times W \to k$ such that $\mathrm{supp}(f)$ is finite. A basis for $\mathcal{F}$ is given by the delta functions of points $(x, y) \in V \times W$ defined by

$$\delta_{(x,y)}(a, b) = \begin{cases} 0 & (a, b) \neq (x, y) \\ 1 & (a, b) = (x, y) \end{cases}$$

Now, let $\mathcal{F}_0 \subset \mathcal{F}$ be the subspace spanned by elements of the form

$$\delta_{(x'+x'',y)} - \delta_{(x',y)} - \delta_{(x'',y)}$$
$$\delta_{(x,y'+y'')} - \delta_{(x,y')} - \delta_{(x,y'')}$$
$$\delta_{(cx,y)} - c\delta_{(x,y)}$$
$$\delta_{(x,cy)} - c\delta_{(x,y)}$$

for any $x, x', x'' \in V$ and $y, y', y'' \in W$ and $c \in k$. Finally, set $T = {}^{\mathcal{F}}\!/_{\mathcal{F}_0}$ and define $\xi : (x, y) \mapsto \delta_{(x,y)} + \mathcal{F}_0$. We usually write T as $V \otimes_k W$.

Remark 32. Instead of constructing the reals as equivalence classes of Cauchy sequences or as Dedekind cuts, we can pick out the interval $[0, 1]$ among all topological spaces as follows. We see that $[0, 1] \cong_M \left({}^{[0,1] \coprod [0,1]}\!/_{\text{first } 1 = \text{second } 0}\right)$ by the mean function M. Let $\mathscr{C}$ denote the category of pairs (X, α) where X is a topological space with two marked points r_x, l_x and $\alpha : {}^{X \coprod X}\!/_{\sim} \cong X$ such that the first r_x is $\sim$-equal to the second l_x.

Theorem 8. (Freyd) $([0, 1], M)$ is the terminal object in $\mathscr{C}$.

(Lecture 21)

Definition. Let $\mathscr{C}$ be a category and I be any set. Let $A_\alpha \in \operatorname{ob} \mathscr{C}$ for each $\alpha \in I$.

1. Define the *product functor* $\mathscr{C}^{\mathrm{op}} \to \mathbf{Set}$ by

$$B \mapsto \prod_{\alpha \in I} \mathrm{Hom}_{\mathscr{C}}(B, A_\alpha) \qquad f \mapsto (f_\alpha \mapsto f_\alpha \circ f).$$

If the product functor is representable by some object P in $\mathscr{C}$, then we say that P is the *product* of the A_α's in $\mathscr{C}$. (This wording makes sense as limits are unique up to isomorphism.)

2. Define the *coproduct functor* $\mathscr{C} \to \mathbf{Set}$ by

$$B \mapsto \prod_{\alpha \in I} \mathrm{Hom}_{\mathscr{C}}(A_\alpha, B) \qquad f \mapsto (f_\alpha \mapsto f \circ f_\alpha).$$

   If the coproduct functor is representable by some object Q in $\mathscr{C}$, then we say that Q is the *coproduct* of the A_α's in $\mathscr{C}$.

Remark 33.

1. By the Yoneda lemma, if P is the product of $\{A_\alpha\}$, then there is some $\xi \coloneqq \{\mathrm{pr}_\alpha : P \to A_\alpha\}_\alpha \in \prod_\alpha \mathrm{Hom}_{\mathscr{C}}(P, A_\alpha)$ such that

$$\eta_B^\xi : h_P = \mathrm{Hom}_{\mathscr{C}}(B, P) \to \prod_\alpha \mathrm{Hom}_{\mathscr{C}}(B, A_\alpha) \qquad f \mapsto \{\mathrm{pr}_\alpha \circ f\}_\alpha$$

   is a natural bijection in $B \in \mathrm{ob}\,\mathscr{C}$. This gives an isomorphism of set-valued presheaves $h_P \cong \mathrm{Hom}_{\mathscr{C}}(-, A_\alpha)$. Let

$$\prod_\alpha A_\alpha \coloneqq P.$$

   Then we have a natural bijection $\mathrm{Hom}_{\mathscr{C}}(B, \prod_\alpha A_\alpha) \cong \prod_\alpha \mathrm{Hom}_{\mathscr{C}}(B, A_\alpha)$ in B.

2. Likewise, if Q is the coproduct of $\{A_\alpha\}$, then by viewing the coproduct functor as a presheaf on $\mathscr{C}^{\mathrm{op}}$ we get some $\xi \coloneqq \{i_\alpha : A_\alpha \to Q\}_\alpha \in \prod_\alpha \mathrm{Hom}_{\mathscr{C}}(A_\alpha, Q)$ such that

$$\mathrm{Hom}_{\mathscr{C}}(Q, B) \xrightarrow{\cong} \prod_\alpha \mathrm{Hom}_{\mathscr{C}}(A_\alpha, B) \qquad f \mapsto \{f \circ i_\alpha\}_\alpha$$

   for each $B \in \mathrm{ob}\,\mathscr{C}$. Let

$$\coprod_\alpha A_\alpha \coloneqq Q.$$

   Then $\mathrm{Hom}_{\mathscr{C}}(\coprod_\alpha A_\alpha, B) \cong \prod_\alpha \mathrm{Hom}_{\mathscr{C}}(A_\alpha, B)$ for each B.

Example 31. Let R be a unital ring and $\mathscr{C} \coloneqq \mathbf{Mod}_R$, whose objects are precisely the pairs (M, ρ) where M is an abelian group and $\rho : R \to \mathrm{End}(M)$ satisfying

$$\begin{aligned}
&\rho(0) = 0\\
&\rho(1) = \mathrm{id}_M\\
&\rho(a+b) = \rho(a) + \rho(b)\\
&\rho(ab) = \rho(a) \circ \rho(b).
\end{aligned}$$

The morphisms $(M, \rho) \to (N, \lambda)$ are precisely the group homomorphisms $\phi : M \to N$ intertwining ρ and λ, i.e., for any $x \in R$,

$$\begin{tikzcd}
M \arrow[r, "\rho(x)"] \arrow[d, "\phi"'] & M \arrow[d, "\phi"] \\
N \arrow[r, "\lambda(x)"] & N
\end{tikzcd}.$$

Now, let $\{A_\alpha\}$ be a collection of R-modules. If we endow the Cartesian product $\prod_\alpha A_\alpha$ with the component-wise module structure inherited from the A_α's, then this becomes the product of $\{A_\alpha\}$ in $\mathbf{Mod}_R$. Moreover, the coproduct (or direct sum) of $\{A_\alpha\}$ is defined as the submodule of the product consisting of the tuples (a_α) such that $a_\alpha \neq 0$ for at most finitely many $\alpha \in I$.

Exercise 21.

1. Verify that the direct sum is a categorical coproduct in $\mathbf{Mod}_R$.

2. Prove that similar constructions show that arbitrary products and coproducts exist in $\mathbf{Mod}_G$, the category of modules over a group G.

Definition. Let $a \in \operatorname{ob}\mathscr{C}$. Let $\mathscr{C}_a$ denote the overcategory ${}^{\mathscr{C}}\!/_{a}$ and $\mathscr{C}^a$ denote the undercategory ${}^{a}\!/_{\mathscr{C}}$.

1. If $\{A_\alpha\}$ is a collection of objects in $\mathscr{C}_a$, then we call the product of the A_α's in $\mathscr{C}_a$ the *fibered product of the A_α's over a*, denoted by $\prod_{\alpha, a} A_\alpha$.

2. If $\{A_\alpha\}$ is a collection of objects in $\mathscr{C}^a$, then we call the coproduct of the A_α's in $\mathscr{C}^a$ the *fibered coproduct under a*, denoted by $\coprod^{a}_{\alpha} A_\alpha$.

Example 32.

1. We have arbitrary fibered products and coproducts in $\mathscr{C} := \mathbf{Set}$. Indeed, let a be a set and $\{(A_\alpha, \pi_\alpha)\}_\alpha$ be a collection of objects in $\mathscr{C}_a$. Then define

$$\prod_{\substack{\alpha \\ a}} A_\alpha = \{x \in \prod_{\alpha} A_\alpha : (\exists y \in a)(\forall \alpha \in I)(\pi_\alpha(x_\alpha) = y)\}.$$

   Next, let $\{(A_\alpha, i_\alpha)\}_\alpha$ be a collection of objects in $\mathscr{C}^a$. Then define

$$\coprod^{a}_{\alpha} A_\alpha = {}^{\coprod_\alpha A_\alpha}\!/_{\sim_a}$$

   where $\eta \sim_a \xi$ if there is some $y \in a$ such that $\eta = i_\alpha(y) = i_\beta(y) = \xi$ for some $\alpha, \beta \in I$.

2. Arbitrary fibered products and fibered coproducts exists in $\mathbf{Mod}_R$ and $\mathbf{Mod}_G$ by the same constructions in Example 32.

3. $\mathbf{Grp}$ inherits arbitrary products and fibered products from $\mathbf{Set}$. We will also construct arbitrary coproducts and fibered coproducts in $\mathbf{Grp}$.

(Lecture 22)

Theorem 9. The category $\mathbf{Grp}$ has arbitrary coproducts and fibered coproducts.

Proof. The coproduct $\coprod_\alpha G_\alpha$ is precisely the free product of $\{G_\alpha\}$, i.e., the group of admissible words in the G_α. (Sometimes this is denoted by $*_\alpha G_\alpha$.)

For fibered coproducts, let $\{G_\alpha, s_\alpha : G \to G_\alpha\}_\alpha$ be collection of objects in $\mathbf{Grp}^G$. Let $N \trianglelefteq \coprod_\alpha G_\alpha$ be generated by all elements of the form $s_\alpha(x)s_\beta(x)^{-1}$ for any $\alpha, \beta \in I$ and $x \in G$. Note that we have a map $G \to \coprod_\alpha G_\alpha$ given by the composite

$$\begin{tikzcd}
G \arrow[r, dashed] \arrow[d, "s_\alpha"'] & \coprod_\alpha G_\alpha \\
G_\alpha \arrow[ur, hook]
\end{tikzcd}.$$

Define

$$\coprod^{G}_{\alpha} G_\alpha = {}^{\coprod_\alpha G_\alpha}\!/_{N}.$$

(This used to be called *the amalgamated product of G_α over G.*) $\square$

Example 33.

1. Let M be a set and $U, V \subset M$. We have the inclusions $i_U : U \cap V \to U$ and $i_V : U \cap V \to V$. Then $U \cup V = U \coprod_{U \cap V} V$, the fibered coproduct of U and V under $U \cap V$.

2. Let $\mathscr{C} := \mathbf{Top}_*^{\text{conn, lc}}$ and $M \in \operatorname{ob}\mathscr{C}$. Let $U, V \subset M$ be open. As before, we get $(U \cup V, *) = (U,*)\coprod_{(U\cap V,*)}(V,*)$. Van Kampen states that

$$\pi_1(U \cup V, *) = \pi_1(U,*)\coprod_{\pi_1(U\cap V,*)}\pi_1(V,*).$$

That is, the functor $\pi_1 : \mathbf{Top}_*^{\text{conn, lc}} \to \mathbf{Grp}$ respects fibered coproducts.

Definition. The bifunctor $\operatorname{Hom}_{\mathscr{C}}(-,-) : \mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \mathbf{Set}$ maps any morphism (f, g) in $\mathscr{C}^{\mathrm{op}} \times \mathscr{C}$ to the set map $\varphi \mapsto g \circ \varphi \circ f$.

Suppose that $L : \mathscr{C} \to \mathscr{D}$ and $R : \mathscr{D} \to \mathscr{C}$ are functors. We say that (L, R) is an *adjoint pair of functors* if the bifunctors

$$\operatorname{Hom}_{\mathscr{D}}(L(-),-) : \mathscr{C}^{\mathrm{op}} \times \mathscr{D} \to \mathbf{Set}$$
$$\operatorname{Hom}_{\mathscr{C}}(-,R(-)) : \mathscr{C}^{\mathrm{op}} \times \mathscr{D} \to \mathbf{Set}$$

are isomorphic.

Remark 34.

1. Suppose $L : \mathscr{C} \to \mathscr{D}$ is a functor. Then L induces a functor $L_* : \widehat{\mathscr{D}} \to \widehat{\mathscr{C}}$ given by $F \mapsto F \circ L$. We can compose L_* with the Yoneda functor $h^{\mathscr{D}} : \mathscr{D} \to \widehat{\mathscr{D}}$ to get $L_* \circ h^{\mathscr{D}} : \mathscr{D} \to \widehat{\mathscr{C}}$.

   Exercise 22. Then L has a right adjoint R if and only if for each $y \in \operatorname{ob}\mathscr{D}$, the presheaf $L_* \circ h^{\mathscr{D}}(y) : \mathscr{C}^{\mathrm{op}} \to \mathbf{Set}$ is representable in $\mathscr{C}$. In this case, $L_* \circ h^{\mathscr{D}} \cong h^{\mathscr{C}} \circ R$.

   Proposition 6. The right adjoint is unique up to a unique isomorphism.

2. Let $\mathscr{C} \underset{R}{\overset{L}{\rightleftarrows}} \mathscr{D}$ be an adjoint pair of functors. Then there is a natrual bijection

$$\operatorname{Hom}_{\mathscr{D}}(L(x), L(x)) \cong \operatorname{Hom}_{\mathscr{C}}(x, R \circ L(x))$$

   for every $x \in \operatorname{ob}\mathscr{C}$. This gives a map of functors $\xi : \mathrm{id}_{\mathscr{C}} \to R \circ L$. Likewise, we get a map $\eta : L \circ R \to \mathrm{id}_{\mathscr{D}}$. This induces the functors

$$\begin{gathered} L \xrightarrow{\xi} L \circ R \circ L \xrightarrow{\eta} L \\ R \xrightarrow{\xi} R \circ L \circ R \xrightarrow{\eta} R \end{gathered}.$$

   Exercise 23. $\mathrm{id} \cong \eta \circ \xi$.

   Proposition 7. Conversely, if (L, R, ξ, η) satisfies $\eta \circ \xi \cong \mathrm{id}_L$ and $\eta \circ \xi \cong \mathrm{id}_R$, then (L, R) is an adjoint pair.

(Lecture 23)

Example 34. 1. Let $|\cdot| : \mathbf{Grp} \to \mathbf{Set}$ denote the forgetful functor. Then it has as left adjoint the free group functor $\operatorname{Fr} : \mathbf{Set} \to \mathbf{Grp}$. This means that $\operatorname{Hom}(\operatorname{Fr}(S), G) \cong \operatorname{Hom}(S, |G|)$ for any set S and group G. That is, for any function $f : S \to |G|$, there is a unique homomorphism $\phi : \operatorname{Fr}(S) \to G$ such that $\phi\restriction_S = f$, where we embed $S \hookrightarrow \coprod_{s\in S} G_s$ in $\mathbf{Set}$ by $s \mapsto \underbrace{1_{G_s}}_{\text{generator}}$.

Proof.

$$\operatorname{Hom}(\operatorname{Fr}(S), G) = \operatorname{Hom}(\coprod_S \mathbb{Z}, G) \cong \prod_{s\in S}\operatorname{Hom}(\mathbb{Z}, G) \cong \prod_s \operatorname{Hom}(\{1\}, |G|) \cong \operatorname{Hom}(\coprod_s\{1\}, |G|) \cong \operatorname{Hom}(S, |G|).$$

$\square$

2. Let $\mathbf{Ab} \xrightarrow{i} \mathbf{Grp}$ denote the full subcategory of abelian groups. It has as left adjoint the abelianization functor $(-)^{\mathrm{ab}}$.

   Proof. Let G be a group and A and abelian group. The universal property of G^{ab} states that for any homomorphism $\phi : G \to A$, there is a unique group map $\psi : G^{\mathrm{ab}} \to A$ such that $\psi \circ \pi = \phi$. This determines a bijection $\mathrm{Hom}_{\mathbf{Ab}}(G^{\mathrm{ab}}, A) \xrightarrow{\cong} \mathrm{Hom}_{\mathbf{Grp}}(G, A)$ by $\phi \mapsto \psi \circ \pi$. $\square$

Remark 35. The notion of adjunction is strictly weaker than that of inverse. For example, **Grp** and **Set** cannot be equivalent, for $\emptyset \in \mathbf{Set}$. Also, **Ab** and **Grp** cannot be equivalent, for the former is an preadditive category whereas the latter is not. Any inverse pair of functors (F, G), however, is automatically an adjunction.

Proposition 8. $(-)^{\mathrm{ab}}$ admits no left adjoint.

Proof. Suppose, for contradiction, that $F : \mathbf{Ab} \to \mathbf{Grp}$ is left adjoint to $(-)^{\mathrm{ab}}$. Then

$$\mathrm{Hom}_{\mathbf{Grp}}(F(A), G) \cong \mathrm{Hom}_{\mathbf{Ab}}(A, G^{\mathrm{ab}})$$

for any abelian group A. This entails the following three properties.

1. $F(A)$ cannot be simple.

   Proof. If $F(A)$ is simple and nonabelian, then $F(A)^{\mathrm{ab}} = \{e\}$. But we know that

   $$\{e\} \ncong \mathrm{Hom}_{\mathbf{Grp}}(F(A), F(A)) \cong \mathrm{Hom}_{\mathbf{Ab}}(A, \{e\}) \cong \{e\},$$

   a contradiction.

   If $F(A)$ is simple and abelian, then $F(A) \cong C_p$ for some prime p. Set $G = A_{3p}$, so that $G^{\mathrm{ab}} = \{e\}$. Then we have $\mathrm{Hom}_{\mathbf{Grp}}(C_p, G) \cong \mathrm{Hom}_{\mathbf{Ab}}(A, \{e\}) \cong \{e\}$. But $C_p \leq G$, so that $\mathrm{Hom}_{\mathbf{Grp}}(C_p, G)$ is nontrivial, giving a contradiction. $\square$

2. If $F(A)$ is trivial, then so is A.

   Proof. Suppose $F(A) = \{e\}$. Then

   $$\{e\} \cong \mathrm{Hom}_{\mathbf{Grp}}(\{e\}, G) \cong \mathrm{Hom}_{\mathbf{Ab}}(A, G^{\mathrm{ab}}) \supset \{\mathrm{id}_A, 0_A\}.$$

   Thus, $\mathrm{id}_A = 0_A$, implying that A is trivial. $\square$

3. If A is nontrivial, then $F(A)$ contains no proper maximal normal subgroup.

   Proof. Suppose A is nontrivial and $M \trianglelefteq F(A)$ is proper and maximal. Then ${F(A)}/{M}$ is simple. If ${F(A)}/{M}$ is also nonabelian, then we get

   $$\{e\} \ncong \mathrm{Hom}_{\mathbf{Grp}}(F(A), {F(A)}/{M}) \cong \mathrm{Hom}_{\mathbf{Ab}}(A, \left({F(A)}/{M}\right)^{\mathrm{ab}}) \cong \{e\},$$

   a contradiction. If ${F(A)}/{M}$ is abelian, then it is isomorphic to C_p and we can make an argument as before. $\square$

$\square$

Now, we have $\mathrm{Hom}_{\mathbf{Grp}}(F(C_2), C_2) \cong \mathrm{Hom}_{\mathbf{Ab}}(C_2, C_2) = \{0, \mathrm{id}\}$. Hence there is some group map $f : F(C_2) \to C_2$ such that $\{e\} < \ker f < F(C_2)$. But then ${F(C_2)}/{\ker f}$ is nonzero finite, which implies that $F(C_2)$ has a proper maximal normal subgroup, a contradiction.

Lemma 12. If $f : S \to T$ is a surjective group map, then so is $\mathrm{Fr}(f) : \mathrm{Fr}(S) \to \mathrm{Fr}(T)$.

Proof. If g is a section of f, then $\mathrm{Fr}(g)$ is a section of $\mathrm{Fr}(f)$. $\square$

Lemma 13. Let S be a set. Then $\mathrm{Fr}(S)^{\mathrm{ab}} = \coprod_{s\in S} G_s$ is a free abelian group on S. Specifically, since each G_s is a $\mathbb{Z}$-module, we can show that
$$\mathrm{Fr}(S)^{\mathrm{ab}} = \bigoplus_{s\in S} G_s.$$

Proof. $\square$

For each $s \in S$, define $\delta_s : S \to \bigoplus_{s\in S} G_s$ by $\delta_s^\alpha = \begin{cases} 1 & \alpha = s \\ 0 & \alpha \neq s. \end{cases}$. We know that δ_s extends to a group homomorphism $\phi : \mathrm{Fr}(S) \to \bigoplus_{s\in S} G_s$. We also have the following commutative diagram.

$$\begin{tikzcd} \mathrm{Fr}(S) \arrow[r, "\phi"] \arrow[d, "\pi"'] & \bigoplus_{s\in S} G_s \\ \mathrm{Fr}(S)^{\mathrm{ab}} \arrow[ur, dashed, "\exists! \phi^{\mathrm{ab}}"'] & \end{tikzcd}$$

Notice that ϕ must be surjective. Hence ϕ^{ab} is also surjective. It remains to show that it is injective. Let $[x] \in \ker \phi^{\mathrm{ab}}$. Then we may write $[x] = n_1 n_2 \cdots n_r + \mathrm{Fr}(S)'$ where each $n_i \in G_i$. Hence
$$0 = \phi^{\mathrm{ab}}([x]) = \sum_{i=1}^{r} n_i \delta_{s_i}.$$

Thus, each $n_i = 0$, so that $[x] = 0$, and $\ker \phi^{\mathrm{ab}}$ is trivial.

Lemma 14. $\mathrm{Fr}(S) \cong \mathrm{Fr}(T) \iff S \cong T$.

Proof.
($\Longleftarrow$) If $u : S \to T$ and $v : T \to S$ are inverses of each other, then so are $F(u)$ and $F(v)$.

($\Longrightarrow$) Assume that $\mathrm{Fr}(S) \cong \mathrm{Fr}(T)$. Then
$$\bigoplus_{s\in S} G_s \cong \mathrm{Fr}(S)^{\mathrm{ab}} \cong \mathrm{Fr}(T)^{\mathrm{ab}} \cong \bigoplus_{t\in T} G_t.$$

Hence $\mathbf{Fun}^{\mathrm{fs}}(S, C_2) \cong \bigoplus_{s\in S} G_s \big/ 2\bigoplus_{s\in S} G_s \cong \bigoplus_{t\in T} G_t \big/ 2\bigoplus_{t\in T} G_t \cong \mathbf{Fun}^{\mathrm{fs}}(T, C_2)$. But then $\mathbf{Fun}^{\mathrm{fs}}(S, C_2)$ and $\mathbf{Fun}^{\mathrm{fs}}(T, C_2)$ are isomorphic as C_2-vector spaces, so that $S \cong T$ as bases.

Remark 36. There is another proof if we restrict our set-theoretic universe.
The adjunction $(\mathrm{Fr}, |-|)$ gives
$$P(T) \cong \mathrm{Hom}_{\mathbf{Set}}(T, C_2) \cong \mathrm{Hom}_{\mathbf{Grp}}(\mathrm{Fr}(T), C_2) \cong \mathrm{Hom}_{\mathbf{Grp}}(\mathrm{Fr}(S), C_2) \cong \mathrm{Hom}_{\mathbf{Set}}(S, C_2) \cong P(S).$$

If we assume the continuum hypothesis, then this implies that $S \cong T$.

$\square$

(Lecture 24)

Remark 37. For any group G, we have
$$\mathrm{Hom}_{\mathbf{Grp}}(\mathrm{Fr}(|G|), G) \cong \mathrm{Hom}_{\mathbf{Set}}(|G|, |G|) \ni \mathrm{id}_{|G|}.$$

Thus, there is a unique group map $\phi : \mathrm{Fr}(|G|) \to G$ such that $\phi \restriction_{|G|} = \mathrm{id}_{|G|}$. This implies that ϕ is surjective, so that G is the quotient of a free group.

Definition. We say that a group G is generated by a subset $S \subset G$ if the homomorphism

$$\phi \circ \mathrm{Fr}(i) : \mathrm{Fr}(S) \to \mathrm{Fr}(|G|) \to G$$

is surjective, where $i : S \to |G|$ denotes inclusion.

Note 6. $\mathrm{im}(\phi \circ \mathrm{Fr}(i)) = \bigcap\{H : H \leq G,\ H \supset S\}$.

Definition. Suppose that the set S generates G and that the set T generates $\ker(\mathrm{Fr}(S) \twoheadrightarrow G)$. Then there is an exact sequence

$$\eta : \mathrm{Fr}(T) \to \mathrm{Fr}(S) \to G \to 1.$$

In this scenario, we call η a *presentation of* G. We also cal S the *set of generators of* G and T the *set of relations of* G.

Remark 38.

1. Any quotient of a finitely generated group is finitely generated.

2. A subgroup of a finitely generated group need not be finitely generated. For example, $F_2 \coloneqq \mathrm{Fr}(\{x, y\})$ is finitely generated, but the subgroup $\{y^k x y^{-k} : k \geq 0\}$ is not.

3. If G is finitely presentable, then any subgroup of G is finitely presentable.

Theorem 10. (Nielsen-Schreier) Any subgroup of a free group is free.

Note 7. Our main setting for ring theory will be **CommRing**, the category of unital, associative, commutative rings.

Definition. Let $A \in \mathbf{CommRing}$. Then we have the A-module $\bigoplus_{\mathbb{N}} A$ For each $k \geq 0$, define

$$m_k = (0, \ldots, 0, \underbrace{1}_{k\text{−th place}}, 0, \ldots).$$

Then the m_k form an A-basis for $\bigoplus_{\mathbb{N}} A$. Define $m_k \cdot m_l = m_{k+1}$ and extend this operation to $\bigoplus_{\mathbb{N}} A$ by linearity. Then $(\bigoplus_{\mathbb{N}} A, +, \cdot) \in \mathbf{CommRing}$. Moreover, $((\bigoplus_{\mathbb{N}} A, +, \cdot), i) \in \mathbf{CommRing}^A$ where $i : A \to \bigoplus_{\mathbb{N}} A$ denotes inclusion by $a \mapsto (a, 0, \ldots, 0, \ldots)$. We call this the *one-variable ring over* A.

Note 8. By convention, we let $\deg(0) = -\infty$.

Lemma 15. $\deg(p_1 + p_2) \leq \max(\deg p_1, \deg p_2)$.

(Lecture 25)

Definition. Let S be a set. Note that $\underbrace{\mathbf{Fun}^{\mathrm{fs}}(S, \mathbb{Z}_{\geq 0})}_{\text{finite support}}$ is an additive monoids because $\mathbb{Z}$ is one. View its elements as monomials in elements of S. For any $s \in S$, define $t_s : S \to \mathbb{Z}_{\geq 0}$ by $x \mapsto \begin{cases} 0 & s \neq x \\ 1 & s = x \end{cases}$. Then for any $\xi \in \mathbf{Fun}^{\mathrm{fs}}(S, \mathbb{Z}_{\geq 0})$, we write $\xi = \prod_{s \in S} t_s^{\xi(s)} = \prod_{s \in \mathrm{supp}(\xi)} t_s^{\xi(s)}$. Let $A \in \mathrm{ob}\,\mathbf{CommRing}$. Define the *multivariable polynomial ring over* A *on* $\{t_s\}_{s \in S}$ as

$$A[S] = \mathbf{Fun}^{\mathrm{fs}}(\mathbf{Fun}^{\mathrm{fs}\,|}(S, \mathbb{Z}_{\geq 0}), A)$$

equipped with the operations

$$(f + g)(\xi) = f(\xi) + g(\xi)$$
$$(f \cdot g)(\xi) = \sum_{\substack{\mu, \nu \\ \mu \cdot \nu = \xi}} f(\mu) \cdot g(\nu).$$

Remark 39.

1. Note that $A[S] \in \operatorname{ob}\mathbf{CommRing}$ with $0_{A[S]}(\xi) = 0$ and and $1_{A[S]}(\xi) = \begin{cases} 0_A & \xi \neq 0 \\ 1_A & \xi = 0 \end{cases}$ for each monomial ξ.

2. There is a natural ring monomorphism $i : A \hookrightarrow A[S]$ given by $a \mapsto a1_{A[S]}$.

3. Given $f \in A[S]$, we can write $f = \sum_{\xi \in \operatorname{supp}(f)} f(\xi)\delta_\xi$. Let $\delta_\xi \coloneqq \prod_{s \in \operatorname{supp}(\xi)} t_s^{\xi(s)}$, so that instead we can write
$$f = \sum_{\xi \in \operatorname{supp}(f)} f(\xi) \prod_{s \in \operatorname{supp}(\xi)} t_s^{\xi(s)}$$
in the form of a polynomial in several variables.

4. Consider the forgetful functor $|{-}| : \mathbf{CommRing}^A \to \mathbf{Set}$. The polynomial functor $A[-] : \mathbf{Set} \to \mathbf{CommRing}^A$ is left adjoint to $|{-}|$.

   Proof. We want a natural bijection $\operatorname{Hom}_{\mathbf{CommRing}^A}(A[S], B) \cong \operatorname{Hom}_{\mathbf{Set}}(S, |B|)$ for any ring map $i : A \to B$ and any set S. Given a commutative diagram
$$\begin{tikzcd} A[S] \arrow[r, "\theta"] & B \\ A \arrow[u, hook] \arrow[ur, "i"'] & \end{tikzcd}$$
of ring maps, define the set map $\hat{\theta} : S \to |B|$ by $s \mapsto \theta(t_s)$. Conversely, given a set map $\phi : S \to |B|$, define the ring map $\hat{\phi} : A[S] \to B$ by
$$\sum_{\xi \in \operatorname{supp}(f)} f(\xi) \prod_{s \in \operatorname{supp}(\xi)} t_s^{\xi(s)} \mapsto \sum_{\xi \in \operatorname{supp}(f)} i(f(\xi)) \prod_{s \in \operatorname{supp}(\xi)} \phi(t_s)^{\xi(s)}.$$
$\square$

5. Any set inclusion $T \subset S$ incudes a ring monomorphism $A[T] \hookrightarrow A[S]$.

   Exercise 24. Apply Yoneda to the adjoint pair $(A[-], |{-}|)$ to prove that $A[S] \cong A[T][S \setminus T]$.

Definition. Given a monomial ξ in elements of S, define $\deg(\xi) = \sum_{s \in S} \xi(s)$. If $f \in A[S]$, then define
$$\deg(f) = \max\{\deg(\xi) : f(\xi) \neq 0\}.$$
By convention, we set $\deg(0) = -\infty$.

Lemma 16.

1. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.
2. $\deg(fg) \leq \deg(f) + \deg(g)$.

Lemma 17. If A is an integral domain, then $(A[S])^\times = A^\times$ and $A[S]$ is an integral domain. In this case, $\deg(fg) = \deg(f) + \deg(g)$.

Proof. Suppose that A has no zero divisors. Given $f, g \in A[S]$, write
$$f = \sum_\xi f(\xi)t^\xi \qquad g = \sum_\xi g(\xi)t^\xi.$$
Say that $\deg(f) = \deg(\eta)$ and $\deg(g) = \deg(\eta')$ where $f(\eta) \neq 0$ and $g(\eta') \neq 0$. Then the coefficient before the term $t^\eta t^{\eta'}$ in fg is equal to $f(\eta)g(\eta') \neq 0$. Hence $\deg(fg) = \deg(f) + \deg(g)$. Also, if $g = 0$ or $f = 0$, then clearly $\deg(fg) = \deg(f) + \deg(g)$.

Both the fact that $(A[S])^\times \subset A^\times$ and the fact that $A[S]$ has no zero divisors follow immediately from this. $\square$

Definition. Any object $i : A \to B$ in the under category $\mathbf{CommRing}^A$ is a *commutative A-algebra* if i is injective.

Definition. Let B be a commutative A-algebra and $S \subset B$. Then S is *algebraically independent over A* if the natural homomorphism $A[S] \to B$ is injective. If $S = \{x\}$, then we say that x is *transcendental over A* if S is algebraically independent over A and *algebraic over A* otherwise.

Definition. Let B be a commutative A-algebra. We say that B is *finitely generated* if $A[T] \to B$ is surjective for some finite $T \subset B$.

Proposition 9. If S and T are sets, then $S \cong T \iff \mathbb{Z}[S] \cong \mathbb{Z}[T]$.

Proof. See Lemma 14. □

(Lecture 26)

Remark 40. Suppose that A is an abelian group. Then $(\mathrm{End}(A), +, \circ)$ is a ring.

Definition. Let R be a unital ring. Then a *(left) R-module* is a pair (A, ρ) where A is an abelian group and $\rho : R \to \mathrm{End}(A)$ is a ring homomorphism.

Note 9. This agree with the usual definition of an R-module in terms of an action map $\alpha : R \times A \to A$ where we set $\rho(r)(a) = \alpha(r, a)$.

Definition. A *morphism of R-modules* $(A_1, \rho_1) \to (A_2, \rho_2)$ is a group map $\phi : A_1 \to A_2$ such that the following commutes for any $r \in R$.

$$\begin{tikzcd} A_1 \arrow[r, "\phi"] \arrow[d, "\rho_1(r)"'] & A_2 \arrow[d, "\rho_2(r)"] \\ A_1 \arrow[r, "\phi"'] & A_2 \end{tikzcd}$$

The category of R-modules is denoted by R-$\mathbf{Mod}$.

Definition. Let R^{op} denote the ring obtained from revering the multiplication on R. Then a*right R-module* is a pair (A, ρ) where A is an abelian group and $\rho : R^{\mathrm{op}} \to \mathrm{End}(A)$ is a ring homomorphism. The category of right R-modules is denoted by R^{op}-$\mathbf{Mod}$.

Note 10. This is equivalent to defining an action map $\alpha : A \times R \to A$ where we set $\alpha(a, r) = \rho(r)(a)$.

Note 11. The category of bimodules is denoted by R-$\mathbf{Mod}$-R or $R \otimes_{\mathbb{Z}} R^{\mathrm{op}}$-$\mathbf{Mod}$.

Example 35. Any ring is a bimodule over itself via left and right multiplication.

Remark 41. Let M be an R-module. Let $\{M_\alpha\}_{\alpha \in A}$ be a collection of submodules of M and i_α denote inclusion.

1. The intersection $\bigcap_\alpha M_\alpha$ is a submodule of M.
2. We have
$$(i_\alpha) \in \prod_\alpha \mathrm{Hom}_{R\text{-}\mathbf{Mod}}(M_\alpha, M) = \mathrm{Hom}_{R\text{-}\mathbf{Mod}}\big(\coprod_\alpha M_\alpha, M\big).$$
Define $\sum_\alpha M_\alpha = \mathrm{im}(i_\alpha)$. Then
$$\sum_\alpha M_\alpha = \{\sum_\alpha m_\alpha : m_\alpha \in M_\alpha,\ m_\alpha \neq 0 \text{ for at most finitely many } \alpha\}.$$
3. Let $S \subset M$ be any subset. We call $\coprod_{s \in S} R$ *the free R-module generated by S*. We have a natural map $g : \coprod_{s \in S} R \to M$ given by $(r_s) \mapsto \sum_s r_s s$. We say that $R \cdot S := \mathrm{im}\, g$ is the *submodule of M generated by S*.

4. The free R-module functor is left adjoint to the forgetful functor.

Definition. Let M be an R-module. Then M is

1. *Noetherian* if it has ACC.
2. *Artinian* if it has DCC.

Definition. Let M be an R-module. Then M has

1. the *maximal property* if every collection of submodules of M has a maximal element.
2. the *minimal property* if every collection of submodules of M has a minimal element.

Lemma 18. Let M be an R-module. TFAE.

(a) M is Noetherian.

(b) M has the maximal property.

(c) Every submodule of M is finitely generated.

Proof.
$(a) \implies (b)$ is easy to show by an iteration argument.

$(b) \implies (c)$. If M has the maximal property, then so does every submodule. Hence it suffices to the prove the following lemma.

Lemma 19. If the R-module M has the maximal property, then M is finitely generated.

Proof. Let $\mathcal{F}$ denote the set of any finitely generated submodule $N \subset M$. This is partially ordered by $\subset$ and nonempty. We can apply Zorn's Lemma to obtain a maximal element T of $\mathcal{F}$. If $T = M$, then we are done. Otherwise, choose $m \in M \setminus T$. Then $T + (m) \in \mathcal{F}$, contrary to the choice of T. $\square$

$(c) \implies (a)$. Let $M_1 \subset M_2 \subset \cdots \subset M$ be an ascending chain of submodules of M. Then set $N = \bigcup_{i=1}^{\infty} M_i$, which is a submodule, hence finitely generated by hypothesis. Let $x_1, \ldots . x_s$ denote the generators. Then each $x_k \in M_{i_k}$ for some some i_k. Set $n = \max\{i_k : 1 \leq k \leq s\}$, so that $N = M_n$. $\square$

Lemma 20. TFAE.

(a) M is Artinian.

(b) M has the minimal property.

(Lecture 27)

Proposition 10.

1. The properties *Noetherian*, *Artinian*, and *finitely generated* are preserved by quotients.
2. The properties *Noetherian* and *Artinian* are preserved by submodules.
3. If both the submodule N of M and the quotient ${}^{M}\!/_{N}$ are Noetherian, then so is M. The same is true of Artinian and finitely generated modules.

   Proof.

(a) Assume that both N and M/N are Noetherian. We have the exact sequence

$$
\begin{tikzcd}
0 \arrow[r] & N \arrow[r, hook, "i"] & M \arrow[r, two heads, "q"] & M/N \arrow[r] & 0 .
\end{tikzcd}
$$

Let $M_1 \subset M_2 \subset \cdots \subset M$ be an ascending chain of submodules. Then $q(M_1) \subset q(M_2) \subset \cdots M/N$ is an ascending chain of submodules, which must stabilize at, say, the k-th position. Also, the ascending chain $N \cap M_1 \subset N \cap M_2 \subset \cdots N$ must stabilize at, say, the l-th position. Set $r = \max\{k, l\}$.

$$
\begin{tikzcd}
N \cap M_i \arrow[r, hook] \arrow[d, equal] & M_i \arrow[r, two heads] & q(M_i) \arrow[d, equal] \\
N \cap M_r \arrow[r, hook] & M_r \arrow[r, two heads] \arrow[u, hook] & q(M_r)
\end{tikzcd} .
$$

Let $x \in M_i$. Then $[x] = [y]$ for some $y \in M_r$, i.e., $x = y + n$ for some $n \in N$. This implies that $x - y \in N \cap M_i = N \cap M_r$. It follows that $x = y + t$ for some $t \in M_r$, so that $x \in M_r$. This proves that $M_r \subset M_i$, hence $M_i = M_r$.

(b) The Artinian case follows from a similar argument. Then for any $i \geq r$, we have

(c) Assume that both N and M/N are finitely generated R-modules. There are finite sets S and T such that

$$
\alpha : \coprod_{s \in S} R \twoheadrightarrow N
$$
$$
\beta : \coprod_{t \in T} R \twoheadrightarrow M/N.
$$

We have the short exact sequence.

$$
\begin{tikzcd}
0 \arrow[r] & N \arrow[r, hook, "i"] & M \arrow[r, two heads, "q"] & M/N \arrow[r] & 0 \\
 & & & \coprod_{t \in T} R \arrow[u, two heads, "\beta"] &
\end{tikzcd} .
$$

Since the free module functor is left adjoint to the forgetful functor, it follows that β lifts to a homomorphism $\coprod_{t \in T} R \xrightarrow{\theta} M$ if and only if the set map $T \to M/N$ lifts to a set map $T \to M$. But there is some set-theoretic section $s : M/N \to M$, making $T \xrightarrow{\beta} M/N \xrightarrow{s} M$ such a lift in **Set**. Thus we obtain such a lift θ in $R-$**Mod**. Define the homomorphism

$$
\phi : (\coprod_{s \in S} R) \coprod (\coprod_{t \in T} R) \to M, \qquad (x, y) \mapsto \alpha(x) + \theta(y),
$$

which satisfies

$$
\begin{tikzcd}
0 \arrow[r] & N \arrow[r, hook, "i"] & M \arrow[r, two heads, "q"] & M/N \arrow[r] & 0 \\
0 \arrow[r] & \coprod_{s \in S} R \arrow[r, hook] \arrow[u, "\alpha"] & (\coprod_{s \in S} R) \coprod (\coprod_{t \in T} R) \arrow[r, two heads] \arrow[u, "\phi"] & \coprod_{t \in T} R \arrow[r] \arrow[u, two heads, "\beta"] & 0
\end{tikzcd} .
$$

If $x \in M$, then we can find some $y \in \coprod_{t \in T} R$ such that $\beta(y) = q(x)$. Also, $q \circ \theta(y) = \beta(y)$, so that $q(x - \theta(y)) = 0$, i.e., $x - \theta(y) \in N$. There is some $m \in \coprod_{s \in S} R$ such that $\alpha(m) = x - \theta(y)$. Hence $x = \phi(m, y)$, proving that ϕ is surjective. This is to say that M is finitely generated.

$\square$

Lemma 21. Let $\{M_\lambda\}_{\lambda\in\Lambda}$ be a set of R-modules. Without loss of generality, assume that each M_λ is nontrivial. If P is any of the three finiteness properties, then $\coprod_{\lambda\in\Lambda} M$ has P if and only if each M_λ has P and Λ is finite.

Proof. Suppose that $\coprod_\lambda M_\lambda$ has P. But each projection π_λ onto M_λ is a surjection, and P is preserved by quotients. Hence each M_λ has P. Now, suppose, for contradiction, that Λ is infinite. We have three cases to consider.

1. Suppose that $\coprod_\lambda M_\lambda$ is Noetherian. By the countable axiom of choice, find some countably infinite subset $\{\lambda_n\} \subset \Lambda$. But this gives an infinite chain

$$M_{\lambda_1} \subsetneq M_{\lambda_1} \coprod M_{\lambda_2} \subsetneq \cdots \subset \coprod_\lambda M_\lambda,$$

a contradiction.

2. For the Artinian case, apply a similar argument.

3. Suppose that $\coprod_\lambda M_\lambda$ is finitely generated. We have a surjection

$$\phi : \coprod_{i=1}^{n} R \twoheadrightarrow \coprod_\lambda M_\lambda$$

for some integer n. For each $1 \le i \le n$, define $x_i = \phi(0, \dots, \underbrace{1}_{i\text{-th spot}}, \dots, 0)$. We can write $x_i = (x_{i_\lambda})_{\lambda\in\Lambda}$. Define

$$\Lambda^0 = \{\lambda \in \Lambda : \exists i . x_{i_\lambda} \neq 0\}.$$

Note that Λ^0 is finite, so that there is some $\mu \in \Lambda \setminus \Lambda^0$. Then the composition map

$$\pi_\mu \circ \phi$$

is the trivial morphism. But it is also a surjection as the composition of surjections, a contradiction.

The converse is clear. □

Definition. A ring R is *Noetherian* if every ideal has ACC. It is *Artinian* if every ideal has DCC.

Proposition 11. Let R be Noetherian (resp. Artinian).

1. Every finitely generated module over R is Noetherian (resp. Artinian).

2. If R is Noetherian, then every finitely generated R-module is finitely presentable.

Proof. We just need to check the second statement. Let M be an R-module generated by the finite set S. Then $\coprod_{s\in S} R$ is Noetherian. But this implies that $\ker(\coprod_{s\in S} R \twoheadrightarrow M)$ is finitely generated. □

Example 36.

1. Any field k is both Noetherian and Artinian since its ideals are precisely (0) and k.

2. Set $R = \mathbb{C}[x_1, x_2, \dots]$. This is not Noetherian, because

$$(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots$$

fails to stabilize. But R is an integral domain since $\mathbb{C}$ is one. If F denotes the fraction field of R, then $R \subset F$ is the subring of a Noetherian ring but is not finitely generated.

Moreover, a finitely generated module over a general ring R need not be finitely presentable. To see this, note that $\mathbb{C}$ is an R-module via the action $f \cdot a = f(0)a$. We get a short exact sequence

$$0 \longrightarrow (x_1, x_2, \dots) \longrightarrow R \xrightarrow{\mathrm{ev}_0} \mathbb{C} \longrightarrow 0 \ .$$

Suppose, for contradiction, that there are finite sets T and S such that

$$\coprod_{t\in T} R \longrightarrow \coprod_{s\in S} R \longrightarrow \mathbb{C} \longrightarrow 0$$

is exact. Then we may construct the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & (x_1, x_2, \ldots) \arrow[r] & R \arrow[r, "\mathrm{ev}_0"] & \mathbb{C} \arrow[r] & 0 \\
& \coprod_{t\in T} R \arrow[r] \arrow[u, "\theta"] & \coprod_{s\in S} R \arrow[r] \arrow[u, "\phi"] & \mathbb{C} \arrow[r] \arrow[u, equal] & 0
\end{tikzcd}$$

so that ϕ is surjective. But a diagram chase shows that this makes θ surjective, contrary to the fact that $(x_1, x_2, \ldots)$ is not finitely generated.

Theorem 11. (Hilbert's basis theorem) If $A \in \mathbf{CommRing}$ is Noetherian, then $A[x]$ is also Noetherian.

Proof. Note that $A[x]$ is an A-module since A is a subring. We see that

$$A[x] = \bigcup_{n\geq 0} A[x]_n$$

where

$$A[x]_n = \{f \in A[x] : \deg f \leq n\}.$$

Note that each $A[x]_n$ is finitely generated by $1, x, \ldots, x^n$, giving a surjection $\coprod_{\{0,1,\ldots,n\}} A \twoheadrightarrow A[x]_n$. Since $\coprod_{\{0,1,\ldots,n\}} A$ is Noetherian by Lemma 19, so is $A[x]_n$.

Let $\Omega \trianglelefteq A[x]$ be an ideal. Then $\Omega \cap A[x]_n$ is an A-submodule in $A[x]_n$ and thus a finitely generated A-module by, say, $\alpha_1, \ldots, \alpha_{k_n}$. Let

$$\widetilde{\Omega} := \{a \in A : a = 0 \text{ or } \exists f \in \Omega. \deg f > 0 \wedge f(x) = ax^r + O(x^{r-1})\}.$$

Lemma 22. $\widetilde{\Omega}$ is an ideal in A.

Proof. Let $a, b \in \widetilde{\Omega}$. If $a = 0$ or $b = 0$, then $a + b \in \widetilde{\Omega}$. Suppose $a, b \neq 0$. Then there are $f, g \in \Omega$ such that $f = ax^r + O(x^{r-1})$ and $g = bx^s + O(x^{s-1})$. Set $t = \max\{r, s\}$. Then $\Omega \ni x^{t-r}f \pm x^{t-s}g = (a \pm b)x^t + O(x^{t-1})$, implying that $a \pm b \in \widetilde{\Omega}$.

Further, it's clear that if $a \in \widetilde{\Omega}$ and $b \in A$, then $ba \in \widetilde{\Omega}$. □

It follows that $\widetilde{\Omega}$ is a finitely generated A-module by, say, the elements $b_1, \ldots, b_s$. For each $i = 1, \ldots, s$, find some $f_i \in \Omega$ such that $f_i = b_i x^{m_i} + O(x^{m_i - 1})$. Set $n = \max\{m_i\}$.

Lemma 23. Ω is generated by $\{\alpha_1, \ldots, \alpha_{k_n}, f_1, \ldots, f_s\}$ as an ideal in $A[x]$.

Proof. Let $f \in \Omega$. Write $f = \beta x^r + O(x^{r-1})$ for some $r \geq 1$. Then $\beta \in \widetilde{\Omega}$. It follows that $\beta = \sum_{i=1}^s c_i b_i$ for some $c_i \in A$. If $r \geq n$, then $f - \sum_{i=1}^s c_i x^{r-n} f_i$ has degree $< r$. We can repeat this to see that $f -$ (some combination of f_i with coefficients in $A[x]$) will have degree $\leq n$. That is, there are $g_1, \ldots, g_s \in A[x]$ such that $\deg(f - \sum_{i=1}^s g_i f_i) \leq n$. But we're done because $f - \sum_{i=1}^s g_i f_i \in \Omega \cap A[x]_n$. □

As Ω was arbitrary, it follows that $A[x]$ is Noetherian as an $A[x]$-module. □

(Lecture 28)

Corollary 15. If $A \in \operatorname{ob} \mathbf{CommRing}$ is Noetherian, then $A[x_1, \ldots, x_n]$ is also Noetherian.

Proof. We have that $A[x_1, \ldots, x_n] \cong A[x_1, \ldots, x_{n-1}][x_n]$. Now use induction. □

Example 37. Both $\mathbb{Z}[x_1, \ldots, x_n]$ and $k[x_1, \ldots, x_n]$ are Noetherian where k is a field.

Corollary 16. From our proof of the theorem, we see that if k is a field, then $k[x]$ is a PID.

Corollary 17. If A is Noetherian and B is a finitely generated commutative A-algebra, then B is Noetherian as a ring.

Proof. We have a ring embedding $i : A \to B$. As B is finitely generated as an A-algebra, there exists a map $\phi : A[x_1, \dots, x_n] \twoheadrightarrow B$ of $A[x_1, \dots, x_n]$-modules. By a previous corollary, $A[x_1, \dots, x_n]$ is Noetherian, which implies that B is the quotient of a Noetherian $A[x_1, \dots, x_n]$-module. Hence B is also Noetherian as a module over $A[x_1, \dots, x_n]$. Let $I \trianglelefteq B$ be an ideal. Then I is a submodule over $A[x_1, \dots, x_n]$ via ϕ and thus is finitely generated as such. It follows automatically that I is also finitely generated as a B-module. $\square$

Definition. Let $A \in \operatorname{ob}\mathbf{CommRing}$, B be a commutative A-algebra, and G be a group. We say that G *acts on B as an A-algebra* if there is an action $\rho : G \to \mathrm{Aut}_{\mathbf{Set}}(B)$ such that each $\rho_g : B \to B$ is an *algebra isomorphism*, i.e.,

$$\rho_g(b_1 + b_2) = \rho_g(b_1) + \rho_g(b_2)$$
$$\rho_g(b_1 b_2) = \rho_g(b_1)\rho_g(b_2)$$
$$\rho_g(a) = a.$$

Theorem 12. (Hilbert's theorem on invariants) Let k be a field, G a finite group, and A a finitely generated k-algebra equipped with a G-action. If $(|G|, \mathsf{char}(k)) = 1$, then $A^G \coloneqq \{a \in A : \forall g \in G. g \cdot a = a\}$ if a finitely generated k-subalgebra.

Proof. Note that A^G is a k-subalgebra because $k \subset A^G$. As $|G|$ is coprime to $\mathsf{char}(k)$, we know that $|G|$ is invertible in A. Define the algebra homomorphism

$$S : A \to A, \quad a \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot a.$$

Let $a \in A$. Then

$$\chi_a(x) \coloneqq \prod_{g \in G} (x - g \cdot a) \in A[x].$$

The coefficients of this polynomials are elementary symmetric functions in $\{g \cdot a\}_{g \in G}$. Further, for any $h \in G$, we get a permutation $\{g \cdot a\}_{g \in G} \xrightarrow{h \cdot (-)} \{hg \cdot a\}_{g \in G}$. Thus, the same coefficients are invariant under the G-action, which proves that $\chi_a(x) \in A^G[x]$.

Definition. Let $P(x)$ be a polynomial of degree k with roots $x_1, \dots, x_k$. If $n \in \mathbb{N}$, then define the *n-th Newton sum* as $P_n = x_1^n + \cdots + x_k^n$.

It is known that any elementary symmetric polynomial can be expressed in terms of Newton sums. In our case, we can express each coefficient of $\chi_a(x)$ in terms of $S(a), S(a^2), \dots, S(a^{|G|})$.

Find generators $u_1, \dots, u_m$ for A over k. Let B denote subalgebra of A^G generated by $\{S(u_i^k)\}_{i=1,\dots,m,\ k=1,\dots,|G|}$ over k. For each i, observe that $X_{u_i}(x) \in B[x]$ and that $X_{u_i}(u_i) = 0$. It follows that $u_i^{|G|}$ can be written as a B-combination of $1, u_i, \dots, u_i^{|G|-1}$. [[Why?]] This implies that any monomial of the form $u_1^{s_1} \cdots u_m^{s_m}$ can be written as a B-combination of monomials of the form $u_1^{\alpha_1} \cdots u_m^{\alpha_m}$ where each $0 \le \alpha_i < |G|$. We may thus write

$$a = \sum_{\alpha := (\alpha_1, \dots, \alpha_m)} \phi_\alpha u^\alpha, \quad \alpha_i < |G|, \quad \phi_\alpha \in B.$$

If $a \in A^G$, then $a = S(a) = \sum_\alpha S(\phi_\alpha) S(u^\alpha) = \sum_\alpha \phi_\alpha S(u^\alpha)$. As each $\alpha_i < |G|$, the set $\{S(u^\alpha)\}_\alpha$ is finite. Also, B is finitely generated over k. As a result, A^G is finitely generated over k. $\square$

(Lecture 29)

Note 12. We now turn to the homology of modules, which offers a quantitative measure of the complexity of objects in $R-\mathbf{Mod}$.

Definition. An *additive invariant of modules* is a class function $\phi : \mathrm{ob}(R{-}\mathbf{Mod}) \to \mathbb{Z}$ such that for every R-module M and submodule $N \subset M$ we have $\phi(M) = \phi(N) + \phi({}^{M}\!/_{N})$.

Example 38.

1. $\dim_k : \mathrm{ob}(\mathbf{Vect}_k) \to \mathbb{Z}$ where k is a field.

2.

   Definition. An R-module M is called

   (a) *simple* if it has no proper nontrivial submodules.

   (b) *indecomposable* if $M = M_1 \coprod M_2$ implies that M_1 or M_2 is trivial.

   We have exact analogues of Jordan-Holder and Krull-Schmidt for $R{-}\mathbf{Mod}$. Define the *length of* M as the length of any composition series of M. By Jordan-Holder, the length function $\lambda : \mathrm{ob}(R{-}\mathbf{Mod}) \to \mathbb{Z} \cup \{\infty\}$ is an additive invariant.

Definition. Let R and S be rings and $F : R{-}\mathbf{Mod} \to S{-}\mathbf{Mod}$ be a functor. Let M and N be R-modules. We say that F

1. is *additive* if $F : \mathrm{Hom}(M, N) \to \mathrm{Hom}(F(M), F(N))$ is a homomorphism of abelian groups.

2. is *exact* if for any short exact sequence $0 \longrightarrow N \xrightarrow{i} M \xrightarrow{q} {}^{M}\!/_{N} \longrightarrow 0$, the sequence $0 \longrightarrow F(N) \xrightarrow{F(i)} F(M) \xrightarrow{F(q)} F({}^{M}\!/_{N}) \longrightarrow 0$ is also exact.

3. is *left exact* (resp. *right exact*) if for any short exact sequence $0 \to M' \to M \to M'' \to 0$ of R-modules, the sequence $0 \to F(M') \to F(M) \to F(M'')$ (resp. $F(M') \to F(M) \to F(M'') \to 0$) of S-modules is also exact.

Example 39.

1. The forgetful functor $U : R{-}\mathbf{Mod} \to \mathbb{Z}{-}\mathbf{Mod}$ is both additive and exact.

2. If R is a ring, then the functors $\mathrm{Hom}_R(M, -) : R{-}\mathbf{Mod} \to \mathbb{Z}{-}\mathbf{Mod}$ and $\mathrm{Hom}_R(-, M) : R{-}\mathbf{Mod}^{\mathrm{op}} \to \mathbb{Z}{-}\mathbf{Mod}$ are both left exact.

   Proof. We verify that $\mathrm{Hom}_R(M, -)$ is left exact. Let $0 \longrightarrow X' \xrightarrow{f} X \xrightarrow{g} X'' \longrightarrow 0$ be a short exact sequence of R-modules. Apply $\mathrm{Hom}_R(M, -)$ to get a sequence of abelian groups.

   $$0 \longrightarrow \mathrm{Hom}_R(M, X') \xrightarrow{f\circ(-)} \mathrm{Hom}_R(M, X) \xrightarrow{g\circ(-)} \mathrm{Hom}_R(M, X'') \longrightarrow 0$$

   Let $\phi : M \to X'$ satisfy $f \circ \phi = 0$. Then $\phi = 0$ since ϕ is injective by assumption. Hence $f \circ (-)$ is injective. Let $\psi : M \to X$ satisfy $g \circ \psi = 0$. If $m \in M$, then

   $$g(\psi(m)) = 0 \implies \psi(m) \in \ker g = \mathrm{im}\, f \implies \exists! x' \in X'. f(x') = \psi(m).$$

   Define $\gamma(m) = x'$. Then $f \circ \gamma = \psi$. Since it is unique, γ is a morphism of R-modules. Thus, $\psi \in \mathrm{im}(f\circ(-))$. Also, it's clear that $\mathrm{im}(f\circ(-)) \subset \ker(g\circ(-))$. It follows that $\mathrm{im}(f\circ(-)) = \ker(g\circ(-))$. $\square$

   Note 13. This proof works for any abelian category.

3. If $M \in \mathrm{ob}(R^{\mathrm{op}}{-}\mathbf{Mod})$, then we have the functor $(-) \otimes_R M : R{-}\mathbf{Mod} \to \mathbb{Z}{-}\mathbf{Mod}$. If M is an R-module, then we have the functor $M \otimes_R (-) : R^{\mathrm{op}}{-}\mathbf{Mod} \to \mathbb{Z}{-}\mathbf{Mod}$. Both are right exact.

Proof. We verify that $M \otimes_R (-) : R^{\mathrm{op}}\text{-}\mathbf{Mod} \to \mathbb{Z}\text{-}\mathbf{Mod}$ is right exact. Let $0 \longrightarrow X' \xrightarrow{f} X \xrightarrow{g} X'' \longrightarrow 0$ be a short exact sequence of right R-modules. Apply the functor to get a sequence of abelian groups.

$$0 \longrightarrow M \otimes_R X' \xrightarrow{\mathrm{id}_M \otimes f} M \otimes_R X \xrightarrow{\mathrm{id}_M \otimes g} M \otimes_R X'' \longrightarrow 0$$

If $m \otimes x'' \in M \otimes_R X''$, then there is some $x \in X$ such that $g(x) = x''$, so that $\mathrm{id}_M \otimes g(m \otimes x) = m \otimes x''$. Hence $\mathrm{id}_M \otimes g$ is surjective. To show that $\mathrm{im}(\mathrm{id}_M \otimes f) = \ker(\mathrm{id}_M \otimes g)$, it is enough to construct a map of modules $h : M \otimes_R X'' \to M \otimes_R X \big/ \mathrm{im}(\mathrm{id}_M \otimes f)$ such that $h \circ (\mathrm{id}_M \otimes g) : M \otimes_R X \to M \otimes_R X \big/ \mathrm{im}(\mathrm{id}_M \otimes f)$ equals the natural projection. Define $h(m \otimes x'') = m \otimes x + \mathrm{im}(\mathrm{id}_M \otimes f)$ for any x such that $g(x) = x''$. Note that $g(a) = x'' = g(b)$ implies $a - b \in \ker g = \mathrm{im}\, f$, so that $m \otimes (a - b) \in \mathrm{im}(\mathrm{id}_M \otimes f)$. As $m \otimes b + m \otimes (a - b) = m \otimes a$, we see that h is well-defined. $\square$

Definition. An R-module M is called

1. *projective* if $\mathrm{Hom}_R(M, -)$ is exact (i.e., right exact).
2. *injective* if $\mathrm{Hom}_R(-, M)$ is exact (i.e., right exact).
3. *flat* if $(-) \otimes_R M$ is exact (i.e., left exact).

Note 14. Projective and injective are dual notions.

Remark 42.

1. M is projective if and only if $\mathrm{Hom}_R(M, -)$ preserves epimorphisms $X \xrightarrow{q} X'' \to 0$. That is, for any map $\phi : M \to X''$, there is some map ψ such that

$$\begin{tikzcd} M \arrow[d, dashed, "\psi"'] \arrow[dr, "\phi"] & & \\ X \arrow[r, two heads, "q"'] & X'' \arrow[r] & 0 \end{tikzcd}$$

commutes.

2. M is injective if and only if $\mathrm{Hom}_R(-, M)$ maps monomorphisms $0 \to X' \xrightarrow{i} X$ to epimorphisms. That is, $\mathrm{Hom}_R(X, M) \xrightarrow{(-)\circ i} \mathrm{Hom}_R(X', M)$ is surjective, so that for any map $\phi : X' \to M$, there is some map $\psi : X \to M$ such that

$$\begin{tikzcd} & M & \\ 0 \arrow[r] & X' \arrow[u, "\phi"] \arrow[r, hook, "i"'] & X \arrow[ul, dashed, "\psi"'] \end{tikzcd}$$

commutes.

(Lecture 30)

Proposition 12. An R-module M is projective if and only if it is a direct summand of a free R-module, i.e., $M \coprod N$ is free for some R-module N.

Proof. ($\Longleftarrow$) For now, suppose that M is free. Then

$$M \cong \coprod_{\lambda \in \Lambda} R.$$

We have a basis (m_λ) for M. Let $X \xrightarrow{q} X'' \to 0$ be an exact sequence of R-modules. Let $\phi : M \to X''$ be a homomorphism. For each λ, find some lift $x_\lambda \in X$ of $\phi(m_\lambda)$. Then the assignment $\lambda \mapsto x_\lambda$ determines a set function $x : \Lambda \to |X|$. By adjointness, there is some $\psi \in \mathrm{Hom}_{R-\mathbf{Mod}}(\coprod_\lambda R, X)$ such that $\psi(m_\lambda) = x_\lambda$.

Explicitly, if $a \in M$, then $a = \sum_\lambda a_\lambda m_\lambda$ where $a_\lambda \in R$. Then $\psi(a) = \sum_\lambda a_\lambda x_\lambda$. This implies that $q(\psi(a)) = \sum_\lambda a_\lambda \phi(m_\lambda) = \phi(a)$. It follows that

$$\begin{tikzcd}
M \arrow[d, "\psi"'] \arrow[dr, "\phi"] & & \\
X \arrow[r, two heads, "q"'] & X'' \arrow[r] & 0
\end{tikzcd}$$

commutes.

Now, drop the assumption that M is free but assume that $M \coprod N$ is free for some R-module N. Let

$$\begin{tikzcd}
M \arrow[dr, "\phi"] & & \\
X \arrow[r, two heads, "q"'] & X'' \arrow[r] & 0
\end{tikzcd} \tag{η}$$

be a projectivity diagram. As $M \coprod N$ is free, our previous argument shows that there is some morphism f such that

$$\begin{tikzcd}
M \coprod N \arrow[d, "f"'] \arrow[dr, "\phi \coprod 0"] & & \\
X \arrow[r, "q"'] & X'' \arrow[r] & 0
\end{tikzcd}$$

commutes. Define $\psi : M \to X$ by the composition $M \hookrightarrow M \coprod N \xrightarrow{f} X$. Then ψ fills (η).

$(\Longrightarrow)$ Suppose that M is projective. We have the exact sequence $\coprod_{m \in M} R \xrightarrow{q} M \to 0$. Hence there is some map s such that

$$\begin{tikzcd}
M \arrow[d, "s"'] \arrow[dr, "\mathrm{id}_M"] & & \\
\coprod_m R \arrow[r, "q"'] & M \arrow[r] & 0
\end{tikzcd}$$

commutes. Then $M \coprod \ker q \cong \coprod_m R$. $\square$

Definition. Let M be an R-module. A *projective resolution of* M is an exact sequence of R-modules

$$\cdots \to P^3 \to P^2 \to P^1 \to M \to 0$$

such that each P^i is projective.

Remark 43. Every module has a free, hence projective, resolution.

Corollary 18. Any short exact sequence of R-modules $0 \to X' \to X \to M \to 0$ with M projective splits.

Proof. Find a map s such that

$$\begin{tikzcd}
M \arrow[d, "s"'] \arrow[dr, "\mathrm{id}_M"] & & \\
X \arrow[r, "q"'] & M \arrow[r] & 0
\end{tikzcd}$$

commutes. $\square$

Corollary 19. Any short exact sequence of R-modules $0 \to M \to X \to X'' \to 0$ with M injective splits.

Corollary 20. If $\{M_\lambda\}$ is a collection of R-modules, then $\coprod_\lambda M_\lambda$ is projective if and only if each M_λ is projective.

Proof. ($\Longleftarrow$) As each M_λ is projective, we know that $\operatorname{Hom}_R(M_\lambda, -)$ is an exact functor. This implies that $\operatorname{Hom}_R(\coprod_\lambda M_\lambda, -) \cong \prod_\lambda \operatorname{Hom}_R(M_\lambda, -)$ is exact as well.

($\Longrightarrow$) As $\coprod_\lambda M_\lambda$ is projective, there is some R-module N such that $(\coprod_\lambda M_\lambda) \coprod N \cong M_\lambda \coprod (\coprod_{\alpha \neq \lambda} M_\alpha) \coprod N$ is free. $\square$

Corollary 21. If $\{M_\lambda\}$ is a collection of R-modules, then $\prod_\lambda M_\lambda$ is injective if and only if each M_λ is injective.

Remark 44. Projectivity has to do with the non-existence of relations among "good" generators, whereas injectivity has to do with the divisibility of generators and hence all elements.

Let M be an R-module and $x \in M$. We want to know if x is divisible by $a \in R$, i.e., $x = a \cdot y$ for some $y \in M$. Suppose that we know that M extends $0 \to M \hookrightarrow N$ to a module N so that $x = a \cdot z$ for some $z \in N$. Suppose also that M is injective. Then find some map ψ so that

$$\begin{tikzcd} & M & \\ 0 \arrow[r] & M \arrow[u, "\mathrm{id}_M"] \arrow[r, hook, "i"'] & N \arrow[ul, dashed, "\psi"'] \end{tikzcd}$$

commutes. This gives $a\psi(z) = \psi(az) = \psi(x) = x$. Hence x is divisible by a in this situation.

Example 40. $\mathbb{Z}$ is not injective in **Ab**.

Example 41.

1. $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

   Proof. Let

$$\begin{tikzcd} & \mathbb{Q} & \\ 0 \arrow[r] & X' \arrow[u, "\phi"] \arrow[r, hook, "i"'] & X \end{tikzcd}$$

   be an injectivity diagram. The set

$$\{(A, \xi) : X' \subset \underbrace{A}_{\text{abelian}} \subset X,\ \xi : A \to \mathbb{Q} \text{ lifts } \phi.\}$$

   is nonempty and partially ordered by $\leq$ where $(A_1, \xi_1) \leq (A_2, \xi_2)$ if $A_1 \subset A_2$ and $\xi_1 = \xi_2 \restriction_{A_1}$. By Zorn, there is some maximal element (A, ξ). If $A = X$, then we are done. Suppose, for contradiction, that $A \subsetneq X$. There is some $x \in X \setminus A$. Let $\tilde{A} = \langle A, x \rangle \subset X$.

   We can extend $\xi : A \to \mathbb{Q}$ to a homomorphism $\tilde{\xi} : \tilde{A} \to \mathbb{Q}$ by deciding where to send x. Indeed, if $nx \notin A$ for every nonzero integer n, then set $\tilde{\xi}(x) = 0$. If there is some $n \in \mathbb{Z} \setminus \{0\}$ such that $nx \in A$, then $\{n \in \mathbb{Z} : nx \in A\}$ is an ideal in $\mathbb{Z}$ and thus equals (n_0) for some integer $n_0 > 0$. Define $\tilde{\xi}(x) = \frac{\xi(n_0 x)}{n_0} \in \mathbb{Q}$.

   For each $\tilde{a} \in \tilde{A}$, write $\tilde{a} = a + mx$ for some $a \in A$ and some $m \in \mathbb{Z}$. Define $\tilde{\xi}(\tilde{a}) = \xi(a) + m\tilde{\xi}(x)$.

   We claim that $\tilde{\xi}$ is well-defined. If $\{n \in \mathbb{Z} : nx \in A\} = (0)$, then $\tilde{\xi}(x) = 0$ and $\tilde{\xi}(\tilde{a}) = \xi(a)$, where a is uniquely determined from $\tilde{a}$. If $\{n \in \mathbb{Z} : nx \in A\} = (n_0)$, then $\tilde{\xi}(\tilde{a}) = \xi(a) + \frac{m\xi(n_0 x)}{n_0}$. If $\tilde{a} = b + kx$, then $a - b = (k - m)x$. If this equals 0, then we're done. Otherwise, $k - m = dn_0$ for some integer $d \neq 0$. Then

$$\begin{aligned} 0 &= \xi(a - b) - \xi((k - m)x) = \xi(a) - \xi(b) - \xi(dn_0 x) \\ &= \xi(a) - \xi(b) - \tilde{\xi}(dn_0 x) = \xi(a) - \xi(b) - dn_0 \tilde{\xi}(x) \\ &= \xi(a) - \xi(b) - (k - m)\tilde{\xi}(x) = \xi(a) - \xi(b) + \frac{m - k}{n_0} \xi(n_0 x) \\ &= \tilde{\xi}(a + mx) - \tilde{\xi}(b + kx). \end{aligned}$$

We have shown that $(\tilde{A}, \tilde{\xi}) > (A, \xi)$, a contradiction. $\square$

Corollary 22. Any divisible abelian group is injective.

2. The circle group S^1 is injective.
3. Any field of characteristic zero is injective as a $\mathbb{Z}$-module.
4. $\mathbb{Q}_{(p)} / \mathbb{Z}$ is injective as a $\mathbb{Z}$-module where $\mathbb{Q}_{(p)} \coloneqq \{\frac{n}{p^k} : n \in \mathbb{Z},\ k \geq 0,\ p \text{ prime}\}$.