Perry Hart
MATH 602
Fall 2018

Abstract

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

Contents

1 Group actions

1.1 Lecture 1

Definition 1.1.1. A *(left) action of a group G on a set S* is a homomorphism $\theta : G \to \mathrm{Aut}(S)$, where $\mathrm{Aut}(S)$ denotes the group of all set bijections $S \to S$.

Notation. We may write $g \cdot x$ for $\theta(g)(x)$.

Equivalently, a group action is a function $a : G \times S \to S$ such that

(i) $a(g, a(g', x)) = a(gg', x)$ and

(ii) $a(e, x) = x$

for any $g, g' \in G$ and $x \in S$. Indeed, given a homomorphism $\theta : G \to \mathrm{Aut}(S)$, we have a function $G \times S \to S$ defined by $(g, x) \mapsto \theta(g)(x)$. Conversely, given an action $a : G \times S \to S$, we have a homomorphism $G \to \mathrm{Aut}(S)$ defined by $g \mapsto (x \mapsto a(g, x))$.

Example 1.1.2. The *trivial group action* sends each element g to the identity function id_S on S.

Definition 1.1.3. A *right group action* is a function $b : S \times G \to S$ such that

(i) $b(b(x, g), g') = b(x, gg')$ and

(ii) $b(x, e) = x$

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

Exercise 1.1.4. *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. □

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

$$G \xrightarrow{\theta} \operatorname{im}\theta \hookrightarrow \mathrm{Aut}(S) \ .$$

Moreover, we have a commutative triangle

$$\begin{array}{ccc} G & \xrightarrow{q} & G/\ker(\theta) \\ & \searrow^{\theta} & \downarrow \cong \\ & & \theta(G) \end{array} \ .$$

Definition 1.1.5. Consider a group action $\theta : G \to \mathrm{Aut}(S)$.

1. We say that θ is *faithful* or *effective* if it is injective.

2. We say that θ is *free* if for any $g \in G$ and $s \in S$,

$$\theta(g)(s) = s \implies g = e.$$

Let $x \in S$. Define the *stabilizer subgroup of* x as

$$\mathrm{Stab}_\theta(x) \equiv \{g \in G \mid g \cdot x = x\}.$$

Further, define the *orbit of* x as

$$\mathrm{Orb}_\theta(x) \equiv \{y \in S \mid \exists g \in G \text{ s.t. } g \cdot x = y\}.$$

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

Exercise 1.1.6.

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 $f : {}^{G}\!/_{\mathrm{Stab}_\theta(x)} \to \mathrm{Orb}_\theta(x)$ given by $[g] \mapsto g \cdot x$ is well-defined and bijective.*

Proof.

1. This follows directly from the equation $R_a = \{(s, gs) : s \in S,\ g \in G\}$.
2. Let $g \sim h$, so that $g = hs$ for some $s \in \mathrm{Stab}_\theta(x)$.Then $g \cdot x = (hs) \cdot x = h \cdot x$, which means that f is well-defined. The fact that it's injective and surjective is obvious.

□

Corollary 1.1.7. *If G is finite, then $|\mathrm{Orb}_\theta(x)| = \frac{|G|}{|\mathrm{Stab}_\theta(x)|}$.*

Example 1.1.8. 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 any 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 any set X, the *pullback action* $\theta^* : G \to \mathrm{Aut}(X^S)$ given by $g \mapsto \big(f \mapsto f \circ \theta(g^{-1})\big)$.
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 1.1.9. Let $R \subset S \times S$ be an equivalence relation such that $\theta^{\times 2}(g)(R) = R$ for each $g \in G$. Then the map ${}^{G}\!/_{R} : G \to \mathrm{Aut}\left({}^{S}\!/_{R}\right)$ given by $g \mapsto ([s] \mapsto [gs])$ is an action.

Example 1.1.10. Let $a : G \times S \to G$ be an action. If $S = G$, then

(a) the *left regular action* is given by $a(g,x) = gx$;

(b) the *right regular action* is given by $a(g,x) = xg^{-1}$; and

(c) the *conjugation action.* given by $a(g,x) = gxg^{-1}$.

If $\mathrm{conj} : G \to \mathrm{Aut}(G)$ denotes the conjugation action $g \mapsto \left(x \mapsto gxg^{-1}\right)$, then we call

$$G/Z(G) \cong \mathrm{Inn}(G) \coloneqq \mathrm{im}(\mathrm{conj})$$

the subgroup of *inner automorphisms of* G, which is a normal subgroup. Further, we call the quotient group

$$\mathrm{Aut}(G)/\mathrm{Inn}(G)$$

the group of *outer automorphisms of* G, denoted by $\mathrm{Out}(G)$.

Exercise 1.1.11. *Let θ denote the conjugation action. Show that* $\ker\theta$ *equals the center* $Z(G) \coloneqq \{g \in G : gx = xg,\ x \in G\}$ *of* G

1.2 Lecture 2

Suppose that a set S possesses additional structure Φ (such as a group law). Let the subgroup $\mathrm{Aut}_\Phi(S) \leq \mathrm{Aut}(S)$ consists of all those automorphisms of S preserving Φ. We say that a group G *acts on S by automorphisms of* Φ if we have an action $\theta : G \to \mathrm{Aut}(S)$ such that $\theta(g)$ preserves Φ for every $g \in G$. In this case, there is a commutative triangle of the form

$$\begin{array}{ccc} G & \xrightarrow{\theta} & \mathrm{Aut}(S) \\ & \searrow & \uparrow \\ & & \mathrm{Aut}_\Phi(S) \end{array} .$$

Example 1.2.1. The conjugation action maps elements of a group G to $\mathrm{Aut}_+(G)$ the group of automorphisms of G.

We can define a further class of examples with the following notion from representation theory.

Definition 1.2.2. Let S be a set and G be a group. Let k be a field.

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

Example 1.2.3 (The permutation representation). Let $S = \{1,\dots,n\}$ and $G = S_n$. Let X be a set. Then we have an action $\theta^* : G \to \mathrm{Aut}(X^S) \cong \mathrm{Aut}(X^n)$ given by

$$\theta^*(\sigma)(x_1,\dots,x_n) = \left(x_{\sigma^{-1}(1)},\dots,x_{\sigma^{-1}(n)}\right)$$

. If X is a field, then $X^S \cong X^n$, which is an n-dimensional vector space. In this case, θ^* is an X-linear representation of S_n and factors as

$$\begin{array}{ccc} G & \xrightarrow{\theta^*} & \mathrm{Aut}(X^n) \\ & \searrow & \uparrow \\ & & \mathrm{GL}_n(X) \end{array}.$$

Example 1.2.3 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 1.2.4 (Power set representation). 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 1.2.5 (Galois theory). Let $f(x) = a_n x^n + \cdots + a_0$ over $\mathbb{Q}$ where $a_n \neq 0$. Thanks to the fundamental theorem of algebra, we know that $f(x) = a_n (x - \beta_1) \cdots (x - \beta_n)$ for some $(\beta_1, \ldots, \beta_n) \in \mathbb{C}^n$. As it turns out, each β_i has the form $f(a_0, \ldots, a_n)$ 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).

Consider

$$\mathbb{Q}\left[\tilde{\beta}\right] \coloneqq \mathbb{Q}\left[\beta_1, \ldots, \beta_n\right] = \{F(\beta_1, \ldots, \beta_n) : F \in \mathbb{Q}\left[x_1, \ldots, x_n\right]\}$$

$$\underbrace{\mathrm{Gal}(f) \coloneqq \left\{\sigma \in S_n : \exists \text{ bijection } g : \mathbb{Q}\left[\tilde{\beta}\right] \to \mathbb{Q}\left[\tilde{\beta}\right] \text{ s.t. } g(F(\beta_1, \ldots, \beta_n)) = F(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)}) \ \forall F \in \mathbb{Q}\left[x_1, \ldots, x_n\right]\right\}}_{\textit{Galois group of } f}.$$

Exercise 1.2.6. *Show that* $g : G \to \mathrm{Aut}(\mathbb{Q}\left[\tilde{\beta}\right])$ *is a homomorphism where* $G \coloneqq \{g(\sigma) : \sigma \in \mathrm{Gal}(f)\}$.

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

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(\mathbb{Q}\left[\tilde{\beta}\right]) \\ & \searrow & \uparrow \\ & & \mathrm{GL}_{\mathbb{Q}}(\mathbb{Q}\left[\tilde{\beta}\right]) \end{array}.$$

Now, consider the polynomial $f(x) \equiv (x^2 - 3)(x^2 - 5)$, which has roots $\left\{\pm\sqrt{3}, \pm\sqrt{5}\right\}$. 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 $\mathrm{Gal}(f) = \{(1), (12), (34), (12)(34)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

1.3 Lecture 3

Notation. If G acts on S, then let $G \backslash S$ denote the set of orbits.

Definition 1.3.1. 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*.

If θ is simple, then for any $x \in S$, the mapping $f : G \to S$ given by $g \mapsto \theta(g)(x)$ is a bijection.

Example 1.3.2.

1. Consider the action $\rho : S^1 \to \mathrm{Aut}(\mathbb{C})$ given by $\theta \mapsto \rho_\theta \coloneqq \left(z \mapsto e^{i\theta} z\right)$. 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, $S^1 \backslash \mathbb{R}^2 = \mathbb{R}_{\geq 0}$, which induces a map $\mathbb{C} \to \mathbb{R}_{\geq 0}$ given by $z \mapsto |z|$.

2. Let $H \leq G$. Consider the restriction $\ell \restriction_H : H \to \mathrm{Aut}(G)$ of the *left translation* action ℓ of G on itself. Then $H \backslash G$ 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 1.3.3.

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 $S_n \backslash_{\mathrm{conj}} S_n$ and the set of unordered partitions of $\{1, \ldots, n\}$.*

Definition 1.3.4. 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 square commutes.

$$\begin{array}{ccc} S & \xrightarrow{f} & T \\ {\scriptstyle \theta(g)}\downarrow & & \downarrow{\scriptstyle \psi(g)} \\ S & \xrightarrow[f]{} & T \end{array}$$

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

Note 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 $f_2 \circ f_1 = \mathrm{id}_S$.

Example 1.3.5.

1. If $\theta : G \to \mathrm{Aut}(S)$ is simply transitive and $x \in S$, then $f_x : G \to S$ defined by $g \mapsto \theta(g)(x)$ 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.

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.

Theorem 1.3.6. *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

$$\theta(g)(x) = \theta(hs)(x) = \theta(h)(\theta(s)(x)) = \theta(h)(x),$$

which proves that f_x is well-defined.

Define the map $F : K \to \mathrm{Stab}_\theta(x)$ by $F(y) = S_y \coloneqq \{g \in G : \theta(g)(x) = y\} = [s_0]$ 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

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

□

Corollary 1.3.7. *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 denotes any chosen stabilizer subgroup $\mathrm{Stab}_\theta(x)$.*

Corollary 1.3.8. *If $\theta : G \to \mathrm{Aut}(S)$ is an action, then*

$$S = \coprod_{\omega \in G \backslash S} \omega$$
$$\theta = \coprod_{\omega \in G \backslash S} \theta_\omega$$

such that each θ_ω is isomorphic to the left translation action of G on ${}^{G}\!/_{\mathrm{Stab}_\theta(x)}$ for any chosen $x \in S$.

Corollary 1.3.9 (Orbit-stabilizer). *Let G be finite and $\theta : G \to \mathrm{Aut}(S)$ be an action. Then*

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

for any $x \in S$.

Corollary 1.3.10 (Class equation). *If G is finite, then*

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

Exercise 1.3.11. *Suppose that $H \leq G$.*

1. *Compute the kernel of the left translation action ℓ by G on G/H*
2. *Show that $H \trianglelefteq G$ if and only if the kernel of ℓ restricted to H is trivial.*

1.4 Lecture 4

Corollary 1.4.1. *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 $\ell : G \to \mathrm{Aut}(G/H)$. Let ω be any orbit of the restricted action $\ell \restriction_H$, so that $|\omega| = \frac{|H|}{|\mathrm{Stab}|}$. Since $|\omega| \mid |H|$, it follows that $|\omega| = 1$ or $|\omega| \geq p$. 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, $\ell \restriction_H$ is trivial, which means that $H \trianglelefteq G$. □

If G and S are finite and $\theta : G \to \mathrm{Aut}(S)$ is an action, then for each $g \in G$, consider the subset $\mathrm{Fix}(g) \subset S$ consisting of all elements s such that $g \cdot s = s$.

Exercise 1.4.2 (Burnside's lemma). *Check that*

$$|G \backslash S| = \frac{1}{|G|} \sum_g |\mathrm{Fix}(g)| .$$

For a hint, consider $\{(g, x) : g \cdot x = x\} \subset G \times S$.

Definition 1.4.3. Let p be a prime. A finite group G is a *p-group* if $|G| = p^k$ for some $k \geq 0$.

Proposition 1.4.4.

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

Proof.

1. Choose an element $x \in G$ such that $x \neq e$. Note that $|\langle x \rangle| \mid |G| = p$. Hence $|\langle x \rangle| = p$ since p is prime. This means that $\langle x \rangle = G$.
2. The class equation implies that $|Z(G)| \equiv 0 \mod p$. But $Z(G)$ contains at least the identity element, so that $|Z(G)| > 0$. It follows that $|Z(G)| \geq p$.

□

2 Solvable and nilpotent groups

Let G be any group. We say that a sequence of subgroups

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

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 $i \geq 0$.

Set $\Delta^{(0)}G = G$ and $\Delta^{(k+1)}G = \Delta(\Delta^{(k)}G)$, where

$$\Delta G \coloneqq \Delta^{(1)}G \coloneqq \left\{x \in G : x = aba^{-1}b^{-1}\right\},$$

known as the *commutator* or *derived* subgroup of G.

Then 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.

The group $G^{\mathrm{ab}} \coloneqq G/\Delta G$ is called the *abelianization of* G. If $f : G \longrightarrow \underset{\text{abelian}}{A}$, then f factors uniquely as follows.

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ & \searrow^{g} & \uparrow \tilde{f} \\ & & G^{\mathrm{ab}}. \end{array}$$

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

Definition 2.0.1.

1. We say that the derived series of G *terminates* if $\Delta^{(t+1)}G = \Delta^{(t)}G$ for some t.

   In this case, if $\Delta^{(t)}G = \{e\}$, then we say that the series *terminates at* $\{e\}$.

2. 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 2.0.2. *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 2.0.3. 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 $G_{i-1}/G_i \subset Z\left(G/G_i\right)$ for each $1 \leq i \leq n$.

Note 2.0.4.

1. Every quotient and subgroup of a nilpotent group is nilpotent.

2. Every p-group G is nilpotent.

   Proof. Let $G_0 = \{e\}$ and $G_1 = Z(G)$. Further, for each $i > 1$, let G_i satisfy

   $$G \geq G_i \geq G_{i-1}$$
   $$G_i/G_{i-1} = Z\left(G/G_{i-1}\right).$$

   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. □

2.1 Lecture 5

Example 2.1.1.

1. Every abelian group is nilpotent and thus solvable.

2. There are abelian groups which are not polycyclic, e.g., $G \coloneqq \mathbb{Q}/\mathbb{Z} \cong \mu_\infty$ 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 that $\langle x_i \rangle = G$, 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. Indeed, its only normal subgroup is $\langle (123) \rangle$, which is nontrivial and thus cannot be contained in $Z(D_3)$.

Exercise 2.1.2. *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 $n = 2^k m$ with m odd and $k \geq 1$, then $Z(D_n) = \left\{e, m2^{k-1}\right\}$, 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 our claim. □

Note 2.1.3. We have the following two chains of strict containments for certain classes of groups.

(i) Cyclic $\subsetneq$ Abelian $\subsetneq$ Nilpotent $\subsetneq$ Solvable.

(ii) Cyclic $\subsetneq$ Polycyclic $\subsetneq$ Solvable.

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

Example 2.1.4. 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 $(x, a) \cdot (y, b) \equiv (x + y, a + b + \omega(x, y))$. This is called the *Heisenberg group of* H. It is the group of symmetries of the observables in a simple quantum mechanical system.

Exercise 2.1.5. *Check that* $Z(H(V, \omega)) \cong \mathbb{R}$ *and that* $H(V,\omega)/Z(H(V,\omega)) \cong (V, +)$ *as groups.*

This means that $H(V, \omega)$ is nilpotent but not abelian.

Example 2.1.6. 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 each $n > 1$.

We prove by induction that it is solvable. In the case where $n = 1$, it is abelian, hence solvable. Now suppose it's solvable for each $n - 1$ 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 $n - 1 \times n - 1$ matrix contained 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 $\ker g \cong \left(k^{n-1}, +\right)$, which is abelian. Two applications of Exercise 2.0.2(2) show that $B_n(k)$ is solvable, thereby completing our proof.

Proposition 2.1.7. *S_n is solvable if and only if $n \leq 4$.*

Proof. Recall the surjective homomorphism $\operatorname{sgn} : S_n \to \{\pm 1\}$ given by $\sigma \mapsto \det(P_\sigma)$ where P_σ denotes the permutation matrix. Then the *alternating group* $A_n \coloneqq \ker(\operatorname{sgn})$ consists of all *even* permutations of $\{1, 2, \ldots, n\}$. Note that if $\sigma = (i_1 \ \cdots \ i_k)$, then $\operatorname{sgn}(\sigma) = (-1)^{k-1}$ since since σ can be written as a cycle of $k-1$ transpositions, each having a permutation matrix with determinant -1. We now see that S_n is solvable if and only if A_n is solvable. □

Lemma 2.1.8. *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

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

□

Lemma 2.1.9. $\Delta S_n = A_n$.

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 each $n > 3$, 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 $\Delta S_n = A_n$. □

Lemma 2.1.10.

1. $\Delta^{(2)} S_4 = \Delta A_4 \cong C_2 \times C_2$.
2. $\Delta^{(2)} S_n = \Delta A_n = A_n$ *for each* $n \geq 5$.

Proof.

1. 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 that $C_2 \times C_2 \supset \Delta A_4 \neq \{e\}$. Since ΔA_4 is normal, it must equal $C_2 \times C_2$.
2. Note that $\Delta A_4 \subset \Delta A_n$ for each $n \geq 5$. Thus, $(1\ 2)\,(3\ 4) \in \Delta A_n = \Delta^{(2)} S_n \subset S_n$ for each $n \geq 4$. 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 that $\Delta A_n = A_n$ for each $n \geq 5$.

□

Corollary 2.1.11. *A_n is not solvable when $n \geq 5$.*

Aside. We have that $A_5 \cong {\mathrm{SL}_2(\mathbb{Z}/5)}/{(\pm\mathbb{I})}$.

Indeed, by inspection, there are exactly six lines in the vector space $(\mathbb{Z}/5)^2$. Enumerate the bases for these as follows.

$$\underbrace{\begin{bmatrix}1\\1\end{bmatrix}}_{\ell_1} \quad \underbrace{\begin{bmatrix}1\\2\end{bmatrix}}_{\ell_2} \quad \underbrace{\begin{bmatrix}1\\3\end{bmatrix}}_{\ell_3} \quad \underbrace{\begin{bmatrix}1\\4\end{bmatrix}}_{\ell_4} \quad \underbrace{\begin{bmatrix}0\\1\end{bmatrix}}_{\ell_5} \quad \underbrace{\begin{bmatrix}1\\0\end{bmatrix}}_{\ell_6}.$$

Let $L = \{\ell_1, \ldots, \ell_6\}$. Define the group action $\theta : \mathrm{SL}_2(\mathbb{Z}/5) \to \mathrm{Aut}(L) \cong S_6$ by

$$M \cdot \{n\ell_i : n \in \mathbb{Z}/5\} = \{nM\ell_i : n \in \mathbb{Z}/5\}.$$

It's clear that $(\pm\mathbb{I}) \subset \ker\theta$. By the universal property of the natural projection, there is some unique homomorphism $\phi : {\mathrm{SL}_2(\mathbb{Z}/5)}/{(\pm\mathbb{I})} \to S_6$ such that

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}/5) & \xrightarrow{\theta} & \mathrm{Aut}(L) \\ {\scriptstyle\pi}\downarrow & \nearrow_{\phi} & \\ {\mathrm{SL}_2(\mathbb{Z}/5)}/{(\pm\mathbb{I})} & & \end{array}$$

commutes. Let $X = \begin{bmatrix}0 & 4\\ 1 & 0\end{bmatrix}$ and $Y = \begin{bmatrix}0 & 4\\ 1 & 4\end{bmatrix}$. Then a few straightforward computations show that

$$|\phi(\pi(X))| = 2$$
$$|\phi(\pi(Y))| = 3$$
$$|\phi(\pi(XY))| = 5.$$

It is a fact of elementary group theory that

$$A_5 = \left\langle x, y \mid x^2 = y^3 = (xy)^5 = e \right\rangle.$$

From this we see that the restriction $\phi\restriction_{\langle\pi(X),\pi(Y)\rangle} : \langle\pi(X), \pi(Y)\rangle \to A_5$ is a surjective homomorphism. Since ${\mathrm{SL}_2(\mathbb{Z}/5)}/{(\pm\mathbb{I})}$ has order 60, it follows that

$${\mathrm{SL}_2(\mathbb{Z}/5)}/{(\pm\mathbb{I})} = \langle\pi(X), \pi(Y)\rangle \cong A_5,$$

as desired.

2.2 Lecture 6

Remark 2.2.1. In Galois theory, one finds that a polynomial $f(x)$ over $\mathbb{Q}$ is solvable in radicals if and only if the group $\mathrm{Gal}(f)$ is solvable.

Note 2.2.2. In the setting of finite groups, we can add information to our chain of containments in Note 2.1.3 as follows.

(i) Cyclic $\subsetneq$ Abelian $\subsetneq$ Nilpotent $\subsetneq$ Solvable.

(ii) Cyclic $\subsetneq$ **Abelian** $\subsetneq$ Polycyclic $=$ Solvable.

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

Moreover, if the space X has an interesting underlying geometry, then the possibilities of $\pi_1(X)$ belonging to one of the classes of groups listed in Note 2.1.3 are constrained. For example, a compact complex submanifold of $\mathbb{C}P^n$ is known as a Kähler manifold. It is known that any finite group is realizable as $\pi_1(X)$ for some Kähler manifold X.

Definition 2.2.3. 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.

Theorem 2.2.4 (Arapura-Nuri (2005)). *For all groups of the form $\pi_1(X)$ with X a Kähler manifold, we have the following chains of containments.*

$$\begin{aligned} &v.\ Cyclic \subsetneq v.\ Abelian \subsetneq v.\ Nilpotent = v.\ Solvable. \\ &v.\ Cyclic \subsetneq v.\ Abelian \subsetneq v.\ Polycyclic = v.\ Solvable. \end{aligned}$$

Example 2.2.5. If $|G| = p^2$ with p prime, then G is abelian.

Proof. Note that G has nontrivial center as a result of the class equation. If $|Z(G)| = p^2$, then $Z(G) = G$, as desired. Suppose that $|Z(G)| = p$.

Claim. *For any group H, if the quotient group ${}^{H}\!/_{Z(H)}$ is cyclic $\langle [a] \rangle$, then H is abelian.*

Proof. Let $f, h \in H$, so that $[f] = [a]^n$ and $[h] = [a]^m$ for some $n, m \in \mathbb{Z}_{\geq 0}$. This means that $f = a^n c_1$ and $h = a^m c_2$ for some $c_1, c_2 \in Z(H)$. Therefore,

$$\begin{aligned} fh &= (a^n c_1)(a^m c_2) \\ &= a^n a^m c_1 c_2 \\ &= a^m a^n c_2 c_1 \\ &= (a^m c_2)(a^n c_1) \\ &= hf. \end{aligned}$$

□

As the group ${}^{G}\!/_{Z(G)}$ has order p, it is cyclic. Thus, G is abelian. □

Exercise 2.2.6. *Suppose, again, that $|G| = p^2$ with p prime. Show that G is isomorphic to either $C_p \times C_p$ or C_{p^2}.*

3 Sylow theorems

Definition 3.0.1. Let G be a group with

- $|G| = p^k m$,
- 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 $|H| = p^k$.

Notation.

1. Let $\mathrm{Syl}_p(G)$ denote the set of p-Sylow subgroups of G.
2. Let both $n_p(G)$ and $\mathrm{syl}_p(G)$ denote $\#\mathrm{Syl}_p(G)$.

Theorem 3.0.2 (Weak Sylow-I). *Every finite group G with $|G| = p^\beta m$ contains a p-Sylow subgroup.*

Proof. Proceed by induction on $|G|$. We can write G as the union of conjugacy classes

$$Z(G) \coprod_{x \notin Z(G)} C(x).$$

We have three cases to consider.

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 $\left|{}^{G}\!/_{H}\right| = p^{\beta-\alpha}\frac{m}{n} < |G|$. Hence there is some p-Sylow subgroup $S \leq {}^{G}\!/_{H}$. Let $S' \coloneqq q^{-1}(S)$, the pullback of S under the natural projection $q : G \twoheadrightarrow {}^{G}\!/_{H}$. Then ${}^{S'}\!/_{H} = S$, which implies that $p^\beta = |S'|$.

Case 3: Assume that $Z(G) = G$. In this case, we can apply Theorem 3.2.1 (proven below) to get an isomorphism of the form

$$G \cong C_{s_1} \times \cdots \times C_{s_k}.$$

By induction, we can take a direct product of p-Sylow subgroups of the C_{s_i}, which must be a p-Sylow subgroup of G. □

We have another proof of Theorem 3.0.2. Let $|G| = p^\beta m$ with $(p, m) = 1$. Let

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

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 $|\Omega_x|\,|\mathrm{Stab}_G(x)| = |G|$, we must have that $p^\beta \mid |\mathrm{Stab}_G(x)|$. Note that $\mathrm{Stab}_G(x)$ acts on A by left translation. As this action is free, each orbit must have cardinality equal to $|\mathrm{Stab}_G(x)|$ and thus be divisible by $p^\beta = |A|$. This implies that A is the only orbit, and thus $|A| = \mathrm{Stab}_G(x)$.

Exercise 3.0.3 (Strong Sylow-I). *Use the fact that every p-group is nilpotent to prove that any finite group contains a p-subgroup of every possible order.*

3.1 Lecture 7

Theorem 3.1.1 (Sylow-II). *Let G have $|G| = p^\beta m$ as before.*

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 that $G/S = \coprod (H\text{-orbits})$, where each H-orbit has cardinality dividing $|H|$. If $\mathcal{O}$ is a nontrivial orbit, then $p \mid |\mathcal{O}|$, so that if every orbit is nontrivial, then $p \mid \left|G/S\right| = m$, a contradiction. Thus, there is some orbit $\mathcal{O} = \{gS\}$. Since $hgS = gS$ for every $h \in H$, we have $g^{-1}Hg \subset S$, i.e., $H \leq gSg^{-1}$. Note that $\left|gSg^{-1}\right| = |S|$.
2. We just have showed that $H \leq gSg^{-1}$ for some $g \in G$. Hence if $|H| = p^\beta$, then $H = gSg^{-1}$.

□

Corollary 3.1.2. *If $n_p(G) = 1$, then the p-Sylow subgroup is normal in G.*

Corollary 3.1.3. *Let $S \in \mathrm{Syl}_p(G)$. Then $N_G(N_G(S)) = N_G(S)$.*

Proof. We know that $N_G(S) \subset N_G(N_G(S))$. 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 any p-Sylow subgroup H of $N_G(N_G(S))$. If $h \in H$, then $|h| = p^K$ for some $K \geq 0$. Consider $\bar{h} \in N_G(N_G(S))/N_G(S)$, so that $\left|\bar{h}\right|$ 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, $\left|\bar{h}\right| = 1$, 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 3.1.4. *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 this action has a fixed point other than eH.*

2. *Show that* $H < N_G(H)$.

3. *Show that there is some* $\tilde{H} \leq G$ *such that* $\left|\tilde{H}\right| = p^{\alpha+1}$ *and* $H \leq \tilde{H} \leq G$.

Theorem 3.1.5 (Sylow-III). *Suppose that* $|G| = p^\beta m$ *as before.*

(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, so that $n_p(G) \mid |G|$ by the orbit-stabilizer theorem. But (2) shows 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 $\mathrm{Syl}_p(G)$. Note that if $T \in \mathrm{Syl}_p(G)$, then $\mathrm{Stab}_T(G) = N_G(T)$. Now restrict the action to a chosen p-Sylow subgroup S. We have that

$$\mathrm{Syl}_p(G) = \coprod (\text{fixed points}) \sqcup \coprod (\text{nontrivial } S\text{-orbits}).$$

This implies that if there is exactly one fixed point (namely S), then

$$n_p(G) \equiv 1 \mod p.$$

To this end, suppose that H is a fixed point. Then both H and S are p-Sylow subgroups of $N_G(H)$ since $|N_G(H)| \mid |G|$. Thus, they are conjugate. Hence $H = S$.

□

Note 3.1.6. Let $S \in \mathrm{Syl}_p(G)$. The number of p-Sylow subgroups of G is precisely $[G : N_G(S)]$.

Corollary 3.1.7. *If* $|G| = pq$ *with* p *and* q *primes such that* $p < q$ *and* $q \not\equiv 1 \mod p$, *then* $G \cong C_{pq}$.

Proof. It suffices to show that $n_p(G) = n_q(G) = 1$ for in this case G is isomorphic to the direct product its p-Sylow subgroup and its q-Sylow subgroup. Note that $n_q(G) \mid p$ and $n_q(G) \equiv 1 \mod q$. Hence $n_q(G) = 1 + qk$ for some $k \in \mathbb{Z}_{\geq 0}$. But $n_q(G) \leq p < q$, so that $k = 0$. This proves that $n_q(G) = 1$.

Likewise, we have that $n_p(G) \mid q$ and $n_p(G) \equiv 1 \mod p$. Since $q \not\equiv 1 \mod p$ by assumption, it follows that $n_p(G) = 1$ as well. □

Example 3.1.8. Every group G of order 45 is abelian.

Proof. We have that $|G| = 3^2 5$. Thus, $n_3(G) \in \{1, 5\}$ with $n_3(G) \equiv 1 \mod 3$. This implies that $n_3(G) = 1$. Further, $n_5(G) \in \{1, 3, 9\}$ with $n_5(G) \equiv 1 \mod 5$. This implies that $n_5(G) = 1$. Hence there are two normal subgroups $F, H \leq G$ such that $|F| = 9$ and $|H| = 5$. But $H \cap F$ must be trivial, and thus $G \cong H \times F$. This means that $G \cong C_5 \times F$. But recall that any group of order 9 is cyclic or isomorphic to $C_3 \times C_3$. Hence F is abelian, and so is G.

Alternatively, we can define an isomorphism $\psi : H \times F \to G$ by $(h, f) \mapsto hf$. Indeed, as both H and F are normal in G, they commute with each other, making ψ a homomorphism. As $|FH| = 45$, we see that $FH = G$, so that ψ is surjective. If $hf = e_G$, then $h = f^{-1}$, in which case $h \in F \cap H$. Such an element must be trivial, which implies that $\ker \psi$ is trivial, i.e., that ψ is injective. Thus, ψ is an isomorphism. □

3.2 Lecture 8

Theorem 3.2.1 (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 is a positive integer 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. *N is free, i.e., $N \cong \mathbb{Z}^n$.*

Proof. Proceed by induction on $n \in \mathbb{Z}_{\geq 1}$. 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 our claim holds for any subgroup $M \leq \mathbb{Z}^m$ of finite index where $m < n$. Let $M = \langle e_1, \ldots, e_{n-1} \rangle \cap N$. 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 consider the surjective group homomorphism $p : \mathbb{Z}^n \to \mathbb{Z}$ defined 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. Let $f_n = (0, \ldots, 0, k) \in \mathbb{Z}^n$, 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 $0 = a_1 f_1 + \cdots + a_n f_n$, we see that $0 = p(0) = a_n k$. 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. It follows that $\det(C) \neq 0$.

Claim. *By elementary row and column operations, C is equivalent to a diagonal matrix $(u_1, \ldots, u_n)$ such that $u_i \in \mathbb{Z}_{>0}$ and $u_i \mid u_{i+1}$ for each $i = 1, \ldots, n-1$.*

Proof omitted. □

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 have that $G \cong \mathbb{Z}^n / N \cong \mathbb{Z}/u_1 \times \cdots \times \mathbb{Z}/u_n$. □

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 unique integer $r \geq 0$ (known as the *Betti number* of G).

Corollary 3.2.2. *Weak Sylow-I (Theorem 3.0.2).*

4 Composition series

4.1 Lecture 9

Definition 4.1.1. A group G is *simple* if it has no nontrivial proper normal subgroup.

Example 4.1.2.

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

Definition 4.1.3. A *composition series for* G is a subnormal series $G = G_0 > G_1 > \cdots > G_k = \{e\}$ where each quotient group G_i/G_{i+1} is simple.

Example 4.1.4.

1. Any finite group G has a composition series.

   Proof. By Zorn's lemma, G contains a maximal normal subgroup G_1. Likewise, G_1 contains a maximal normal subgroup G_2, and so on. Note that G_i/G_{i+1} has no nontrivial normal subgroup H, for otherwise $\pi^{-1}(H)$ is a nontrivial normal subgroup in G_i such that $\pi^{-1}(H) \supsetneq G_{i+1}$, contrary to our choice of G_{i+1}. Therefore,

   $$G > G_1 > G_2 > \cdots > \{e\}$$

   is a composition series for G. □

2. 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 subgroups H. Note that S satisfies the hypotheses of Zorn's lemma, thereby yielding 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.

3. $\mathbb{Z}$ has no composition series, since no nontrivial subgroup of $\mathbb{Z}$ is simple.

4. Every p-group has a composition series where each factor is $\mathbb{Z}/p$.

5. Let $|G| = pq$ with p and q distinct primes. Let G_1 be the unique q-Sylow subgroup of G. Then $G > G_1 > \{e\}$ is a composition series for G.

Proposition 4.1.5. *A_5 is simple.*

Proof. Suppose that $N \trianglelefteq A_5$ 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.

Claim. *If $\sigma \in A_n \subset S_n$ and in the decomposition of σ we have either*

(i) two even cycles of equal length or

(ii) an odd cycle,

then the conjugacy class of σ in A_n is the same as its conjugacy class in S_n.

Proof. If condition (i) holds, then $\sigma = (i_1 \cdots i_r)(j_1 \cdots j_r) \cdots$ for some odd r. In this case, construct the odd permutation $\tau \equiv (i_1\ j_1)(i_2\ j_2) \cdots (i_r\ j_r)$. Note that

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

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 that 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, which completes our proof. □

We have three cases to consider. First, if $p = 2$, then σ is the product of two independent transpositions. By our claim, it follows that $N = A_5$. Second, if $p = 3$, then N contains all 3-cycles because any two 3-cycles are conjugate in A_5. Finally, suppose that $p = 5$. Let $\sigma = (i_1 \cdots i_5)$ and consider

$$\tau \coloneqq (i_1\ i_2\ i_3)\,\sigma\,(i_1\ i_2\ i_3)^{-1} = (i_2\ i_3\ i_1\ i_4\ i_5).$$

Then $\tau\sigma^{-1} = (i_1\ i_2\ i_3) \in N$, which implies that N contains all 3-cycles. In conclusion, N cannot be proper. □

Why did we need that whole claim?

Now, if $|G| = pq$ with p and q distinct primes, then we have a sequence

$$\mathbb{Z}/q \overset{i}{\hookrightarrow} F \overset{\pi}{\twoheadrightarrow} \mathbb{Z}/p$$

of group maps such that $\mathrm{im}(i) = \ker \pi$.

Question. What data do we need to reconstruct G from $\mathbb{Z}/p$ and $\mathbb{Z}/q$?

Definition 4.1.6. A sequence of groups with homomorphisms $S \xrightarrow{\phi} G \xrightarrow{\pi} Q$ is called a *short exact sequence* if

(i) ϕ is injective,

(ii) π is surjective, and

(iii) $\ker \pi = \operatorname{im} \phi$.

In this case, we say that G is an *extension of Q by S*. If $\phi(S) \leq Z(G)$, then we say this is a *central extension*.

In general, a sequence $G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_k} G_k$ is called *exact at the term G_i* if

$$\ker \phi_i = \operatorname{im}(\phi_{i-1}) \tag{$*$}$$

and is called *exact* if it is exact at all terms for which ($*$) makes sense.

If G has subnormal series $G = G_0 > G_1 > \cdots > G_k = \{e\}$, then for each $0 \leq i \leq k-1$, 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.

(I) understanding all possible simple groups and

(II) understanding ways of extending simple groups by a subgroup.

Definition 4.1.7. A group extension $1 \to H \xrightarrow{i} G \xrightarrow{q} K \to 1$ is called *split* if we can find a homomorphism $s : K \to G$ such that $q \circ s = \mathrm{id}_K$. In symbols,

$$1 \longrightarrow H \xrightarrow{i} G \underset{s}{\overset{q}{\rightleftarrows}} K \longrightarrow 1.$$

Example 4.1.8. Let $|G| = pq$. Then $1 \to {}^{Z}\!/_{q} \to G \to {}^{Z}\!/_{p}$ is split.

If

$$1 \longrightarrow H \xrightarrow{i} G \underset{s}{\overset{q}{\rightleftarrows}} K \longrightarrow 1.$$

is a split exact sequence, then we say that 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 $S \coloneqq s(K) \cong K$. To see that $G = HS$, notice that if $g \in G$, then $q(g) \in K$ and $x \coloneqq s(q(g)) = g \in S$ with $q(gx^{-1}) = q(g)q(x)^{-1} = e$. In this case, $gx^{-1} \in \ker q = H$.

4.2 Lecture 10

Let G be a group and $\{G_1, \ldots, G_k\}$ be a collection of subgroups. 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

(i) Each $g \in G$ can be written uniquely as $g_1 g_2 \cdots g_k$, i..e, ϕ is bijective.

(ii) We have $xy = yx$ for any $x \in G_i$ and $y \in G_j$, i.e., ϕ is a morphism.

Exercise 4.2.1.

1. *Check that condition (i) is equivalent to the condition that* $G_1 \cdots G_k = G$ *and* $G_i \cap \Big(G_1 \cdots \widehat{G}_i \cdots G_k\Big) = \{e\}$.

2. *Check that condition (ii) is equivalent to the condition that* $G_i \trianglelefteq G$ *for each* i.

Example 4.2.2.

1. $\mathbb{C}^* \cong S^1 \times \mathbb{R}$ via the mapping $z \mapsto \big(e^{i\theta}, r\big)$. 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 $A \mapsto \left(\frac{A}{\sqrt[n]{\det A}}, \det A\right)$. We have a short exact sequence

$$1 \longrightarrow \mathrm{SL}_n \xrightarrow{\ i\ } \mathrm{GL}_n^+(\mathbb{R}) \underset{s}{\overset{\det}{\rightleftarrows}} \mathbb{R}_{>0} \longrightarrow 1,$$

   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 denote the group of diagonal matrices over k. Then $\mathsf{Diag}_n \cong \underbrace{k^* \times \cdots \times k^*}_{n \text{ copies}}$.

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 $K \neq H$, contrary to the fact that $\mathbb{Z}/p^2$ has 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 $\mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b$. Yet, $S_3 \ncong \mathbb{Z}/2 \times \mathbb{Z}/3$, as the subgroup $s\left(\mathbb{Z}/2\right)$ in

$$1 \longrightarrow \mathbb{Z}/3 \xrightarrow{\ i\ } S_3(\mathbb{R}) \underset{s}{\overset{\mathrm{sgn}}{\rightleftarrows}} \mathbb{Z}/2 \longrightarrow 1,$$

   is *not* normal.

Definition 4.2.3. Suppose that $H, K \leq G$ with H normal and $G = HK$. If $H \cap K$ is trivial, we call G the *semidirect product of H and K*, denoted by $H \rtimes K$.

Note 4.2.4. Recall that if $H \trianglelefteq G$ and $K \leq G$, then HK is a subgroup of G and $HK = KH$.

Suppose that $G = HK$ with $H \trianglelefteq G$ and $H \cap K = \{e\}$. Let $\alpha : K \to \mathrm{Aut}_{\mathbf{Grp}}(H)$ be the inner automorphism of H, which depends on the group law $*_G$. Then $*_G$ can be recovered from $*_H$, $*_K$, and α. Indeed, let $g_1, g_2 \in G$. Then decompose $g_1 = h_1 k_1$ and $g_2 = h_2 k_2$ uniquely, so that

$$g_1 g_1 = \left(h_1 \alpha_{k_1}\left(h_2\right)\right) k_1 k_2.$$

We are ready to state an equivalent formulation of the notion *semidirect product*. To this end, 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

$$\left(h_1, k_1\right)\left(h_2, k_2\right) \equiv \left(h_1 \alpha_{k_1}\left(h_2\right), k_1 k_2\right).$$

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. Hence

$$1 \longrightarrow H \xrightarrow{i_H} K \ltimes_\alpha H \underset{i_K}{\overset{p_K}{\rightleftarrows}} K \longrightarrow 1$$

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

Conversely, if

$$1 \longrightarrow H \xrightarrow{i} G \underset{s}{\overset{q}{\rightleftarrows}} K \longrightarrow 1$$

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 4.2.5. Let

$$1 \longrightarrow H \xrightarrow{i_1} G_1 \xrightarrow{q_1} K \longrightarrow 1$$

and

$$1 \longrightarrow H \xrightarrow{i_2} G_2 \xrightarrow{q_2} K \longrightarrow 1$$

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

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \longrightarrow & G_1 & \longrightarrow & K & \longrightarrow & 1 \\ & & \Big\downarrow{\scriptstyle \mathrm{id}} & & \Big\downarrow{\scriptstyle \phi} & & \Big\downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \longrightarrow & G_2 & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes.

Example 4.2.6.

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

Exercise 4.2.7. *Recall the Heisenberg group $H(V, W)$. Show that the exact sequence*

$$0 \to \mathbb{R} \to H(V, W) \to V \to 0$$

cannot be split.

4.3 Lecture 11

There is no general theory for classifying all group extensions. There is one in the setting of abelian groups, but it relies on spectral sequences.

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. 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 4.3.1. 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 4.3.2. Any scenario can happen.

1. Every finite group has both ACC and DCC.
2. $\mathbb{Z}$ has ACC but not DCC. On the one hand, if $a\mathbb{Z} \leq b\mathbb{Z}$, then $b \mid a$. But any positive integer has only finitely many divisors. Hence $\mathbb{Z}$ has ACC. On the other hand, we have a descending normal series
$$\mathbb{Z} > 2\mathbb{Z} > 4\mathbb{Z} > \cdots > 2^n\mathbb{Z} > \cdots > \{0\},$$
which never stabilizes.
3. Given p prime, let $G_p \coloneqq \left\{ z \in \mathbb{C}^* : z^{p^k} = 1 \text{ for some } k \right\}$. This has DCC but not ACC. Why?
4. $\mathbb{Q}$ has neither ACC nor DCC.

Exercise 4.3.3. *Prove the following assertions.*

1. *Given a short exact sequence*
$$1 \longrightarrow H \xrightarrow{a} G \xrightarrow{b} K \longrightarrow 1\ ,$$
if both H and K have ACC (resp. DCC), then G has ACC (resp. DCC).

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

Proof.

1. For simplicity, let us consider just the case where H and K have DCC. Suppose that

$$G \geq J_1 \geq J_2 \geq J_3 \geq \cdots \geq \{e\}$$

is any descending normal series. We must show that it stabilizes.By hypothesis, the descending normal series $(b(J_i))_{i\geq 1}$ and $\left(a^{-1}(J_i)\right)_{i\geq 1}$ both stabilize at, say, $k \in \mathbb{N}$. Suppose that $i \geq k$ and let $x \in J_i$. Then $b(x) \in b(J_i) = b(J_{i+1})$, and thus there is some $y \in J_{i+1}$ such that $b(x) = b(y)$. From this we deduce that $x - y \in \ker b = \operatorname{im} a$, so that there is some $z \in H$ such that $x - y = a(z)$. Since $x - y \in J_i$, it follows that $z \in a^{-1}(J_i) = a^{-1}(J_{i+1})$. Hence $x - y \in J_{i+1}$ as a is injective. This implies that $x = (x - y) + y \in J_{i+1}$, so that $J_i = J_{i+1}$, thereby completing our proof.

2. Both H and K are normal in G, and any normal subgroup of either one is normal in G. It follows automatically that if either H or K lacks ACC (resp. DCC), then so does G.

□

Proposition 4.3.4. *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, toward a contradiction, that G has DCC and $G \notin D$. 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 4.3.5 (Krull-Schmidt). *Suppose that 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 $\operatorname{End}(G) = \{\phi : G \to G \mid \phi \text{ is a homomorphism}\}$. This is a monoid under composition.

Definition 4.3.6. An endomorphism ϕ of G is *normal* if $\phi \circ \mathrm{conj}_x = \mathrm{conj}_x \circ \phi$ for any $x \in G$.

Lemma 4.3.7.

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 subset $\{a_1, \ldots, a_r\} \subset \{1, \ldots, k\}$, we have that $\sum_{j=1}^{r} f_{a_j} p_{a_j}$ is normal.*

Proposition 4.3.8. *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 a nontrivial $g_1 \in \ker \phi$. Suppose, toward a 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 this process to get a chain

$$\ker \phi < \ker \phi^2 < \cdots,$$

which fails to stabilize, a contradiction. □

Definition 4.3.9. An endomorphism ϕ is *nilpotent* if $\phi^n = (g \mapsto e)$ for some $n \geq 1$.

Lemma 4.3.10 (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 $H_n = \mathrm{im}\, \phi^n$. This yields a 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, $\phi(K) = \phi(K_a) = \{\phi(x) : x \in \ker \phi^a\}$, and thys $\phi^a\phi(x) = \phi(\phi^a(x)) = e$. Hence both H and K are stable under ϕ. Note that we've shown $\phi \restriction_H$ is surjective. By Proposition 4.3.4, $\phi \restriction_H$ is an isomorphism provided that H has ACC and DCC. But we can show that $G = K \times H$ as follows.

(a) Let $x \in K \cap H$. Then

$$\begin{aligned} x \in H = H_a = \phi^a(G) &\implies \phi^a(G) = x \text{ for some } g \\ &\implies \phi^a(\phi^a(g)) = \phi^a(x) = 0 \\ &\implies g \in K_{2a} = K_a = K \\ &\implies \phi^a(g) = e \\ &\implies x = e. \end{aligned}$$

(b) Let $g \in G$. Then

$$\begin{aligned} \phi^a(g) \in H = H_a = H_{2a} &\implies \phi^a(g) = \phi^{2a}(x) \text{ for some } x \in G \\ &\implies \phi^a(g\phi^a(x^{-1})) = e \\ &\implies g\phi^a(x) \\ &\implies g\phi^a(x^{-1}) \in K_a = K \\ &\implies g = kh \text{ for some } k \in K \text{ and } h \in H. \end{aligned}$$

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

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

4.4 Lecture 12

Corollary 4.4.1. *Suppose that G is indecomposable and has ACC + DCC. Then any normal map $\phi : G \to G$ is either nilpotent or an automorphism.*

Lemma 4.4.2. *Suppose that G is indecomposable and has ACC + DCC and that ϕ and ψ are endomorphisms such that $\phi + \psi$ is an endomorphism. If ϕ and ψ are nilpotent, so is $\phi + \psi$.*

Proof. Thanks to Corollary 4.4.1, as long as $\phi + \psi$ 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 the equation $U(x)V(x) = x$ 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 $\mathrm{id}_G = (U+V)^n = 0$. It follows that G is trivial, and this contradicts that G is indecomposable. □

We finally return to our proof of Krull-Schmidt. Suppose that $r = 1$. 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

$$\mathrm{id}_{A_1} = p_1 \circ \mathrm{id}_G \circ f_1 = p_1 \circ \left(\sum_{j=1}^{t} g_j \circ g_j \right) \circ f_1 = \sum_{j=1}^{t} (p_1 \circ g_j \circ q_j \circ f_1).$$

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 Lemma 4.4.2 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 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 that $(\gamma \circ p_1 \circ g_1) \circ (q_1 \circ f_1) = \mathrm{id}_{A_1}$, 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 $B_1 \cong A_1$.

Consider $\theta \coloneqq (q_1 f_1)(\gamma p_1 g_1) : B_1 \to B_1$, which is normal. We want to check that this is the identity map. It's easy to check that $\theta^2 = \theta$. 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

$$\mathrm{id}_{A_1}^2 = (\gamma p_1 g_1)\,(q_1 f_1)\,(\gamma p_1 g_1)\,(q_1 f_1) = (\gamma p_1 g_1)\,\theta (q_1 f_1) = 0,$$

meaning $A_1 = \{e\}$, a contradiction.

Even after reindexing?

Now, $\ker q_1 = B_2 \times \cdots \times B_t$, and $\ker(q_1 \circ f_1) = \{e\}$. 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

$$b_1 b_2 \cdots b_t \mapsto \gamma f_1 p_1(b_1) b_2 b_3 \cdots b_t,$$

whose output is precisely

$$(q_1 f_1)^{-1}(b_1) b_2 \cdots b_t = f_1 (q_1 f_1)^{-1} q_1 + g_2 q_2 + \cdots + g_t q_t.$$

Then ψ 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 means that $H = G$.

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 preceding argument to see that $s = t$ and that $A_i \cong B_i$ up to reindexing. □

Corollary 4.4.3. *Suppose that G is a finite abelian group, 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.*

Suppose that G is finite and that

$$G = F^0G \geq F^1G \geq \cdots \geq F^sG = \{e\}$$
$$G = T^0G \geq T^1G \geq \cdots \geq T^tG = \{e\}$$

are two composition series for G. Consider the *graded groups*

$$\mathsf{gr}_F(G) \equiv \prod {F^i}/{F^{i+1}}$$
$$\mathsf{gr}_T(G) \equiv \prod {T^i}/{T^{i+1}}.$$

Corollary 4.4.4. *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 4.4.5. If $F^\bullet G$ and $T^\bullet G$ are two composition series for G, then they are *equivalent* or *isomorphic* if $\mathsf{gr}_F(G) \cong \mathsf{gr}_T(G)$.

4.5 Lecture 13

Definition 4.5.1. Let G be a group. A *filtration $F^\bullet G$ on G* is a subnormal series of the form

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

Note 4.5.2. Suppose that $F^\bullet G$ is a filtration on G.

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

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

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

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

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

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

Thanks to Note 4.5.2, 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 4.5.3 (Zassenhaus or butterfly). *Suppose that G is a group with $A \trianglelefteq \widetilde{A} \leq G \geq \widetilde{B} \trianglerighteq B$. Then we have a group isomorphism*

$$A \cdot \left(\widetilde{A} \cap \widetilde{B}\right) \Big/ A \cdot \left(\widetilde{A} \cap B\right) \cong B \cdot \left(\widetilde{A} \cap \widetilde{B}\right) \Big/ B \cdot (A \cap \widetilde{B}).$$

Proof. We know that

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

Then

$$D \coloneqq \left(A \cap \widetilde{B}\right) \cdot \left(\widetilde{A} \cap B\right) \cong \left(\widetilde{A} \cap B\right) \cdot \left(A \cap \widetilde{B}\right)$$

is normal in $\widetilde{A} \cap \widetilde{B}$. Let $x \in B \cdot \left(\widetilde{A} \cap \widetilde{B}\right)$ and write $x = bc$. Take $cD \in {\widetilde{A} \cap \widetilde{B}}\big/{D}$. 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 $c_2c_1^{-1} \in B \cap \widetilde{A} \cap \widetilde{B} = \widetilde{A} \cap B \leq D$, 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

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

Therefore, ${B \cdot \left(\widetilde{A} \cap \widetilde{B}\right)}\big/{B \cdot \left(A \cap \widetilde{B}\right)} \cong {\widetilde{A} \cap \widetilde{B}}\big/{D}$.

The other isomorphism with ${\widetilde{A} \cap \widetilde{B}}\big/{D}$ is obtained by swapping $A \longleftrightarrow B$ and $\widetilde{A} \longleftrightarrow \widetilde{B}$. □

Corollary 4.5.4. $\mathsf{gr}_T^j \mathsf{gr}_F^i G \cong \mathsf{gr}_F^i \mathsf{gr}_T^j G$.

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

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

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

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

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

Definition 4.5.6. We say that $\left\{R^i G\right\}_{i=1}^t$ is a *refinement* of $\left\{F^i G\right\}_{i=1}^s$ if there is a non-decreasing map $j : [s] \to [t]$ such that $F^a G = R^{j(a)} G$ for every $a \in [s]$.

Theorem 4.5.7 (Schreier refinement). *Suppose that $\left\{F^i G\right\}_{i=0}^s$ and $\left\{T^j G\right\}_{j=0}^t$ 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 that $F^\bullet$ and $T^\bullet$ are non-repetitious. Let $\widetilde{F}_{i-1}^{(j)} = \left(F^{i-1} \cap T^j\right) \cdot F^i$. 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, $\widetilde{T}_{j-1}^{(i)} \coloneqq (T^{j-1} \cap F^i) \cdot T^j$ 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 4.5.8 (Jordan-Holder). *Any two composition series for 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. This completes our proof thanks to Theorem 4.5.7. □

5 Group cohomology

5.1 Lectures 14 and 15

Suppose that

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

is an extension. Since q is surjective, we can lift any $x \in K$ to some $\tilde{x} \in G$ via q^{-1}. 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 induce 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

$$\begin{aligned} q(\tilde{x}) = x = q(\tilde{\tilde{x}}) &\implies q(\tilde{x}^{-1}\tilde{\tilde{x}}) = e \\ &\implies \tilde{\tilde{x}} = \tilde{x}h \text{ for some } h \in H \\ &\implies \mathrm{conj}_{\tilde{\tilde{x}}} \restriction_H = \mathrm{conj}_{\tilde{x}} \restriction_H \circ \mathrm{conj}_h \\ &\implies \mathrm{conj}_{\tilde{\tilde{x}}} \restriction_H \sim \mathrm{conj}_{\tilde{x}} \restriction_H . \end{aligned}$$

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. As $\mathrm{conj}_{\tilde{x}\tilde{y}} \restriction_H = \mathrm{conj}_{\tilde{x}} \restriction_H \circ \mathrm{conj}_{\tilde{y}} \restriction_H$, it follows that $\alpha^\xi(xy) = \alpha^\xi(x)\alpha^\xi(y)$, as desired.

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 $x \mapsto \mathrm{conj}_{s(x)} \restriction_H$. Note that $\alpha^{\xi,s}(x) \cdot \mathrm{Inn}(H) = \alpha^\xi(x)$. This implies that

$$\begin{array}{ccc} K & \xrightarrow{\alpha^{\xi,s}} & \mathrm{Aut}(H) \\ & \searrow^{\alpha^\xi} & \downarrow \pi \\ & & \mathrm{Out}(H) \end{array}$$

commutes.

Given a homomorphism $\alpha : K \to \mathrm{Out}(H)$, we can now reduce the problem of classifying all extensions of K by H to the problem of classifying all extensions ξ such that $\alpha^\xi = \alpha$.

Notation. Let $\mathrm{Ext}(K, (H, \alpha))$ denote the set of all isomorphism classes of extensions of K by H with invariant α.

Example 5.1.1.

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 $S_3 \leq \mathrm{Aut}(S_3)$, and thus $\mathrm{Aut}(S_3) = S_3$.

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

Is ϕ^f well-defined?

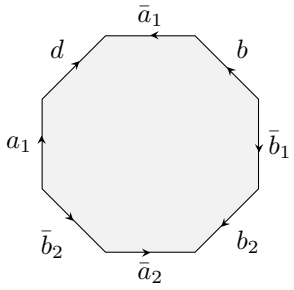
Let $f : G \to H$ be a surjective map and $\phi \in \mathrm{Aut}(G)$ such that $\phi(\ker f) = \ker f$. This induces an automorphism $\phi^f : H \to H$ given by $h = f(g) \mapsto f(\phi(g))$. Note that if $x \in G$, then $\mathrm{conj}_x : G \to G$ preserves any normal subgroup. Thus, we get a map $(\mathrm{conj}_x)^f : H \to H$ 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 does this induce $(-)^f$?

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 5.1.2. Let Σ_g denote the orientable surface of genus g. We can draw Σ_g as an oriented $4g$-gon with pairs of sides identified as follows.



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

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

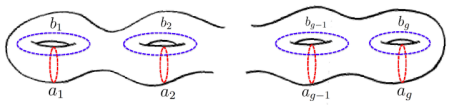


Figure 1: copied from http://inspirehep.net/record/1352145/plots

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

$$\begin{array}{ccccc} \mathrm{Out}(\pi_1(\Sigma_g)) & \xrightarrow{(-)^{\mathrm{ab}}} & \mathrm{Aut}(H_1(\Sigma_g)) & \xrightarrow{\cong} & \mathrm{GL}_{2g}(\mathbb{Z}) \\ & \overset{G}{\searrow} & & & \downarrow \det \\ & & & & \{\pm 1\} \end{array}.$$

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

Remark 5.1.3. For the remainder of our classification problem, we assume that the subgroup of G is abelian. Thus, any map $\alpha : K \to \mathrm{Out}(H) \cong \mathrm{Aut}(H)$ is an action.

Definition 5.1.4. A *K-module* is a pair (A, α) where A is an abelian group and $\alpha : K \to \mathrm{Aut}(A)$ is a group map.

Note 5.1.5 (Operations on $\mathrm{Ext}(K,(A,\alpha))$).

(1) Let $\phi : L \to K$ be a group map and

$$1 \to A \xrightarrow{i} G \xrightarrow{q} K \to 1$$

be an extension. We can use ϕ to produce an extension of L by A. Consider the *fiber product* $G \times_K L \equiv \{(g,l) \in G \times L : q(g) = \phi(l)\}$, 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 provides us with a commutative diagram

$$\begin{array}{ccccccccc} \xi: & 1 & \longrightarrow & A & \xrightarrow{i} & G & \xrightarrow{q} & K & \longrightarrow & 1 \\ & & & \| & & \uparrow & & \uparrow{\scriptstyle \phi} & & \\ \phi^*\xi: & 1 & \longrightarrow & A & \longrightarrow & G \times_K L & \xrightarrow{p} & L & \longrightarrow & 1 \end{array} . \tag{A}$$

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 in (A). 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 a group map $i \times \psi : A \to G \ltimes_{\beta\circ q} B$ given by $a \mapsto (a, \psi(a))$.

Claim. *The map $i \times \psi$ is injective, and*

$$\overbrace{\mathrm{im}(i \times \psi)}^{A} \trianglelefteq G \ltimes_{\beta\circ q} B.$$

Moreover, $A \leq \ker(G \ltimes_{\beta\circ q} B \twoheadrightarrow K)$.

Proof. Injectivity follows from the fact that i is injective. Recall that the group law on $G \ltimes_{\beta\circ q} B$ is given by

$$(g_1,b_1)\,(g_2,b_2) = (g_1g_2, b_1(\beta \circ q(g_1)(b_2)))\,.$$

To see that A is normal, we compute

$$\begin{aligned}
(g,b)(a,\psi(a))(g,b)^{-1} &= (g,b)\,(a,\psi(a))(g^{-1},\beta\circ q(g^{-1})(b^{-1})) \\
&= (ga,b\beta\circ q(g)(\psi(a)))\,(g^{-1},\beta\circ q(g^{-1})(b^{-1})) \\
&= \left(gag^{-1},b\beta\circ q(g)(\psi(a))\beta\circ q(ga)\beta\circ q(g^{-1})(b^{-1})\right) \\
&= \left(gag^{-1},b\beta\circ q(g)(\psi(a))\beta(q(g)\underbrace{q(a)}_{1}q(g^{-1}))(b^{-1})\right) \\
&= \left(gag^{-1},b\beta\circ q(g)(\psi(a))b^{-1}\right) \\
&= \left(gag^{-1},\beta\circ q(g)(\psi(a))\right) \\
&= \left(gag^{-1},\psi(\alpha\circ q(g)(a))\right) \\
&= (\alpha\circ q(g)(a),\psi(\alpha\circ q(g)(a)))\,,
\end{aligned}$$

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

which belongs to $\mathrm{im}(i\times\psi)$.

Finally, observe that

$$\begin{aligned}
\ker(G\ltimes_{\beta\circ q}B\twoheadrightarrow K) &= \{(g,b) : q(g)=e\} \\
&= \{(g,b) : g\in A\} \\
&\geq A\times\{e\}\cong A.
\end{aligned}$$

□

Now, let $G_{\psi_*\xi}$ denote $G\cup_A B$, which equals ${}^{G\ltimes_{\beta\circ q}B}\!/_{(i\times\psi)(A)}$. We have obtained a commutative diagram.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \longrightarrow & G & \longrightarrow & K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & A\times B & \xrightarrow{i} & G\ltimes_{\beta\circ q}B & \xrightarrow{q} & K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & \underbrace{B}_{A\times B/(i\times\psi)(A)} & \longrightarrow & G_{\psi_*\xi} & \longrightarrow & K & \longrightarrow & 1
\end{array}, \qquad \text{(B)}$$

where $B\cong {}^{A\times B}\!/_{(i\times\psi)(A)}$ via the mapping $b\mapsto[(e,b)]$.

Let ψ_* denote the induced map $G\to G_{\psi_*\xi}$. Define the extension $\psi_*\xi$ as the bottom row of (B).

(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, as is the function $\mathrm{mult} : A\times A\to A$ since A abelian. This is also equivariant for $\alpha\times\alpha$ and α. Therefore, we can form the following commutative diagram.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A\times A & \longrightarrow & G_\xi\times G_\eta & \longrightarrow & K\times K & \longrightarrow & 1 \\
 & & \| & & \uparrow & & \uparrow{\scriptstyle \Delta} & & \\
1 & \longrightarrow & A\times A & \longrightarrow & (G_\xi\times G_\eta)\times_{K\times K} K & \longrightarrow & K & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{mult}} & & \downarrow & & \| & & \\
1 & \longrightarrow & A & \longrightarrow & ((G_\xi\times G_\eta)\times_{K\times K} K)\cup_{A\times A} A & \longrightarrow & K & \longrightarrow & 1
\end{array} \tag{C}$$

Define $\xi+\eta$ as the bottom row of (C).

Exercise 5.1.6. *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 5.1.7.

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.*

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 $\operatorname{im} f\subset A$, giving us $f: K\times K\to A$.

Definition 5.1.8. 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.

5.2 Lecture 16

Lemma 5.2.1. *Let* ξ *be as in* (A) *with* s *and hence* f *normalized. Then the data* $(K,(A,\alpha),f)$ *determine* ξ *up to isomorphism.*

Proof. Let G_f be the group with underlying set $K\times A$ and group law given by

$$(x,a)\,(y,b)\equiv\left(xy, a\alpha_x(b)f(x,y)\right).$$

Then the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \xrightarrow{i_f} & G_f & \xrightarrow{q_f} & K & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle s\times i} & & \downarrow & & \\
1 & \longrightarrow & A & \xrightarrow{i} & G & \underset{s}{\overset{q}{\rightleftarrows}} & K & \longrightarrow & 1
\end{array},$$

commutes where $(s\times i)\,(x,a)\equiv s(x)a$. □

Note 5.2.2. In general, given $(K,(A,\alpha))$ and a normalized function $f : K \times K \to A$, 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 5.2.3.

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 $Z^2(K,(A,\alpha)) \coloneqq \big\{f \in C^2 : (*) \text{ holds}\big\}$ the set of *second cocycles of K with coefficients in (A,α)*.

Note 5.2.2 implies that there is a one-to-one correspondence

$$\{(\xi,s) : \xi \in \mathrm{Ext}(K,(A,\alpha)),\ s \text{ a normalized section}\} \longleftrightarrow Z^2(K,(A,\alpha))_0 = Z^2 \cap C_0^2.$$

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

$$\tilde{f}(x,y) = \tilde{s}(x)\tilde{s}(y)\tilde{s}(xy)^{-1} = c(x)s(x)c(y)s(y)(c(xy)s(xy))^{-1},$$

and 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 us a map $\delta : C_0^1 \to Z_0^2$ defined by $c \mapsto \Big((x,y) \overset{\delta_c}{\longmapsto} c(x)\alpha_x(c(y))c(xy)^{-1}\Big)$, known as the *first Hochschild differential of K with coefficients in (A,α)*. We in turn obtain a natural map

How do we know any first normalized cochain can be written in that form?

$$\delta' :\ \mathrm{Ext}(K,(A,\alpha)) \to HH^2(K,(A,\alpha)) \coloneqq {}^{Z_0^2}\!/_{\mathrm{im}\,\delta} \tag{$\star$}$$

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 5.2.4. *Show that δ' is an isomorphism of abelian groups.*

Example 5.2.5. Let us find all extensions of ${}^{\mathbb{Z}}\!/_2 \cong \mathbb{M}_2 \coloneqq \{\pm 1\}$ by $\mathbb{Z}$, i.e., classify all short exact sequences of the form

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

Case 1: $\mathbb{M}_2$ acts trivially on $\mathbb{Z}$.

Then $C_0^2 = \{f : \mathbb{M}_2 \times \mathbb{M}_2 \to \mathbb{Z} \mid f(1,y) = f(x,1) = 0 \text{ for any } x,y \in \mathbb{M}_2\}$. Each $f \in C_0^2$ is thus determined by $f(-1,-1)$, so that $C_0^2 \cong \mathbb{Z}$ via $f \mapsto f(-1,1)$.

Note that $f \in Z_0^2 \iff f(y,z) - f(xy,z) + f(x,yz) - f(x,y) = 0$ for any $x,y,z \in \mathbb{M}_2$. It's easy to check this is always satisfied. Hence $Z_0^2 \cong \mathbb{Z}$ as well.

Moreover, $C_0^1 = \{c : \mathbb{M}_2 \to \mathbb{Z} : c(1) = 0\} \cong \mathbb{Z}$, yielding 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 $\delta_c(x,y) = c(x) + c(y) - c(xy)$, so that $\delta_c(-1,-1) = c(-1) + c(-1) = 2b$. 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 precisely

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

Case 2: 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

$$\begin{aligned} 0 &= \alpha_x(f(-1,-1)) - f(-x,-1) + f(x,1) - f(x,-1) \\ &= \alpha_x(\underbrace{f(-1,-1)}_{a}) - f(-x,-1) - f(x,-1) \\ &= \begin{cases} 0 & x = 1 \\ -2a & x = -1 \end{cases}. \end{aligned}$$

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

6 Categories and functors

6.1 Lecture 17

Definition 6.1.1. 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 partial *composition* 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.

(i) $\operatorname{mor}\mathscr{C} = \coprod_{x,y \in \operatorname{ob}\mathscr{C}} \operatorname{Hom}_{\mathscr{C}}(x,y)$.

(ii) Composition is associative.

(iii) 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 maps $f : x \to y$ and $g : z \to x$.

When $\mathscr{C}$ is small, we see that $(\operatorname{mor}\mathscr{C}, \circ)$ is a partially defined monoid encoding all information about $\mathscr{C}$. We may believe, therefore, that monoid homomorphisms are the correct tools for comparing categories. These, however, are not flexible enough. In particular, an isomorphism of monoids will prove stronger than our chosen notion of equivalence of categories.

Example 6.1.2. The following are examples of categories.

1. **Set**, the category of all sets with functions as morphisms.
2. **Grp**, the category of all groups with group homomorphisms as morphisms.
3. **Ab**, the category of all abelian groups.
4. **Top**, the category of all topological spaces with continuous maps as morphisms.
5. C^k**−Mfld**, the category of all C^k-manifolds with C^k maps as morphisms.
6. $\mathbf{Vect}_k$, the category of all vector spaces over a field k with linear maps as morphisms.
7. The *simplicial category* Δ has all finite ordinals $[n] \coloneqq \{0 < 1 < \cdots < n\}$ as objects and all functions $f : [m] \to [n]$ satisfying $a \leq b \implies f(a) \leq f(b)$ as morphisms.
8. Recall the functor category $\mathbf{sSet} \coloneqq \mathbf{Fun}(\Delta^{\mathrm{op}}, \mathbf{Set})$ of simplicial sets (cf. Definition 6.1.3 below). We can view simplicial sets as books that record the combinatorics of gluing simplices into a topological space.

   Also, recall the *standard n-simplex*

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

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

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

   which is linear over $\mathbb{R}$. We see that $\Delta_f(\Delta^m) \subset \Delta^n$, where $\Delta_f(\Delta^m)$ is either a face of Δ^n or the entire simplex Δ^n. Note that $\Delta^{(-)}$ is a covariant functor $\Delta \to \mathbf{Set}$, hence a *cosimplicial set*.

   Given a simplicial set $X_\bullet$, endow each set X_n with the discrete topology. Define the *geometric realization of $X_\bullet$* as the space

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

   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 morphism $f : [n] \to [m]$.

9. We have the category of *correspondences* **Corr** with objects all sets and morphisms all binary relations. Given any two binary relations $u \subset X \times Y$ and $v \subset Y \times Z$, let

$$v \circ u = \{(x, y) \in X \times Z : (\exists b \in Y)\,((x, b) \in u \text{ and } (b, y) \in v)\}.$$

   Then the identity morphisms are precisely the diagonal maps.

10. Let $(I, \leq)$ be a partially ordered set. Then we have the *order category I associated to* $\leq$ with $\mathrm{ob}(I) \equiv I$ and for any $x, y \in I$,

$$\mathrm{Hom}_I(x, y) \equiv \begin{cases} \left\{x \xrightarrow{i} y\right\} & x \leq y \\ \emptyset & \text{otherwise} \end{cases}.$$

11. Let $\mathbf{Ouv}_X$ denote the category of open sets of a topological space (X, τ) with inclusion maps as morphisms. This is precisely the order category of τ associated to the poset $\subseteq$.

12. For any category $\mathscr{C}$, we have the *opposite category* $\mathscr{C}^{\mathrm{op}}$ where $\mathrm{ob}\,\mathscr{C}^{\mathrm{op}} \equiv \mathrm{ob}\,\mathscr{C}$ and $\mathrm{Hom}_{\mathscr{C}^{\mathrm{op}}}(x, y) \equiv \mathrm{Hom}_{\mathscr{C}}(y, x)$. Thus, $\mathscr{C}^{\mathrm{op}}$ is formed by keeping the objects but switching all of the arrows in $\mathscr{C}$.

13. Let G be a group. Then the *classifying category BG of G* is the category with a single object $*$ and $\mathrm{Hom}_{BG}(*, *) \equiv G$. Composition here is given by the group law of G, and the identity morphism is precisely e_G.

    Note that $B\,(G^{\mathrm{op}}) = (BG)^{\mathrm{op}}$.

    Aside. Suppose that G is a discrete group. Then the geometric realization $|N(BG)|$ of the nerve of BG is homotopy equivalent to the classifying space for principal G-bundles.

Definition 6.1.3. 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 $F : \mathrm{ob}\,\mathscr{C} \to \mathrm{ob}\,\mathscr{D}$ and $F : \mathrm{mor}\,\mathscr{C} \to \mathrm{mor}\,\mathscr{D}$ such that

(i) $F(f) : F(x) \to F(y)$ in $\mathscr{D}$ whenever $f : x \to y$ in $\mathscr{C}$,

(ii) $F(f \circ g) = F(f) \circ F(g)$, and

(iii) $F(\mathrm{id}_x) = \mathrm{id}_{F(x)}$.

Terminology.

1. We call a covariant functor $\mathscr{C}^{\mathrm{op}} \to \mathscr{D}$ a *contravariant* functor $\mathscr{C} \to \mathscr{D}$.

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

We now can form the category **Cat** of all small categories with functors between them as morphisms.

6.2 Lecture 18

Example 6.2.1. The following are examples of functors.

1. We have a family of *forgetful* functors $U : \mathscr{C} \to \mathscr{D}$, which simply forget certain structure which the objects in $\mathscr{C}$ carry.

$$\mathbf{Grp} \to \mathbf{Set}$$
$$\mathbf{Ab} \to \mathbf{Set}$$
$$\mathbf{Vect}_k \to \mathbf{Ab}$$
$$\mathbf{Vect}_k \to \mathbf{Set}$$

   Let **Ring** denote the category of (unital) rings. Then the forgetful functor $\mathbb{G}_A : \mathbf{Ring} \to \mathbf{Ab}$ is known as the *additive group functor*.

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

$$\Gamma_f : \mathbf{Ouv}_Y^{\mathrm{op}} \to \mathbf{Set}$$
$$\mathcal{U} \mapsto \left\{ s : \mathcal{U} \underset{\text{continuous}}{\to} X \mid f \circ s = \mathrm{id}_{\mathcal{U}} \right\}$$
$$\Gamma_f(\mathcal{U} \subset V) : (s : V \to X) \mapsto (s \restriction_{\mathcal{U}} : \mathcal{U} \to X) .$$

   This is also denoted by $\Gamma_{X/Y}$.

3. Let $n \geq 0$ be an integer. 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. For each $n \geq 1$, the general linear group functor $\mathrm{GL}_n(-) : \mathbf{CommRing} \to \mathbf{Grp}$, defined on morphisms by sending a ring map $f : R \to S$ to the group map $\mathrm{GL}_n(R) \to \mathrm{GL}_n(S)$ given by sending a matrix M over R to the matrix $f(M)$ over S obtained by applying f to each entry of M.

5. The homotopy functor $\pi_i : \mathbf{Top}_*^{(\text{conn, lc})} \to \begin{cases} \mathbf{Set} & i = 0 \\ \mathbf{Grp} & i = 1 \\ \mathbf{Ab} & i > 1 \end{cases}$.

6. Define the functor $(-)_\bullet : \mathbf{Set} \to \mathbf{sSet}$ by sending each set S to the *constant/discrete* functor $(S)_\bullet$ at S, i.e., $S_n \equiv S$ for every $n \geq 0$.

   Alternatively, say that an n-simplex $x \in X_n$ is *nondegenerate* if it is *not* of the form $x = s_i(y)$ where $1 \leq i \leq n-1$ and $y \in X_{n-1}$ and let X_n^{nd} denote the subset of all nondegenerate n-simplices. Define $(S)_\bullet$ as the unique simplicial set such that

$$S_n^{\mathrm{nd}} = \begin{cases} S & n = 0 \\ \emptyset & n > 0 \end{cases} .$$

   Then $|(S)_\bullet|$ is homotopy equivalent to S equipped with the discrete topology.

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

8. Define the *singular chains functor* $\mathrm{Sing}_\bullet : \mathbf{Top} \to \mathbf{sSet}$ by

$$\mathrm{Sing}_n(X) \equiv \left\{ \phi \mid \phi : \Delta^n \to X \atop \text{continuous} \right\} \qquad (f : [m] \to [n]) \mapsto \big(\mathrm{Sing}_f(X) : \phi \mapsto \phi \circ \Delta_f\big)$$
$$\mathrm{Sing}_n(u : X \to Y) : \mathrm{Sing}_n(X) \to \mathrm{Sing}_n(Y), \qquad \phi \mapsto u \circ \phi.$$

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

9. If $n = 1, 2$, then we have the functor $HH^n(G, -) : {}_G\mathbf{Mod} \to \mathbf{Ab}$ as in ($\star$). This extends to all $n \in \mathbb{Z}_{\geq 1}$.

Definition 6.2.2. Let F and G be functors $\mathscr{C} \to \mathscr{D}$. A *natural transformation* $\phi : F \Rightarrow G$ *from* F *to* G is a class function $\phi_{(-)} : \mathrm{ob}\,\mathscr{C} \to \mathrm{mor}\,\mathscr{D}$ such that ϕ_x is a morphism $F(x) \to G(x)$ and for each morphism $h : x \to y$ in $\mathscr{C}$, the square

$$\begin{array}{ccc} F(x) & \xrightarrow{F(h)} & F(y) \\ {\scriptstyle \phi_x}\downarrow & & \downarrow{\scriptstyle \phi_y} \\ G(x) & \xrightarrow[G(h)]{} & G(y) \end{array}$$

commutes. The maps $(\phi_x)_{x \in \mathrm{ob}\,\vec{x}}$ are called the *components of* ϕ.

When $\mathscr{C}$ is small, this gives us the *functor category* $\mathbf{Fun}(\mathscr{C}, \mathscr{D})$ consisting of all functors $\mathscr{C} \to \mathscr{D}$ with natural transformations between them as morphisms. Here, composition is given componentwise by $(A \circ B)_x \equiv A_x \circ B_x$, and the identity map is given componentwise by $(\mathrm{id}_F)_x \equiv \mathrm{id}_{F(x)}$.

Definition 6.2.3. A morphism $\phi : A \to B$ in $\mathscr{C}$ is an *isomorphism* if $\psi \circ \phi = \mathrm{id}_A$ and $\phi \circ \psi = \mathrm{id}_B$ for some morphism $\psi : B \to A$ in $\mathscr{C}$. In this case, we write $A \cong B$.

Terminology. An isomorphism in a functor category is called a *natural isomorphism.*

Exercise 6.2.4. *Show that a natural transformation is an isomorphism if and only if each component is an isomorphism.*

Example 6.2.5. The following are examples of natural transformations.

1. The determinant $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathrm{GL}_1(\mathbb{F})$.

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

$$\begin{array}{ccc} \pi_1 & \xrightarrow{\mathrm{Hur}} & H_1 \\ {\scriptstyle (-)^{\mathrm{ab}}}\downarrow & \nearrow_{q} & \\ (\pi_1)^{\mathrm{ab}} & & \end{array} .$$

   Hurewicz's theorem states that q is actually an isomorphism in $\mathbf{Fun}((\pi_1)^{\mathrm{ab}}, H_1)$.

Example 6.2.6. Consider the *dualization functor* $(-)^\vee : \mathbf{Vect}_k^{\mathrm{op}} \to \mathbf{Vect}_k$ given by

$$V \mapsto V^\vee \equiv \mathrm{Hom}(V, k)$$
$$(f : V \to W) \mapsto (\phi \mapsto \phi \circ f)\,.$$

There is an analogous functor $(-)^\vee : \mathbf{Vect}_k \to \mathbf{Vect}_k^{\mathrm{op}}$. The *double dualization* functor $(-)^{**} : \mathbf{Vect}_k \to \mathbf{Vect}_k$ is the composite of these, inducing a map of functors $\epsilon : \mathrm{id}_{\mathbf{Vect}_k} \to (-)^{\vee\vee}$ given componentwise by

$$\epsilon_V : x \mapsto (\phi \mapsto \phi(x))\,.$$

Exercise 6.2.7.

1. *Show that ϵ 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 $V^{\vee\vee}$ have uncountable bases.*
2. *Show, however, that it is an isomorphism in the setting of finite-dimensional vector spaces over k.*

Definition 6.2.8.

1. We say that a category $\mathscr{C}$ is *small* if $\mathrm{ob}\,\mathscr{C}$ is a set.
2. Let $\pi_0(\mathscr{C})$ denote the class of equivalence classes $\mathrm{ob}\,\mathscr{C}/_{\cong}$. We say that $\mathscr{C}$ is *essentially small* if $\pi_0(\mathscr{C})$ is a set.

6.3 Lectures 19 and 20

We want a weaker notion of sameness between categories that *isomorphism*.

Definition 6.3.1. A functor $F : \mathscr{C} \to \mathscr{D}$ is an *equivalence* if there is a functor $G : \mathscr{D} \to \mathscr{C}$ such that $F \circ G \cong \mathrm{id}_{\mathscr{D}}$ and $G \circ F \cong \mathrm{id}_{\mathscr{C}}$. In this case, we say that G is a *quasi-inverse of* F and that $\mathscr{C}$ and $\mathscr{D}$ are *equivalent*.

This is weaker than *isomorphism* as $F \circ G$ and $G \circ F$ need not be *equal* the identity functor.

Example 6.3.2. Let $\mathscr{C} = \mathbf{Vect}_k^n$, which consists of all n-dimensional vector spaces over k, and $\mathscr{D} = B\mathrm{Mat}_n(k)$. Consider the functor $F : \mathscr{D} \to \mathscr{C}$ defined on objects by $* \mapsto k^n$ and on morphisms by $A \mapsto (v \mapsto Av)$. Define the functor $G : \mathscr{C} \to \mathscr{D}$ using the axiom of choice as follows. Choose a basis for each space $V \in \mathscr{C}$ and send each linear map f to the matrix of f with respect to the two chosen bases. Then F is an equivalence with quasi-inverse G.

Exercise 6.3.3. *Show that $\mathscr{C}$ is essentially small if and only if it is equivalent to a small category.*

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

Definition 6.3.4. We say that F is *essentially surjective* if $\pi_0(F)$ is surjective.

Definition 6.3.5. If $\mathscr{C}$ is a category, then a category $\mathscr{A}$ is a *subcategory of* $\mathscr{C}$ if

(i) $\operatorname{ob}\mathscr{A}$ is a subclass of $\operatorname{ob}\mathscr{C}$,

(ii) $\operatorname{Hom}_{\mathscr{A}}(x,y) \subset \operatorname{Hom}_{\mathscr{C}}(x,y)$ for any $x, y \in \operatorname{ob}\mathscr{A}$, and

(iii) composition and identity in $\mathscr{A}$ are exactly as they are in $\mathscr{C}$.

Any subcategory $\mathscr{A}$ of $\mathscr{C}$ yields an inclusion functor $i : \mathscr{A} \to \mathscr{C}$. Example 6.3.2 shows that the inclusion functor $B\mathrm{Mat}_n(k) \to \mathbf{Vect}_k^n$ is an equivalence.

Definition 6.3.6. Let $F : \mathscr{C} \to \mathscr{D}$ be a functor. Consider the set map $F(-) : \operatorname{Hom}_{\mathscr{C}}(x,y) \to \operatorname{Hom}_{\mathscr{D}}(F(x), F(y))$.

1. We say that F is *faithful* if $F(-)$ is injective.
2. We say that F is *full* if $F(-)$ is surjective.
3. We say that F is *fully faithful* if it is both full and faithful, i.e., $F(-)$ is bijective.

Example 6.3.7. The inclusion functor $i : \mathscr{A} \to \mathscr{C}$ is faithful.

Exercise 6.3.8. *Show that a functor is an equivalence if and only if it is fully faithful and essentially surjective.*

7 The Yoneda lemma

Notice that $\operatorname{Hom}_{\mathbf{Set}}(*, x) \cong x$ for any set x via the mapping $f \mapsto f(*)$. In a general category $\mathscr{C}$, we may not have an initial object $*$, like a singleton. In order to view objects in $\mathscr{C}$ as themselves collections of objects, we define the following notion.

Definition 7.0.1. Given $x \in \operatorname{ob}\mathscr{C}$, a *$y$-point/probe of x* is the set $\operatorname{Hom}_{\mathscr{C}}(y, x)$.

The class $\{\operatorname{Hom}_{\mathscr{C}}(y,x)\}_{y \in \operatorname{ob}\mathscr{C}}$ of y-points reconstructs x as an object in $\mathscr{C}$. To see this, consder the presheaf category

$$\widehat{\mathscr{C}} \coloneqq \mathbf{Fun}(\mathscr{C}^{\mathrm{op}}, \mathbf{Set})$$

and let $x \in \operatorname{ob}\mathscr{C}$. Define the functor $h_x : \mathscr{C}^{\mathrm{op}} \to \mathbf{Set}$ on objects and morphisms, respectively, by

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

Definition 7.0.2. A presheaf $F \in \widehat{\mathscr{C}}$ is *representable* if $F \cong h_x$ for some $x \in \operatorname{ob}\mathscr{C}$. 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

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

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

Lemma 7.0.3 (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, i.e., $h : \mathscr{C} \to \widehat{\mathscr{C}}$ is fully faithful.

(2) There is a natural isomorphism

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

of functors $\mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \mathbf{Set}$.

Thanks to (2), we can treat objects in $\mathscr{C}$ as set-valued presheaves of $\mathscr{C}$.

Proof. We prove just the first statement, from which the second follows formally. Let us define an inverse $i : \mathrm{Hom}_{\widehat{\mathscr{C}}}(h_x, h_y) \to \mathrm{Hom}_{\mathscr{C}}(x, y)$ of the given map. If $\alpha : h_x \to h_y$ is a morphism in $\widehat{\mathscr{C}}$, then let

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

Note that $\alpha_x(\mathrm{id}_x) \in h_y(x) = \mathrm{Hom}_{\mathscr{C}}(x, y)$.

If $f : x \to y$ in $\mathscr{C}$, then $h(f)$ is a map $h_x \to h_y$ 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 $z \in \mathrm{ob}\,\mathscr{C}$. In this case, $h(f)_x(\mathrm{id}_x) = f \circ \mathrm{id}_x = f$. This proves that i is a left inverse of h.

It remains to show that i is a right inverse of h. Let α be a map $h_x \to h_y$. We have that $i(\alpha) = \alpha_x(\mathrm{id}_x) \in h_y(x)$, so that $i(\alpha)$ is a morphism $x \to y$ 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 $z \in \mathrm{ob}\,\mathscr{C}$ and map $\phi : z \to x$ in $\mathscr{C}$, the square

$$\begin{array}{ccc} h_x(x) & \xrightarrow{\alpha_x} & h_y(x) \\ {\scriptstyle h_x(\phi)}\downarrow & & \downarrow{\scriptstyle h_y(\phi)} \\ h_x(z) & \xrightarrow[\alpha_z]{} & h_y(z) \end{array}$$

commutes because α is a natural transformation. By evaluating this at the morphism id_x, we see that

$$\left(\alpha_z \circ h_x(\phi)\right)(\mathrm{id}_x) = \left(h_y(\phi) \circ \alpha_x\right)(\mathrm{id}_x).$$

But the lefthand side equals $\alpha_z\left(h_x(\phi)\left(\mathrm{id}_x\right)\right) = \alpha_z\left(\mathrm{id}_x \circ \phi\right) = \alpha_z(\phi)$, and the righthand side equals $h_y(\phi)(i(\alpha)) = i(\alpha) \circ \phi$. That is, $\alpha_z(\phi) = i(\alpha) \circ \phi$, as required. □

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 our proof of the Yoneda lemma, this is completely determined by the object $\xi \coloneqq h_x(\mathrm{id}_x) \in F(x)$. Conversely, given $\xi \in F(x)$, we get a natural map

$$\begin{aligned} h_x(y) &\to F(y) \\ f &\mapsto F(f)(\xi). \end{aligned}$$

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

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 7.0.4.

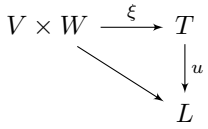
1. Define the presheaf $\mathcal{P} : \mathbf{Set}^{\mathrm{op}} \to \mathbf{Set}$ on objects by $S \mapsto \mathcal{P}(S)$ and on morphisms by $\mathcal{P}(f : S \to T) : A \mapsto f^{-1}(A)$. For $\mathcal{P}$ to be representable, we need to find some set Q and $\xi \subset Q$ such that $\mathrm{Hom}(S,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

2. Consider the forgetful presheaf $U : \mathbf{Ring} \to \mathbf{Set}$ on $\mathbf{Ring}^{\mathrm{op}}$. For any unital ring R, any ring map $\phi : \mathbb{Z}[t] \to R$ is determined by the value $\phi(t)$. Therefore, the map $\mathrm{Hom}_{\mathbf{Ring}}(\rho, R) \to R$ given by $u \mapsto U(u)(\xi)$ is bijective where $\rho \equiv \mathbb{Z}[t]$ and $\xi \equiv t$ (which belongs to $U(\mathbb{Z}[t])$). This shows that U is represented by $\mathbb{Z}[t]$.

Example 7.0.5 (Tensor product). Let $V, W \in \operatorname{ob}\mathbf{Vect}_k$ and define the presheaf $B : \mathbf{Vect}_k \to \mathbf{Set}$ on $(\mathbf{Vect}_k)^{\mathrm{op}}$ by

$$L \mapsto \{\phi : V \times W \to L \mid \phi \text{ bilinear}\}.$$

We want to find some k-vector space T and some bilinear map $\xi \in B(T)$ such that the map $\mathrm{Hom}_{(\mathbf{Vect}_k)^{\mathrm{op}}}(L, T) \to B(L)$ given by $u \mapsto u \circ \xi$ is bijective for any space L.



We construct such a pair (T, ξ) as follows. Let $\mathcal{F}$ denote the vector space of set maps $f : V \times W \to k$ 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 any of the forms

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

where $x, x', x'' \in V$ and $y, y', y'' \in W$ and $c \in k$. Finally, set $T = {}^{\mathcal{F}}\!/_{\mathcal{F}_0}$ and define ξ by $(x, y) \mapsto \delta_{(x,y)} + \mathcal{F}_0$. Then T represents B. We usually write $V \otimes_k W$ for T.

Instead of constructing the real numbers as equivalence classes of Cauchy sequences or as Dedekind cuts, we want to find a special property distinguishing $\mathbb{R}$ (equivalently, an open or closed interval) in **Top**.

We can pick out the interval $[0, 1]$ among all topological spaces as follows. We see that

$$[0,1] \cong \left([0,1] \coprod [0,1] \Big/ \text{first } 1 = \text{second } 0 \right)$$

via the mean function M. Let $\mathscr{C}$ denote the category of pairs (X, α) where X is a topological space with two ordered marked points ℓ_x and r_x along with a map $\alpha : X \coprod X /_{\sim} \xrightarrow{\cong} X$ where the first r_x is equal under $\sim$ to the second ℓ_x.

Theorem 7.0.6 (Freyd). *The pair $([0, 1], M)$ is the terminal object in $\mathscr{C}$.*

7.1 Lecture 21

Definition 7.1.1. Let $\mathscr{C}$ be a category and I be any set. Suppose that $A_\alpha \in \operatorname{ob}\mathscr{C}$ for each $\alpha \in I$.

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

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

   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 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

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

   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 in $\mathscr{C}$.

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

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

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

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

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

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

Notation. The symbol $\bigoplus$ may be used in place of $\coprod$.

Example 7.1.2.

1. **Set** has all products and coproducts, in the form of Cartesian products and disjoints unions, respectively.

2. Let R be a unital ring and $\mathscr{C} = \mathbf{Mod}_R$, the category of R-modules, i.e., pairs (M, ρ) where M is an abelian group and ρ is a map $R \to \mathrm{End}(M)$ satisfying

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

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

$$\begin{array}{ccc} M & \xrightarrow{\rho(x)} & M \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ N & \xrightarrow{\lambda(x)} & N \end{array}$$

   commutes.

   Let $\{(A_\alpha, \rho_\alpha)\}_{\alpha \in I}$ be a collection of R-modules. If we endow the Cartesian product $\prod_\alpha A_\alpha$ with the componentwise module structure inherited from the A_α, then it becomes the product of $\{A_\alpha\}$ in $\mathbf{Mod}_R$. Specifically, the underlying group law and zero element are given by

$$\begin{aligned} (a_\alpha)_{\alpha \in I} + (b_\alpha)_{\alpha \in I} &\equiv (a_\alpha + b_\alpha)_{\alpha \in I} \\ 0 &\equiv (0)_{\alpha \in I}\,, \end{aligned}$$

   and scalar multiplication is given by

$$\left(\prod_\alpha \rho_\alpha\right)(x)\left((a_\alpha)\right) = \left(\rho_\alpha(x)\,(a_\alpha)\right), \quad x \in R.$$

   Moreover, the coproduct (or direct sum) of $\{A_\alpha\}$ is defined as the submodule of the product consisting of all tuples (a_α) such that $a_\alpha \neq 0$ for at most finitely many $\alpha \in I$. This means that the product and coproduct coincide when I is finite.

Exercise 7.1.3.

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

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

Let $\mathscr{C}$ be a category and $a \in \mathrm{ob}\,\mathscr{C}$. The *overcategory* ${}^{\mathscr{C}}\!/_a$ has as objects all pairs (x, f) where $x \in \mathrm{ob}\,\mathscr{C}$ and f is a map $f : x \to a$ in $\mathscr{C}$. Also, a generic morphism $\beta : (x, f) \to (y, g)$ is a commutative triangle of the form

$$\begin{array}{ccc} x & \xrightarrow{\beta} & y \\ {\scriptstyle f}\downarrow & \swarrow_{g} & \\ a & & \end{array} .$$

The *undercategory* ${}^{a}\!/_{\mathscr{C}}$ is defined similarly.

Definition 7.1.4. Let $a \in \mathrm{ob}\,\mathscr{C}$. Let $\mathscr{C}_a$ be another name for the overcategory ${}^{\mathscr{C}}\!/_a$ and $\mathscr{C}^a$ another name for 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 in $\mathscr{C}_a$ the *fibered product of the* A_α *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 in $\mathscr{C}^a$ the *fibered coproduct under* a, denoted by $\coprod_{\alpha}^{a} A_\alpha$.

Example 7.1.5.

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

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

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

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

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

(2) Arbitrary fibered products and fibered coproducts exist in $\mathbf{Mod}_R$ and $\mathbf{Mod}_G$ by the same constructions as those in (1) since the π_α and i_α are module homomorphisms.

(3) **Grp** inherits arbitrary products and fibered products from **Set**, equipped the componentwise group law. In Section 7.2, we shall construct arbitrary coproducts and fibered coproducts in **Grp**.

7.2 Lecture 22

Theorem 7.2.1. *The category* **Grp** *has arbitrary coproducts and fibered coproducts.*

Proof. Let us begin with coproducts (also called *free products* in this setting). Let $\{G_\alpha\}_{\alpha\in I}$ be a collection of groups. Consider the set

$$S \coloneqq \coprod_{\alpha\in I} G_\alpha \setminus \{e\},$$

which we view as a formal alphabet with elements of S^n corresponding to words of length n. We say that a word $(\sigma_{\alpha_1},\dots,\sigma_{\alpha_n})$ in S is *admissible* if $\alpha_i \neq \alpha_{i+1}$ for each $i = 1,\dots,n-1$. Let $S^n_{\text{adm}} \subset S^n$ denote the set of all admissible words in S^n. Let

$$Q = \left(\coprod_{n\geq 1} S^n_{\text{adm}}\right) \sqcup \{\epsilon\}$$

where ϵ denotes the empty word. Raw concatenation

$$\kappa : \left(\overbrace{(\sigma_{\alpha_1},\dots,\sigma_{\alpha_n})}^{\sigma}, \overbrace{(\tau_{\beta_1},\dots,\tau_{\beta_n})}^{\tau}\right) \mapsto (\sigma_{\alpha_1},\dots,\sigma_{\alpha_n},\tau_{\beta_1},\dots,\tau_{\beta_n})$$

of admissible words is unital and associative but may not be a well-defined binary operation on Q, since the concatenation of two admissible words may not be admissible. To repair this, we must consider the case where $\alpha_n = \beta_1$. There are two cases to consider.

(a) Suppose that $\alpha_n\beta_1 = e_{G_{\alpha_n}} = e_{G_{\beta_1}}$. Then let

$$\kappa(\sigma,\tau) = (\sigma_{\alpha_1},\dots,\sigma_{\alpha_n}\tau_{\beta_1},\dots,\tau_{\beta_n})\,.$$

(b) Suppose that $\alpha_n\beta_1 \neq e$. Then let

$$\kappa(\sigma,\tau) = \left(\sigma_{\alpha_1},\dots,\sigma_{\alpha_{n-1}},\tau_{\alpha_2},\dots,\tau_{\beta_n}\right).$$

This *reduced word* still may be non-admissible, and thus we keep reducing our new words until we get an admissible one.

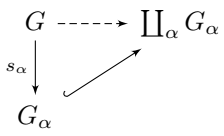
Our modified operation κ makes Q into a group. Further, we have a monomorphism

$$i_\alpha : G_\alpha \to Q, \qquad g \mapsto \begin{cases} (g) & g \neq e \\ \epsilon & g = 0 \end{cases}$$

for each $\alpha \in I$. Then $(Q,\{i_\alpha\})$ represents the functor $\prod_\alpha \operatorname{Hom}_{\mathbf{Grp}}(G_\alpha,-)$, i.e., (Q,κ) is the coproduct of the G_α.

Notation. Sometimes the coproduct is denoted by $*_\alpha G_\alpha$.

For fibered coproducts, let $\{(G_\alpha, s_\alpha : G \to G_\alpha)\}$ be a collection of objects in $\mathbf{Grp}^G$. Note that we have a map $j_\alpha : G \to \coprod_\alpha G_\alpha$ given by the composite



for each α. Let $N \trianglelefteq \coprod_\alpha G_\alpha$ be generated by all elements of the form $j_\alpha(x)j_\beta(x)^{-1}$ for any $\alpha, \beta \in I$ and $x \in G$. Finally, set

$$\coprod_\alpha^G G_\alpha = \coprod_\alpha G_\alpha / N.$$

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

Definition 7.2.2. The *free group* $\mathrm{Fr}(S)$ *on a set* S is the coproduct $\coprod_{s\in S} G_s$ in **Grp** where $G_s \cong \mathbb{Z}$ for each $s \in S$. (This is always isomorphic to $\coprod_{s\in S} \mathbb{Z}$.)

Example 7.2.3.

(1) Let M be a set and $U, V \subset M$, so that U and V are objects in $\mathcal{P}(M)$. 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 $M \in \mathrm{ob}\mathscr{C}$. Let $U, V \subset M$ be open. As in (1), we have that $(U \cup V, *) = (U, *) \coprod_{(U\cap V,*)} (V, *)$. The van Kampen theorem 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.

8 Adjoint functors

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

Definition 8.0.1. 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

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

are isomorphic.

The notion of an adjunction lets us compare statements about $\mathscr{C}$ and about $\mathscr{D}$ without assuming that they are equivalent. Rather, we merely assume that the effect these properties have on morphisms is the same.

Suppose that $L : \mathscr{C} \to \mathscr{D}$ 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 $L_* \circ h^{\mathscr{D}} : \mathscr{D} \to \widehat{\mathscr{C}}$. 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, $L_* \circ h^{\mathscr{D}} \cong h^{\mathscr{C}} \circ R$. 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 8.0.2. *The right adjoint is unique up to a unique isomorphism.*

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

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

in $x \in \operatorname{ob} \mathscr{C}$. This yields a map of functors $\epsilon : \mathrm{id}_{\mathscr{C}} \to R \circ L$, called the *unit of the adjunction*. Likewise, we get a map $\eta : L \circ R \to \mathrm{id}_{\mathscr{D}}$, called the *counit of the adjunction*. In turn, these induce two natural transformations

$$L \xrightarrow{\ \epsilon\ } L \circ R \circ L \xrightarrow{\ \eta\ } L$$

$$R \xrightarrow{\ \epsilon\ } R \circ L \circ R \xrightarrow{\ \eta\ } R$$

such that $\mathrm{id}_L = \eta \circ \epsilon$ and $\epsilon \circ \eta = \mathrm{id}_R$.

Proposition 8.0.3. *Conversely, if (L, R, ϵ, η) satisfies $\eta \circ \epsilon \cong \mathrm{id}_L$ and $\eta \circ \epsilon \cong \mathrm{id}_R$, then (L, R) is an adjoint pair.*

Example 8.0.4. Let $|\cdot| : \mathbf{Grp} \to \mathbf{Set}$ denote the forgetful functor. Then it is right adjoint to the free group functor $\mathrm{Fr} : \mathbf{Set} \to \mathbf{Grp}$. This means that $\operatorname{Hom}(\mathrm{Fr}(S), G) \cong \operatorname{Hom}(S, |G|)$ for any set S and group G. That is, for any function $f : S \to |G|$, there is a unique homomorphism $\phi : \mathrm{Fr}(S) \to G$ 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.

$$\begin{aligned}
\operatorname{Hom}(\mathrm{Fr}(S), G) &= \operatorname{Hom}\left(\coprod_S \mathbb{Z}, G\right) \\
&\cong \prod_{s \in S} \operatorname{Hom}(\mathbb{Z}, G) \\
&\cong \prod_s \operatorname{Hom}\left(\{1\}, |G|\right) \\
&\cong \operatorname{Hom}\left(\coprod_s \{1\}, |G|\right) \\
&\cong \operatorname{Hom}\left(S, |G|\right).
\end{aligned}$$

□

8.1 Lecture 23

Example 8.1.1. Consider the inclusion $\mathbf{Ab} \overset{i}{\hookrightarrow} \mathbf{Grp}$ of the full subcategory of abelian groups. It is right adjoint to the abelianization functor $(-)^{\mathrm{ab}}$.

Proof. Let G be a group and A an 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 yields a bijection $\mathrm{Hom}_{\mathbf{Ab}}(G^{\mathrm{ab}}, A) \xrightarrow{\cong} \mathrm{Hom}_{\mathbf{Grp}}(G, A)$ defined by $\phi \mapsto \psi \circ \pi$. □

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 a preadditive category whereas the latter is not. Any inverse pair of functors (F, G), however, always gives rise to an adjunction.

Theorem 8.1.2. $(-)^{\mathrm{ab}}$ *has no left adjoint.*

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

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

naturally in any abelian group A.

Lemma 8.1.3.

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

Proof. On the one hand, if $F(A)$ is simple and nonabelian, then $F(A)^{\mathrm{ab}} = \{e\}$. But, in this case,

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

a contradiction.

On the other hand, 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, a contradiction. □

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

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

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

Thus, $\mathrm{id}_A = 0_A$, and thus A is trivial. □

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

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

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

a contradiction. If ${}^{F(A)}\!/_{M}$ is abelian, then it is isomorphic to C_p, in which case we can use an argument as in (a). □

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 nontrivial and finite, which implies that $F(C_2)$ has a proper maximal normal subgroup, contrary to Lemma 8.1.3(c). □

Lemma 8.1.4. *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 $\mathrm{Fr}(f)$. □

Lemma 8.1.5. *Let S be a set. Then $\mathrm{Fr}(S)^{\mathrm{ab}} \cong \coprod_{s\in S} G_s$ in $\mathbf{Ab} = \mathbb{Z}\text{–}\mathbf{Mod}$ where $G_s \cong \mathbb{Z}$ for each s, i.e., the free abelian group on S. In other notation,*

$$\mathrm{Fr}(S)^{\mathrm{ab}} \cong \bigoplus_{s\in S} G_s.$$

Proof. 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.

$$\begin{array}{ccc} \mathrm{Fr}(S) & \xrightarrow{\phi} & \bigoplus_{s\in S} G_s \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists!\phi^{\mathrm{ab}}} & \\ \mathrm{Fr}(S)^{\mathrm{ab}} & & \end{array}$$

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 $n_i \in G_i$. This implies that

$$0 = \phi^{\mathrm{ab}}([x]) = \sum_{i=1}^{r} n_i \delta_{s_i},$$

and thus each n_i vanishes. This proves that $[x] = 0$, so that $\ker \phi^{\mathrm{ab}}$ is trivial. □

Lemma 8.1.6. $\mathrm{Fr}(S) \cong \mathrm{Fr}(T) \iff S \cong T$.

Proof.

($\Longleftarrow$)

If $u : S \to T$ and $v : T \to S$ are inverses of each other, then so are $\mathrm{Fr}(u)$ and $\mathrm{Fr}(v)$ thanks to functoriality of Fr.

($\Longrightarrow$)

Assume that $\mathrm{Fr}(S) \cong \mathrm{Fr}(T)$. We see that

$$\bigoplus_{s\in S} G_s \cong \mathrm{Fr}(S)^{\mathrm{ab}} \cong \mathrm{Fr}(T)^{\mathrm{ab}} \cong \bigoplus_{t\in T} G_t$$

$$\Downarrow$$

$$\overbrace{\mathbf{Fun}^{\mathrm{fs}}(S, C_2)}^{\text{functions of finite support}} \cong \bigoplus_{s\in S} G_s \Big/ 2\bigoplus_{s\in S} G_s \cong \bigoplus_{t\in T} G_t \Big/ 2\bigoplus_{t\in T} G_t \cong \mathbf{Fun}^{\mathrm{fs}}(T, C_2)$$

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 8.1.7. There is another proof of Lemma 8.1.6 provided that we restrict our set-theoretic universe. Specifically, the adjunction $(\mathrm{Fr}, |-|)$ yields

$$\begin{aligned}
\mathcal{P}(T) &\cong \mathrm{Hom}_{\mathbf{Set}}(T, C_2) \\
&\cong \mathrm{Hom}_{\mathbf{Grp}}(\mathrm{Fr}(T), C_2) \\
&\cong \mathrm{Hom}_{\mathbf{Grp}}(\mathrm{Fr}(S), C_2) \\
&\cong \mathrm{Hom}_{\mathbf{Set}}(S, C_2) \\
&\cong \mathcal{P}(S).
\end{aligned}$$

If we assume the continuum hypothesis, then $S \cong T$ for otherwise $|S| < |T| < |\mathcal{P}(T)| = |\mathcal{P}(S)|$, a contradiction.

□

8.2 Lecture 24

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 8.2.1. 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 8.2.2. $\mathrm{im}(\phi \circ \mathrm{Fr}(i)) = \bigcap \{H : H \leq G,\ H \supset S\}$.

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 case, we call η a *presentation of* G. We also call S the *set of generators of* G and T the *set of relations of* G.

Note 8.2.3.

1. Any quotient H of a finitely generated group G is finitely generated. Indeed, we have a finite set T such that $\mathrm{Fr}(T) \to G$ is surjective. But then the composite $\mathrm{Fr}(T) \to G \twoheadrightarrow H$ is surjective as well.
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 $\left\{y^k x y^{-k} : k \geq 0\right\}$ is not.
3. If G is finitely presentable, then any subgroup of G is finitely presentable.

Theorem 8.2.4 (Nielsen-Schreier). *Any subgroup of a free group is free.*

9 Polynomial rings

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

Let $A \in \mathbf{CommRing}$. Then A is a module over itself with scalar multiplication given by ring multiplication. Then we have an A-module $\bigoplus_{\mathbb{Z}_{\geq 0}} A$, where

$$a \cdot (a_0, a_1, a_2, \ldots) = (a \cdot a_0, a \cdot a_1, a \cdot a_2, \ldots), \qquad a \in A.$$

For each $k \geq 0$, consider the element

$$m_k \coloneqq \left(0, \ldots, 0, \underbrace{1}_{k\text{-th place}}, 0, \ldots\right).$$

Then the m_k form an A-basis for $\bigoplus_{\mathbb{Z}_{\geq 0}} A$. Let $m_k \cdot m_l = m_{k+1}$ and extend this operation to $\bigoplus_{\mathbb{Z}_{\geq 0}} A$ by linearity. Then $\left(\bigoplus_{\mathbb{Z}_{\geq 0}} A, +, \cdot\right) \in \mathrm{ob}\,\mathbf{CommRing}$. Moreover, $\left(\left(\bigoplus_{\mathbb{Z}_{\geq 0}} A, +, \cdot\right), i\right) \in \mathrm{ob}\,\mathbf{CommRing}^A$ where $i : A \to \bigoplus_{\mathbb{Z}_{\geq 0}} A$ is defined by by $a \mapsto (a, 0, 0 \ldots, 0, \ldots)$. We call this the *one-variable polynomial ring over* A.

Any element p of $\bigoplus_{\mathbb{Z}_{\geq 0}} A$ has the form $\sum_{k \in \mathbb{N}} a_k m_k$. But $m_k = \underbrace{m_1 \cdots m_1}_{k \text{ copies}}$. Therefore, if $a_k = 0$ for any $k \geq n + 1$ and $a_n \neq 0$, then

$$p = a_0 + a_1 m_1 + \cdots + a_n (m_1)^n.$$

Writing t for m_1 and calling the integer n the *degree* $\deg p$ *of* p, we recover an ordinary polynomial $a_0 + a_1 t + \cdots a_n t^n$ of degree n in the indeterminate t. By convention, we let $\deg(0) = -\infty$.

Proposition 9.0.1. $\deg(p_1 + p_2) \leq \max(\deg p_1, \deg p_2)$.

9.1 Lecture 25

Let S be a set. Note that $\mathbf{Fun}^{\mathrm{fs}}(S, \mathbb{Z}_{\geq 0})$ is an additive monoid because $\mathbb{Z}$ is one. We can view its elements as finite subsets of S where each element of S is "colored" by a nonnegative integer. Alternatively, we can 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 have that

$$\xi = \prod_{s \in S} t_s^{\xi(s)} = \prod_{s \in \mathrm{supp}(\xi)} t_s^{\xi(s)},$$

Let $A \in \mathrm{ob}\,\mathbf{CommRing}$. Define the *multivariable polynomial ring over A on $\{t_s\}_{s \in S}$* as

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

equipped with the operations

$$\begin{aligned} (f+g)(\xi) &\equiv f(\xi) + g(\xi) \\ (f \cdot g)(\xi) &\equiv \sum_{\substack{\mu,\nu \\ \mu\cdot\nu=\xi}} f(\mu) \cdot g(\nu). \end{aligned}$$

Note that $A[S] \in \mathrm{ob}\,\mathbf{CommRing}$ 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.

Note 9.1.1. There is a natural ring monomorphism $i_A : A \hookrightarrow A[S]$ given by $a \mapsto a1_{A[S]}$.

Any $f \in A[S]$ has the form $\sum_{\xi \in \mathrm{supp}(f)} f(\xi)\delta_\xi$. Let $\delta_\xi \coloneqq \prod_{s \in \mathrm{supp}(\xi)} t_s^{\xi(s)}$, allowing us to write f uniquely in the form of a polynomial in several variables, namely

$$\sum_{\xi \in \mathrm{supp}(f)} f(\xi) \prod_{s \in \mathrm{supp}(\xi)} t_s^{\xi(s)}.$$

Proposition 9.1.2.

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

   Proof. We want a natural bijection $\mathrm{Hom}_{\mathbf{CommRing}^A}(A[S], B) \cong \mathrm{Hom}_{\mathbf{Set}}(S, |B|)$ for any ring B and any set S. Given a commutative diagram

$$\begin{array}{ccc} A[S] & \xrightarrow{\theta} & B \\ \uparrow & \nearrow_{i} & \\ A & & \end{array}$$

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

$$\sum_{\xi \in \mathrm{supp}(f)} f(\xi) \prod_{s \in \mathrm{supp}(\xi)} t_s^{\xi(s)} \mapsto \sum_{\xi \in \mathrm{supp}(f)} i(f(\xi)) \prod_{s \in \mathrm{supp}(\xi)} \phi(t_s)^{\xi(s)}.$$

□

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

Exercise 9.1.3. *Apply the Yoneda lemma to the adjoint pair $(A[-], |-|)$ to prove that*

$$A[S] \cong A[T][S \setminus T].$$

Given a monomial ξ in elements of S, let $\deg(\xi) = \sum_{s \in S} \xi(s)$. If $f \in A[S]$, then define the *degree of f* as

$$\deg(f) \equiv \max\{\deg(\xi) : f(\xi) \neq 0\}.$$

By convention, $\deg(0) = -\infty$.

Lemma 9.1.4.

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

(2) $\deg(fg) \leq \deg(f) + \deg(g)$.

Proof. We may assume, wlog, that S is finite because every polynomial consists of only finitely many monomials. Let $S = \{1, \ldots, n\}$. Order the set of all monomials of length n by the dictionary order $<$, so that $t_1^{\alpha_1} \cdots t_n^{\alpha_n} < t_1^{\beta_1} \cdots t_n^{\beta_n}$ iff there is some $2 \leq k \leq n$ such that $\alpha_k = \beta_k$ and $\alpha_i < \beta_i$ for each $1 \leq i < k$.

Now, we may write

$$f = \sum_{\xi} f(\xi) t^{\xi}$$
$$g = \sum_{\xi} g(\xi) t^{\xi}.$$

This means that

$$f + g = \sum_{\xi} \left(f(\xi) + g(\xi)\right) t^{\xi}$$
$$fg = \sum_{\xi} \left(\sum_{\substack{\eta, \eta' \\ \eta \cdot \eta' = \xi}} f(\eta) \cdot g\left(\eta'\right) \right) t^{\xi}.$$

(1) If η satisfies $\deg \eta > \max\{\deg f, \deg g\}$, then $f(\eta) = g(\eta) = 0$. In this case, $f(\eta) + g(\eta) = 0$, so that $\deg(f + g) < \deg(\eta)$.

(2) If $f(\eta) \neq 0$, then $\deg(t^\eta) = \deg(\eta) \leq \deg(g)$. Likewise, if $g(\eta') \neq 0$, then $\deg(t^{\eta'}) \leq \deg(g)$. But

$$\deg(t^\eta) + \deg(t^{\eta'}) = \deg(t^{\eta\eta'}) = \deg(t^\eta) = \deg(\eta),$$

and thus $\deg(\eta) \leq \deg(f) + \deg(g)$.

□

Recall that a commutative ring R is called an *integral domain* if it has no zero divisors, i.e.,

$$xy = 0 \implies x = 0 \text{ or } y = 0$$

for any $x, y \in R$. If R is unital, then let $R^\times = \{x \in R \mid xy = yx = 1_R \text{ for some } y \in R\}$, the group of units of R under multiplication.

Lemma 9.1.5. *If A is an integral domain, then* $\deg(fg) = \deg(f) + \deg(g)$.

Proof. Suppose that A has no zero divisors. Given $f, g \in A[S]$, write

$$f = \sum_\xi f(\xi) t^\xi$$
$$g = \sum_\xi g(\xi) t^\xi.$$

Say that $\deg(f) = \deg(\eta)$ and $\deg(g) = \deg(\eta')$ where $f(\eta) \neq 0$ and $g(\eta') \neq 0$. Then the coefficient for the term $t^\eta t^{\eta'}$ in fg equals $f(\eta)g(\eta')$, which must be nonzero. Hence $\deg(fg) = \deg(f) + \deg(g)$.

Also, if $g = 0$ or $f = 0$, then clearly $\deg(fg) = \deg(f) + \deg(g)$. □

Corollary 9.1.6. *Let A be an integral domain.*

1. $(A[S])^\times = A^\times$.
2. *$A[S]$ is an integral domain.*

Definition 9.1.7. Consider an object $(B, i : A \to B)$ in the undercategory $\mathbf{CommRing}^A$. We say that B is a *commutative A-algebra* if i is injective.

Definition 9.1.8. 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 9.1.9. Let B be a commutative A-algebra. We say that B is *finitely generated* (or *has finite type*) if $A[T] \to B$ is surjective for some finite subset $T \subset B$.

Proposition 9.1.10. *If S and T are sets, then $S \cong T \iff \mathbb{Z}[S] \cong \mathbb{Z}[T]$.*

Proof. See Remark 8.1.7. □

Let R be a ring and S be a set. For any object B in $\mathbf{Ring}^R$, consider the collection of set maps

$$\mathrm{Hom}^{(c)}_{\mathbf{Set}}(S, |B|) \coloneqq \{\phi : S \to B : \phi(s)(\xi) = \xi \cdot \phi(s),\ s \in S,\ \xi \in \mathrm{im}(R \to B)\}.$$

This induces a functor $\mathrm{Hom}^{(c)}_{\mathbf{Set}}(S, |-|) : \mathbf{Ring}^R \to \mathbf{Set}$, which has a left adjoint $R\langle - \rangle : \mathbf{Set} \to \mathbf{Ring}^R$.

10 Noetherian and Artinian modules

10.1 Lecture 26

Suppose that A is an abelian group and consider the set of *endomorphisms* $\mathrm{End}(A) \coloneqq \mathrm{Hom}_{\mathbf{Ab}}(A, A)$. Then $(\mathrm{End}(A), +, \circ)$ is a ring, under pointwise addition inherited from A and composition. Further, it has a unit, namely the identity morphism.

Now, 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. 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 $\rho(r)(a) = \alpha(r, a)$. The condition that ρ is a homomorphism is equivalent to the condition that $\alpha(r_1, \alpha(r_2, a)) = \alpha(r_1 r_2, a)$.

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 square commutes for any $r \in R$.

$$\begin{array}{ccc} A_1 & \xrightarrow{\phi} & A_2 \\ {\scriptstyle \rho_1(r)}\downarrow & & \downarrow{\scriptstyle \rho_2(r)} \\ A_1 & \xrightarrow[\phi]{} & A_2 \end{array}$$

As a result, we may form $R\text{–}\mathbf{Mod}$ the category of R-modules.

Furthermore, let R^{op} denote the ring obtained from by 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. This is equivalent to defining an action map $\alpha : A \times R \to A$ by $\alpha(a, r) = \rho(r)(a)$ such that $\alpha(\alpha(a, r_1), r_2) = \alpha(a, r_1 r_2)$. The category of right R-modules is denoted by $R^{\mathrm{op}}\text{–}\mathbf{Mod}$.

Finally, the category of *R-bimodules* consists of all abelian groups carrying the structure of both left and right R-modules. It is denoted by $R\text{–}\mathbf{Mod}\text{–}R$ or $R \otimes_{\mathbb{Z}} R^{\mathrm{op}}\text{–}\mathbf{Mod}$. Note that any ring is canonically a bimodule over itself via left and right multiplication.

Definition 10.1.1. A subgroup of R is called

1. a *left ideal* if it is a submodule of R with R viewed as a left module.
2. a *right ideal* if it is a submodule of R with R viewed as a right module.
3. a *two-sided ideal* if it is a submodule of R with R viewed as a bimodule.

If R is commutative, then these three notions coincide. In general, we have three full subcategories:

$$R\text{–}\mathbf{Ideal} \subset R\text{–}\mathbf{Mod}$$
$$R^{\mathrm{op}}\text{–}\mathbf{Ideal} \subset R^{\mathrm{op}}\text{–}\mathbf{Mod}$$
$$R\text{–}\mathbf{Ideal}\text{–}R \subset R\text{–}\mathbf{Mod}\text{–}R.$$

Note 10.1.2. Let M be an R-module. Let $\{M_\alpha\}_{\alpha\in A}$ be a collection of submodules of M and let $i_\alpha : M_\alpha \hookrightarrow M$ denote inclusion.

1. The intersection $\bigcap_\alpha M_\alpha$ is a submodule of M.

2. Note that
$$(i_\alpha) \in \prod_\alpha \mathrm{Hom}_{R\text{-}\mathbf{Mod}}(M_\alpha, M) = \mathrm{Hom}_{R\text{-}\mathbf{Mod}}\left(\coprod_\alpha M_\alpha, M\right).$$
Let $\sum_\alpha M_\alpha = \mathrm{im}(i_\alpha)$. Then
$$\sum_\alpha M_\alpha = \left\{\sum_\alpha m_\alpha : m_\alpha \in M_\alpha,\ m_\alpha \neq 0 \text{ for at most finitely many } \alpha\right\},$$
which we can think of as the smallest submodule of M containing each M_α.

3. Let $S \subset M$ be any subset. We call $\coprod_{s\in S} R$ *the free R-module generated by S*. Recall that the free R-module functor is left adjoint to the forgetful functor. Therefore, 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 $R \cdot S \coloneqq \mathrm{im}\, g$ is the *submodule of M generated by S*.

   Aside. We can view g as the *copowering functor* over **Set** for R–**Mod**.

4. Suppose that there is an exact sequence
$$\bigoplus_{t\in T} R \to \bigoplus_{s\in S} R \to M \to 0$$
of R-modules with T and S finite. In this case, we say that M is *finitely presentable*.

We say that a module M satisfies the *ascending chain condition (ACC)* if every sequence
$$M_1 \subset M_2 \subset \cdots \subset M$$
of submodules stabilizes after finitely many steps. We define the *descending chain condition (DCC)* similarly.

Definition 10.1.3. Let M be an R-module. Then M is

1. *Noetherian* if it has ACC.

2. *Artinian* if it has DCC.

Definition 10.1.4. Let M be an R-module. Then M has

1. the *maximal property* if every nonempty collection of submodules of M has a maximal element with respect to inclusion.

2. the *minimal property* if every nonempty collection of submodules of M has a minimal element with respect to inclusion.

Lemma 10.1.5. *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.

To establish (a) $\implies$ (b), let M be Noetherian and suppose, towards a contradiction, that we have a nonempty collection $\mathcal{F}$ of submodules without a maximal element. Pick any element $M_1 \in \mathcal{F}$. As this is not maximal, there is some $M_2 \in \mathcal{F}$ such that $M_1 \subsetneq M_2$, and so on. This yields an ascending chain

$$M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M,$$

which never stabilizes, a contradiction.

To establish (b) $\implies$ (c), notice that if M has the maximal property, then so does every submodule. Therefore, it suffices to the prove the following lemma.

Lemma 10.1.6. *If the R-module M has the maximal property, then M is finitely generated.*

Proof. Let $\mathcal{F}$ denote the set of all finitely generated submodules $N \subset M$. 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 our choice of T. □

Finally, we must establish (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 $N = M_n$. □

Lemma 10.1.7. *TFAE.*

(a) M is Artinian.

(b) M has the minimal property.

10.2 Lecture 27

We shall refer to the properties *Noetherian*, *Artinian*, and *finitely generated* as the *finiteness properties*.

Proposition 10.2.1.

(1) The finiteness properties 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 the other two finiteness properties.

Proof.

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

$$0 \longrightarrow N \xhookrightarrow{i} M \xrightarrow{q} M/N \longrightarrow 0 \ .$$

Let $M_1 \subset M_2 \subset \cdots \subset M$ be an ascending chain of submodules. Then

$$q(M_1) \subset q(M_2) \subset \cdots \subset M/N$$

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

$$\begin{array}{ccccc} N \cap M_i & \hookrightarrow & M_i & \twoheadrightarrow & q(M_i) \\ \| & & \uparrow & & \| \\ N \cap M_r & \hookrightarrow & M_r & \twoheadrightarrow & q(M_r) \end{array} \ .$$

Suppose that $i \geq r$ and 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 $M_i = M_r$.

(2) The Artinian case follows from a similar argument to (1).

(3) Assume that both N and M/N are finitely generated R-modules. Then there are finite sets S and T together with maps

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

Furthermore, we have the short exact sequence.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xhookrightarrow{i} & M & \xrightarrow{q} & M/N & \longrightarrow & 0 \\ & & & & & & \uparrow{\scriptstyle \beta} & & \\ & & & & & & \coprod_{t \in T} R & & \end{array} \ .$$

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

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

which fits in a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xhookrightarrow{\ i\ } & M & \xrightarrow{\ q\ } & {}^{M}\!/_{N} & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \phi} & & \uparrow{\scriptstyle \beta} & & \\ 0 & \longrightarrow & \coprod_{s\in S} R & \hookrightarrow & \left(\coprod_{s\in S} R\right) \coprod \left(\coprod_{t\in T} R\right) & \twoheadrightarrow & \coprod_{t\in T} R & \longrightarrow & 0 \end{array}.$$

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 means that M is finitely generated.

□

Lemma 10.2.2. *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 denotes 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.

($\Longrightarrow$)

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

(a) 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 yields an infinite chain

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

a contradiction.

(b) For the Artinian case, use a similar argument to (a).

(c) 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 $1 \leq i \leq n$, let $x_i = \phi(0, \ldots, \underbrace{1}_{i\text{-th spot}}, \ldots, 0)$, so that $x_i = (x_{i_\lambda})_{\lambda \in \Lambda}$. Let

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

Note that Λ^0 is finite, which means that there is some $\mu \in \Lambda \setminus \Lambda^0$. Then the composite

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

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

($\Longrightarrow$)
This direction is clear. □

Definition 10.2.3. A ring R is *Noetherian* if every ideal has ACC. It is *Artinian* if every ideal has DCC.

Proposition 10.2.4. *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 (2). 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 10.2.5.

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

2. Let $R = \mathbb{C}[x_1, x_2, \ldots]$. 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. Thus, not all integral domains are Noetherian.

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 $f \cdot a \equiv f(0)a$. We get a short exact sequence

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

Suppose, toward a 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 a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (x_1, x_2, \ldots) & \longrightarrow & R & \xrightarrow{\mathrm{ev}_0} & \mathbb{C} & \longrightarrow & 0 \\ & & \theta\uparrow & & \phi\uparrow & & \| & & \\ & & \coprod_{t\in T} R & \longrightarrow & \coprod_{s\in S} R & \longrightarrow & \mathbb{C} & \longrightarrow & 0 \end{array}$$

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 10.2.6 (Hilbert's basis). *If $A \in \operatorname{ob}\mathbf{CommRing}$ 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

$$A[x] = \bigcup_{n\geq 0} A[x]_n, \quad A[x]_n \coloneqq \{f \in A[x] : \deg f \leq n\}.$$

Note that each $A[x]_n$ is finitely generated by $1, x, \ldots, x^n$, giving us a surjection $\coprod_{\{0,1,\ldots,n\}} A \twoheadrightarrow A[x]_n$. Since $\coprod_{\{0,1,\ldots,n\}} A$ is Noetherian by Lemma 10.1.6, 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 with generators, say, $\alpha_1, \ldots, \alpha_{k_n}$. Let

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

Claim. *$\widetilde{\Omega}$ 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 that $a, b \neq 0$. 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 $\Omega \ni x^{t-r} f \pm x^{t-s} g = (a \pm b)\, x^t + O(x^{t-1})$, which means 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 with generators, say, $b_1, \ldots, b_s$. 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 $n = \max\{m_i\}$.

Claim. *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 such reasoning to find that

$$f - (\text{some combination of } f_i \text{ with coefficients in } A[x])$$

has degree $\leq n$. That is, there are $g_1, \ldots, g_s \in A[x]$ such that $\deg\left(f - \sum_{i=1}^s g_i f_i\right) \leq n$. But now 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. □

10.3 Lecture 28

Corollary 10.3.1. *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 induct on n. □

Example 10.3.2. Both $\mathbb{Z}[x_1, \ldots, x_n]$ and $k[x_1, \ldots, x_n]$ are Noetherian where k is a field.

Corollary 10.3.3. *If k is a field, then $k[x]$ is a PID, i.e., every ideal of $k[x]$ is generated by exactly one element.*

Corollary 10.3.4. *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 $i : A \hookrightarrow B$. As B is finitely generated as an A-algebra, there exists a map $\phi : A[x_1, \ldots, x_n] \twoheadrightarrow B$ of $A[x_1, \ldots, x_n]$-modules. By Corollary 10.3.1, $A[x_1, \ldots, x_n]$ is Noetherian, which implies that B is the quotient of a Noetherian $A[x_1, \ldots, x_n]$-module. Hence B is also Noetherian as a module over $A[x_1, \ldots, x_n]$. Let $I \trianglelefteq B$ be an ideal. Then I is a submodule over $A[x_1, \ldots, x_n]$ via ϕ and thus is finitely generated as such. It follows automatically that I is also finitely generated as a B-module. □

Definition 10.3.5. 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 $\rho : G \to \operatorname{Aut}_{\mathbf{Set}}(B)$ such that each $\rho_g : B \to B$ is an *algebra isomorphism*, i.e.,

$$\begin{aligned} \rho_g(b_1 + b_2) &= \rho_g(b_1) + \rho_g(b_2) \\ \rho_g(b_1 b_2) &= \rho_g(b_1)\rho_g(b_2) \\ \rho_g(a) &= a. \end{aligned}$$

Theorem 10.3.6 (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*

$$A^G \coloneqq \{a \in A : \forall g \in G . g \cdot a = a\}$$

is 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

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

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

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 $S(a), S(a^2), \ldots, S\left(a^{|G|}\right)$.

Find generators $u_1, \ldots, u_m$ for A over k. Let B denote subalgebra of A^G generated by

$$\left\{S\left(u_i^k\right)\right\}_{i=1,\ldots,m,\ k=1,\ldots,|G|}$$

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 the elements $1, u_i, \ldots, u_i^{|G|-1}$. 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 $0 \leq \alpha_i < |G|$. We thus have

Why can it be written like this?

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

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 $\alpha_i < |G|$, 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. □

11 Projective and injective modules

11.1 Lecture 29

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

Definition 11.1.1. 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 $\phi(M) = \phi(N) + \phi\left(M/N\right)$.

Example 11.1.2. $\dim_k : \mathrm{ob}(\mathbf{Vect}_k) \to \mathbb{Z}$ where k is a field.

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

Definition 11.1.3. An R-module M is called

1. *simple* if it has no proper nontrivial submodules.
2. *indecomposable* if whenever $M = M_1 \coprod M_2$, at least one of M_1 and M_2 is trivial.

Definition 11.1.4. 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

$$0 \longrightarrow F(N) \xrightarrow{F(i)} F(M) \xrightarrow{F(q)} F\left(M/N\right) \longrightarrow 0$$

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 11.1.5.

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

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

Proof. For simplicity, let us verify just 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 it 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

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

Let $\gamma(m) = x'$. 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 $\mathrm{im}(f \circ (-)) = \ker(g \circ (-))$. □

Remark 11.1.6. This proof works for any abelian category.

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

Let us verify just 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 $M \otimes_R (-)$ to it 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

$$h : M \otimes_R X'' \to {}^{M \otimes_R X}\!/_{\mathrm{im}(\mathrm{id}_M \otimes f)}$$

such that the composite $h \circ (\mathrm{id}_M \otimes g) : M \otimes_R X \to {}^{M \otimes_R X}\!/_{\mathrm{im}(\mathrm{id}_M \otimes f)}$ equals the natural projection. Let $h(m \otimes x'') = m \otimes x + \mathrm{im}(\mathrm{id}_M \otimes f)$ for any x such that $g(x) = x''$. Note that

$$g(a) = x'' = g(b) \implies a - b \in \ker g = \mathrm{im}\, f,$$

and thus $m \otimes (a - b) \in \mathrm{im}(\mathrm{id}_M \otimes f)$. As $m \otimes b + m \otimes (a - b) = m \otimes a$, we see that h is well-defined.

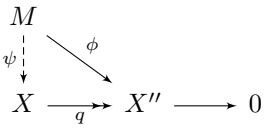
Definition 11.1.7. An R-module M is called

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 that *projective* and *injective* are dual notions.

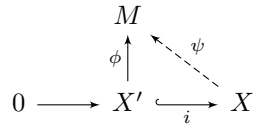
Note 11.1.8.

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



   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



   commutes.

11.2 Lecture 30

Proposition 11.2.1. *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.

($\Longleftarrow$)

To begin, suppose that M is free. Then

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

Pick 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-theoretic function $x : \Lambda \to |X|$. By adjointness, there is some $\psi \in \mathrm{Hom}_{R-\mathbf{Mod}}\left(\coprod_\lambda R, X\right)$ 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

$$\begin{array}{ccccc} M & & & & \\ {\scriptstyle\psi}\downarrow & \searrow^{\phi} & & & \\ X & \xrightarrow[q]{} & X'' & \longrightarrow & 0 \end{array}$$

commutes.

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

$$\begin{array}{ccccc} M & & & & \\ & \searrow^{\phi} & & & \\ X & \xrightarrow[q]{} & X'' & \longrightarrow & 0 \end{array} \tag{η}$$

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

$$\begin{array}{ccccc} M \coprod N & & & & \\ {\scriptstyle f}\downarrow & \searrow^{\phi \coprod 0} & & & \\ X & \xrightarrow[q]{} & X'' & \longrightarrow & 0 \end{array}$$

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

($\Longrightarrow$)

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

$$\begin{array}{ccccc} M & & & & \\ {\scriptstyle s}\downarrow & \searrow^{\mathrm{id}_M} & & & \\ \coprod_m R & \xrightarrow[q]{} & M & \longrightarrow & 0 \end{array}$$

commutes. This means that $M \coprod \ker q \cong \coprod_m R$. □

Definition 11.2.2. 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.

Every module has a free, hence projective, resolution.

Corollary 11.2.3. *Any short exact sequence of R-modules $0 \to X' \to X \to M \to 0$ with M projective splits.*

Proof. We can find a map s such that

$$\begin{array}{ccccc} M & & & & \\ {\scriptstyle s}\downarrow & \searrow^{\mathrm{id}_M} & & & \\ X & \xrightarrow[q]{} & M & \longrightarrow & 0 \end{array}$$

commutes. □

Corollary 11.2.4. *Any short exact sequence of R-modules $0 \to M \to X \to X'' \to 0$ with M injective splits.*

Corollary 11.2.5. *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 $\mathrm{Hom}_R(M_\lambda, -)$ is an exact functor. This implies that the functor $\mathrm{Hom}_R\left(\coprod_\lambda M_\lambda, -\right) \cong \prod_\lambda \mathrm{Hom}_R(M_\lambda, -)$ is exact as well.

($\Longrightarrow$)

As $\coprod_\lambda M_\lambda$ is projective, there is some R-module N such that

$$\left(\coprod_\lambda M_\lambda\right) \coprod N \cong M_\lambda \coprod \left(\coprod_{\alpha \neq \lambda} M_\alpha\right) \coprod N$$

is free. □

Corollary 11.2.6. *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.*

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. We can find a map ψ such that

$$\begin{array}{ccccc} & & M & & \\ & & \uparrow{\scriptstyle \mathrm{id}_M} & \nwarrow^{\psi} & \\ 0 & \longrightarrow & M & \xhookrightarrow[i]{} & N \end{array}$$

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

Example 11.2.7. $\mathbb{Z}$ is *not* injective in **Ab**.

Example 11.2.8.

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

   Proof. Let

   $$\begin{array}{ccccc} & & \mathbb{Q} & & \\ & & \uparrow{\scriptstyle \phi} & & \\ 0 & \longrightarrow & X' & \xhookrightarrow[i]{} & X \end{array}$$

   be an injectivity diagram. The set

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

   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's lemma, there is some maximal element (A, ξ). If $A = X$, then we are done. Suppose, toward a contradiction, that $A \subsetneq X$, i.e., 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 $n_0 > 0$. In this case, set $\tilde{\xi}(x) = \frac{\xi(n_0 x)}{n_0} \in \mathbb{Q}$.

   For each $\tilde{a} \in \tilde{A}$, write $\tilde{a} = a + mx$ for some $a \in A$ and some $m \in \mathbb{Z}$. Let

   $$\tilde{\xi}(\tilde{a}) = \xi(a) + m\tilde{\xi}(x).$$

   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

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

   This confirms that $\tilde{\xi}$ is well-defined. Thus, we have shown that $\left(\tilde{A}, \tilde{\xi}\right) > (A, \xi)$, a contradiction.

   □

Corollary 11.2.9. *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 $\mathbb{Q}_{(p)} \coloneqq \left\{ \frac{n}{p^k} : n \in \mathbb{Z},\ k \geq 0,\ p \text{ prime} \right\}$.