

# Abstract

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

## Contents

<b>1</b>	<b>Group actions</b>	<b>2</b>
1.1	Lecture 1 . . . . .	2
1.2	Lecture 2 . . . . .	4
1.3	Lecture 3 . . . . .	5
1.4	Lecture 4 . . . . .	7
<b>2</b>	<b>Solvable and nilpotent groups</b>	<b>8</b>
2.1	Lecture 5 . . . . .	9
2.2	Lecture 6 . . . . .	12
<b>3</b>	<b>Sylow theorems</b>	<b>13</b>
3.1	Lecture 7 . . . . .	14
3.2	Lecture 8 . . . . .	15
<b>4</b>	<b>Composition series</b>	<b>16</b>
4.1	Lecture 9 . . . . .	16
4.2	Lecture 10 . . . . .	19
4.3	Lecture 11 . . . . .	21
4.4	Lecture 12 . . . . .	24
4.5	Lecture 13 . . . . .	25
<b>5</b>	<b>Group cohomology</b>	<b>28</b>
5.1	Lectures 14 and 15 . . . . .	28
5.2	Lecture 16 . . . . .	32
<b>6</b>	<b>Categories and functors</b>	<b>34</b>
6.1	Lecture 17 . . . . .	34
6.2	Lecture 18 . . . . .	36
6.3	Lectures 19 and 20 . . . . .	37
<b>7</b>	<b>The Yoneda lemma</b>	<b>38</b>
7.1	Lecture 21 . . . . .	40
7.2	Lecture 22 . . . . .	42

<b>8</b>	<b>Adjoint functors</b>	<b>43</b>
8.1	Lecture 23 . . . . .	44
8.2	Lecture 24 . . . . .	47
<b>9</b>	<b>Polynomial rings</b>	<b>48</b>
9.1	Lecture 25 . . . . .	48
<b>10</b>	<b>Noetherian and Artinian modules</b>	<b>50</b>
10.1	Lecture 26 . . . . .	50
10.2	Lecture 27 . . . . .	52
10.3	Lecture 28 . . . . .	56
<b>11</b>	<b>Projective and injective modules</b>	<b>58</b>
11.1	Lecture 29 . . . . .	58
11.2	Lecture 30 . . . . .	60

# 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  $\theta : G \rightarrow \text{Aut}(S)$ .

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

$$(i) \ a(g, a(g', x)) = a(gg', x) \text{ and}$$

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

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

**Definition 1.1.2.** A *right group action* is a function  $b : S \times G \rightarrow S$  such that

$$(i) \ b(b(x, g), g') = b(x, gg') \text{ and}$$

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

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

**Exercise 1.1.3.** Find a homomorphism representing a right group action  $a : S \times G \rightarrow S$ .

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

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

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

**Definition 1.1.4.** Consider a group action  $\theta : G \rightarrow \text{Aut}(S)$ .

1. We say that  $\theta$  is *faithful* or *effective* if it is injective.
2. We say that  $\theta$  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

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

Further, define the *orbit of  $x$*  as

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

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

**Exercise 1.1.5.**

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

*Proof.*

1. This follows from the fact that  $R_a = \{(s, gs) : s \in S, g \in G\}$ .
- 2.

□

**Corollary 1.1.6.** If  $G$  is finite, then  $|\text{Orb}_\theta(x)| = \frac{|G|}{|\text{Stab}_\theta(x)|}$ .

Note that there is a set bijection  $G/\text{Stab}_\theta x \xrightarrow{\cong} \text{Orb}(x)$  given by  $[g] \mapsto gx$  for any  $x \in S$ , even if  $S$  is infinite.

**Example 1.1.7.** Any action  $\theta : G \rightarrow \text{Aut}(S)$  induces the following group actions.

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

**Example 1.1.8.** 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  $G/R : G \rightarrow \text{Aut}(S/R)$  given by  $g \mapsto ([s] \mapsto [gs])$  is an action.

**Example 1.1.9.** Let  $a : G \times S \rightarrow S$  be an action. If  $S = G$ , then we have

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

In general, only (iii) maps elements to automorphisms of  $G$ .

If  $\theta$  denotes conjugation, then we call

$$G/Z(G) \cong \text{Inn}(G) := \text{im}(\theta)$$

the subgroup of *inner automorphisms* of  $G$ , which is a normal subgroup. We call the quotient  $\text{Aut}(G)/\text{Inn}(G)$  the group of *outer automorphisms* of  $G$ , denoted by  $\text{Out}(G)$ .

Let the subgroup  $\text{Aut}_\phi(S) \leq \text{Aut}(S)$  consists of all those automorphisms preserving the structure  $\phi$  of  $S$ . In this case, there is a commutative triangle

$$\begin{array}{ccc} G & \xrightarrow{\theta} & \text{Aut}(S) \\ & \searrow & \downarrow \\ & & \text{Aut}_\phi(S) \end{array}$$

## 1.2 Lecture 2

### Definition 1.2.1.

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

**Example 1.2.2 (The permutation representation).** Set  $S = \{1, \dots, n\}$  and  $G = S_n$ . Then  $\theta^*(x_1, \dots, x_n) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$ , where  $x_i \in X$  for a fixed set  $X$ . If  $X$  is a field, then  $X^S \cong X^n$  is an  $n$ -dimensional vector space and  $\theta^*$  is an  $X$ -linear representation of  $S_n$ .

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

Example 1.2.2 holds for any action  $\theta : F \rightarrow \text{Aut}(S^k)$  where  $k$  is a field. This is called the *regular representation* of  $G$ .

Given an action  $\theta : G \rightarrow \text{Aut}(S)$ , we get an action  $\mathcal{P}(\theta) : G \rightarrow \text{Aut}(\mathcal{P}(S))$  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 1.2.3 (Galois theory).** Let  $f(x) = a_n x^n + \dots + a_0$  over  $\mathbb{Q}$  where  $a_n \neq 0$ . We know that  $f(x) = a_n(x - \beta_1) \cdots (x - \beta_n)$  for some  $(\beta_1, \dots, \beta_n) \in \mathbb{C}^n$ . As it turns out, each  $\beta_i$  has the form  $f(a_0, \dots, a_n)$  for some algebraic function  $f$  if and only if a certain symmetry group of  $\{\beta_i\}$  has a special property (to be covered next semester).

Consider

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

$$\text{Gal}(f) := \{\sigma \in S_n : \exists \text{ bijection } g : \mathbb{Q}[\tilde{\beta}] \rightarrow \mathbb{Q}[\tilde{\beta}] \text{ s.t. } g(F(\beta_1, \dots, \beta_n)) = F(\beta_{\sigma(1)}, \dots, \beta_{\sigma(n)}) \text{ for all } F \in \mathbb{Q}[x_1, \dots, x_n]\}.$$

**Exercise 1.2.4.** Show that  $g : G \rightarrow \text{Aut}(\mathbb{Q}[\tilde{\beta}])$  is a homomorphism where  $G := \{g(\sigma) : \sigma \in \text{Gal}(f)\}$ .

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

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

Now, consider the polynomial  $f(x) \equiv (x^2 - 3)(x^2 - 5)$ , which has roots  $\{\pm\sqrt{3}, \pm\sqrt{5}\}$ . Then  $\text{Gal}(f) \subset S_4$ . Note that  $g \cdot q = q$  for each  $g \in \text{Gal}(f)$  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  $\text{Gal}(f) = \{(1), (12), (34), (12)(34)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ .

### 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  $\theta : G \rightarrow \text{Aut}(S)$  be an action.

1. We say that  $\theta$  is *transitive* if for any  $s, s' \in S$ , there is some  $g \in G$  such that  $g(s) = s'$ .
2. We say that  $\theta$  is *simple* if  $\text{Stab}_{\theta}(x) = \{e\}$  for any  $x \in S$ .
3. If  $\theta$  is both simple and transitive, then it's called a *G-torsor*.

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

**Example 1.3.2.**

1. Consider the action  $\rho : S^1 \rightarrow \text{Aut}(\mathbb{C})$  given by  $\theta \mapsto \rho_{\theta} := (z \mapsto e^{i\theta}z)$ . Then

$$\rho_{\theta} = \begin{bmatrix} \cos(\theta) & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

for each  $\theta$ . Note that  $\text{Orb}_{\rho}(0) = \{0\}$  and  $\text{Orb}_{\rho}(z) = \{w \mid |w| = |z|\}$ . Therefore,  $S^1 \backslash \mathbb{R}^2 = \mathbb{R}_{\geq 0}$ , which induces a map  $\mathbb{C} \rightarrow \mathbb{R}_{\geq 0}$  given by  $z \mapsto |z|$ .

2. Let  $H \leq G$ . Consider the restriction  $\ell \upharpoonright_H : H \rightarrow \text{Aut}(G)$  of the *left translation* action  $\ell$  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  $\sigma$  and  $\tau$  have the same type of cyclic decomposition.
2. Show that there is a natural bijection between  $S_n \backslash_{\text{conj}} S_n$  and the set of unordered partitions of  $\{1, \dots, n\}$ .

**Definition 1.3.4.** Let  $\theta : G \rightarrow \text{Aut}(S)$  and  $\psi : G \rightarrow \text{Aut}(T)$  be actions. A function  $f : S \rightarrow T$  is called *equivariant* or an *intertwiner* for  $\theta$  and  $\psi$  if for each  $g \in G$ , the following commutes.

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

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

Note that  $\theta \cong \psi$  if and only if there exist intertwiners  $f_1 : S \rightarrow T$  and  $f_2 : T \rightarrow S$  such that  $f_1 \circ f_2 = \text{id}_T$  and  $f_2 \circ f_1 = \text{id}_S$ .

**Example 1.3.5.**

1. If  $\theta : G \rightarrow \text{Aut}(S)$  is simply transitive and  $x \in S$ , then  $f_x : G \rightarrow S$  defined by  $g \mapsto \theta(g)(x)$  intertwines  $\theta$  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  $\theta : G \rightarrow \text{Aut}(S)$  be an action and  $K \subset S$  be an orbit. Then  $\theta \upharpoonright_K$  is a transitive action.

**Theorem 1.3.6.** If  $x \in K$ , then  $f_x : G/\text{Stab}_\theta(x) \rightarrow K$  given by  $[g] \mapsto \theta(g)(x)$  is well-defined and an equivariant bijection for  $\theta \upharpoonright_K$  and left translation by  $G$  on  $G/\text{Stab}_\theta(x)$ .

*Proof.* Let  $[g] = [h]$ . Then  $g = hs$  for some  $s \in \text{Stab}_\theta(x)$ . Hence

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

proving that  $f_x$  is well-defined.

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

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

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

□

**Corollary 1.3.7.** *If  $\theta : G \rightarrow \text{Aut}(S)$  is a transitive action, then  $\theta$  is isomorphic to the left translation action of  $G$  on  $G/H$  where  $H$  denotes any chosen stabilizer subgroup  $\text{Stab}_\theta(x)$ .*

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

$$S = \coprod_{\omega \in G \setminus S} \omega$$

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

*such that each  $\theta_\omega$  is isomorphic to the left translation action of  $G$  on  $G/\text{Stab}_\theta(x)$  for any chosen  $x \in S$ .*

**Corollary 1.3.9 (Orbit-stabilizer theorem).** *Let  $G$  be a finite group and  $\theta : G \rightarrow \text{Aut}(S)$  be an action. Then*

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

*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  $\ell$  by  $G$  on  $G/H$*
2. *Show that  $H \trianglelefteq G$  if and only if the kernel of  $\ell$  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  $\ell : G \rightarrow \text{Aut}(G/H)$ . Let  $\omega$  be any orbit of the restricted action  $\ell \upharpoonright_H$ , so that  $|\omega| = \frac{|H|}{|\text{Stab}|}$ . 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,  $\ell \upharpoonright_H$  is trivial, which means that  $H \trianglelefteq G$ .  $\square$

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

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

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

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

*Proof.*

1. This is obvious,
2. The class equation implies that  $|Z(G)| \equiv 0 \pmod{p}$ . Since  $|Z(G)| > 0$ , 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

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

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

Then  $\Delta G$  is the smallest subgroup  $H$  such that  $G/H$  is abelian, so that

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

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

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

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

where  $\tilde{f} : G^{\text{ab}} \rightarrow A$  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.** 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*  $\{e\}$ .

**Definition 2.0.2.** 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 2.0.3.** 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 2.0.4.** 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  $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$  where  $G_{i-1}/G_i \subset Z(G/G_i)$  for each  $1 \leq i \leq n$ .

**Note 2.0.5.**

1. Every quotient and subgroup of a nilpotent group is nilpotent.
2. Every  $p$ -group  $G$  is nilpotent.

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

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

Since any quotient of  $G$  is a  $p$ -group, it has nontrivial center unless it equals  $G$ . Thus, the  $G_i$  form a strictly increasing sequence bounded above by  $G$ . Since  $G$  is finite,  $G = G_k$  for some  $k$ . Note that each  $G_i$  is the pullback of a normal subgroup under the natural projection and thus itself normal in  $G$ , completing our proof.  $\square$

## 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.,  $G := \mathbb{Q}/\mathbb{Z} \cong \mu_\infty$  where  $\mu_\infty$  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  $G = G_0 \supseteq G_1 \cdots \supseteq G_n$ . Choose  $x_i$  that generates each factor  $G_{i-1}/G_i$  for  $1 \leq i \leq n$ . This implies that  $\langle x_i \rangle = G_i$ , 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  $Z(D_n) = \{e, m2^{k-1}\}$ , so that  $D_n/Z(D_n) \cong D_{m2^{k-1}}$ , which by induction we can assume is not nilpotent. Since every quotient of a nilpotent group is nilpotent,  $D_n$  cannot be nilpotent when  $n = 2^k m$  for any  $k \geq 0$ . This proves the claim.  $\square$

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

- (i) Cyclic  $\subsetneq$  Abelian  $\subsetneq$  Nilpotent  $\subsetneq$  Solvable.
- (ii) Cyclic  $\subsetneq$  Polycyclic  $\subsetneq$  Solvable.

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

**Example 2.1.4.** Let  $V$  be a finite-dimensional vector space over  $\mathbb{R}$ . Let  $\omega : V \times V \rightarrow \mathbb{R}$  be a bilinear map on  $V$  such that

- (a)  $\omega$  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  $\omega$  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  $H(V, \omega)/Z(H(V, \omega)) \cong (V, +)$ , which is abelian as a vector space.

This means that  $H(V, \omega)$  is nilpotent yet 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  $\text{GL}_n(k)$ . 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

$f : B_n(k) \rightarrow B_{n-1}(k)$  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  $g : \ker f \rightarrow k^\times$  given by sending this matrix to  $c_n$ . Then  $\ker g$  consists of matrices of the form

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

so that  $\ker g \cong (k^{n-1}, +)$ , which is abelian. Two applications of Exercise 2.0.3(2) show that  $B_n(k)$  is solvable, completing the proof.

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

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

**Lemma 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

$$(i \ j)(j \ k) = (i \ j \ k) \tag{1}$$

$$(i \ j)(k \ l) = (i \ j \ k)(j \ k \ l) \tag{2}$$

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

$\square$

**Lemma 2.1.9.**  $\Delta S_n = A_n$ .

*Proof.* Clearly  $A_n \supset \Delta S_n$ . When  $n = 3$ ,  $S_n \cong C_3$  and  $\Delta S_n$  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  $\Delta S_n$  is normal, it follows that  $\Delta S_n = A_n$ .  $\square$

**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  $A_4 \cong \{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \cong C_2 \times C_2$ . 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  $\Delta A_4$  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  $\Delta A_n \leq S_n$  so that  $\Delta A_n$  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  $n \geq 5$ .

## 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  $\text{Gal}(f)$  is solvable.

**Note 2.2.2.** In the setting of finite groups, we can add information to our chain of implications 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  $\text{Gal}(f) \longleftrightarrow \pi_1(X)$ .

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  $\Gamma$  is a group and  $P$  a property of groups, then we say that  $\Gamma$  is *virtually*  $P$  if there exist a finite subgroup  $F \trianglelefteq \Gamma$  and a subgroup  $I \leq \Gamma$  of finite index so that if  $q : \Gamma \rightarrow \Gamma/F$  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 implications.

- $v.$  Cyclic  $\subsetneq v.$  Abelian  $\subsetneq v.$  Nilpotent =  $v.$  Solvable.
- $v.$  Cyclic  $\subsetneq v.$  Abelian  $\subsetneq v.$  Polycyclic =  $v.$  Solvable.

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

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

**Exercise 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  $|H| = p^k$ .

**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  $|G|$ . Write  $G = Z(G) \coprod_{x \notin Z(G)} C(x)$  as the union of conjugacy classes.

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

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

Case 3: Assume that  $Z(G) = G$ . Then we can apply Theorem 3.2.1 and induction to get a direct product of *p-Sylow subgroups* of  $G$ 's invariant factors, which will be a *p-Sylow subgroup* of  $G$ .  $\square$

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

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

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

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

### 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  $G/S = \coprod (H\text{-orbits})$ , 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  $p \mid |G/S| = m$ , 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  $|gSg^{-1}| = |S|$ .
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  $S \in \text{Syl}_p(G)$ . Then  $N_G(N_G(S)) = N_G(S)$ .*

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

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  $|\bar{h}|$  is also a  $p$ -power. Observe that

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

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

**Exercise 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 there is a fixed point other than  $eH$ .*
2. *Show that  $H \leq N_G(H)$ .*
3. *Show that there is some  $\tilde{H} \leq G$  such that  $|\tilde{H}| = p^{\alpha+1}$  and  $H \leq \tilde{H} \leq G$ .*

*Notation.*

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

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

1.  $n_p(G) \mid m$ .
2.  $n_p(G) \equiv 1 \pmod{p}$ .

*Proof.*

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

□

**Note 3.1.6.** Pick an element  $S \in \text{Syl}_p(G)$ . 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  $q \not\equiv 1 \pmod{p}$ , then  $G \cong C_{pq}$ .

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

## 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  $i = 1, \dots, n-1$ .

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

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

*Proof.* Induct on  $n \geq 1$ . For the base case, notice that  $N = d\mathbb{Z}$  for some integer  $d \neq 0$ , so that  $N \cong \mathbb{Z}$ . For the induction step, suppose that our claim holds for any subgroup  $M \leq \mathbb{Z}^m$  of finite index where  $m < n$ . Set  $M = \langle e_1, \dots, e_{n-1} \rangle \cap N$ . Then

$$\langle e_1, \dots, e_{n-1} \rangle / M \leq \mathbb{Z}^n / N,$$

which is finite. By our induction hypothesis, it follows that  $M \cong \langle e_1, \dots, e_{n-1} \rangle$ .

Find a basis  $(f_1, \dots, f_{n-1})$  for  $M$  and define the surjective group map  $p : \mathbb{Z}^n \rightarrow \mathbb{Z}$  by  $(x_1, \dots, x_n) \mapsto x_n$ . Then  $\ker p = \langle e_1, \dots, e_{n-1} \rangle$ . 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  $f_n = (0, \dots, 0, k) \in \mathbb{Z}^n$ , so that  $p(f_n) = k$ .



Then  $(f_1, \dots, f_n)$  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  $\xi \in \langle f_1, \dots, f_n \rangle$ .

Moreover, given the equation  $0 = a_1f_1 + \dots + a_nf_n$ , we see that  $0 = p(0) = a_nk$ . Since  $f_1, \dots, f_{n-1}$  are linearly independent, it follows that  $a_i = 0$  for each  $i = 1, \dots, n$ . Thus,  $f_1, \dots, f_n$  are linearly independent as well.  $\square$

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

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

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

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

for some integer  $r \geq 0$ .

## 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  $G = G_0 > G_1 > \dots > G_k = \{e\}$  where each  $G_i/G_{i+1}$  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,

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

is a composition series for  $G$ .  $\square$

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  $H \triangleleft G$  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.  $\square$

3.  $\mathbb{Z}$  has no composition series, since no nontrivial subgroup of  $\mathbb{Z}$  is simple.
4. Any  $p$ -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  $\sigma$  can be decomposed into disjoint cycles each of length  $p$ .

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

- (i) two even cycles of equal length or  
(ii) an odd cycle,

then the conjugacy class of  $\sigma$  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

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

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  $\phi \in \text{conj}_{S_n}(\sigma)$ . Write  $\phi = \alpha\sigma\alpha^{-1}$ . Assume that  $\alpha$  is odd. Then there is some odd  $\tau \in Z_{S_n}(\sigma)$ . Note that

$$(\alpha\tau)\sigma(\alpha\tau)^{-1} = \alpha\tau\sigma\tau^{-1}\alpha^{-1} = \alpha\sigma\alpha^{-1} = \phi.$$

But  $\alpha\tau$  is even, completing our proof.  $\square$

We have three cases to consider. First, if  $p = 2$ , then  $\sigma$  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

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

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

How do we proceed if  $H'$  is not simple or finitely generated? If  $G$  is abelian, then we're good, but not otherwise.

Why did we need that whole claim?

Now, if  $|G| = pq$ , then  $\mathbb{Z}/q \xrightarrow{i} F \xrightarrow{\pi} \mathbb{Z}/p$  where  $\text{im}(i) = \ker \pi$ . 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)  $\phi$  is injective,
- (ii)  $\pi$  is surjective, and
- (iii)  $\ker \pi = \text{im}(\phi)$ .

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

$$\ker \phi_i = \text{im}(\phi_{i-1}) \quad (*)$$

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

$$\eta_i : 1 \rightarrow G_{i+1} \rightarrow G_i \rightarrow G_i/G_{i+1} \rightarrow 1.$$

Thus,  $G$  can be built successively from the  $G_i/G_{i+1}$  and  $\eta_i$ .

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  $1 \rightarrow H \xrightarrow{i} G \xrightarrow{q} K \rightarrow 1$  is called *split* if we can find a homomorphism  $s : K \rightarrow G$  such that  $q \circ s = \text{id}_K$ . In symbols,

$$1 \longrightarrow H \xrightarrow{i} G \xrightleftharpoons[s]{q} K \longrightarrow 1.$$

**Example 4.1.8.** Let  $|G| = pq$ . Then  $1 \rightarrow \mathbb{Z}/q \rightarrow G \rightarrow \mathbb{Z}/p$  is split.

If

$$1 \longrightarrow H \xrightarrow{i} G \xrightleftharpoons[s]{q} K \longrightarrow 1.$$

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

## 4.2 Lecture 10

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

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

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.,  $\phi$  is bijective.
- (ii) We have  $xy = yx$  for any  $x \in G_i$  and  $y \in G_j$ , i.e.,  $\phi$  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  $G_i \cap (G_1 \cdots \widehat{G_i} \cdots G_k) = \{e\}$ .
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  $z \mapsto (e^{i\theta}, r)$ . Note also the extension

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

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

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

$\curvearrowright \quad s$

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

3. Let  $\mathrm{Diag}_n$  be the group of diagonal matrices over  $k$ . Then  $\mathrm{Diag}_n \cong \underbrace{k^* \times \cdots \times k^*}_n$ .
4. If  $p$  is prime, then  $\mathbb{Z}/p^2$  is not a product of any nontrivial subgroups. For if  $\mathbb{Z}/p^2 \cong H \times K$ , then  $H \trianglelefteq \mathbb{Z}/p^2$  is nontrivial, so that  $H = \langle x^p \rangle$  where  $\langle x \rangle = \mathbb{Z}/p$ . Similarly,  $K \cong C_p$ . But  $K \neq H$ , contrary to the fact that  $\mathbb{Z}/p^2$  has a unique subgroup of order  $p$ .

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

5. If  $a, b > 0$  are coprime, then  $\mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b$ . Yet,  $S_3 \not\cong \mathbb{Z}/2 \times \mathbb{Z}/3$ , as the subgroup  $s\left(\mathbb{Z}/2\right)$  in

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

$\curvearrowright \quad s$

is *not* normal.

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

**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  $\alpha : K \rightarrow \text{Aut}_{\text{grp}}(H)$  be the inner automorphism of  $H$ , which depends on the group law  $*_G$ . Then  $*_G$  can be recovered from  $*_H$ ,  $*_K$ , and  $\alpha$ .

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

$$g_1 g_2 = (h_1 \alpha_{k_1}(h_2)) k_1 k_2.$$

We are ready to state an equivalent formulation of the notion *semidirect product*. To this end, let  $K$  and  $H$  be groups and  $\alpha : K \rightarrow \text{Aut}(H)$  be a structure-preserving action. Then the *semidirect product of  $K$  with  $H$  along  $\alpha$* , denoted by  $H \rtimes_{\alpha} K$ , is the group with underlying set  $H \times K$  and group law

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

Every semidirect product is naturally a split extension of  $K$  by  $H$ . Indeed, if  $K \rtimes_{\alpha} H$ , then  $i_H : H \rightarrow K \rtimes_{\alpha} H$  is normal and  $p_K : K \rtimes_{\alpha} H \rightarrow K$  is a surjective homomorphism with kernel  $H$ . Hence

$$1 \longrightarrow H \xrightarrow{i_H} K \rtimes_{\alpha} H \xrightarrow{p_K} K \longrightarrow 1$$

$\quad \quad \quad \curvearrowright \quad \quad \quad$   
 $\quad \quad \quad i_K \quad \quad \quad$

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

Conversely, if

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

$\quad \quad \quad \curvearrowright \quad \quad \quad$   
 $\quad \quad \quad s \quad \quad \quad$

is a split extension, then we get an inner automorphism  $\alpha : s(K) \rightarrow \text{Aut}(H)$ . Note that  $s(K)$  is normal if and only if  $\alpha$  is trivial. The map  $\phi : \rtimes_{\alpha} H \rightarrow G$  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

$$\begin{array}{ccccccc} 1 & \longrightarrow & H & \longrightarrow & G_1 & \longrightarrow & K \longrightarrow 1 \\ & & \downarrow \text{id} & & \downarrow \phi & & \downarrow \text{id} \\ 1 & \longrightarrow & H & \longrightarrow & G_2 & \longrightarrow & K \longrightarrow 1 \end{array}$$

commutes.

**Example 4.2.6.**

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

**Exercise 4.2.7.** Recall the Heisenberg group  $H(V, W)$ . Show that  $0 \rightarrow \mathbb{R} \rightarrow H(V, W) \rightarrow V \rightarrow 0$  cannot be split.

**4.3 Lecture 11**

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. Any finite group has both ACC and DCC.
2.  $\mathbb{Z}$  has ACC but not DCC.
3. Given  $p$  prime, let  $G_p := \left\{ z \in \mathbb{C}^* : z^{p^k} = 1 \text{ for some } k \right\}$ . This has DCC but not ACC.
4.  $\mathbb{Q}$  has neither property.

**Exercise 4.3.3.** Prove the following assertions.

1. Given the exact sequence  $1 \rightarrow H \rightarrow G \rightarrow K \rightarrow 1$ , if both  $H$  and  $K$  have ACC and DCC, then so does  $G$ .
2. If  $G = H \times K$  and  $G$  has ACC and DCC, then so do  $H$  and  $K$ .

*Proof.*

- 1.
2. Both  $H$  and  $K$  are normal in  $G$ , and any normal subgroup of either is normal in  $G$ .

□

**Proposition 4.3.4.** If  $G$  has either ACC or DCC, then it can be written as the product of indecomposables.

Why?

*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 but  $G \notin D$ . Set  $H_0 = G$  so that  $H_0 = H_1 \times K_1$  with  $H_1 \notin D$  and  $K_1 \neq \{e\}$ . Proceeding in this way, we can construct  $H_n = H_{n+1} \times K_{n+1}$  with  $H_{n+1} \notin D$  and  $K_{n+1}$  nontrivial. Thus we get a normal series  $G = H_0 > H_1 > H_2 > \dots$ . 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

$$K_1 < K_1 \times K_2 < K_1 \times K_2 \times K_3 < \dots < \dots < G.$$

But this must stabilize as well, a contradiction.  $\square$

**Theorem 4.3.5 (Krull-Schmidt).** *Suppose that  $G$  has ACC and DCC, so that  $G$  is a product of indecomposables*

$$\begin{aligned} G &= A_1 \times \dots \times A_s \\ G &= B_1 \times \dots \times B_t. \end{aligned}$$

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

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

**Definition 4.3.6.** An endomorphism  $\phi$  of  $G$  is *normal* if  $\phi \circ \text{conj}_x = \text{conj}_x \circ \phi$  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  $\phi$  and  $\psi$  are normal, then  $\phi + \psi$  is normal, where  $\phi + \psi$  is given by  $g \mapsto \phi(g)\psi(g)$ .*
5. *If  $G = G_1 \times \dots \times G_k$  and  $p_i$  and  $f_i$  denote projection and inclusion, respectively, then each  $f_i p_i$  is normal. Moreover, for any  $\{a_1, \dots, a_r\} \subset \{1, \dots, k\}$ , 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  $\phi$  is normal, then  $\phi$  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  $G > \phi(G) > \phi^2(G) > \dots$  is a normal series that fails to terminate, a contradiction.

Now suppose that  $\phi$  is not injective. Find 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 to get the chain  $\ker \phi < \ker \phi^2 < \dots$ , which fails to stabilize, a contradiction.  $\square$

**Definition 4.3.9.** An endomorphism  $\phi$  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  $\phi : G \rightarrow G$  is normal, then  $G = K \times H$  where*

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

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

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

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

*Proof.* For each  $n \in \mathbb{N}$ , set  $K_n = \ker \phi^n$  and  $H_n = \text{im } \phi^n$ . This yields a normal series

$$G = H_0 \geq H_1 \geq \dots$$

$$K_1 \leq K_2 \leq \dots \leq G.$$

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  $\phi$ . Note that we've shown  $\phi \upharpoonright_H$  is surjective. By Proposition 4.3.4,  $\phi \upharpoonright_H$  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  $\phi \upharpoonright_K$  is nilpotent. But it's clear that  $(\phi \upharpoonright_K)^a = e$ .  $\square$



## 4.4 Lecture 12

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

**Lemma 4.4.2.** *Suppose that  $G$  is indecomposable and has  $\text{ACC} + \text{DCC}$  and that  $\phi$  and  $\psi$  are endomorphisms such that  $\phi + \psi$  is an endomorphism. Then if  $\phi$  and  $\psi$  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  $\underbrace{\phi \circ \gamma}_U + \underbrace{\psi \circ \gamma}_V = (\phi + \psi) \circ \gamma = \text{id}_G$ . Hence  $U + V = \text{id}_G$ . (We call  $U$  and  $V$  a *normal decomposition* of  $\text{id}_G$ .) We see that  $V + U$  is also a normal decomposition of  $\text{id}_G$  by applying  $(-)^{-1}$  to  $U(x)V(x) = x$  for any  $x \in G$ . Now,  $U^2 + UV = U(U + V) = U = (U + V)U = U^2 + VU$ . This implies that  $UV = VU$ . Hence we can apply the binomial theorem to get

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

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

We finally return to the proof of Krull-Schmidt. Suppose that  $r = 1$ . Let  $p_i : G \rightarrow A_i$  and  $q_j : G \rightarrow B_j$  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  $\sum_{j=1}^t g_j \circ q_j = \text{id}_G$ . Note also that  $p_i \circ f_i = \text{id}_{A_i}$  and  $q_j \circ g_j = \text{id}_{B_j}$ . This gives

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

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  $B_i$ 's so that  $B_j = B_1$ .

Thus,  $G = A_1 \times \cdots \times A_r$  and  $G = B_j \times \cdots \times B_t$ . Further,  $\phi := p_1 \circ g_1 \circ q_1 \circ f_1$  is an automorphism. Let  $\gamma := \phi^{-1}$ . This implies that  $(\gamma \circ p_1 \circ g_1) \circ (q_1 \circ f_1) = \text{id}_{A_1}$ , 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  $\theta := (q_1 f_1)(\gamma p_1 g_1) : B_1 \rightarrow B_1$ , which is normal. We want to check that this is the identity map. It's easy to compute  $\theta^2 = \theta$ . By Fitting,  $\theta$  is either an automorphism or nilpotent. If  $\theta$  is an automorphism, then  $\theta^2 = \theta \implies \theta = \text{id}_{B_1}$ , 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

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

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

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

Define  $\psi : G \rightarrow G$  by

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

which is a normal endomorphism with image equal to  $H$ . Moreover, since  $A_1 \cap (B_2 \times \cdots \times B_t) = \{e\}$ , we have  $\ker \psi = \{e\}$ . Therefore,  $\psi$  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 above argument to see that  $s = t$  and that  $A_i \cong B_i$  up to reindexing.  $\square$

**Corollary 4.4.3.** *Suppose that  $G$  is finite abelian, so that  $G \cong C_{p_1^{k_1}} \times \cdots \times C_{p_n^{k_n}}$ . Then the  $(p_i, k_i)$  are uniquely determined up to reordering.*

Suppose that  $G$  is finite and that

$$\begin{aligned} G &= F^0 G \geq F^1 G \geq \cdots \geq F^s G = \{e\} \\ G &= T^0 G \geq T^1 G \geq \cdots \geq T^t G = \{e\} \end{aligned}$$

are two composition series of  $G$ . Consider the *graded groups*

$$\begin{aligned} \text{gr}_F(G) &\equiv \prod F^i / F^{i+1} \\ \text{gr}_T(G) &\equiv \prod T^i / T^{i+1}. \end{aligned}$$

**Corollary 4.4.4.** *If  $\text{gr}_F(G) \cong \text{gr}_T(G)$ , 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  $\text{gr}_F(G) \cong \text{gr}_T(G)$ .

## 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

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

**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

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

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

$$F^a K := q(F^a G) = F^a G / F^a G \cap \ker q.$$

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

$$\mathrm{gr}_F^i(G) \equiv F^i G / F^{i+1} G.$$

Thanks to Note 4.5.2, there is an induced filtration  $T^\bullet \mathrm{gr}_F^i(G)$ . Similarly, there is an induced filtration  $F^\bullet \mathrm{gr}_T^j(G)$ . Then we get graded pieces  $\mathrm{gr}_T^j \mathrm{gr}_F^i G$  and  $\mathrm{gr}_F^i \mathrm{gr}_T^j G$ . These produce two *bigraded* groups  $\mathrm{gr}_F \mathrm{gr}_T G$  and  $\mathrm{gr}_T \mathrm{gr}_F G$ .

**Lemma 4.5.3 (Zassenhaus or butterfly).** *Suppose that  $G$  is a group with  $A \trianglelefteq \tilde{A} \leq G \geq \tilde{B} \trianglerighteq B$ . Then we have a group isomorphism*

$$A \cdot (\tilde{A} \cap \tilde{B}) /_{A \cdot (\tilde{A} \cap B)} \cong B \cdot (\tilde{A} \cap \tilde{B}) /_{B \cdot (A \cap \tilde{B})}.$$

*Proof.* We know that

$$\begin{aligned} A \trianglelefteq \tilde{A} &\implies A \cap \tilde{B} \trianglelefteq \tilde{A} \cap \tilde{B} \\ B \trianglelefteq \tilde{B} &\implies \tilde{A} \cap B \trianglelefteq \tilde{A} \cap \tilde{B}. \end{aligned}$$

Then

$$D := (A \cap \tilde{B}) \cdot (\tilde{A} \cap B) \cong (\tilde{A} \cap B) \cdot (A \cap \tilde{B})$$

is normal in  $\tilde{A} \cap \tilde{B}$ . Let  $x \in B \cdot (\tilde{A} \cap \tilde{B})$  and write  $x = bc$ . Take  $cD \in \tilde{A} \cap \tilde{B} /_D$ . The map  $f : x \mapsto cD$  is well-defined. Indeed, if  $x = b_1 c_2 = b_2 c_2$ , then  $b_2^{-1} b_1 = c_2 c_1^{-1}$ , so that  $c_2 c_1^{-1} \in B \cap \tilde{A} \cap \tilde{B} = \tilde{A} \cap B \leq D$ , i.e.,  $c_2 D = c_1 D$ .

It's clear that  $f$  is surjective. We show that  $f$  is a homomorphism. Let  $x_1 = b_1 c_1$  and  $x_2 = b_2 c_2$ . Then  $x_1 x_2 = b_1 (c_1 b_2 c_1^{-1}) c_1 c_2$ . Thus,  $f(x_1 x_2) = c_1 c_2 D = (c_1 D)(c_2 D)$ .

Moreover, we compute

$$\begin{aligned} \ker f &= \{x = bc : c \in D\} \\ &= \{x = bc_1 c_2 : c_1 \in A \cap \tilde{B}, c_2 \in \tilde{A} \cap B\} \\ &= \{x = bc_1 c_2 : c_2 \in A \cap \tilde{B}, c_1 \in \tilde{A} \cap B\} \\ &= \{x = bc : c \in A \cap \tilde{B}\} \\ &= B \cdot (A \cap \tilde{B}). \end{aligned}$$

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

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

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

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

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

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

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

Likewise, we can show that

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

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

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

**Theorem 4.5.7 (Schreier refinement theorem).** Suppose that  $\{F^i G\}_{i=0}^s$  and  $\{T^j G\}_{j=0}^t$  are filtrations on  $G$ . Then we can find respective refinements  $\tilde{F}^\bullet G$  and  $\tilde{T}^\bullet G$  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  $\tilde{F}_{i-1}^{(j)} = (F^{i-1} \cap T^j) \cdot F^i$ . Then for any  $q \leq i \leq s$ , we get a filtration

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

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

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

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

$\square$

**Corollary 4.5.8 (Jordan-Holder).** *Any two composition series of  $G$  are equivalent.*

*Proof.* Since each intermediate term in a composition series is a maximal normal subgroup, neither series admits a proper refinement. Hence any refinement must be identical to the original series. This completes our proof thanks to Theorem 4.5.7.  $\square$

## 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  $\text{conj}_{\tilde{x}} : G \rightarrow G$  is a (group) automorphism. Since  $H \trianglelefteq G$ , we thus have an automorphism  $\text{conj}_{\tilde{x}} \upharpoonright_H$ . Hence we get a map  $K \ni x \mapsto \text{conj}_{\tilde{x}} \upharpoonright_H \in \text{Aut}(H)$ . It turns out that distinct lifts of  $x$  induce distinct automorphisms whose difference is an inner automorphism.

Indeed, consider the map  $\alpha^\xi : K \rightarrow \text{Out}(H)$  defined by  $x \mapsto \text{conj}_{\tilde{x}} \cdot \text{Inn}(H)$ . This is well-defined. If  $\tilde{x}$  and  $\tilde{\tilde{x}}$  are distinct lifts of  $x$ , then

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

Moreover,  $\alpha^\xi$  is a homomorphism. If  $x, y \in K$ , then  $\tilde{x}\tilde{y}$  is a lift of  $xy$  since  $q$  is a homomorphism. As  $\text{conj}_{\tilde{x}\tilde{y}} \upharpoonright_H = \text{conj}_{\tilde{x}} \upharpoonright_H \circ \text{conj}_{\tilde{y}} \upharpoonright_H$ , it follows that  $\alpha^\xi(xy) = \alpha^\xi(x)\alpha^\xi(y)$ , as desired.

Now, if  $\xi$  is split via  $s : K \rightarrow G$ , then we get a homomorphism  $\alpha^{\xi, s} : K \rightarrow \text{Aut}(H)$  given by  $x \mapsto \text{conj}_{s(x)} \upharpoonright_H$ . Note that  $\alpha^{\xi, s}(x) \cdot \text{Inn}(H) = \alpha^\xi(x)$ . This implies that

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

commutes.

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

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

**Example 5.1.1.**

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

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

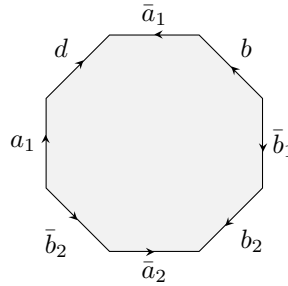
Let  $\phi$  be an automorphism of  $S^3$ . Then  $\phi(a) \in \{a, ab, ab^2\}$  and  $\phi(b) \in \{b, b^2\}$ . Hence  $|\text{Aut}(S_3)| \leq 6$ . But  $S_3 \leq \text{Aut}(S_3)$ , and thus  $\text{Aut}(S_3) = S_3$ .

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

Let  $f : G \rightarrow H$  be a surjective map and  $\phi \in \text{Aut}(G)$  such that  $\phi(\ker f) = \ker f$ . This induces an automorphism  $\phi^f : H \rightarrow H$  given by  $h = f(g) \mapsto f(\phi(g))$ . Note that if  $x \in G$ , then  $\text{conj}_x : G \rightarrow G$  preserves any normal subgroup. Thus, we get a map  $(\text{conj}_x)^f : H \rightarrow H$  given by  $h \mapsto \text{conj}_{f(x)}(h)$ . In general, we have a group map  $\text{Inn}(G) \rightarrow \text{Inn}(H)$ , which in turn induces a group map  $(-)^f : \{\phi \in \text{Aut}(G) : \phi(\ker f) = \ker f\} / \text{Inn}(G) \rightarrow \text{Out}(H)$ .

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

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



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

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

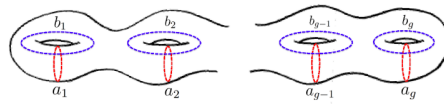


Figure 1: copied from <http://inspirehep.net/record/1352145/plots>

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

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

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

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

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

**Note 5.1.5 (Operations on  $\text{Ext}(\cdot, (A, \alpha))$ ).**

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

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

be an extension. We can use  $\phi$  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  $p : G \times_K L \rightarrow L$  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

$$\begin{array}{ccccccccc} (\xi) : 1 & \longrightarrow & A & \xrightarrow{i} & G & \xrightarrow{q} & K & \longrightarrow & 1 \\ & & \parallel & & \uparrow & & \uparrow \phi & & \\ (\phi^* \xi) : 1 & \longrightarrow & A & \longrightarrow & G \times_K L & \xrightarrow{p} & L & \longrightarrow & 1 \end{array} \quad . \quad (\text{A})$$

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

- (2) Let  $A$  and  $B$  be  $K$  modules and  $\xi$  be as in (A). Let  $\psi : (A, \alpha) \rightarrow (B, \beta)$  be an equivariant map. We construct the *pushout*  $G \cup_A B$  of  $i$  and  $\psi$ .

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

**Claim.** The map  $i \times \psi$  is injective with  $\overbrace{\text{im}(i \times \psi)}^A \trianglelefteq G \ltimes_{\beta \circ q} B$ . 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

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

To see that  $A$  is normal, we compute

$$\begin{aligned}
(g, b)(a, \psi(a))(g, b)^{-1} &= (g, b)(a, \psi(a))(g^{-1}, \beta \circ q(g^{-1})(b^{-1})) \\
&= (ga, b\beta \circ q(g)(\psi(a)))(g^{-1}, \beta \circ q(g^{-1})(b^{-1})) \\
&= (gag^{-1}, b\beta \circ q(g)(\psi(a))\beta \circ q(ga)\beta \circ q(g^{-1})(b^{-1})) \\
&= \left( gag^{-1}, b\beta \circ q(g)(\psi(a))\beta(q(g)\underbrace{q(a)}_1q(g^{-1}))(b^{-1}) \right) \\
&= (gag^{-1}, b\beta \circ q(g)(\psi(a))b^{-1}) \\
&= (gag^{-1}, \beta \circ q(g)(\psi(a))) \\
&= (gag^{-1}, \psi(\alpha \circ q(g)(a))) \\
&= (\alpha \circ q(g)(a), \psi(\alpha \circ q(g)(a))),
\end{aligned}$$

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

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

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 the commutative diagram.

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

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

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

- (3) Given  $\xi, \eta \in \text{Ext}(K, (A, \alpha))$ , we can take  $\xi \times \eta \in \text{Ext}(K \times K, (A \times A, \alpha \times \alpha))$ . The diagonal map  $\Delta : K \rightarrow K \times K$  is a homomorphism, as is the function  $\text{mult} : A \times A \rightarrow A$  since  $A$  abelian. This is also equivariant for  $\alpha \times \alpha$  and  $\alpha$ . Therefore, we can form the following commutative diagram.



$$\begin{array}{ccccccc}
1 & \longrightarrow & A \times A & \longrightarrow & G_\xi \times G_\eta & \longrightarrow & K \times K \longrightarrow 1 \\
& & \parallel & & \uparrow & & \uparrow \Delta \\
1 & \longrightarrow & A \times A & \longrightarrow & (G_\xi \times G_\eta) \times_{K \times K} K & \longrightarrow & K \longrightarrow 1 \\
& & \downarrow \text{mult} & & \downarrow & & \parallel \\
1 & \longrightarrow & A & \longrightarrow & ((G_\xi \times G_\eta) \times_{K \times K} K) \cup_{A \times A} A & \longrightarrow & K \longrightarrow 1
\end{array} \quad (\text{C})$$

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

**Exercise 5.1.6.** Show that

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

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

**Exercise 5.1.7.**

1. Verify that  $(\text{Ext}(K, (A, \alpha)), +)$  is an abelian group with identity  $K \ltimes_\alpha A$ .
2. Verify that  $\phi^*$  and  $\psi_*$  are homomorphisms.

Suppose that  $(\xi) : 1 \rightarrow A \rightarrow G \rightarrow K \rightarrow 1$  is an extension. If it is not split, then by the axiom of choice there is some set-theoretic section  $s : K \rightarrow G$  of  $q$ . Define  $f : K \times K \rightarrow G$  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  $\text{im } f \subset A$ , giving us  $f : K \times K \rightarrow A$ .

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

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

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

Then the diagram

$$\begin{array}{ccccccc}
1 & \longrightarrow & A & \xrightarrow{i_f} & G_f & \xrightarrow{q_f} & K \longrightarrow 1 \\
& & \downarrow & & \downarrow s \times i & & \downarrow \\
1 & \longrightarrow & A & \xrightarrow{i} & G & \xrightarrow{q} & K \longrightarrow 1
\end{array},$$

$\xleftarrow{s}$

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  $f : K \times K \rightarrow A$ , 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

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

**Definition 5.2.3.**

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

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

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

If  $\tilde{s}$  and  $s$  are both normalized sections, then  $c(x) := \tilde{s}(x)s(x)^{-1}$  defines a map  $c : K \rightarrow A$  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  $\delta : C^1_0 \rightarrow Z^2_0$  defined by  $c \mapsto ((x, y) \mapsto c(x)\alpha_x(c(y))c(xy)^{-1})$ , known as the *first Hochschild differential of  $K$  with coefficients in  $(A, \alpha)$* . We in turn obtain a natural map

$$\delta' : \text{Ext}(K, (A, \alpha)) \rightarrow HH^2(K, (A, \alpha)) := Z^2_0 / \text{im } \delta \quad (*)$$

given by  $(\xi, f) \mapsto [f]$ . We call  $HH^2(K, (A, \alpha))$  the *second cohomology group of  $K$  with coefficients in  $(A, \alpha)$* .

**Exercise 5.2.4.** Show that  $\delta'$  is an isomorphism of abelian groups.

**Example 5.2.5.** Let us find all extensions of  $\mathbb{Z}/2 \cong \mathbb{M}_2 := \{\pm 1\}$  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  $\mathbb{Z}$ .

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

Then  $C_0^2 = \{f : \mathbb{M}_2 \times \mathbb{M}_2 \rightarrow \mathbb{Z} \mid f(1, y) = f(x, 1) = 0 \text{ for any } x, y \in \mathbb{M}_2\}$ . 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,  $C_0^1 = \{c : \mathbb{M}_2 \rightarrow \mathbb{Z} : c(1) = 0\} \cong \mathbb{Z}$ , yielding the correspondence

$$\mathbb{Z} \ni b \longleftrightarrow (c : -1 \mapsto b).$$

Then the differential  $\delta : C_0^1 \rightarrow Z_0^2 \cong \mathbb{Z}$  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,  $\delta : \mathbb{Z} \rightarrow \mathbb{Z}$  is given by  $b \mapsto 2b$ . This implies that  $HH^2 = \mathbb{Z}/2$ , so that the only nontrivial extension is precisely

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

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*  $\mathcal{C}$  consists of

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

These data must satisfy the following properties.

- (i)  $\text{mor } \mathcal{C} = \coprod_{x, y \in \text{ob } \mathcal{C}} \text{Hom}_{\mathcal{C}}(x, y)$ .
- (ii) Composition is associative.

- (iii) For each  $x \in \text{ob } \mathcal{C}$ , there is an *identity morphism*  $\text{id}_x : x \rightarrow x$  such that  $f \circ \text{id}_x = f$  and  $\text{id}_x \circ g = g$  for any maps  $f : x \rightarrow y$  and  $g : z \rightarrow x$ .

**Definition 6.1.2.** A morphism  $\phi : A \rightarrow B$  in  $\mathcal{C}$  is an *isomorphism* if  $\psi \circ \phi = \text{id}_A$  and  $\phi \circ \psi = \text{id}_B$  for some morphism  $\psi : B \rightarrow A$ .

**Note 6.1.3.** if  $\mathcal{C}$  is small, then  $(\text{mor } \mathcal{C}, \circ)$  is a partially-defined monoid.

**Example 6.1.4.** The following are examples of categories.

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

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

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

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

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

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

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

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

3. Let **Ouv<sub>X</sub>** denote the category of open sets of the topological space  $X$  with inclusion maps as morphisms.

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

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

**Definition 6.1.5.** Let  $\mathcal{C}$  and  $\mathcal{D}$  be categories. A (covariant) functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  from  $\mathcal{C}$  to  $\mathcal{D}$  consists of two functions  $F : \text{ob } \mathcal{C} \rightarrow \text{ob } \mathcal{D}$  and  $F : \text{mor } \mathcal{C} \rightarrow \text{mor } \mathcal{D}$  such that

- (i)  $F(f) : F(x) \rightarrow F(y)$  in  $\mathcal{D}$  whenever  $f : x \rightarrow y$  in  $\mathcal{C}$  and
- (ii)  $F$  respects both composition and identity.

*Terminology.*

1. We call a covariant functor of the form  $F : \mathcal{C}^{\text{op}} \rightarrow \mathcal{D}$  *contravariant*.
2. We call a contravariant functor  $\mathcal{C} \rightarrow \mathcal{D}$  a *presheaf* of  $\mathcal{C}$  with values in  $\mathcal{D}$ .

## 6.2 Lecture 18

**Example 6.2.1.** The following are examples of functors.

1. The forgetful functor  $\mathbb{G}_A : \mathbf{Ring} \rightarrow \mathbf{Ab}$  is called the *additive group functor*.
2. Let  $f : X \rightarrow Y$  be a map of spaces. Define the *section functor*

$$\begin{aligned} \Gamma_f : \mathbf{Ouv}_Y^{\text{op}} &\rightarrow \mathbf{Set} \\ \mathcal{U} &\mapsto \{s : \mathcal{U} \rightarrow X \mid f \circ s = \text{id}_{\mathcal{U}}\} \\ \Gamma_f(\mathcal{U} \subset V) : (s : V \rightarrow X) &\mapsto (s|_{\mathcal{U}} : \mathcal{U} \rightarrow X). \end{aligned}$$

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

3. Let  $n \geq 0$  be an integer. We have the *homology functor*  $H_n(-, \mathbb{Z}) : \mathbf{Top} \rightarrow \mathbf{Ab}$  sending each space  $X$  to  $H_n(X, \mathbb{Z})$ , the *n-th singular homology of  $X$* .
4. Recall the homotopy functor  $\pi_i : \mathbf{Top}_*^{(\text{conn}, \text{lc})} \rightarrow \begin{cases} \mathbf{Grp} & i = 1 \\ \mathbf{Ab} & i > 1 \end{cases}$ .
5. Define  $(-)_\bullet : \mathbf{Set} \rightarrow \mathbf{sSet}$  by sending each set  $S$  constant/discrete functor  $(S)_\bullet$  at  $S$ , i.e.,  $S_n \equiv S$  for every  $n \geq 0$ . Alternatively, say that an element  $x \in X_n$  is *nondegenerate* if it is *not* of the form  $x = s_i(y)$  for any  $1 \leq i \leq n-1$  and  $y \in X_{n-1}$  and define  $(S)_\bullet$  as the unique simplicial set such that

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

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

6. The geometric realization functor  $|\cdot| : \mathbf{sSet} \rightarrow \mathbf{Top}$ .
7. Define  $\text{Sing}_\bullet : \mathbf{Top} \rightarrow \mathbf{sSet}$  by

$$\begin{aligned} \text{Sing}_n(X) &\equiv \{\phi \mid \phi : \Delta^n \rightarrow X\} & (f : [m] \rightarrow [n]) &\mapsto (\text{Sing}_f(X) : \phi \mapsto \phi \circ \Delta_f) \\ \text{Sing}_n(u : X \rightarrow Y) : \text{Sing}_n(X) &\rightarrow \text{Sing}_n(Y), & \phi &\mapsto u \circ \phi. \end{aligned}$$

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

8. If  $n = 1, 2$ , then we have the functor  $HH^n(G, -) : {}_G\mathbf{Mod} \rightarrow \mathbf{Ab}$  as in  $(\star)$ .

**Example 6.2.2.** The following are examples of natural transformations.

1. The determinant  $\det : \text{GL}_n(\mathbb{F}) \rightarrow \text{GL}_1(\mathbb{F})$ .
2. The *Hurewicz map*  $\text{Hur} : \pi_1 \rightarrow H_1$ .

3. The universal property of  $(-)^{\text{ab}}$  induces a commutative diagram of functors

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

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

The *double dualization* functor  $(-)^{**} : \mathbf{Vect}_k \rightarrow \mathbf{Vect}_k$  induces a map of functors  $\text{id}_{\mathbf{Vect}_k} \rightarrow (-)^{**}$  given component-wise by

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

**Exercise 6.2.3.**

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

**Definition 6.2.4.**

1. We say that a category  $\mathcal{C}$  is *small* if  $\text{ob } \mathcal{C}$  is a set.
2. Let  $\pi_0(\mathcal{C}) := \text{ob } \mathcal{C} / \cong$ . We say that  $\mathcal{C}$  is *essentially small* if  $\pi_0(\mathcal{C})$  is a set.

**Exercise 6.2.5.** Show that  $\mathcal{C}$  is essentially small if and only if it is equivalent to a small category.

### 6.3 Lectures 19 and 20

**Example 6.3.1.** Let  $\mathcal{C} = \mathbf{Vect}_k^n$  and  $\mathcal{D} = B\text{Mat}_n(k)$ . There is a functor  $F : \mathcal{D} \rightarrow \mathcal{C}$  defined on objects by  $* \mapsto k^n$  and on morphisms by  $A \mapsto (v \mapsto Av)$ . Define the functor  $G : \mathcal{C} \rightarrow \mathcal{D}$  with the axiom of choice. Specifically, choose a basis for each space  $V \in \mathcal{C}$  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  $G$ .

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

**Definition 6.3.2.** If  $\mathcal{C}$  is a category, then we call  $\mathcal{A}$  a subcategory of  $\mathcal{C}$  if

- (i)  $\text{ob } \mathcal{A}$  is a subclass of  $\text{ob } \mathcal{C}$ ,
- (ii)  $\text{Hom}_{\mathcal{A}}(x, y) \subset \text{Hom}_{\mathcal{C}}(x, y)$  for any  $x, y \in \text{ob } \mathcal{A}$ , and
- (iii) composition and identity in  $\mathcal{A}$  are exactly as they are in  $\mathcal{C}$ .

**Definition 6.3.3.** Let  $F : \mathcal{C} \rightarrow \mathcal{D}$  be a functor. Consider the set map  $F(-) : \text{Hom}_{\mathcal{C}}(x, y) \rightarrow \text{Hom}_{\mathcal{D}}(F(x), F(y))$ .

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 6.3.4.** The inclusion functor  $i : \mathcal{A} \rightarrow \mathcal{C}$  is faithful.

## 7 The Yoneda lemma

Notice that  $\text{Hom}_{\mathbf{Set}}(*, x) \cong x$  for any set  $x$ . In general, we have the following notion.

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

The class  $\{\text{Hom}_{\mathcal{C}}(y, x)\}_{y \in \text{ob } \mathcal{C}}$  of *y-points* reconstructs  $x$  as an object in  $\mathcal{C}$ . To see this, let  $\widehat{\mathcal{C}} := \mathbf{Fun}(\mathcal{C}^{\text{op}}, \mathbf{Set})$  and  $x \in \text{ob } \mathcal{C}$ . Define the functor  $h_x : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$  on objects and morphisms, respectively, by

$$\begin{aligned} y &\mapsto \text{Hom}_{\mathcal{C}}(y, x) \\ h_x(f) : u &\mapsto u \circ f. \end{aligned}$$

**Definition 7.0.2.** A presheaf  $F \in \widehat{\mathcal{C}}$  is *representable* if  $F \cong h_x$  for some  $x$ . We say that  $x$  *represents*  $F$  in this case.

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

$$h(\phi)_y : \text{Hom}_{\mathcal{C}}(y, x) \rightarrow \text{Hom}_{\mathcal{C}}(y, x'), \quad u \mapsto \phi \circ u.$$

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

**Lemma 7.0.3 (Yoneda).** *Let  $\mathcal{C}$  be a category.*

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

$$\text{Hom}_{\mathcal{C}}(-, -) \cong \text{Hom}_{\widehat{\mathcal{C}}}(h_{(-)}, h_{(-)})$$

*of functors  $\mathcal{C}^{\text{op}} \times \mathcal{C} \rightarrow \mathbf{Set}$ , so that  $h : \mathcal{C} \rightarrow \widehat{\mathcal{C}}$  is fully faithful.*

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

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

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

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

If  $f : x \rightarrow y$  in  $\mathcal{C}$ , then  $h(f)$  is a map  $h_x \rightarrow h_y$  and  $h(f)_z : \text{Hom}_{\mathcal{C}}(z, x) \rightarrow \text{Hom}_{\mathcal{C}}(z, y)$  is given by  $(-) \mapsto f \circ (-)$  for any  $z \in \text{ob } \mathcal{C}$ . In this case,  $h(f)_x(\text{id}_x) = f \circ \text{id}_x = f$ .

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

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

commutes because  $\alpha$  is a natural transformation. By evaluating this at the morphism  $\text{id}_x$ , we see that  $\alpha_z(\phi) = i(\alpha) \circ \phi$ .  $\square$

Let  $F \in \widehat{\mathcal{C}}$ . Recall that  $F$  is representable by  $x$  if there is some isomorphism of functors  $h_x \cong F$ . By the proof of the Yoneda lemma, this is completely determined by the object  $\xi := h_x(\text{id}_x) \in F(x)$ . Conversely, given  $\xi \in F(x)$ , we get a natural map

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

This defines a map of functors  $\eta^\xi : h_x \rightarrow F$  where  $\eta_y^\xi(f) = F(f)(\xi)$  for any  $y \in \text{ob } \mathcal{C}$ .

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

#### Example 7.0.4.

1. Define the presheaf  $\mathcal{P} : \mathbf{Set}^{\text{op}} \rightarrow \mathbf{Set}$  on objects by  $S \mapsto \mathcal{P}(S)$  and on morphisms by  $\mathcal{P}(f : S \rightarrow T) : A \mapsto f^{-1}(A)$ . To see whether  $\mathcal{P}$  is representable, we need to find some set  $Q$  and  $\xi \in \mathcal{P}(Q)$  such that  $\text{Hom}(S, Q) \rightarrow \mathcal{P}(S)$  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  $\text{Hom}(S, \{0, 1\}) \cong \mathcal{P}(S)$  via the characteristic function on  $S$ .
2. Consider the forgetful presheaf  $F : \mathbf{Ring}^{\text{op}} \rightarrow \mathbf{Set}$ . For any unital ring  $R$ , any ring map  $\phi : \mathbb{Z}[t] \rightarrow R$  is determined by the value  $\phi(t)$ . Therefore, the map  $\text{Hom}(R, \rho) \rightarrow R$  given by  $u \mapsto F(u)(\xi)$  is bijective where  $\rho = \mathbb{Z}[t]$  and  $\xi = t$ . Hence  $F$  is represented by  $\mathbb{Z}[t]$ .

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

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



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

$$\begin{array}{ccc} V \times W & \xrightarrow{\xi} & T \\ & \searrow & \downarrow B(u) \\ & & L \end{array}$$

We construct such a pair  $(T, \xi)$  as follows. Let  $\mathcal{F}$  denote the vector space of set maps  $f : V \times W \rightarrow k$  such that  $\text{supp}(f)$  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

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

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  $\xi$  by  $(x, y) \mapsto \delta_{(x,y)} + \mathcal{F}_0$ . 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  $\mathcal{C}$  denote the category of pairs  $(X, \alpha)$  where  $X$  is a topological space with two ordered marked points  $\ell_x$  and  $r_x$  along with a map  $\alpha : X \coprod X \Big/_{\sim} \xrightarrow{\cong} X$  where the first  $r_x$  is equal under  $\sim$  to the second  $\ell_x$ .

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

## 7.1 Lecture 21

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

1. Define the *product functor*  $\mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$  by

$$B \mapsto \prod_{\alpha \in I} \text{Hom}_{\mathcal{C}}(B, A_\alpha), \quad f \mapsto (f_\alpha \mapsto f_\alpha \circ f).$$

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

2. Define the *coproduct functor*  $\mathcal{C} \rightarrow \mathbf{Set}$  by

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

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

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

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

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

$$\prod_{\alpha} A_{\alpha} := P.$$

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

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

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

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

$$\coprod_{\alpha} A_{\alpha} := Q.$$

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

**Example 7.1.2.** Let  $R$  be a unital ring and  $\mathcal{C} = \mathbf{Mod}_R$ , whose objects are precisely the pairs  $(M, \rho)$  where  $M$  is an abelian group and  $\rho$  is a map  $R \rightarrow \mathrm{End}(M)$  satisfying

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

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

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

commutes.

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

**Exercise 7.1.3.**

1. Verify that the direct sum is a categorical coproduct in  $\mathbf{Mod}_R$ .
2. Prove that similar constructions show that arbitrary products and coproducts exist in  $\mathbf{Mod}_G$ , the category of modules over a group  $G$ .

**Definition 7.1.4.** Let  $a \in \text{ob } \mathcal{C}$ . Let  $\mathcal{C}_a$  denote the overcategory  $\mathcal{C}/_a$  and  $\mathcal{C}^a$  denote the undercategory  $^a/\mathcal{C}$ .

1. If  $\{A_\alpha\}$  is a collection of objects in  $\mathcal{C}_a$ , then we call the product of the  $A_\alpha$ 's in  $\mathcal{C}_a$  the *fibered product of the  $A_\alpha$ 's over  $a$* , denoted by  $\prod_a A_\alpha$ .
2. If  $\{A_\alpha\}$  is a collection of objects in  $\mathcal{C}^a$ , then we call the coproduct of the  $A_\alpha$ 's in  $\mathcal{C}^a$  the *fibered coproduct under  $a$* , denoted by  $\coprod_a A_\alpha$ .

**Example 7.1.5.**

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

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

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

$$\coprod_a A_\alpha = \coprod_\alpha A_\alpha / \sim_a$$

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).
- (3)  $\mathbf{Grp}$  inherits arbitrary products and fibered products from  $\mathbf{Set}$ . In Section 7.2, we will construct arbitrary coproducts and fibered coproducts in  $\mathbf{Grp}$ .

**7.2 Lecture 22**

**Theorem 7.2.1.** *The category  $\mathbf{Grp}$  has arbitrary coproducts and fibered coproducts.*

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

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

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \coprod_\alpha G_\alpha \\ s_\alpha \downarrow & \nearrow & \\ G_\alpha & & \end{array}.$$

Finally, set

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

(This used to be called *the amalgamated product of  $G_{\alpha}$  over  $G$* .)  $\square$

**Example 7.2.2.**

- (1) Let  $M$  be a set and  $U, V \subset M$ . We have the inclusions  $i_U : U \cap V \rightarrow U$  and  $i_V : U \cap V \rightarrow V$ . Then  $U \cup V = U \coprod_{U \cap V} V$ , the fibered coproduct of  $U$  and  $V$  under  $U \cap V$ .
- (2) Let  $\mathcal{C} := \mathbf{Top}_*^{\text{conn}, \text{lc}}$  and  $M \in \text{ob } \mathcal{C}$ . 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  $\pi_1 : \mathbf{Top}_*^{\text{conn}, \text{lc}} \rightarrow \mathbf{Grp}$  respects fibered coproducts.

## 8 Adjoint functors

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

**Definition 8.0.1.** Suppose that  $L : \mathcal{C} \rightarrow \mathcal{D}$  and  $R : \mathcal{D} \rightarrow \mathcal{C}$  are functors. We say that  $(L, R)$  is an *adjoint pair of functors* if the bifunctors

$$\text{Hom}_{\mathcal{D}}(L(-), -) : \mathcal{C}^{\text{op}} \times \mathcal{D} \rightarrow \mathbf{Set}$$

$$\text{Hom}_{\mathcal{C}}(-, R(-)) : \mathcal{C}^{\text{op}} \times \mathcal{D} \rightarrow \mathbf{Set}$$

are isomorphic.

Suppose that  $L : \mathcal{C} \rightarrow \mathcal{D}$  is a functor. Then  $L$  induces a functor  $L_* : \widehat{\mathcal{D}} \rightarrow \widehat{\mathcal{C}}$  given by  $F \mapsto F \circ L$ . We can compose  $L_*$  with the Yoneda functor  $h^{\mathcal{D}} : \mathcal{D} \rightarrow \widehat{\mathcal{D}}$  to get  $L_* \circ h^{\mathcal{D}} : \mathcal{D} \rightarrow \widehat{\mathcal{C}}$ . Then  $L$  has a right adjoint  $R$  if and only if for each  $y \in \text{ob } \mathcal{D}$ , the presheaf  $L_* \circ h^{\mathcal{D}}(y) : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$  is representable in  $\mathcal{C}$ . In this case,  $L_* \circ h^{\mathcal{D}} \cong h^{\mathcal{C}} \circ R$ . Then  $L$  has a right adjoint  $R$  if and only if for each  $y \in \text{ob } \mathcal{D}$ , the presheaf  $L_* \circ h^{\mathcal{D}}(y) : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$  is representable in  $\mathcal{C}$ . In this case,  $L_* \circ h^{\mathcal{D}} \cong h^{\mathcal{C}} \circ R$ .

**Proposition 8.0.2.** *The right adjoint is unique up to a unique isomorphism.*

Let  $\mathcal{C} \xrightleftharpoons[R]{L} \mathcal{D}$  be an adjoint pair of functors. Then there is a natural bijection

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

in  $x \in \text{ob } \mathcal{C}$ . This yields a map of functors  $\epsilon : \text{id}_{\mathcal{C}} \rightarrow R \circ L$ , called the *unit of the adjunction*. Likewise, we get a map  $\eta : L \circ R \rightarrow \text{id}_{\mathcal{D}}$ , 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  $\text{id}_L = \eta \circ \epsilon$  and  $\epsilon \circ \eta = \text{id}_R$ .

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

**Example 8.0.4.** Let  $|\cdot| : \mathbf{Grp} \rightarrow \mathbf{Set}$  denote the forgetful functor. Then it is right adjoint to the free group functor  $\text{Fr} : \mathbf{Set} \rightarrow \mathbf{Grp}$ . This means that  $\text{Hom}(\text{Fr}(S), G) \cong \text{Hom}(S, |G|)$  for any set  $S$  and group  $G$ . That is, for any function  $f : S \rightarrow |G|$ , there is a unique homomorphism  $\phi : \text{Fr}(S) \rightarrow G$  such that  $\phi|_S = f$ , where we embed  $S \hookrightarrow \coprod_{s \in S} G_s$  in  $\mathbf{Set}$  by  $s \mapsto \underbrace{1_{G_s}}_{\text{generator}}$ .

*Proof.*

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

□

## 8.1 Lecture 23

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

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

The notion of adjunction is strictly weaker than that of inverse. For example,  $\mathbf{Grp}$  and  $\mathbf{Set}$  cannot be equivalent, for  $\emptyset \in \mathbf{Set}$ . Also,  $\mathbf{Ab}$  and  $\mathbf{Grp}$  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.**  $(-)^{\text{ab}}$  has no left adjoint.

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

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

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  $F(A)^{\text{ab}} = \{e\}$ . But, in this case,

$$\{e\} \not\cong \text{Hom}_{\mathbf{Grp}}(F(A), F(A)) \cong \text{Hom}_{\mathbf{Ab}}(A, \{e\}) \cong \{e\},$$

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  $G^{\text{ab}} = \{e\}$ . Then we have  $\text{Hom}_{\mathbf{Grp}}(C_p, G) \cong \text{Hom}_{\mathbf{Ab}}(A, \{e\}) \cong \{e\}$ . But  $C_p \leq G$ , so that  $\text{Hom}_{\mathbf{Grp}}(C_p, G)$  is nontrivial, a contradiction.  $\square$

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

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

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

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

(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

$$\{e\} \not\cong \text{Hom}_{\mathbf{Grp}}(F(A), F(A)/M) \cong \text{Hom}_{\mathbf{Ab}}(A, (F(A)/M)^{\text{ab}}) \cong \{e\},$$

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).  $\square$

Now, we have

$$\text{Hom}_{\mathbf{Grp}}(F(C_2), C_2) \cong \text{Hom}_{\mathbf{Ab}}(C_2, C_2) = \{0, \text{id}\}.$$

Hence there is some group map  $f : F(C_2) \rightarrow C_2$  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).  $\square$

**Lemma 8.1.4.** *If  $f : S \rightarrow T$  is a surjective group map, then so is  $\text{Fr}(f) : \text{Fr}(S) \rightarrow \text{Fr}(T)$ .*

*Proof.* If  $g$  is a section of  $f$ , then  $\text{Fr}(g)$  is a section of  $\text{Fr}(f)$ . □

**Lemma 8.1.5.** *Let  $S$  be a set. Then  $\text{Fr}(S)^{\text{ab}} \cong \coprod_{s \in S} G_s$ , a free abelian group on  $S$ . Specifically, since each  $G_s$  is a  $\mathbb{Z}$ -module, we have that*

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

*Proof.* For each  $s \in S$ , define  $\delta_s : S \rightarrow \bigoplus_{s \in S} G_s$  by

$$\delta_s^\alpha = \begin{cases} 1 & \alpha = s \\ 0 & \alpha \neq s. \end{cases}$$

We know that  $\delta_s$  extends to a group homomorphism  $\phi : \text{Fr}(S) \rightarrow \bigoplus_{s \in S} G_s$ . We also have the following commutative diagram.

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

Notice that  $\phi$  must be surjective. Hence  $\phi^{\text{ab}}$  is also surjective.

It remains to show that it is injective. Let  $[x] \in \ker \phi^{\text{ab}}$ . Then we may write

$$[x] = n_1 n_2 \cdots n_r + \text{Fr}(S)'$$

where each  $n_i \in G_i$ . This implies that

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

and thus each  $n_i$  vanishes. Thus,  $[x] = 0$ , and  $\ker \phi^{\text{ab}}$  is trivial. □

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

*Proof.*

( $\Leftarrow$ )

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

( $\Rightarrow$ )

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

$$\begin{aligned} \bigoplus_{s \in S} G_s &\cong \text{Fr}(S)^{\text{ab}} \cong \text{Fr}(T)^{\text{ab}} \cong \bigoplus_{t \in T} G_t \\ &\Downarrow \\ \overbrace{\mathbf{Fun}^{\text{fs}}(S, C_2)}^{\text{functions of finite support}} &\cong \bigoplus_{s \in S} G_s / 2 \bigoplus_{s \in S} G_s \cong \bigoplus_{t \in T} G_t / 2 \bigoplus_{t \in T} G_t \cong \mathbf{Fun}^{\text{fs}}(T, C_2) \end{aligned}$$

But then  $\mathbf{Fun}^{\text{fs}}(S, C_2)$  and  $\mathbf{Fun}^{\text{fs}}(T, C_2)$  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  $(\text{Fr}, |-|)$  yields

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

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

□

## 8.2 Lecture 24

For any group  $G$ , we have

$$\text{Hom}_{\mathbf{Grp}}(\text{Fr}(|G|), G) \cong \text{Hom}_{\mathbf{Set}}(|G|, |G|) \ni \text{id}_{|G|}.$$

Thus, there is a unique group map  $\phi : \text{Fr}(|G|) \rightarrow G$  such that  $\phi \upharpoonright_{|G|} = \text{id}_{|G|}$ . This implies that  $\phi$  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

$$\phi \circ \text{Fr}(i) : \text{Fr}(S) \rightarrow \text{Fr}(|G|) \rightarrow G$$

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

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

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

$$\eta : \text{Fr}(T) \rightarrow \text{Fr}(S) \rightarrow G \rightarrow 1.$$

In this case, we call  $\eta$  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 of a finitely generated group is finitely generated.
2. A subgroup of a finitely generated group need *not* be finitely generated. For example,  $F_2 := \text{Fr}(\{x, y\})$  is finitely generated, but the subgroup  $\{y^k x y^{-k} : k \geq 0\}$  is not.
3. If  $G$  is finitely presentable, then any subgroup of  $G$  is finitely presentable.

**Theorem 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 we have an  $A$ -module  $\bigoplus_{\mathbb{N}} A$ . For each  $k \geq 0$ , consider the element

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

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

Any element  $p$  of  $\bigoplus_{\mathbb{N}} A$  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  $\mathbf{Fun}^{\text{fs}}(S, \mathbb{Z}_{\geq 0})$  is an additive monoid because  $\mathbb{Z}$  is one. We can view its elements as monomials in elements of  $S$ . For any  $s \in S$ , define  $t_s : S \rightarrow \mathbb{Z}_{\geq 0}$  by

$$x \mapsto \begin{cases} 0 & s \neq x \\ 1 & s = x \end{cases}.$$

Then for any  $\xi \in \mathbf{Fun}^{\text{fs}}(S, \mathbb{Z}_{\geq 0})$ , we write

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

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

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

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  $A[S] \in \text{ob } \mathbf{CommRing}$  with  $0_{A[S]}(\xi) = 0$  and

$$1_{A[S]}(\xi) = \begin{cases} 0_A & \xi \neq 0 \\ 1_A & \xi = 0 \end{cases}$$

for each monomial  $\xi$ .

**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  $\sum_{\xi \in \text{supp}(f)} f(\xi) \delta_\xi$ . Let  $\delta_\xi := \prod_{s \in \text{supp}(\xi)} t_s^{\xi(s)}$ , allowing us to write  $f$  instead in the form of a polynomial in several variables, namely

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

**Proposition 9.1.2.**

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

*Proof.* We want a natural bijection  $\text{Hom}_{\mathbf{CommRing}^A}(A[S], B) \cong \text{Hom}_{\mathbf{Set}}(S, |B|)$  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  $\hat{\theta} : S \rightarrow |B|$  by  $s \mapsto \theta(t_s)$ . Conversely, given a set map  $\phi : S \rightarrow |B|$ , define the ring map  $\hat{\phi} : A[S] \rightarrow B$  by

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

□

2. Any set inclusion  $T \subset S$  induces 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  $\xi$  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.  $\deg(fg) \leq \deg(f) + \deg(g)$ .

**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  $\deg(fg) = \deg(f) + \deg(g)$ .  $\square$

**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  $(B, i : A \rightarrow B)$  in the under category  $\mathbf{CommRing}^A$ . 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  $A[S] \rightarrow B$  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* if  $A[T] \rightarrow B$  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 Lemma 8.1.6.  $\square$

## 10 Noetherian and Artinian modules

### 10.1 Lecture 26

Suppose that  $A$  is an abelian group. Then  $(\text{End}(A), +, \circ)$  is a ring. Now, let  $R$  be a unital ring. Then a (left)  $R$ -module is a pair  $(A, \rho)$  where  $A$  is an abelian group and  $\rho : R \rightarrow \text{End}(A)$  is a ring homomorphism. This agrees with the usual definition of an  $R$ -module in terms of an action map  $\alpha : R \times A \rightarrow A$  where we set  $\rho(r)(a) = \alpha(r, a)$ .

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

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

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

Furthermore, let  $R^{\text{op}}$  denote the ring obtained from revering the multiplication on  $R$ . Then a *right  $R$ -module* is a pair  $(A, \rho)$  where  $A$  is an abelian group and  $\rho : R^{\text{op}} \rightarrow \text{End}(A)$  is a ring homomorphism. This is equivalent to defining an action map  $\alpha : A \times R \rightarrow A$  by  $\alpha(a, r) = \rho(r)(a)$ . The category of right  $R$ -modules is denoted by  $R^{\text{op}}\text{-}\mathbf{Mod}$ .

Finally, the category of  *$R$ -bimodules* is denoted by  $R\text{-}\mathbf{Mod}\text{-}R$  or  $R \otimes_{\mathbb{Z}} R^{\text{op}}\text{-}\mathbf{Mod}$ . Note that any ring is a bimodule over itself via left and right multiplication.

**Note 10.1.1.** Let  $M$  be an  $R$ -module. Let  $\{M_\alpha\}_{\alpha \in A}$  be a collection of submodules of  $M$  and  $i_\alpha$  denote inclusion.

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

2. We have

$$(i_\alpha) \in \prod_\alpha \text{Hom}_{R\text{-}\mathbf{Mod}}(M_\alpha, M) = \text{Hom}_{R\text{-}\mathbf{Mod}}\left(\prod_\alpha M_\alpha, M\right).$$

Let  $\sum_\alpha M_\alpha = \text{im}(i_\alpha)$ . Then

$$\sum_\alpha M_\alpha = \left\{ \sum_\alpha m_\alpha : m_\alpha \in M_\alpha, m_\alpha \neq 0 \text{ for at most finitely many } \alpha \right\}.$$

3. Let  $S \subset M$  be any subset. We call  $\coprod_{s \in S} R$  the *free  $R$ -module generated by  $S$* . We have a natural map  $g : \coprod_{s \in S} R \rightarrow M$  given by  $(r_s) \mapsto \sum_s r_s s$ . We say that  $R \cdot S := \text{im } g$  is the *submodule of  $M$  generated by  $S$* .

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

**Definition 10.1.2.** Let  $M$  be an  $R$ -module. Then  $M$  is

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

**Definition 10.1.3.** Let  $M$  be an  $R$ -module. Then  $M$  has

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

**Lemma 10.1.4.** 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.*

The implication (a)  $\implies$  (b) is easy to prove by an iteration argument.

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

**Lemma 10.1.5.** *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  $T$ .  $\square$

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  $x_1, \dots, x_s$  denote the generators. Then each  $x_k \in M_{i_k}$  for some  $i_k$ . Set  $n = \max\{i_k : 1 \leq k \leq s\}$ , so that  $N = M_n$ .  $\square$

**Lemma 10.1.6.** *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

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

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  $r = \max\{k, l\}$ .

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

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

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

Furthermore, we have the short exact sequence.

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

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

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

which fits in the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \xhookrightarrow{i} & M & \xrightarrow{q} & M/N \longrightarrow 0 \\ & & \uparrow \alpha & & \uparrow \phi & & \uparrow \beta \\ 0 & \longrightarrow & \coprod_{s \in S} R & \hookrightarrow & (\coprod_{s \in S} R) \amalg (\coprod_{t \in T} R) & \longrightarrow & \coprod_{t \in T} R \longrightarrow 0 \end{array}.$$

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  $\phi$  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  $M_\lambda$  is nontrivial. If  $P$  denotes any of the three finiteness properties, then  $\coprod_{\lambda \in \Lambda} M_\lambda$  has  $P$  if and only if each  $M_\lambda$  has  $P$  and  $\Lambda$  is finite.*

*Proof.* For the forward direction, suppose that  $\coprod_{\lambda} M_\lambda$  has  $P$ . Each projection  $\pi_\lambda$  onto  $M_\lambda$  is a surjection, and  $P$  is preserved by quotients. Hence each  $M_\lambda$  has  $P$ . Now, suppose, toward a contradiction, that  $\Lambda$  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, apply 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  $x_i = \phi(0, \dots, \underbrace{1}_{i\text{-th spot}}, \dots, 0)$ . We can write  $x_i = (x_{i_\lambda})_{\lambda \in \Lambda}$ . Let

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

Note that  $\Lambda^0$  is finite, so 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.

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

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

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

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

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 the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & (x_1, x_2, \dots) & \longrightarrow & R & \xrightarrow{\text{ev}_0} & \mathbb{C} \longrightarrow 0 \\ & & \uparrow \theta & & \uparrow \phi & & \parallel \\ & & \coprod_{t \in T} R & \longrightarrow & \coprod_{s \in S} R & \longrightarrow & \mathbb{C} \longrightarrow 0 \end{array}$$

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

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

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

Note that each  $A[x]_n$  is finitely generated by  $1, x, \dots, x^n$ , giving us a surjection  $\coprod_{\{0,1,\dots,n\}} A \twoheadrightarrow A[x]_n$ . Since  $\coprod_{\{0,1,\dots,n\}} A$  is Noetherian by Lemma 10.1.5, 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,  $\alpha_1, \dots, \alpha_{k_n}$ . Let

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



**Claim.**  $\tilde{\Omega}$  is an ideal in  $A$ .

*Proof.* Let  $a, b \in \tilde{\Omega}$ . If  $a = 0$  or  $b = 0$ , then  $a + b \in \tilde{\Omega}$ . 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  $a \pm b \in \tilde{\Omega}$ .

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

It follows that  $\tilde{\Omega}$  is a finitely generated  $A$ -module with generators, say,  $b_1, \dots, b_s$ . For each  $i = 1, \dots, s$ , 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.**  $\Omega$  is generated by  $\{\alpha_1, \dots, \alpha_{k_n}, f_1, \dots, f_s\}$  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  $\beta \in \tilde{\Omega}$ . 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  $g_1, \dots, g_s \in A[x]$  such that  $\deg(f - \sum_{i=1}^s g_i f_i) \leq n$ . But now we're done because  $f - \sum_{i=1}^s g_i f_i \in \Omega \cap A[x]_n$ . □

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

### 10.3 Lecture 28

**Corollary 10.3.1.** If  $A \in \text{ob CommRing}$  is Noetherian, then  $A[x_1, \dots, x_n]$  is also Noetherian.

*Proof.* We have that  $A[x_1, \dots, x_n] \cong A[x_1, \dots, x_{n-1}][x_n]$ . Now induct on  $n$ . □

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

**Corollary 10.3.3.** If  $k$  is a field, then  $k[x]$  is a PID.

**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  $\phi : A[x_1, \dots, x_n] \twoheadrightarrow B$  of  $A[x_1, \dots, x_n]$ -modules. By Corollary 10.3.1,  $A[x_1, \dots, x_n]$  is Noetherian, which implies that  $B$  is the quotient of a Noetherian  $A[x_1, \dots, x_n]$ -module. Hence  $B$  is also Noetherian as a module over  $A[x_1, \dots, x_n]$ . Let  $I \trianglelefteq B$  be an ideal. Then  $I$  is a submodule over  $A[x_1, \dots, x_n]$  via  $\phi$  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  $A \in \text{ob } \mathbf{CommRing}$ ,  $B$  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  $\rho : G \rightarrow \text{Aut}_{\mathbf{Set}}(B)$  such that each  $\rho_g : B \rightarrow B$  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  $(|G|, \text{char}(k)) = 1$ , then

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

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  $\text{char}(k)$ , we know that  $|G|$  is invertible in  $A$ . Define the algebra homomorphism

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

Let  $a \in A$ . Then

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

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  $x_1, \dots, x_k$ . If  $n \in \mathbb{N}$ , then define the  $n$ -th Newton sum as  $P_n \equiv x_1^n + \dots + x_k^n$ .

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

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

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

over  $k$ . For each  $i$ , observe that  $X_{u_i}(x) \in B[x]$  and that  $X_{u_i}(u_i) = 0$ . It follows that  $u_i^{|G|}$  can be written as a  $B$ -combination of the elements  $1, u_i, \dots, u_i^{|G|-1}$ . This implies that any monomial of the form  $u_1^{s_1} \dots u_m^{s_m}$  can be written as a  $B$ -combination of monomials of the form  $u_1^{\alpha_1} \dots u_m^{\alpha_m}$  where  $0 \leq \alpha_i < |G|$ . We thus have

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

If  $a \in A^G$ , then

$$a = S(a) = \sum_{\alpha} S(\phi_\alpha) S(u^\alpha) = \sum_{\alpha} \phi_\alpha S(u^\alpha).$$

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

## 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  $R\text{-Mod}$ .

**Definition 11.1.1.** An *additive invariant of modules* is a class function  $\phi : \text{ob}(R\text{-Mod}) \rightarrow \mathbb{Z}$  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.**  $\dim_k : \text{ob}(\mathbf{Vect}_k) \rightarrow \mathbb{Z}$  where  $k$  is a field.

We have exact analogues of the Jordan-Holder and Krull-Schmidt theorems for  $R\text{-Mod}$ . Define the *length of  $M$*  as the length of any composition series of  $M$ . By the Jordan-Holder theorem, the length function  $\lambda : \text{ob}(R\text{-Mod}) \rightarrow \mathbb{Z} \cup \{\infty\}$  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  $M = M_1 \amalg M_2$ , at least one of  $M_1$  and  $M_2$  is trivial.

**Definition 11.1.4.** Let  $R$  and  $S$  be rings and  $F : R\text{-Mod} \rightarrow S\text{-Mod}$  be a functor. Let  $M$  and  $N$  be  $R$ -modules. We say that  $F$

1. is *additive* if  $F : \text{Hom}(M, N) \rightarrow \text{Hom}(F(M), F(N))$  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  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  of  $R$ -modules, the sequence  $0 \rightarrow F(M') \rightarrow F(M) \rightarrow F(M'')$  (resp.  $F(M') \rightarrow F(M) \rightarrow F(M'') \rightarrow 0$ ) of  $S$ -modules is also exact.

**Example 11.1.5.**

1. The forgetful functor  $U : R\text{-Mod} \rightarrow \mathbb{Z}\text{-Mod}$  is both additive and exact.
2. If  $R$  is a ring, then the functors  $\text{Hom}_R(M, -) : R\text{-Mod} \rightarrow \mathbb{Z}\text{-Mod}$  and  $\text{Hom}_R(-, M) : R\text{-Mod}^{\text{op}} \rightarrow \mathbb{Z}\text{-Mod}$  are both left exact.

*Proof.* For simplicity, let us verify just that  $\text{Hom}_R(M, -)$  is left exact. Let

$$0 \longrightarrow X' \xrightarrow{f} X \xrightarrow{g} X'' \longrightarrow 0$$

be a short exact sequence of  $R$ -modules. Apply  $\text{Hom}_R(M, -)$  to it to get a sequence of abelian groups

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

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

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

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

*Remark 11.1.6.* This proof works for any abelian category.

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

Let us verify just that  $M \otimes_R (-) : R^{\text{op}}\text{-}\mathbf{Mod} \rightarrow \mathbb{Z}\text{-}\mathbf{Mod}$  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

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

If  $m \otimes x'' \in M \otimes_R X''$ , then there is some  $x \in X$  such that  $g(x) = x''$ , so that  $\text{id}_M \otimes g(m \otimes x) = m \otimes x''$ . Hence  $\text{id}_M \otimes g$  is surjective.

To show that  $\text{im}(\text{id}_M \otimes f) = \ker(\text{id}_M \otimes g)$ , it is enough to construct a map of modules

$$h : M \otimes_R X'' \rightarrow M \otimes_R X / \text{im}(\text{id}_M \otimes f)$$

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

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

and thus  $m \otimes (a - b) \in \text{im}(\text{id}_M \otimes f)$ . 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  $\text{Hom}_R(M, -)$  is exact (i.e., right exact).

2. *injective* if  $\text{Hom}_R(-, M)$  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  $\text{Hom}_R(M, -)$  preserves epimorphisms  $X \xrightarrow{q} X'' \rightarrow 0$ . That is, for any map  $\phi : M \rightarrow X''$ , there is some map  $\psi$  such that

$$\begin{array}{ccc} M & & \\ \psi \downarrow & \searrow \phi & \\ X & \xrightarrow{q} & X'' \longrightarrow 0 \end{array}$$

commutes.

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

$$\begin{array}{ccccc} & & M & & \\ & & \uparrow \phi & \nwarrow \psi & \\ 0 & \longrightarrow & X' & \xrightarrow{i} & X \end{array}$$

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.*

( $\Leftarrow$ )

To begin, suppose that  $M$  is free. Then

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

Pick a basis  $(m_\lambda)$  for  $M$ . Let  $X \xrightarrow{q} X'' \rightarrow 0$  be an exact sequence of  $R$ -modules. Let  $\phi : M \rightarrow X''$  be a homomorphism. For each  $\lambda$ , find some lift  $x_\lambda \in X$  of  $\phi(m_\lambda)$ . Then the assignment  $\lambda \mapsto x_\lambda$  determines a set-theoretic function  $x : \Lambda \rightarrow |X|$ . By adjointness, there is some  $\psi \in \text{Hom}_{R\text{-Mod}}(\coprod_{\lambda} R, X)$  such that  $\psi(m_\lambda) = x_\lambda$ . Explicitly, if  $a \in M$ , then  $a = \sum_{\lambda} a_{\lambda} m_{\lambda}$  where  $a_{\lambda} \in R$ . Then  $\psi(a) = \sum_{\lambda} a_{\lambda} x_{\lambda}$ . This implies that  $q(\psi(a)) = \sum_{\lambda} a_{\lambda} \phi(m_{\lambda}) = \phi(a)$ . It follows that

$$\begin{array}{ccc} M & & \\ \psi \downarrow & \searrow \phi & \\ X & \xrightarrow{q} & X'' \longrightarrow 0 \end{array}$$

commutes.

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

$$\begin{array}{ccc} M & & \\ & \searrow \phi & \\ X & \xrightarrow{q} & X'' \longrightarrow 0 \end{array} \quad (\eta)$$

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

$$\begin{array}{ccc} M \amalg N & & \\ f \downarrow & \searrow \phi \amalg 0 & \\ X & \xrightarrow{q} & X'' \longrightarrow 0 \end{array}$$

commutes. Define  $\psi : M \rightarrow X$  as the composite  $M \hookrightarrow M \amalg N \xrightarrow{f} X$ . Then  $\psi$  fills  $(\eta)$ .

( $\Rightarrow$ )

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

$$\begin{array}{ccc} M & & \\ s \downarrow & \searrow \text{id}_M & \\ \amalg_m R & \xrightarrow{q} & M \longrightarrow 0 \end{array}$$

commutes. This means that  $M \amalg \ker q \cong \amalg_m R$ . □

**Definition 11.2.2.** Let  $M$  be an  $R$ -module. A *projective resolution* of  $M$  is an exact sequence of  $R$ -modules

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

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  $0 \rightarrow X' \rightarrow X \rightarrow M \rightarrow 0$  with  $M$  projective splits.

*Proof.* We can find a map  $s$  such that

$$\begin{array}{ccc} M & & \\ s \downarrow & \searrow \text{id}_M & \\ X & \xrightarrow{q} & M \longrightarrow 0 \end{array}$$

commutes. □

**Corollary 11.2.4.** Any short exact sequence of  $R$ -modules  $0 \rightarrow M \rightarrow X \rightarrow X'' \rightarrow 0$  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  $M_\lambda$  is projective.*

*Proof.*

( $\Leftarrow$ )

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

( $\Rightarrow$ )

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  $M_\lambda$  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  $0 \rightarrow M \hookrightarrow N$  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  $\psi$  such that

$$\begin{array}{ccccc} & & M & & \\ & \text{id}_M \uparrow & \swarrow \psi & & \\ 0 & \longrightarrow & M & \xhookrightarrow{i} & N \end{array}$$

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  $\mathbf{Ab}$ .

**Example 11.2.8.**

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

*Proof.* Let

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

be an injectivity diagram. The set

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

is nonempty and partially ordered by  $\leq$  where  $(A_1, \xi_1) \leq (A_2, \xi_2)$  if  $A_1 \subset A_2$  and  $\xi_1 = \xi_2 \upharpoonright_{A_1}$ . By Zorn's lemma, there is some maximal element  $(A, \xi)$ . 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  $\xi : A \rightarrow \mathbb{Q}$  to a homomorphism  $\tilde{\xi} : \tilde{A} \rightarrow \mathbb{Q}$  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  $\tilde{\xi}(x) = \frac{\xi(n_0x)}{n_0} \in \mathbb{Q}$ .

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  $\tilde{\xi}(\tilde{a}) = \xi(a) + \frac{m\xi(n_0x)}{n_0}$ . 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

$$\begin{aligned} 0 &= \xi(a - b) - \xi((k - m)x) = \xi(a) - \xi(b) - \xi(dn_0x) \\ &= \xi(a) - \xi(b) - \tilde{\xi}(dn_0x) = \xi(a) - \xi(b) - dn_0\tilde{\xi}(x) \\ &= \xi(a) - \xi(b) - (k - m)\tilde{\xi}(x) = \xi(a) - \xi(b) + \frac{m - k}{n_0}\xi(n_0x) \\ &= \tilde{\xi}(a + mx) - \tilde{\xi}(b + kx). \end{aligned}$$

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

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