Math 210A Lecture Notes

Professor: Romyar Sharifi
Scribe: Daniel Raban

Contents

1 Introduction to Category Theory **5**
- 1.1 Categories and subcategories . . . 5
- 1.2 Monoids and groups . . . 6
- 1.3 Rings, fields, and modules . . . 7

2 Morphisms, Functors, and Commutative Diagrams **8**
- 2.1 Types of morphisms . . . 8
- 2.2 Functors . . . 8
- 2.3 Diagrams . . . 9
- 2.4 Yoneda Embedding . . . 10

3 The Yoneda Lemma **11**
- 3.1 Two versions of the Yoneda lemma . . . 11
- 3.2 Partially ordered sets . . . 12

4 Limits and colimits **13**
- 4.1 Limits . . . 13
- 4.2 Colimits . . . 14

5 Equivalences, Cayley's Theorem, and More Limits **17**
- 5.1 Equivalence of categories . . . 17
- 5.2 Cayley's theorem . . . 17
- 5.3 Completeness . . . 18
- 5.4 Initial and terminal objects . . . 18
- 5.5 Sequential limits and colimits . . . 19

6 Inverse Limits, Direct Limits, and Adjoint Functors **20**
- 6.1 Inverse and direct limits . . . 20
- 6.2 Adjoint functors . . . 21

7 Representable Functors and Free Groups **23**
7.1 Representable functors 23
7.2 Free groups 23

8 Free Groups, Normal Subgroups, and Quotient Groups **25**
8.1 Free groups 25
8.2 Normal subgroups and quotient groups 26

9 Equalizers, Kernels, and Ideals **27**
9.1 Equalizers and coequalizers 27
9.2 Kernels and ideals 29

10 Images, Coimages, and Generating Sets **31**
10.1 Images 31
10.2 Coimages 32
10.3 Generating sets 33

11 Group Presentations and Automorphisms **34**
11.1 Cyclic groups and principal ideals 34
11.2 Presentations of groups 34
11.3 Automorphism groups 35

12 Automorphisms, Lagrange's Theorem, Isomorphism Theorems, and Semidirect Products **37**
12.1 Automorphisms and Lagrange's theorem 37
12.2 The second and third isomorphism theorems 38
12.3 Semidirect products 38

13 Krull-Schmidt, Structure of Finitely Generated Abelian Groups, and Group Actions **40**
13.1 The Krull-Schmidt theorem 40
13.2 The structure theorem for finitely generated abelian groups 40
13.3 Group actions 41

14 Orbit-Stabilizer and Symmetric Groups **43**
14.1 The orbit-stabilizer theorem 43
14.2 Action of symmetric groups 43
14.3 Alternating groups 44

15 Simple Groups, Burnside's Formula, and p-Groups **46**
15.1 Simple groups 46
15.2 Burnside's formula 46

15.3 p-groups . . . 48

16 Sylow Theorems **50**
16.1 Sylow p-subgroups . . . 50
16.2 Sylow theorems . . . 50

17 Applications of the Sylow theorems **52**
17.1 Groups of order p^n, pq, and p^2q . . . 52
17.2 Subgroups of S_n . . . 52

18 Composition Series **54**
18.1 Restrictions on simple groups . . . 54
18.2 Composition series . . . 54

19 The Jordan-Hölder Theorem and Solvable Groups **56**
19.1 The Jordan-Hölder theorem . . . 56
19.2 Solvable groups . . . 56

20 Schreier's Refinement Theorem and Nilpotent Groups **58**
20.1 Schreier's refinement theorem . . . 58
20.2 Nilpotent groups . . . 58

21 Frattini's Argument and Characterizations of Nilpotent Groups **60**
21.1 Frattini's argument . . . 60
21.2 Characterizations of nilpotent groups . . . 60
21.3 Linear groups . . . 61

22 Properties of Linear Groups **62**
22.1 The special linear group $\mathrm{SL}_n(F)$ . . . 62
22.2 The projective special linear group $\mathrm{PSL}_n(\mathbb{F}_q)$. . . . 63

23 Principal Ideal Domains, Maximal Ideals, and Prime Ideals **64**
23.1 Group extensions . . . 64
23.2 Simple rings and ideals . . . 64
23.3 Principal ideal domains . . . 65
23.4 Maximal and prime ideals . . . 66

24 Artinian and Noetherian Rings **67**
24.1 Maximal ideals . . . 67
24.2 Artinian and noetherian rings . . . 67

25 Localization of Rings **70**
25.1 Construction and properties 70
25.2 Examples of localizations 71

26 Ideals of Localizations, Hilbert's Basis Theorem, and UFDs **73**
26.1 Ideals of localizations 73
26.2 Hilbert's basis theorem 73
26.3 Unique factorization domains 74

27 Unique Factorization in PIDs and Polynomials, Gauss' Lemma, and Eisenstein's Criterion **75**
27.1 Unique factorization in PIDs 75
27.2 Gauss' lemma and unique factorization of polynomials over a UFD 75
27.3 Eisenstein's criterion 76

1 Introduction to Category Theory

1.1 Categories and subcategories

Definition 1.1. A **category** $\mathcal{C}$ is

1. a class[1] $\mathrm{Obj}(\mathcal{C})$ of **objects**,
2. for each $A, B \in \mathrm{Obj}(\mathcal{C})$, a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ of **morphisms** from A to B (we write $f : A \to B$ for $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$),
3. a composition map $\mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) \to \mathrm{Hom}_{\mathcal{C}}(A, C)$ for all $A, B, C \in \mathrm{Obj}(\mathcal{C})$ (we write this as $(f, g) \mapsto g \circ f$),

such that

1. for each $A \in \mathrm{Obj}(\mathcal{C})$, we have an **identity morphism** $\mathrm{id}_A : A \to A$ such that $f \circ \mathrm{id}_A = f$ and $\mathrm{id}_A \circ g = g$ for all $f : A \to B, g : B \to A$ and $B \in \mathrm{Obj}(\mathcal{C})$.
2. $h \circ (g \circ f) = (h \circ g) \circ f$ for all $f : A \to B, g : B \to C, h : C \to D$ with $A, B, C, D \in \mathrm{Obj}(\mathcal{C})$.

Notation: we usually say $A \in \mathcal{C}$ to mean $A \in \mathrm{Obj}(\mathcal{C})$.

Definition 1.2. A category is **small** if $\mathrm{Obj}(\mathcal{C})$ is a set.

Example 1.1. Set is the category of sets. $\mathrm{Obj}(\mathrm{Set}) = \{\text{sets}\}$. $\mathrm{Hom}_{\mathrm{Set}}(A, B) = \{\text{functions } f : A \to B\}$.

Definition 1.3. A **semigroup** S is a pair $(S, \cdot)$ of a set S and a binary operation $\cdot : S \times S \to S$ on S that is associative. A **homomorphism of semigroups** is a function $f : S \to T$ of semigroups such that $f(a \cdot_S b) = f(a) \cdot_T f(b)$ for all $a, b \in S$.

The idea of a homomorphism is that the function "respects" the operations on S and T. Sometimes, we write ab when we mean $a \cdot b$.

Example 1.2. The category Semi is the category with objects being semigroups and morphisms being homomorphisms of semigroups.

Definition 1.4. A **subcategory** $\mathcal{D}$ of a category $\mathcal{C}$ is a category with

1. $\mathrm{Obj}(\mathcal{D})$ a subclass of $\mathrm{Obj}(\mathcal{C})$,
2. $\mathrm{Hom}_{\mathcal{D}}(A, B) \subseteq \mathrm{Hom}_{\mathcal{C}}(A, B)$ for all $A, B \in \mathcal{D}$,
3. the composition in $\mathcal{D}$ agrees with the composition in $\mathcal{C}$,
4. the identity $\mathrm{id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ for $A \in \mathcal{D}$ is the identity in $\mathrm{Hom}_{\mathcal{D}}(A, A)$.

Example 1.3. Here is a nonexample. Semi is not a subcategory of Set.

[1] We cannot use sets here because, for example, there is no set of all sets.

1.2 Monoids and groups

Definition 1.5. A **monoid** S is a semigroup with an identity element $e \in S$ such that $ex = x = xe$ for all $x \in S$. A **homorphism of monoids** is a function $f : S \to T$ of monoids such that $f(ab) = f(a)f(b)$ for all $a, b \in S$ and $f(e_S) = e_T$.

Example 1.4. The category Mon is the category with objects being monoids and morphisms being homomorphisms of monoids. Mon is a subcategory of Semi.

Example 1.5. A monoid G gives a category $\mathbb{G}$ with $\mathrm{Obj}(\mathbb{G}) = \{G\}$ and $\mathrm{Hom}_{\mathbb{G}}(G, G) = \{\text{elements of } G\} = G$. For all $g, h \in G$, we define $g \circ h = g \cdot h$.

This goes the other way, as well. If you have a category with one object, then its morphisms form a monoid.

Definition 1.6. A **group** G is a monoid in which every element has an inverse; i.e. for every $g \in G$, there exists a $g^{-1} \in G$ such that $g \cdot g^{-1} = e = g^{-1} \cdot g$.

Example 1.6. Grp is the category of groups. The objects are groups, and the morphisms are homomorphisms of semigroups between groups ("group homomorphisms"). These are also monoid homomorphisms because $f(g) = f(eg) = f(e)f(g)$ implies that $e = f(e)$ by multiplication by $f(g)^{-1}$. Also, $e = f(gg^{-1}) = f(g)f(g^{-1})$ implies that $f(g^{-1}) = f(g)^{-1}$.

Definition 1.7. A subcategory $\mathcal{D}$ of a category $\mathcal{C}$ is **full** if $\mathrm{Hom}_{\mathcal{D}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$ for all $A, B \in \mathcal{D}$.

Example 1.7. Grp is a full subcategory of Semi.

Definition 1.8. A group G is **abelian** if its operation is commutative; i.e. $gh = hg$ for all $g, h \in G$.

Example 1.8. Ab is the category of abelian groups. This is a full subcategory of Grp. with objects the abelian groups.

Notation: If the operation on a group is $+$, then the group is assumed to be abelian. The identity element is denoted 0, and the inverse of a is denoted $-a$.

Definition 1.9. **Cyclic groups** are the groups $\langle x \rangle$ consisting of powers

$$x^n = \begin{cases} x \cdots x & n > 0 \\ e & n = 0 \\ (x^{-n})^{-1} & n < 0 \end{cases}$$

of a single element.

Example 1.9. $\mathbb{Z} = \langle 1 \rangle$, and $\mathbb{Z}/n\mathbb{Z} = \langle 1 \pmod{n} \rangle = \{\text{integers} \pmod{n}\}$.

Definition 1.10. A **ring** R is a triple $(R, +, \cdot)$ of an abelian group $(R, +)$ and an associative operation $\cdot$ on R with identity denoted 1 such that the distributive laws $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ hold. A **ring homomorphism** is a function $f : R \to R'$ of rings such that $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$, and $f(1) = 1$ for all $x, y \in R$.

1.3 Rings, fields, and modules

Definition 1.11. A **commutative ring** is a ring for which $\cdot$ is commutative. A **division ring** (or skew field) is a ring such that $R \setminus \{0\}$ is a group under $\cdot$. A **field** is a commutative division ring.

Example 1.10. Ring is the category of rings. It has the full subcategories CRing of commutative rings and Fld of fields.

Definition 1.12. A (left) **module** A for a ring R is a triple $(A, +, \cdot)$, where $(A, +)$ is an abelian group and $\cdot : R \times A \to A$

1. is associative ($(rs)a = r(sa)$ for all $r, s \in R$ and $a \in A$)
2. satisfies $1 \cdot a = a$ for all $a \in A$
3. is distributive ($(r+s)a = ra + sa$ and $r(a+b) = ra + rb$ for all $r, s \in R$ and $a, b \in A$).

2 Morphisms, Functors, and Commutative Diagrams

2.1 Types of morphisms

Definition 2.1. Let $\mathcal{C}$ be a category. $\mathcal{C}$ is **locally small** if $\mathrm{Hom}(A, B)$ is always a set. $\mathcal{C}$ is **small** if $\mathrm{Obj}(\mathcal{C})$ is a set and $\mathcal{C}$ is locally small.

Definition 2.2. Let $f : X \to Y$ be a morphism in $\mathcal{C}$. f is a **monomorphism** if for any $g, h : U \to X$, $fg = fh$ implies that $g = h$ (f is left-cancellative). f is a **epimorphism** if for any $g, h : Y \to Z$, $gf = hf$ implies that $g = h$ (f is right-cancellative).

Example 2.1. The inclusion $i : \mathbb{Z} \to \mathbb{Q}$ is an epimorphism in the category of rings.

Definition 2.3. If $C \in \mathrm{Obj}(\mathbb{C})$, a **subobject** (A, i) of C is a pair such that $i : A \to C$ is a monomorphism. A **quotient** (B, π) of C is a pair such that $\pi : C \to B$ is an epimorphism.

2.2 Functors

Definition 2.4. Let $\mathcal{C}, \mathcal{D}$ be categories. A **(covariant) functor** $F : \mathcal{C} \to \mathcal{D}$ is a map $F : \mathrm{Obj}(\mathcal{C}) \to \mathrm{Obj}(\mathcal{D})$ and a map $F : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ such that $F(gf) = F(g) \circ F(f)$ and $F(1_X) = 1_{F(X)}$.

There is a dual notion, in which the functor switches the direction of the arrows (composition goes backwards).

Definition 2.5. Let $\mathcal{C}$ be a category. The **opposite category** $\mathcal{C}^{op}$ is the category with the same objects but the morphisms are reversed in direction; i.e. $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ corresponds to $f^{op} \in \mathrm{Hom}_{\mathcal{C}^{op}}(B, A)$.

With this definition, the dual type of functor can be viewed as follows.

Definition 2.6. A **contravariant functor** $F : \mathcal{C} \to \mathcal{D}$ is a covariant functor $F : \mathcal{C}^{op} \to \mathcal{D}$.

Example 2.2. Forgetful functors are functors which "forget information." The forgetful functor from Ab $\to$ Set takes an abelian group and gives back the underlying set. The forgetful functor from Ring $\to$ Set takes a ring and gives back the underlying set. The forgetful functor from Ring $\to$ Ab takes a ring and gives back the underlying abelian group.

Example 2.3. If $A \in \mathrm{Obj}(\mathcal{C})$, the functor $h_A : \mathcal{C}^{op} \to \mathrm{Set}$ is given by $h_A(B) = \mathrm{Hom}_{\mathcal{C}}(B, A)$.

Remark 2.1. A contravariant functor $\mathcal{C} \to \mathrm{Set}$ is sometimes called a **presheaf**.

Definition 2.7. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor. F is **faithful** if $F : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ is injective for all X, Y. $\mathcal{F}$ is **full** if $F : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ is surjective for all X, Y. F is **fully faithful** if F is both faithful and full.

Note that a category $\mathcal{E}$ is a subcategory of $\mathcal{C}$ if $\mathrm{Obj}(\mathcal{E}) \subseteq \mathrm{Obj}(\mathcal{C})$ and the inclusion functor $i : \mathcal{E} \to \mathcal{C}$ is full.

Example 2.4. Ab is a full subcategory of Grp.

2.3 Diagrams

Definition 2.8. A **directed graph** G is a set V_G of vertices (dots) and a set E_G of arrows (ordered pairs $(v, w) \in V_G \times V_G$).

Definition 2.9. $\mathbb{F}(G)$ is the **free category** on G if $\mathrm{Obj}(\pi(G)) = V_G$ and $\mathrm{Hom}_{\mathbb{F}(G)}(v, w) = \{e_n e_{n-1} \cdots e_1 : e_i \in E_G(v_{i-1}, v_i), v_0 = v, v_n = w\}$. Composition is concatenation of words.

Definition 2.10. A G**-shaped diagram** in a category $\mathcal{C}$ is a functor $\mathbb{F}(G) \to \mathcal{C}$.

Definition 2.11. A **commutative diagram** is a G-shaped diagram that is constant on $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ for each pair X, Y. In other words, taking any path in the diagram should give the same result. For example, in the diagram below, $g_2 \circ f_1 = f_2 \circ g_1$.

$$\begin{tikzcd} A \arrow[r, "f_1"] \arrow[d, "g_1"] & B \arrow[d, "g_2"] \\ C \arrow[r, "f_2"] & D \end{tikzcd}$$

Definition 2.12. Let $F, G : \mathcal{C} \to \mathcal{D}$ be functors. A **natural transformation** $\eta : F \to G$ is a collection of maps $\eta_X : F(X) \to G(X)$ for each $X \in \mathrm{Obj}(\mathbb{C})$ such that if $f : X \to Y$, then

$$\begin{tikzcd} F(X) \arrow[r, "\eta_X"] \arrow[d, "F(f)"] & G(X) \arrow[d, "G(f)"] \\ F(Y) \arrow[r, "\eta_Y"] & G(Y) \end{tikzcd}$$

Example 2.5. Look at the category Vec_K. Let $V^* = \mathrm{Hom}_K(V, K)$, and let $(-)^* : \mathrm{Vec}_K \to \mathrm{Vec}_K$. There is a natural transformation $\eta : \mathbb{1} \to (-)^{**}$ sending $V \to V^{**}$ by sending $v \mapsto (\lambda \mapsto \lambda(v))$.

Definition 2.13. η is a **natural isomorphism** if each η_X is an isomorphism.

Remark 2.2. In this case, $\{\eta_X^{-1}\}$ will also be a natural transformation.

Definition 2.14. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor. F is an **equivalence of categories** if there is a functor $G : \mathcal{D} \to \mathcal{C}$ and natural isomorphisms $FG \to \mathbb{1}_{\mathcal{D}}$, $GF \cong \mathcal{C}$. In this case, G is called a **quasi-inverse**.

Definition 2.15. Let $\mathcal{C}, \mathcal{D}$ be categories. The **functor category** $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ is the category with objects functors $\mathcal{C} \to \mathcal{D}$ and morphisms natural transformations.

Example 2.6. If $\mathcal{C}$ is small and $\mathcal{D}$ is locally small, then $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ is locally small.

2.4 Yoneda Embedding

Lemma 2.1. *Let* $\mathcal{C}$ *be a small category. Let* $\mathrm{Yo} : \mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{op}, \mathrm{Set})$ *be the functor with* $A \mapsto h_A(B) = \mathrm{Hom}_{\mathcal{C}}(B, A)$*. Then* Yo *is a fully faithful functor.*

Proof. To show that Yo is faithful, suppose that $\mathrm{Yo}(f) = \mathrm{Yo}(g)$. Then $f = \mathrm{Yo}(f)_A(1_A) = \mathrm{Yo}(g)_A(1_A) = g$.

We will show that Yo is full next time. □

3 The Yoneda Lemma

3.1 Two versions of the Yoneda lemma

Lemma 3.1 (Yoneda)**.** *Let $\mathcal{C}$ be a small category, and let $h^{\mathcal{C}} : \mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{op}, \mathrm{Set})$ be $h^{\mathcal{C}}(A) = h^A = \mathrm{Hom}_{\mathcal{C}}(\cdot, A)$ and if $f : A \to B$, then $h^{\mathcal{C}}(f)_X : \mathrm{Hom}(X, A) \to \mathrm{Hom}(X, B)$ sends $(g : X \to A) \mapsto (f \circ g : X \to B)$. Then $h^{\mathcal{C}}$ is fully faithful.*

Proof. To show that $h^{\mathcal{C}}$ is faithful, let $f, g : A \to B$, and suppose that $h^{\mathcal{C}}(f) = h^{\mathcal{C}}(g)$. THen $h^{\mathcal{C}}(f)A, h^{\mathcal{C}}(g)_A : \mathrm{Hom}(A, A) \to \mathrm{Hom}(A, B)$ maps $1_A \mapsto f \circ 1_A = f$ and $1_A \mapsto g \circ 1_A = g$. So $f = g$.

To show that $h^{\mathcal{C}}$ is full, let $\{\eta_X\} : h^A \to h^B$. We claim that $h^{\mathcal{C}}(\eta_A(1_A)) = \eta$.

$$\begin{array}{ccc} h^A(A) & \xrightarrow{\eta_A} & h^B(A) \\ \Big\downarrow{\scriptstyle h^A(f)} & & \Big\downarrow{\scriptstyle h^B(f)} \\ h^A(C) & \xrightarrow{\eta_C} & h^B(C) \end{array}$$

This is

$$\begin{array}{ccc} \mathrm{Hom}(A, A) & \xrightarrow{\eta_A} & \mathrm{Hom}(B, B) \\ \Big\downarrow{\scriptstyle h^A(f)} & & \Big\downarrow{\scriptstyle h^B(f)} \\ \mathrm{Hom}(C, A) & \xrightarrow{\eta_C} & \mathrm{Hom}(C, B). \end{array}$$

Since this diagram commutes, $\eta_C \circ h^A(f) = h^B(f) \circ \eta_A$. So they are equal on evaution on an element. Then $\eta_C \circ h^A(f)[1_A] = h^B(f) \circ \eta_A[1_A]$, so $\eta_C[f] = \eta_A[1_A] \circ f$. In particular, $\eta = h^{\mathcal{C}}(\eta_A[1_A])$. ☐

Lemma 3.2 (Yoneda, strengthened)**.** *Let $\mathcal{C}$ be a small category, let $h^{\mathcal{C}} : \mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{op}, \mathrm{Set})$ be the Yoneda embedding, and let $F : \mathcal{C}^{op} \to \mathrm{Set}$. Then $\mathrm{Nat}(h^A, F)$ is in bijection with $F(A)$.*

Proof. Define $\Phi : \mathrm{Nat}(h^A, F) \to F(A)$ given by $\eta_A : h^A(A) \to F(A)$, which sends $1_A \mapsto \eta_A(1_A)$. Define $\Psi : F(A) \to \mathrm{Nat}(h^A, F)$. Then, for $x \in F(A)$, $\Psi(x)_B : h^A(B) = \mathrm{Hom}(B, A) \to F(B)$ is $\Psi(x) = \mathrm{ev}_x \circ F$.

We claim that $\Phi \circ \Psi$ is the identity on $F(A)$. Let $x \in F(A)$. Then $\Phi(\Psi(x)) = \Phi(\mathrm{ev}_x \circ F) = \mathrm{ev}_x \circ 1_{F(A)} = x$. $(\Psi \circ \Phi)(\eta) = \Psi(\eta_A(1_A)) = \mathrm{ev}_{\eta_A(1_A)} \circ F$. Let $f : B \to A$. Then

$$\begin{array}{ccc} \mathrm{Hom}(A, A) & \xrightarrow{\eta_A} & F(A) \\ \Big\downarrow{\scriptstyle h^A(f)} & & \Big\downarrow{\scriptstyle F(f)} \\ \mathrm{Hom}(B, A) & \xrightarrow{\eta_B} & F(B). \end{array}$$

So $F(f) \circ \eta_A = \eta_B \circ h^A(f)$, which means $F(f) \circ \eta_A(1_A) = \eta_B \circ h^A(f)(1_A)$. The left hand side is $\Phi \circ \Phi(\eta)_B[f]$, and the right hand side is $\eta_B(f)$. Therefore, $\Psi \circ \Phi(\eta) = \eta$. ☐

This form of the Yoneda lemma implies the previous version.

Corollary 3.1 (Yoneda lemma)**.** *Let $\mathcal{C}$ be a small category, and let $h^{\mathcal{C}} : \mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{op}, \mathrm{Set})$. Then $h^{\mathcal{C}}$ is fully faithful.*

Proof. Let $B \in \mathrm{Obj}(\mathcal{C})$. Consider $F = h^B - \mathrm{Hom}_{\mathcal{C}}(\cdot, B)$. Then $\mathrm{Nat}(h^A, h^B)$ is in bijection (via F) with $h^B(A) = \mathrm{Hom}_{\mathcal{C}}(A, B)$. □

3.2 Partially ordered sets

Definition 3.1. A **partially ordered set (poset)** is a set S with a relation $\leq$ on S such that

1. $x \leq x$ for all $x \in S$,
2. if $x \leq y$ and $y \leq x$, then $x = y$,
3. if $x \leq y$ and $y \leq z$, then $x \leq z$.

We can turn a poset into a category. Let $\mathrm{Obj}(\mathcal{C}_S) = S$ and

$$\mathrm{Hom}_{\mathcal{C}_S}(X, Y) = \begin{cases} \{\text{unique morphism}\} & x \leq y \\ \varnothing & \text{otherwise.} \end{cases}$$

4 Limits and colimits

4.1 Limits

Definition 4.1. Let I be a small index category, and let $F : I \to \mathcal{C}$ be a functor. A **limit** $\lim F$ is an object X with morphisms $f_i : X \to F(i)$, characterized by the following properties:

1. If $g_{i,j} : F(i) \to F(j)$ is a morphism, then $f_j = F(g_{i,j}) \circ f_i$.
2. Any Y with this property factors through X; i.e. there exists an unique $\varphi : Y \to X$ such that $f_i' = f_i \circ \varphi$ for all i.

$$\begin{tikzcd}
 & Y \arrow[d, dashed, "\varphi"] \arrow[dl] \arrow[dr] \arrow[dd, bend right] & \\
 & X \arrow[dl, "f_1"'] \arrow[d, "f_2"] \arrow[dr, "f_3"] & \\
F(i) \arrow[r, "F(g_{i,j})"'] & F(j) \arrow[r, "F(g_{j,k})"'] & F(k) \arrow[ll, bend left, "F(g_{k,i})"]
\end{tikzcd}$$

The second property is called a **universal property**.

Remark 4.1. The limit includes the data of the f_α maps.

Proposition 4.1. *If it exists,* $\lim F$ *is unique up to isomorphism. Moreover, this isomorphism is unique,*

Proof. Suppose $(X, \{f_\alpha\})$ and $(Y, \{f_\alpha'\})$ are both limits of F. Since both of them are limits, let $\phi : X \to Y$ and $\psi : Y \to X$ be the unique maps given by the universal property. $\square$

Definition 4.2. Let I be a discrete category (only identity morphisms). Then $F : I \to \mathcal{C}$ is determined by a collection $(X_i)_{i \in I}$ of objects. Then the **product** is $\prod_{i \in I} X_i = \lim F$.

$$\begin{tikzcd}
 & Y \arrow[d, dashed, "\varphi"] \arrow[dl] \arrow[dr] \arrow[dd, bend right] & \\
 & \prod_{i \in I} X_i \arrow[dl] \arrow[d] \arrow[dr] & \\
X_1 & X_2 & X_3
\end{tikzcd}$$

For the morphisms, we have

$$\mathrm{Hom}_{\mathcal{C}}(Z, \prod X_i) \simeq \prod \mathrm{Hom}_{\mathcal{C}}(Z, X_i).$$

Example 4.1. In the category of sets, the product is the set-theoretic product.

Example 4.2. In Ab, Grp, and Mod, the product is the usual product, as well.

Example 4.3. In $\mathcal{C} = \text{Fld}$, the product is not the usual product. $\mathbb{Q} \times \mathbb{Q}$ is not a field. You can also check that the product of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})$ does not exist.

Definition 4.3. The *pull-back* $X = A \times_C B$ is a limit of A and B with morphisms $f : A \to C$ and $g : B \to C$.

$$\begin{tikzcd}
 & Y \arrow[d, dashed, "\varphi"] \arrow[ddl] \arrow[ddr] & \\
 & X \arrow[dl, "\pi_1"] \arrow[dr, "\pi_2"'] & \\
A \arrow[dr, "f"] & & B \arrow[dl, "g"'] \\
 & C &
\end{tikzcd}$$

Remark 4.2. Even though we write the pull-back as $X = A \times_C B$, it depends on the morphisms f, g.

Example 4.4. In Set, the pullback is $A \times_C B = \{(a, b) \in A \times B : f(a) = g(b)\}$.

4.2 Colimits

Definition 4.4. Let I be a small index category, and let $F : I \to \mathcal{C}$ be a functor. A **colimit** $\operatorname{colim} F$ is an object X with morphisms $f_i : F(i) \to X$, characterized by the following properties:

1. If $g_{i,j} : F(i) \to F(j)$ is a morphism, then $f_i = f_j \circ F(g_{i,j})$.
2. Any Y with this property factors through X; i.e. there exists an unique $\varphi : Y \to X$ such that $f_i' = \varphi \circ f_i$ for all i.

$$\begin{tikzcd}
 & Y & \\
 & X \arrow[u, dashed, "\varphi"'] & \\
F(i) \arrow[uur] \arrow[ur, "f_1"] \arrow[r, "F(g_{i,j})"'] & F(j) \arrow[uu, bend left] \arrow[u, "f_2"'] \arrow[r, "F(g_{j,k})"'] & F(k) \arrow[uul] \arrow[ul, "f_3"'] \arrow[ll, bend left, "F(g_{k,i})"]
\end{tikzcd}$$

Definition 4.5. Let I be a discrete category (only identity morphisms). Then $F : I \to \mathcal{C}$ is determined by $(A_i)_{i \in I}$. Then the **coproduct** is $\amalg_{i \in I} X_i = \operatorname{colim} F$.

$$
\begin{tikzcd}
& X & \\
& A \amalg B \arrow[u, dashed, "\varphi"'] & \\
A \arrow[uur, "f"] \arrow[ur, "\pi_1"'] & & B \arrow[uul, "g"'] \arrow[ul, "\pi_2"]
\end{tikzcd}
$$

Example 4.5. In the category of sets, the coproduct is the disjoint union.

Example 4.6. In the category of groups, $G_1 \amalg G_2$ is call the **free product** of G_1, G_2. This is usually denoted by $G_1 * G_2$.

Example 4.7. In the category of R-modules,

$$\coprod_{i \in I} M_i = \bigoplus_{i \in I} M_i = \left\{ \sum_{i=1}^{n} r_i m_i : r_i \in R, m_i \in M_i \right\}.$$

If I is infinite, this is not the same as

$$\prod_{i \in I} M_i = \{(r_i m_i)_{i \in I} : r_i \in R, m_i \in M_i\}.$$

Example 4.8. In the category of commutative rings, $R \amalg A = R \otimes_{\mathbb{Z}} S$.

Definition 4.6. The *push-out* $X = A \amalg_C B$ is a colimit of A and B with morphisms $f : C \to A$ and $g : C \to B$.

$$
\begin{tikzcd}
& Y & \\
& X \arrow[u, dashed, "\varphi"] & \\
A \arrow[uur] \arrow[ur, "\pi_1"'] & & B \arrow[uul] \arrow[ul, "\pi_2"] \\
& C \arrow[ul, "f"] \arrow[ur, "g"'] &
\end{tikzcd}
$$

Example 4.9. In Set, $Y \amalg_C Z = \{x \in Y \amalg Z : f(x) = g(x)\}$.

Example 4.10. In the category of groups, $G_1 \amalg_H G_2$ is called the amalgamated free product and is denoted by $G_1 *_H G_2$.

Example 4.11. In the category of commutative rings, $S_1 \amalg_R S_2 = S_1 \otimes_R S_2$.

Definition 4.7. If $\lim F$ exists, we cay $\mathcal{C}$ **admits the limit** of F. If $\mathcal{C}$ admits all (small) limits, we cay $\mathcal{C}$ is **complete**. If $\mathcal{C}$ admits all (small) colimits, $\mathcal{C}$ is **cocomplete**.

Example 4.12. The category of sets is both complete and cocomplete.

5 Equivalences, Cayley's Theorem, and More Limits

5.1 Equivalence of categories

Definition 5.1. An **equivalence of categories** $F : \mathcal{C} \to \mathcal{D}$ with a **quasi-inverse** $G : \mathcal{D} \to \mathcal{C}$ is a pair of functors such that there exist natural isomorphisms $\eta : F \circ G \to \mathrm{id}_{\mathcal{D}}$ and $\eta' : G \circ F \to \mathrm{id}_{\mathcal{C}}$.

Definition 5.2. A **natural isomorphism** η is a natural transformation such that η_A is an isomorphism for each A.

Example 5.1. Let $\mathcal{C}$ be the category with $\mathrm{Obj}(\mathcal{C}) = \{A\}$ and $\mathrm{Hom}_{\mathcal{C}}(A, A) = \mathrm{id}_A$, and let $\mathcal{C}$ be the category with objects B, C and morphisms $f : B \to C$, $g : C \to B$, id_B, and id_C such that $f \circ g = \mathrm{id}_C$ and $g \circ f = \mathrm{id}_B$. Let $F : \mathcal{C} \to \mathcal{D}$ be $F(A) = B$ with $F(\mathrm{id}_A) = \mathrm{id}_B$, and let $G : \mathcal{D} \to \mathcal{C}$ be $G(B) = G(C) = A$ and $G(h) = \mathrm{id}_A$ for all h. Then $G \circ F(A) = A$, $G \circ F(\mathrm{id}_A) = \mathrm{id}_A$, and you can check that $\eta : G \circ F \to \mathrm{id}_{\mathcal{C}}$ given by $\eta_A = \mathrm{id}_A$ is a natural isomorphism.

5.2 Cayley's theorem

Let $\mathcal{C}$ be a small category, and let $h^{\mathcal{C}} : \mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{op}, \mathrm{Set})$ be

$$h^{\mathcal{C}}(B) = h^B = \mathrm{Hom}_{\mathcal{C}}(\cdot, B)$$

and for $f : B \to C$, $h^{\mathcal{C}}(f) : h^B \to h^C$ sends $g \in \mathrm{Hom}_{\mathcal{C}}(A, B) \mapsto f \circ g$.

Lemma 5.1 (Yoneda)**.** *$h^{\mathcal{C}}$ is fully faithful.*

Definition 5.3. The **symmetric group** on X, S_X, is the set of bijections from X to X with function composition. We call $S_n = S_{\{1,\dots,n\}}$.

Theorem 5.1 (Cayley)**.** *Every group G is isomorphic to a subgroup of S_G.*

Proof. Let $\mathbb{G}$ be the category of the group G, where there is one object, and the group elements of G are morphisms. $h^{\mathbb{G}} : \mathbb{G} \to \mathrm{Fun}(\mathbb{G}^{op}, \mathrm{Set})$ is fully faithful. What is this functor? $h^{\mathbb{G}}(G) = h^G = \mathrm{Hom}(\cdot, G)$, and $h^{\mathbb{G}}(g) : h^G \to h^G$, where

$$h^{\mathbb{G}}(g)_G : \underbrace{h^G(G)}_{=G} \to h^G(G),$$

and

$$\rho = h^{\mathbb{G}}(\cdot)_G : G \to \mathrm{Maps}(G, G).$$

Note that

$$\rho(gh) = h^{\mathbb{G}}(gh)_G = (h^{\mathbb{G}}(g) \circ h^{\mathbb{G}}(h))_G = \rho(g)\rho(h),$$

$$\rho(e) = \mathrm{id}_G,$$

$$\mathrm{id}_G = \rho(e) = \rho(gg^{-1}) = \rho(g)\rho(g^{-1}),$$

so $\rho(g) \in S_G$. So $\rho : G \to S_G$ is a homomorphism. It is injective because if $\rho(g) = \rho(h)$, then $h^{\mathbb{G}}(g)_G = h^{\mathbb{G}}(h)_H$, so $h^{\mathbb{G}}(g) = h^{\mathbb{G}}(h)$. By Yoneda's lemma, $g = h$ because $h^{\mathbb{G}}$ is faithful. $\square$

5.3 Completeness

Definition 5.4. A category is **complete** if it admits all limits. A category is **cocomplete** if it admits all colimits.

Proposition 5.1. Set *is complete and cocomplete.*

Proof. Here is a sketch. Let $F : I \to \mathrm{Set}$. Then

$$\lim F = \left\{ (a_i)_{i \in I} \in \prod_{i \in I} F(i) : \forall \phi : i \to j,\ F(\phi)(a_i) = a_j \right\}.$$

$$\operatorname{colim} F = \coprod_{i \in I} F(i) \Big/ \sim,$$

where $\sim$ is the equivalence relation generated by the conditions $a_i \sim a_j \iff \exists \phi : i \to j$ such that $F(\phi)(a_i) = a_j$ for every $a_i \in F(i)$ and $a_j \in F(j)$. $\square$

Remark 5.1. The same proof works for the category of groups.

5.4 Initial and terminal objects

Definition 5.5. An **initial object** A in a category $\mathcal{C}$ is any object such that for all $B \in \mathcal{C}$, there exists a unique morphism $f : A \to B$. A **terminal object** A in a category $\mathcal{C}$ is any object such that for all $B \in \mathcal{C}$, there exists a unique morphism $f : B \to A$.

Remark 5.2. If they exist, initial and terminal objects are unique up to unique isomorphism.

Remark 5.3. Let $\varnothing$ be the empty category, and let $F : \varnothing \to \mathcal{C}$. If $\lim F$ exists, it is a terminal object. If $\operatorname{colim} F$ exists, it is an initial object.

5.5 Sequential limits and colimits

Definition 5.6. A **sequential limit** (or **inverse limit**) $\varprojlim F$ is a limit of the diagram

$$\cdots \longrightarrow A_3 \xrightarrow{f_2} A_2 \xrightarrow{f_1} A_1$$

A **sequential colimit** (or **direct limit**) $\varinjlim F$ is a colimit of the diagram

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \longrightarrow \cdots$$

Example 5.2. In CRing, $\mathbb{Z}/p^{n+1}\mathbb{Z}$ surjects onto $\mathbb{Z}/p^n\mathbb{Z}$. Then $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is called the p-adic integers $\mathbb{Z}_p$, where

$$\mathbb{Z}_p = \left\{ a_i \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : a_n = a_{n+1} \pmod{p^n} \right\}.$$

6 Inverse Limits, Direct Limits, and Adjoint Functors

6.1 Inverse and direct limits

Example 6.1. Consider the colimit of this diagram in Ab:

$$\mathbb{Z}/p\mathbb{Z} \xrightarrow{\cdot p} \cdots \xrightarrow{\cdot p} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z}/p^{n+1}\mathbb{Z} \xrightarrow{\cdot p} \cdots$$

Then $\varinjlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Q}_p/\mathbb{Z}_p \subseteq \mathbb{Q}/\mathbb{Z}$, where $\mathbb{Q}_p$ is the free field of $\mathbb{Z}_p$. We can also show that $\mathbb{Q}_p/\mathbb{Z}_p : \{a \in \mathbb{Q}/\mathbb{Z} : p^n a = 0 \text{ for some } n \geq 0\}$.

Definition 6.1. A **directed set** I is a set with a partial ordering such that for all $i, j \in I$, there is a $k \in I$ such that $i \leq k$, $j \leq k$.

Definition 6.2. A **directed category** is a category where the objects are elements of a directed set I, and there are morphisms $i \to j$ iff $i \leq j$. A **codirected category** $\mathcal{I}$ is a category where $\mathcal{C}^{op}$ is directed.

Definition 6.3. Suppose $\mathcal{I}$ is codirected with $\mathrm{Obj}(\mathcal{I}) = I$ and $F : \mathcal{I} \to \mathbb{C}$. A limit of F is called the **inverse limit** of the $F(i)$ for all $i \in I$. We write $\lim F = \varprojlim_{i \in I} F(i)$.

$$\begin{tikzcd}
 & & F(i) \\
\varprojlim F(i) \arrow[urr, bend left] \arrow[r] \arrow[drr, bend right] & F(k) \arrow[ur] \arrow[dr] & \\
 & & F(j)
\end{tikzcd}$$

If $\mathcal{I}$ is directed with $\mathrm{Obj}(\mathcal{I}) = I$ and $F : \mathcal{I} \to \mathcal{C}$. A colimit of F is called the **direct limit** of the $F(i)$ for all $i \in I$. We write $\operatorname{colim} F = \varinjlim_{i \in I} \operatorname{colim} F$.

$$\begin{tikzcd}
 & & F(i) \arrow[dll, bend right] \arrow[dl] \\
\varprojlim F(i) & F(k) \arrow[l] & \\
 & & F(j) \arrow[ull, bend left] \arrow[ul]
\end{tikzcd}$$

Definition 6.4. A small category $\mathcal{I}$ is **filtered** if

1. for all $i, j \in I$, there exists $k \in I$ such that there exist morphisms $i \to k, j \to k$,

2. for all $\kappa, \kappa' : i \to j$ in I there exists a morphism $\lambda : j \to k$ such that $\lambda \circ \kappa = \lambda \circ \kappa'$

A category it **cofiltered** if the opposite category is filtered.

Cofiltered limits and diltered limits generalize inverse and direct limits, respectively.

Example 6.2. Let I be cofiltered with an initial object c. Then if $F : I \to \mathcal{C}$, $\lim F = F(e)$.

6.2 Adjoint functors

Definition 6.5. A functor $F : \mathcal{C} \to \mathcal{D}$ is **left adjoint** to a functor $G : \mathcal{D} \to \mathcal{C}$ if for each $C \in \mathcal{C}$, $D \in \mathcal{D}$, there exist bijections $\eta_{C,D} : \mathrm{Hom}_{\mathcal{D}}(F(C), D) \to \mathrm{Hom}_{\mathcal{C}}(C, G(D))$ such that η is a natural transformation between functors $\mathcal{C}^{op} \times \mathcal{D} \to \mathrm{Sets}$. That is,

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{D}}(F(C), D) \arrow[r, "\eta_{C,D}"] \arrow[d, "h \mapsto g \circ h \circ F(f)"] & \mathrm{Hom}_{\mathcal{C}}(C, G(D)) \arrow[d, "h \mapsto G(g) \circ h \circ f"] \\
\mathrm{Hom}_{\mathcal{D}}(F(C'), D') \arrow[r, "\eta_{C',D'}"] & \mathrm{Hom}_{\mathcal{C}}(C', G(D'))
\end{tikzcd}$$

G is **right adjoint** to F if F is left adjoint to G.

Remark 6.1. If $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ are quasi-inverses and $\eta : \mathrm{id}_{\mathcal{C}} \to G \circ F$ is a natural isomorphism, then we can define $\phi_{C,D} : \mathrm{Hom}_{\mathcal{D}}(F(C), D) \to \mathrm{Hom}_{\mathcal{C}}(C, G(D))$ given by $h \mapsto G(h) \circ \eta_C$. Check that $\phi_{C,D}$ is a bijection. So F is left-adjoint to G. Similarly, G is left-adjoint to F.

Proposition 6.1. *Suppose S is a set, and consider $h_S : \mathrm{Set} \to \mathrm{Set}$ given by $h_S(T) = \mathrm{Maps}(S, T)$ and $h_S(f : T \to T') = g \mapsto f \circ g$. Then h_S is right adjoint to $t_S : \mathrm{Set} \to \mathrm{Set}$ given by $t_S(T) = T \times S$ and $t_S(f) = (f, \mathrm{id}_S) : T \times S \to T' \times S$.*

Proof. We need to find a bijection $\tau_{T,U} : \mathrm{Maps}(T \times S, U) \to \mathrm{Maps}(T, \mathrm{Maps}(S, U))$. We can send $f \mapsto (t \mapsto (s \mapsto f(s,t)))$. To show that this is a bijection, we can go backward by sending $\varphi \mapsto ((t,s) \mapsto \varphi(t)(s))$. Check that these maps are inverses of each other and that this is a natural transformation. $\square$

Proposition 6.2. *Suppose all limits $F : I \to \mathcal{C}$ exist. Then the functor $\lim : \mathrm{Fun}(I, \mathcal{C}) \to \mathcal{C}$ given by $F \mapsto \lim F$ and $(\eta : F \to F') \mapsto (\lim F \mapsto \lim F')$ has a left adjoint $\Delta : \mathcal{C} \to \mathrm{Fun}(I, \mathcal{C})$ such that $\Delta(A) = c_A$ is the constant functor $I \to \mathcal{C}$ with value A.*

Proof. We want a bijection $\eta : \mathrm{Hom}_{\mathrm{Fun}(I,\mathcal{C})}(c_A, F) \to \mathrm{Hom}_{\mathcal{C}}(A, \lim F)$. Let $\eta : c_A \to F$ be $\eta_i : \underbrace{c_A(i)}_{=A} \to F(i)$ such that

$$\begin{tikzcd}
A \arrow[r, "\eta_i"] \arrow[d, "\mathrm{id}_A = c_A(f)"'] & F(i) \arrow[d, "F(f)"] \\
A \arrow[r, "\eta_j"] & F(j)
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "\eta_i"] \arrow[dr, "\eta_j"'] & F(i) \arrow[d, "F(f)"] \\
& F(j)
\end{tikzcd}$$

for all $f : i \to j$. So $\eta_j = F(f) \circ \eta_i$ for all $f : i \to j$. There exists a unique morphism $g : A \to \lim F$ such that

$$\begin{tikzcd}
& A \arrow[dl, "\eta_j"'] \arrow[d, dashed, "g"] \arrow[dr, "\eta_i"] & \\
& \lim F \arrow[dl, "p_j"] \arrow[dr, "p_i"'] & \\
F(j) & & F(i) \arrow[ll, "F(f)"]
\end{tikzcd}$$

Send η to g. Conversely if we have $g : A \to \lim F$, $\eta_i = p_i \circ g$ is a morphism from $A \to F(i)$. So we get $\eta \in \mathrm{Hom}_{\mathrm{Fun}(I,\mathcal{C})}(c_A, F)$. $\square$

Definition 6.6. A contravariant functor $F : \mathcal{C} \to \mathrm{Set}$ is **representable** if there exists an object $B \in \mathcal{C}$ and a natural isomorphism $h^B \to F$, where $h^B = \mathrm{Hom}_{\mathcal{C}}(\cdot, B)$. We say that B **represents** F.

Example 6.3. The functor $P : \mathrm{Set} \to \mathrm{Set}$ given by $S \mapsto \mathcal{P}(S)$ and $(f : S \to T) \mapsto (V \mapsto f^{-1}(V))$ is representable by $\{0, 1\}$.

7 Representable Functors and Free Groups

7.1 Representable functors

Definition 7.1. A contravariant functor $F : \mathcal{C} \to \text{Set}$ is **representable** if there is a natural isomorphism $h^B \to F$ for some $B \in \mathcal{C}$, where $h^B = \text{Hom}_{\mathcal{C}}(\cdot, B)$.

Example 7.1. Let $P : \text{Set} \to \text{Set}$ be the morphism such that $P(S) = \mathcal{P}(S)$, the power set of S, and $P(f : S \to T)(V) = f^{-1}(V)$ for $V \subseteq T$. P is representable by $\{0, 1\}$; $P(S) \xrightarrow{\sim} \text{Maps}(S, \{0, 1\})$, which sends $U \mapsto \mathbb{1}_U$, the indicator function of U.

$$\begin{array}{ccc} P(T) & \xrightarrow{\sim} & \text{Maps}(T, \{0,1\}) \\ \downarrow{\scriptstyle P(f)} & & \downarrow{\scriptstyle h^{\{0,1\}}(f)} \\ P(S) & \xrightarrow{\sim} & \text{Maps}(S, \{0,1\}) \end{array}$$

Lemma 7.1. *A representable functor is represented by a unique object up to (unique) isomorphism. That is, if B, C represent $F : \mathcal{C} \to \text{Set}$, then there exists a unique isomorphism $f : B \to C$ such that*

$$\begin{array}{ccc} \text{Hom}_{\mathcal{C}}(A, B) & \xrightarrow{\sim} & F(A) \\ \downarrow{\scriptstyle h_A(f)} & & \downarrow{\scriptstyle \text{id}_A} \\ \text{Hom}_{\mathcal{C}}(A, C) & \xrightarrow{\sim} & F(A) \end{array}$$

Proof. There exist natural isomorphisms $\xi : h^B \to F$, $\xi' : h^C \to F$. Then $(\xi')^{-1} \circ \xi$ is a natural isomorphimsm $h^B \to h^C$. Yoneda's lemma gives a unique $f : B \to C$ such that $h^{\mathcal{C}}(f) = (\xi')^{-1} \circ \xi$ because $h^{\mathcal{C}}(f)_A = h_A(f)$. $\square$

Remark 7.1. A covariant functor $F : \mathcal{C} \to \text{Set}$ is representable if there exists a natural isomorphism $F \to h_A$ for some $A \in \mathcal{C}$.

Example 7.2. Let $\Phi : \text{Grp} \to \text{Set}$ be the forgetful functor. To represent Φ, we want a bijection $\Phi(G) = G \xrightarrow{\sim} \text{Hom}_{\text{Grp}}(\mathbb{Z}, G)$; send $g \mapsto (n \mapsto g^n)$. This image homomorphism is completely determined by whatever 1 gets sent to, which is g. So this is a bijection. So Φ is represented by $\mathbb{Z}$.

7.2 Free groups

Definition 7.2. A group F is **free** on a subset $X \subseteq F$ if for any function $f : X \to G$, where G is a group, there exists a unique homomorphism $\phi_f : F \to G$ such that $\phi_f(x) = f(x)$ for all $x \in X$.

Example 7.3. Let $\Phi : \text{Grp} \to \text{Set}$ be the forgetful functor. If $f \in \text{Hom}_{\text{Set}}(X, \Phi(G)) = \text{Maps}(X, G)$, we want $\phi_f \in \text{Hom}_{\text{Grp}}(F_X, G)$, where F_X is the free group on X. We want a bijection $\text{Hom}_{\text{Grp}}(F_X, G) \xrightarrow{\sim} \text{Hom}_{\text{Set}}(X, \Phi(G))$. Send $\phi \mapsto \phi|_X$. If $f : G \to H$ is a homomorphism,

$$\begin{tikzcd}
\text{Hom}_{\text{Grp}}(F_X, C) \arrow[d, "\phi_f \mapsto \varphi \circ \phi_f"] & \text{Maps}(X, G) \arrow[l, "\sim"'] \arrow[d, "f \mapsto \phi \circ f"] \\
\text{Hom}_{\text{Grp}}(F_X, H) & \text{Maps}(X, H) \arrow[l, "\sim"']
\end{tikzcd}$$

If F_X exists for all X, then $F : \text{Set} \to \text{Grp}$ with $F(X) = F_X$ and $F(\varphi)$ the unqiue morphism is left adjoint to Φ. Why is this morphism unique? $\varphi : X \to Y$ induces a map $h : X \to F_Y$. There exists a unique map $\phi_h : F_X \to F_Y$ by the universal property.

Definition 7.3. Let $\Phi : \mathcal{C} \to \text{Set}$ be a faithful functor and X a set. A **free object** F_X on X in $\mathcal{C}$ is a function $\iota : X \to \Phi(F_X)$ such that $\text{Hom}_{\mathcal{C}}(F_X, B) \xrightarrow{\sim} \text{Maps}(X, \Phi(B))$ via $\alpha \mapsto \Phi(\alpha) \circ \iota$ is a bijection for all $B \in \mathcal{C}$.

Example 7.4. The forgetful functor $\Phi : \text{Top} \to \text{Set}$ takes a topological space and returns the underlying set, forgetting the topology. Let's find a left adjoint. If X is a set, we can map it to a topological space $F_X = X$ with the discrete topology. Then $\text{Hom}_{\text{Top}}(X, B) = \text{Maps}(X, B)$.

Example 7.5. Let $\Phi : \text{Ab} \to \text{Set}$ be the forgetful functor. Let $\iota : X \to \bigoplus_{x \in X} \mathbb{Z}$ send $x \mapsto 1 \cdot x$. We want a bijection $X \mapsto \bigoplus_{x \in X} \mathbb{Z}$. $\text{Hom}_{\text{Ab}}(\bigoplus_{x \in X} \mathbb{Z}, B) \to \text{Maps}(X, B)$. For the backwards direction, send $f \mapsto \phi_f(\sum_x a_x x) = \sum_x a_x f(x)$. In the forward direction, we have $\phi \mapsto (x \mapsto \phi(1 \cdot x))$. $\bigoplus_{x \in X} \mathbb{Z}$ is called the **free abelian group** on X.

How do the free group X and the free abelian group $\bigoplus_{x \in X} \mathbb{Z}$ compare? There is a surjective homomorphism $F_X \to \bigoplus_{x \in X} \mathbb{Z}$ sending $x \mapsto 1 \cdot x$. This is because we have the bijection $\text{Hom}_{\text{Grp}}(F_X, \bigoplus_{x \in X} \mathbb{Z}) \xrightarrow{\sim} \text{Maps}(X, \bigoplus_{x \in X} \mathbb{Z})$. We can't go the other way because a free group is not necessarily abelian.

8 Free Groups, Normal Subgroups, and Quotient Groups

8.1 Free groups

Definition 8.1. A **word** on a set X is a symbol $x_1^{n_1} \cdots x_k^{n_k}$ where $k \geq 0$ ($k = 0$ gives e), $x_i \in X$, and $n_i \in \mathbb{Z}$ for $1 \leq i \leq k$. Write x^1 as x.

Definition 8.2. The **product** of two words is their concatenation.

$$(x_1^{n_1} \cdots x_k^{n_k}) \cdot (y_1^{n_1} \cdots y_k^{n_k}) := x_1^{n_1} \cdots x_k^{x_k} y_1^{n_1} \cdots y_k^{x_k}.$$

Definition 8.3. Two words are equivalent if they are equivalent under the equivalence relation $\sim$ generated by

1. $ww' \sim wx^0w'$
2. $wx^{m+n}w' \sim wx^m x^n w'$

for all words w, w' and $x \in X$.

Definition 8.4. A **reduced word** is a word such that $x_i^j \neq x_{i+1}^\ell$ for any $k, \ell \in \mathbb{Z}$ and for all $1 \leq i \leq k-1$, and $n_i \neq 0$ for all x_i.

This is a word which is the shortest in its equivalence class.

Proposition 8.1. *Every word is equivalent to a unique reduced word.*

Example 8.1. Let's reduce the word $x^3y^2z^{-1}zy^{-2}x^2$.

$$x^3y^2z^{-1}zy^{-2}x^2 \sim x^3y^2z^0y^{-2}x^2 \sim x^3y^2y^{-2}x^2 \sim x^3y^0x^2 \sim x^3x^2 \sim x^5.$$

Let F_X be the group of equivalence classes of words on X. You can check yourself that if $v \sim v'$ and $w \sim w'$, then $vw \sim v'w'$, so products on F_X are well-defined. This is a group under the product of words, where e is the identity element and the inverse is $(x_1^{n_1} \cdots x_k^{n_k})^{-1} = x_k^{-n_k} \cdots x_1^{-n_1}$.

Definition 8.5. F_X is called the **free group on** X. If $X = \{1, \ldots, n\}$, $F_n := F_X$ is called the **free group of rank** n.

Example 8.2. $F_{\{x\}} = \langle x \rangle = \{x^n : n \in \mathbb{Z}\} \cong \mathbb{Z}$.

Example 8.3. $F_{\{x,y\}} = \{x^{n_1}y^{m_1} \cdots x^{n_k}y^{m_k} : k \geq 0, n_i \neq 0 \, \forall i \geq 2, m_i \neq 0 \, \forall i \leq k-1\}$.

Proposition 8.2. *F_X is a free group on X (in the categorical sense). It is the coproduct of the functor $c_{\mathbb{Z}} : X \to \mathrm{Gp}$ which sends $i \mapsto \mathbb{Z}$ and $f \mapsto \mathrm{id}_{\mathbb{Z}}$.*

Proof. We want $\mathrm{Hom}_{\mathrm{Gp}}(F(X), G) \cong \mathrm{Maps}(X, G)$. We send $\phi \mapsto \phi|_X$. Our map $\iota : X \to F_X$ is the inclusion map. To go backwards, mapping $f \mapsto \phi$ for $f : X \to G$, we define $\phi_f(x_1^{n_1} \cdots x_k^{n_k}) = f(x_1)^{n_1} \cdots f(x_k)^{n_k}$. If we can show that ϕ_f is well defined, we will get the homomorphism we want. Observe that

$$\phi_f(wx^0w') = \phi_f(w)f(x)^0\phi_f(w') = \phi_f(w)\phi_f(w') = \phi_f(ww').$$

Check yourself that $\phi_f(wx^{m+n}w') = \phi_f(wx^nx^mw')$. Uniqueness is left as an exercise.

The coproduct property is very similar to a homework problem for this week, so we leave it as an exercise, as well. $\square$

Definition 8.6. The **free product** $*_{i\in I}G_i = \{\text{words in the groups } G_i\}/\sim$ is the coproduct in the category of groups.

8.2 Normal subgroups and quotient groups

Definition 8.7. A subgroup N of a group G is **normal**, written $N \trianglelefteq G$ if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.

Definition 8.8. Let $H \leq G$ and $g \in G$. Then $gH = \{gh : h \in H\}$ is the **left H-coset** of g, and $Hg = \{hg : h \in H\}$ is the **right H-coset** of g.

Remark 8.1.

$$\begin{aligned} N \trianglelefteq G &\iff gNg^{-1} \leq N \; \forall g \in G \\ &\iff gNg^{-1} = N \; \forall g \in G \\ &\iff gN = Ng \; \forall g \in G. \end{aligned}$$

Remark 8.2. Let $G/H = \{gH : g \in G\}$ and $H\backslash G = \{Hg : g \in G\}$. These are in bijection via $gH \mapsto (gH)^{-1} = Hg$.

Proposition 8.3. *$N \trianglelefteq G \iff gN \cdot g'N = gg'N$ gives a well-defined group structure on G/N.*

Definition 8.9. We call $G/N = \{gN : g \in G\}$ the **quotient group**.

Definition 8.10. The index of H in G is the number of left (or right) cosets of H in G.

Example 8.4. $N\mathbb{Z} \leq \mathbb{Z}$. Since $\mathbb{Z}$ is abelian, $N\mathbb{Z} \trianglelefteq \mathbb{Z}$. Then the quotient group $\mathbb{Z}/N\mathbb{Z} = \{a + N\mathbb{Z} : 0 \leq a \leq N-1\}$.

Example 8.5. D_n is the dihedral group of symmetries of a regular n-gon. $|D_n| = 2n$, and the set of rotations is a normal subgroup.[2]

[2] Since $|D_n| = 2n$, some people call this group D_{2n}.

9 Equalizers, Kernels, and Ideals

9.1 Equalizers and coequalizers

Definition 9.1. Let $f, g : A \to B$ be morphisms in $\mathcal{C}$. The **equalizer** is the limit of the diagram

$$\begin{tikzcd} A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \end{tikzcd}$$

It satisfies the following diagram:

$$\begin{tikzcd} \mathrm{eq}(f,g) \arrow[r, "\iota"] & A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \\ Y \arrow[u, dashed] \arrow[ur, "q"'] & & \end{tikzcd}$$

A **coequalizer** is the colimit of the diagram

$$\begin{tikzcd} A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \end{tikzcd}$$

It satisfies the following diagram:

$$\begin{tikzcd} A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \arrow[r, "\pi"] \arrow[dr, "q"] & \mathrm{coeq}(f,g) \arrow[d, dashed] \\ & & Y \end{tikzcd}$$

Lemma 9.1. *$\iota : \mathrm{eq}(f,g) \to A$ is a monomorphism, and $\pi : B \to \mathrm{coeq}(f,g)$ is an epimorphism.*

Proof. Let $\alpha, \beta : C \to \mathrm{eq}(f,g)$ be such that $\iota \circ \alpha = \iota \circ \beta$. Then there is a unique morphism $\phi : C \to \mathrm{eq}(f,g)$ making the following diagram commute:

$$\begin{tikzcd} \mathrm{eq}(f,g) \arrow[r, "\iota"] & A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \\ C \arrow[u, dashed, "\phi"] \arrow[ur, shift left, "\iota\circ\alpha"] \arrow[ur, shift right, "\iota\circ\beta"'] & & \end{tikzcd}$$

But α and β satisfy the property of ϕ, so $\alpha = \phi = \beta$. The property for coequalizers follows from reversing the arrows. $\square$

Theorem 9.1. *Every category with products and equalizers is complete.*

Proof. Let $F : I \to \mathcal{C}$ be a functor. Then

$$\prod_{i \in I} F(i) \underset{g}{\overset{f}{\rightrightarrows}} \prod_{\phi : i \mapsto \phi(i)} F(\phi(i))$$

where f is

$$\prod_{k \in I} F(k) \xrightarrow{\pi_i} F(i) \xrightarrow{F(\phi)} F(\phi(i))$$

and g is

$$\prod_{k \in I} F(k) \xrightarrow{\pi_{\pi(i)}} F(\phi(i))$$

We claim that $\mathrm{eq}(f,g) \to \prod_{i \in I} F(i) \to F(i)$ is the limit. The

$$\begin{tikzcd}
\mathrm{eq}(f,g) \arrow[r] \arrow[dr] & F(i) \arrow[d, "F(\phi)"] \\
& F(\phi(i))
\end{tikzcd}$$

commute for all ϕ. So the equalizer has the property of the limit. To show the universal property, suppose we have the following diagram for some X.

$$\begin{tikzcd}
X \arrow[r, "\psi_i"] \arrow[dr, "\psi_{\phi(i)}"] & F(i) \arrow[d, "F(\phi)"] \\
& F(\phi(i))
\end{tikzcd}$$

This is the same as

$$\begin{tikzcd}
X \arrow[r] \arrow[d, dashed] & \prod_{i \in I} F(i) \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & \prod_{\phi : i \mapsto \phi(i)} F(\phi(i)) \\
\mathrm{eq}(f,g) \arrow[ur]
\end{tikzcd}$$

by the universal property of the equalizer. So $\mathrm{eq}(f,g)$ satisfies the universal property of $\lim F$. $\square$

Example 9.1. In Set, Gp, Ring, Rmod, and Top, the equalizer of $f, g : A \to B$ is $\mathrm{eq}(f,g) = \{x \in A : f(x) = g(x)\}$. These are all complete categories. The are also complete, as they have coproducts and coequalizers.

9.2 Kernels and ideals

Definition 9.2. A **zero object** is an object which is both initial and terminal.

Let $\mathcal{C}$ have a zero object 0. There exists a unique morphism $0 : A \to B$ which is the composition of the unique morphism from $A \to 0$ and $0 \to B$.

Definition 9.3. For $f : A \to B$, the **kernel** $\ker(f) = \mathrm{eq}(f, 0)$ and $\mathrm{coker}(f) = \mathrm{coeq}(f, 0)$, where 0 is the unique zero morphism.

Example 9.2. In Gp, $\ker(f : G \to G') = \{g \in G : f(g) = e\}$. This is the same in Rmod.

Example 9.3. In Ring, we can makes sense of this is we work in a larger category, Rng, of pseudorings (rings without identity). If $f : R \to S$, then $\ker(f) = \{x \in R : f(x) = 0\}$. In fact, $\ker f$ is a two-sided ideal.

In all of these cases, $\ker f = 0$ iff f is a monomorphism iff f is 1 to 1. To show that $\ker(f) = 0$ implies that f is a monomorphism, we have (in Gp)

$$f(g) = f(h) \implies f(gh^{-1}) = e \implies gh^{-1} = e \implies g = h,$$

but this requires internal knowledge of the structure of the category.

Proposition 9.1. *1. If $f : G \to G'$ is a homomorphism,* $\ker(f) \trianglelefteq G$.

2. If $N \trianglelefteq G$, then $N = \ker(\pi)$, where $f : G \to G/N$ sends $g \mapsto gN$.

Proof. To prove the first part, note that $f(gng^{-1}) = f(g)f(n)f(g)^{-1} = e$, so $gng^{-1} \in \ker(f)$. The second follows from the definitions. □

Theorem 9.2. *Let $f : G \to G'$ be a homomorphism. Then $\overline{f} : G/\ker(f) \to \mathrm{im}(f)$ given by $\overline{f}(g\ker(f)) = f(g)$ is an isomorphism.*

Definition 9.4. A **left ideal** I of a ring R is a subgroup such that $ri \in I$ for all $r \in R$ and $i \in I$. A **right ideal** I of a ring R is a subgroup such that $is \in I$ for all $s \in R$ and $i \in I$. A **(two-sided) ideal** I is a right and left ideal.

If we have a left ideal I, left multiplication $R \times I \to R$ makes I a left R-module. So a left ideal of R is exactly a left R-submodule of R.

Definition 9.5. An (R, S)-**bimodule** M is a left R-module that is also a right S-module such that $(rm)s = r(ms)$ for all $r \in R$, $s \in S$, and $m \in M$.

A (two-sided) ideal is an (R, R)-subbimodule of R.

If $I \subseteq R$ is a two-sided idea, then $R/I = \{a + I : a \in R\}$. We have addition $(a + I) + (b + I) = (a + b) + I$ and multiplication $(a + I)(b + I) = ab + I$. Why is multiplication well-defined? For $a, b \in R$ and $i, j \in I$,

$$(a + i)(b + j) = ab + \underbrace{aj}_{\in I} + \underbrace{ib}_{\in I} + \underbrace{ij}_{\in I} \in ab + I.$$

Definition 9.6. R/I is called a **quotient ring**.

Observe that $\ker(f)$ with $f : R \to S$ is an ideal. If $a \in \ker(f)$, $r, s \in R$, then $f(ras) = f(r)f(a)f(s) = 0$. So we have the $\pi : R \to R/I$ with $\pi(r) = r + I$ and $\ker(\pi) = I$. So $R/\ker(f) \cong \operatorname{im}(f)$.

This also works with with left, right, and bimodules. In fact, it works even better! All left R-modules are kernels, so you don't need any conditions like normality.

What about cokernels? In Gp, we have a problem: if $f : G \to G'$, $\operatorname{im}(f)$ may not be normal in G'. We take $\operatorname{coker}(f) = G/\overline{\operatorname{im}(f)}$, where $\overline{\operatorname{im}(f)}$ denotes the **normal closure** of $\operatorname{im}(f)$, the smallest normal subgroup containing $\operatorname{im}(f)$.

We have been using the term image in the sense of groups. Here is a categorical point of view.

Definition 9.7. The **image** $\operatorname{im}(f)$ of $f : A \to B$ is an object and a monomorphism $\iota : \operatorname{im}(f) \to B$ such that there exists $\pi : A \to \operatorname{im}(f)$ with $\pi \circ \iota$ and such that if $e : C \to B$ is a monomorphism and $g : A \to C$ is such that $e \circ g = f$, then there exists a unique morphism $\psi : \operatorname{im}(f) \to C$ such that $g \circ \psi = \iota$.

$$
\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi"] \arrow[ddr, "g"'] & & B \\
& \operatorname{im}(f) \arrow[ur, "\iota"] \arrow[d, dashed, "\psi"'] & \\
& C \arrow[uur, "e"'] &
\end{tikzcd}
$$

Note that $e \circ \psi \circ \pi = e \circ g \implies \psi \circ \pi = g$, since e is a monomorphism.

10 Images, Coimages, and Generating Sets

10.1 Images

Definition 10.1. The **image** $\mathrm{im}(f)$ of $f : A \to B$ is an object and a monomorphism $\iota : \mathrm{im}(f) \to B$ such that there exists $\pi : A \to \mathrm{im}(f)$ with $\pi \circ \iota$ and such that if $e : C \to B$ is a monomorphism and $g : A \to C$ is such that $e \circ g = f$, then there exists a unique morphism $\psi : \mathrm{im}(f) \to C$ such that $g \circ \psi = \iota$.

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi"] \arrow[ddr, "g"'] & & B \\
& \mathrm{im}(f) \arrow[ur, "\iota"'] \arrow[d, dashed, "\psi"'] & \\
& C \arrow[uur, "e"'] &
\end{tikzcd}$$

Example 10.1. In Set, $f(A) = \mathrm{im}(f)$. Then $b \in F(A) \implies b = f(a)$ for some $a \in A$. Then $g(a) \in C$ is the unique element with $e(g(a)) = (a)$ because e is a monomorphism. So $\psi(f(a)) = g(a)$.

Proposition 10.1. *If $\mathcal{C}$ has equalizers, then $\pi : A \to \mathrm{im}(f)$ is an epimorphism.*

Proof. Suppose

$$\begin{tikzcd}
A \arrow[r, "\iota"] & \mathrm{im}(f) \arrow[r, shift left, "\alpha"] \arrow[r, shift right, "\beta"'] & D
\end{tikzcd}$$

commutes. Then $\alpha \circ \pi = \beta \circ \pi$,

$$\begin{tikzcd}
A \arrow[r] \arrow[rr, bend left, "\pi"] \arrow[drr, "f"'] & \mathrm{eq}(\alpha, \beta) \arrow[r, "c"] & \mathrm{im}(f) \arrow[d, "\iota"] \\
& & B
\end{tikzcd}$$

Then there is a unique $d : \mathrm{im}(f) \to \mathrm{eq}(\alpha, \beta)$, and $c \circ d = \mathrm{id}$ and $d \circ c = \mathrm{id}$ by uniqueness. So $(\mathrm{im}(f), \mathrm{id}_{\mathrm{im}(f)})$ equalizes

$$\begin{tikzcd}
\mathrm{im}(f) \arrow[r, shift left, "\alpha"] \arrow[r, shift right, "\beta"'] & D
\end{tikzcd}$$

so $\alpha = \beta$. $\square$

Suppose that in $\mathcal{C}$, every morphism factors through an equalizer and the category has finite limits and colimits. Then $\mathrm{im}(f)$ can be defined as the equalizer of the following diagram:

$$\begin{tikzcd}
B \arrow[r, shift left, "\iota_1"] \arrow[r, shift right, "\iota_2"'] & B \amalg_A B
\end{tikzcd}$$

We get the following diagram.

$$
\begin{tikzcd}
 & A \arrow[dl, "f"'] \arrow[d, dashed, "\pi"] \arrow[dr, "f"] & \\
 & \mathrm{im}(f) \arrow[dl, "\iota"] \arrow[dr, "\iota"'] & \\
B \arrow[dr, "\iota_2"'] & & B \arrow[dl, "\iota_1"] \\
 & B \amalg_A B &
\end{tikzcd}
$$

10.2 Coimages

Definition 10.2. The **coimage** $\mathrm{im}(f)$ of $f : A \to B$ is an object and a monomorphism $\pi : A \to \mathrm{coim}(f)$ such that there exists $\iota : \mathrm{coim}(f) \to B$ such that $\iota \circ \pi$ and such that if $g : A \to C$ is an epinmorphism and $e : C \to B$ is such that $e \circ g = f$, then there exists a unique morphism $\theta : C \to \mathrm{coim}(f)$ such that $\theta \circ g = \pi$.

$$
\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi"] \arrow[ddr, "g"'] & & B \\
 & \mathrm{coim}(f) \arrow[ur, "\iota"] \arrow[d, dashed, "\psi"'] & \\
 & C \arrow[uur, "e"'] &
\end{tikzcd}
$$

So $\iota \circ \theta \circ g = \iota \circ \pi = f = e \circ g$. Since g is an epimorphism, $i \circ \theta = e$.

How are the image and coimage related?

$$
\begin{tikzcd}
A \arrow[rrr, "f"] \arrow[dr] \arrow[drr] & & & B \\
 & \mathrm{im}(f) \arrow[urr] \arrow[r, dashed] & \mathrm{coim}(f) \arrow[ur] &
\end{tikzcd}
$$

Definition 10.3. A morphism $f : A \to B$ is **strict** if $\mathrm{im}(f) \to \mathrm{coim}(f)$ is an isomorphism.

In Grp, Ring, Rmod, Set, and Top, $\mathrm{im}(f)$ is the set theoretic image. The coimages are quotient objects (of A).

Example 10.2. In Set, $\mathrm{coim}(f) = A/\sim$, where $a \sim a$; if $f(a) \sim f(a')$. All the morphisms are strict.

Example 10.3. In Gp, $\mathrm{coim}(f : C \to C') = G/\ker(f)$. $\mathrm{im}(f) \subseteq f(G) \leq G'$. So the image and coimage are isomorphic, which is the first isomorphism theorem.

Example 10.4. In Ring, let $\ker(f)$ be the category theoretic kernel. Then $\mathrm{coim}(f) = R/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$ by the first isomorphism theorem.

Example 10.5. In the category of left R-modules, morphisms are also strict.

10.3 Generating sets

Definition 10.4. Let $\Phi : \mathcal{C} \to \mathrm{Set}$ be a faithful functor, and let F be a left adjoint to Φ. Let $F_X = F(X)$ be the free object on X. If $X \xrightarrow{f} \Phi(A)$ for $A \in \mathcal{C}$, we get $\phi : F_X \to A$. Suppose $\mathrm{im}(\phi)$ exists. Then $\mathrm{im}(\phi)$ is called the **subobject of** A **generated by** X.

Example 10.6. In Gp, let $X \subseteq G$. Then $\langle X \rangle$ is the subgroup of G generated by X. This is $\mathrm{im}(\phi : T_X \to G)$, where $\phi(x_1^{n_1} \cdots x_r^{x_r}) = x_1^{n_1} \cdots x_r^{n_r}$. So this is $\{x_1^{n_1} \cdots x_r^{n_r} : x_1 \in X, n_i \in \mathbb{Z}, 1 \leq i \leq r, r \geq 0\}$. We claim that $\langle X \rangle$ is the smallest subgroup of G containing X, or equivalently, the intersection of all subgroups of G containing X. Indeed, this is a subgroup of G containing X, and any subgroup of G containing X must contain these words, since it must be closed under products.

Example 10.7. In Rmod, if $X \subseteq A$, $R \cdot X = \{\sum_{i=1}^n r_i x_i : r_i \in R, x_i \in X, 1 \leq i \leq n, n \geq 0\}$. So $F_X = \bigoplus_{x \in X} R_x \xrightarrow{\phi} A$, where $\phi(r \cdot x) = rx \in A$.

Example 10.8. In the category of (R, S)-bimodules, $RXS = \{\sum_{i=1}^n r_i x_i s_i : r_i \in R, s_i \in S, x_i \in X, 1 \leq i \leq n, n \geq 0\}$. If we have the set of formal sums $RxS = \{\sum_{i=1}^n r_i x s_i : r_i \in R, s_i \in S, 1 \leq i \leq n, n \geq 0\}$ with $(r + r')xs = rxs + r'xs$ and $rx(s + s') = rxs + rxs'$, then the free object is $\bigoplus_{x \in X} RxS$.

Ideals uses (R, R)-subbimodules of R generated by $X \subseteq R$.

Definition 10.5. The **ideal generated by** X is $(X) = \{\sum_{i=1}^n r_i x_i r_i' : r_i, r_i' \in R, x_i \in X\}$. If $X = \{x_1, \ldots, x_n\}$, then we write $(x_1, \ldots, x_n)$.

Remark 10.1. Even if $X = \{x\}$, we still need to take sums to get (x).

11 Group Presentations and Automorphisms

11.1 Cyclic groups and principal ideals

Definition 11.1. A **cyclic group** is a group $G = \langle x \rangle$ that can be generated by one element.

Definition 11.2. A **principal ideal** is an ideal $(x) \subseteq R$ that can be generated by one element.

Example 11.1. In $\mathbb{Z}[x]$, $(2, x)$ is not principal. The elements are $2f + xg$ for $f, g \in \mathbb{Z}[x]$. If $h \mid 2$ and $h \mid x$, then $h = \pm 1$, but $\pm 1 \notin (2, x)$.

Example 11.2. D_{2n} is not cyclic because it is not abelian.

11.2 Presentations of groups

Suppose $X \subseteq G$ is a generating set of G. We get a surjection $\phi : F_X \to G$ given by $\phi(x) = x$ for all $x \in X$. Let $N = \ker(\phi)$, and let $R \subseteq N$ be such that $\overline{\langle R \rangle}$, the smallest normal subgroup of N containing R, equals N.

$$\overline{\langle R \rangle} = \{n_1 r_1^{\pm 1} n_1^{-1} n_2 r_2^{\pm 1} n_1^{-1} \cdots n_k r_k^{\pm 1} n_k^{-1} : n_i \in N, r_i \in R, 1 \leq i \leq k, k \geq 0\}$$

Definition 11.3. $\langle X | R \rangle$ is called a **presentation** of G.

Example 11.3. In D_n, we have the reflection s across the horizontal axis, and the rotation r by $2\pi/n$ degrees. The elements of R are relations on the generators X. So $D_n = \left\langle r, s \mid r^n, s^2, rsrs \right\rangle$ is a presentation of D_n. The elements on the right side of the presentation are things that are equal to the identity of G. So $rsrs = e$, and we get $rs = sr^{-1}$, which tells us how to commute r and s.

Example 11.4. $\mathbb{Z}^2 = \left\langle a, b \mid aba^{-1}b^{-1} \right\rangle$. Here, $a = (1, 0)$ and $b = (0, 1)$. The relation $aba^{-1}b^{-1} = e$ gives $ab = ba$; i.e. a and b commute. We may also write $\mathbb{Z}^2 = \langle a, b, \mid ab = ba \rangle$.

Definition 11.4. The **commutator** of $x, y \in G$ is $[x, y] = xyx^{-1}y^{-1}$.

Example 11.5. Let

$$H = \left\{ \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{Z} \right\} \leq \mathrm{GL}_3(\mathbb{Z})$$

be the invertible matrices with $\mathbb{Z}$-entries in $M_3(\mathbb{Z})$. This is called the **Heisenberg group**.

If

$$x = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

then

$$xy = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad x^{-1}y^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$

So the commutator is

$$[x, y] = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

If we call this z, then x, y, z generate H. This matrix z commutes with everything in the group (you only need to check that $zx = xz$ and $zy = yz$. So $z \in Z(H)$, the center of G. In fact, $Z(H) = \langle z \rangle$. We get that $H = \langle x, y \mid [x, [x, y]], [y, [x, y]] \rangle$.

Definition 11.5. The **center** $Z(G)$ is the set of elements in G that commute with everything; i.e. $zg = gz$ for all $g \in G$. We can also write $H = \langle x, y, z : [x, y] = z, [x, z], [y, z] \rangle$.

The center is a subgroup of G, and it is in fact normal.

Example 11.6. The **quaternion group** of order 8 is

$$Q_8 = \left\langle i, j, k \mid ij = k, i^2 = j^2 = k^2, i^4 = e \right\rangle.$$

This can also be written as $\{\pm 1, \pm i, \pm j, \pm k\}$, where $-1 = i^2 = j^2 = k^2$.

Definition 11.6. We say a group is **finitely generated** if it has a finite set of generators. We say a group is **finitely presented** if it has a finite set of generators and has a finite set of relations on those generators.

Example 11.7. $F_2 = \langle a, b \rangle$ is the group generated by 2 elements. The **commutator subgroup**

$$[F_2, F_2] = \langle [a, b] \mid a, b \in F_2 \rangle \leq F_2,$$

is not finitely generated.

11.3 Automorphism groups

Definition 11.7. The **automorphism group** $\mathrm{Aut}(G)$ of G is the set of isomorphisms $\phi : G \to G$, with composition as the group operation.

Definition 11.8. The **inner automorphism group** of G is $\mathrm{Inn}(G) = \{\gamma_g : g \in G\} \subseteq \mathrm{Aut}(G)$, where $\gamma_g(h) = ghg^{-1}$.

Observe that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

$$\varphi \gamma_g \varphi^{-1}(x) = \varphi(g \varphi^{-1}(x) g^{-1}) = \varphi(g) \varphi(\varphi^{-1}(x)) \varphi(g) = \gamma_{\varphi(g)}(x).$$

Definition 11.9. The **outer automorphism group** of G is $\mathrm{Out}(G) = \mathrm{Aut}(G)/\operatorname{Inn}(G)$.

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

Example 11.8. $\mathrm{Out}(\mathbb{Z}^2) = \mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}_2(\mathbb{Z})$.

12 Automorphisms, Lagrange's Theorem, Isomorphism Theorems, and Semidirect Products

12.1 Automorphisms and Lagrange's theorem

Last time, we had $\gamma : G \to \mathrm{Inn}(G)$ given by $g \mapsto \gamma_g$, where $\gamma_g(x) = gxg^{-1}$. Then $\ker(\gamma) = Z(G)$, so $G/Z(G) \cong \mathrm{Inn}(G)$.

Theorem 12.1 (Lagrange)**.** *Let $H \leq G$, where H and G are finite, then $|G| = [G : H]|H|$. Also, if $K \leq H \leq G$, then $[G : K] = [G : H][H : K]$.*

Proof. $G = \coprod gH$, where the g are a set of coset representatives. Then, since $H \to gH$ given by $h \mapsto gh$ is a bijection, $G = (\#\text{ left cosets})|H| = [G : H]|H|$. □

Definition 12.1. The **order** of $g \in G$ is the smallest $n \geq 1$ such that $g^n = e$. The **exponent** of G is the smallest n such that $g^n = e$ for all $g \in G$.

Example 12.1. $\mathrm{Aut}(D_n) \cong \mathrm{Aff}(\mathbb{Z}/n\mathbb{Z}) \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, where

$$\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\}.$$

The map is $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mapsto \phi_{a,b}$, where $\phi_{a,b}(r) = r^a$ and $\phi_{a,b}(s) = r^b s$. Let's check that this is an isomorphism.

First, we check that we can use the presentation $D_n = \left\langle r, s \mid r^2, s^2, rsrs \right\rangle$. Let $\Phi : F_{\{r,s\}} \to D_n$ be a homomorphism such that $\Phi(f) = r^a$ and $\Phi(s) = r^b s$.

$$\begin{tikzcd} F_{\{r,s\}} \arrow[r] \arrow[d] & D_n \\ D_n \arrow[ur, dashed, "\phi_{a,b}"'] & \end{tikzcd}$$

Then we can check that this agrees.

$$\Phi(r^n) = r^{an} = e$$

$$\Phi(s^2) = r^b s r^b s = r^b r^{-b} = e$$

$$\Phi(rsrs) = r^{a+b} s r^{a+b} s = e$$

As an exercise, check that this map is injective.

In this example, $\langle r \rangle$ was a characteristic subgroup.

Definition 12.2. A subgroup is **characteristic** if it is preserved by all automorphisms ($\varphi(N) \leq N$ for all φ).

Remark 12.1. Even if $K \trianglelefteq N$ and $N \trianglelefteq G$, we cannot conclude that $K \trianglelefteq G$. However,if $K \leq N$ is characteristic and $N \leq G$ is characteristic, then $K \leq G$ is characteristic.

Lemma 12.1. *Let G be a group.*

1. *$Z(G)$ is characteristic in G.*

2. *$G' = [G, G] = \langle [x, y] \mid x, y \in G \rangle$ is characteristic in G.*

Proof. Let's prove the second statement. If ϕ is an automorphism, $\varphi([x, y]) = [\varphi(x), \varphi(y)] \in G'$. $\square$

12.2 The second and third isomorphism theorems

For $H, K \leq G$, let $HK = \{hk : h \in H, k \in K\}$. This may not be a subgroup of G. When is it a subgroup?

Lemma 12.2. *$HK \leq G$ if and only if $HK = KH$.*

Proof. If $KH \subseteq HK$, then $kh \in HK$ for all $k \in K, h \in K$. So $KH \subseteq HK$. This means that for $k \in K, h \in H$, there exists $h' \in H$ and $k' \in K$ such that $kh = h'k'$. So then $h_1 k_1 \cdots h_r k_r = h_k$ for some $h \in H$ and $k \in K$ by moving all the ks to the right. So $HK \leq G$.

Now observe that $(h^{-1}k^{-1}) = (kh)^{-1} \in HK$. So if HK is group, then $HK = KH$. $\square$

Theorem 12.2 (2nd isomorphism theorem)**.** *Let $K \trianglelefteq G$ and $H \leq G$. Then $HK/K \cong H/(H \cap K)$.*

Proof. Let $\varphi : H \to HK/K$ be $\varphi(h) = hK$. This is surjective, and $\ker(\varphi) = H \cap K$. Now apply the first isomorphism theorem. $\square$

Theorem 12.3 (3rd isomorphism theorem)**.** *Let $K \trianglelefteq G$, $H \trianglelefteq G$, and $K \leq H$. Then $G/H \cong (G/K)/(H/K)$.*

Proof. Let $\pi(gK) = gH$. This is a surjective homomorphism. Then $\ker(\pi) = \{gK : gH = H\} = H/K \leq G/K$. Then use the 1st isomorphism theorem. $\square$

12.3 Semidirect products

Let H, N be groups with a homomorphism $H \to \mathrm{Aut}(N)$.

Definition 12.3. The **(external) semidirect product** of N and H is $N \rtimes_\varphi H = N \times H$ with the group operation

$$(n, h)(n', h') = (n\varphi(h)(n'), hh').$$

Let's check that this is a group:

1. The identity is (e, e).
2. Inverses are given by $(n, h)^{-1} = (\phi(h^{-1})(n^{-1}), h^{-1})$.
3. Associativity is left as an exercise.

How does conjugation work in the semidirect product? We can identify $N \leq N \rtimes_\varphi H$ and $H \leq N \rtimes_\varphi H$ by $n \mapsto (n, e)$ and $h \mapsto (e, h)$. Then $NH = N \rtimes_\varphi H$. Then

$$hnh^{-1} = (e, h)(n, e)(e, h^{-1}) = (\phi(h)(n), h)(e, h^{-1}) = (\phi(h)(n), e)$$

Example 12.2. $\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi (\mathbb{Z}/n\mathbb{Z})^\times$. The isomorphism is $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mapsto (b, a)$. Here, $\varphi(a)(b) = ab$.

Example 12.3. $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, where $\varphi(1)(a) = -a$.

Definition 12.4. Let $N \trianglelefteq G$ and $H \leq G$ be such that $N \cap H = \{e\}$ and $NH = G$. Then G is the **internal semidirect product** $N \rtimes H$ of N and H.

Really, these are the same thing. $G = N \rtimes H \cong N \rtimes_\varphi H$, where $\varphi(h)(n) = hnh^{-1}$.

13 Krull-Schmidt, Structure of Finitely Generated Abelian Groups, and Group Actions

13.1 The Krull-Schmidt theorem

Theorem 13.1 (Krull-Schmidt)**.** *Suppose G has normal subgroups $N_i \trianglelefteq G$ for $1 \leq i \leq r$. Then $G \cong N_1 \times \cdots \times N_r$ iff $N_i \cap \prod_{\substack{j=1 \\ j \neq i}}^{r} N_j = \{e\}$ and $N_1 \cdots N_r = G$.*

Proof. For $r = 2$, $N_1 \cap N_2 = \{e\}$ and $N_1 N_2 = G$. Then if $n_i \in N_i$, $n_1 n_2 n_1^{-1} = n_2' \in N_2$. Then $n_2 n_1^{-1} n_2^{-1} = n_1^{-1} n_2' n_2^{-1} \in N_1$. But this is the product of something in N_1 and something in N_2, and $N_1 \cap N_2 = \{e\}$, so $n_2' n_2^{-1} = e$. So $n_2' = n_2$, which gives us that n_1 and n_2 commute. So $G = N \rtimes N_2 = N_1 \times N_2$.

Now induct on r. Suppose this is true for r. Then $N_1 \cdots N_r \cap N_{r+1} = \{e\}$ and $N_1 \cdots N_{r+1} = G$. By induction, $N_1 \cdots N_r = N_1 \times \cdots \times N_r$. Applying the $r = 2$ case, we get $G = N_1 \times \cdots \times N_r \times N_{r+1}$. □

Corollary 13.1. *Let $n = p_1^{r_1} \cdots p_k^{r_k}$ with p_i distinct primes and $r_i \geq 1$. Then*

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{r_k}\mathbb{Z}.$$

Corollary 13.2. *If $\gcd(m, n) = 1$, then*

$$\mathbb{Z}/mn\mathbb{Z} \cong n\mathbb{Z}/mn\mathbb{Z} \times m\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

13.2 The structure theorem for finitely generated abelian groups

Definition 13.1. An abelian group is **torsion-free** if for all $a \in A \setminus \{0\}$ and $n \geq 1$, $na \neq 0$.

Definition 13.2. The **torsion subgroup** B of A is the subgroup of elements of A of finite order.

Theorem 13.2 (structure theorem for finitely generated abelian groups)**.** *Let A be a finitely generated abelian group. Then there exists a unique $r, k \geq 0$ and positive integers $n_i \geq 1$ with $n_k \mid n_{k-1} \mid \cdots \mid n_1$ such that*

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_k\mathbb{Z}.$$

Proof. We claim that torsion-free finitely generated abelian groups are free. Here is a sketch: Choose $a_1, \ldots, a_r \in A$ giving a minimal set of generators. We get $\pi : \mathbb{Z}^r \to A$ sending $e_i \mapsto a_i$, where e_i is the i-th coordiate unit element. Suppose $x = \sum_{i=1}^{r} b_i e_i \in \ker(\pi)$. Let $d = \gcd(b_1, \ldots, b_r)$. If $d \neq 1$, there exists a $y \in \mathbb{Z}^r$ with $dy = x$. Then $y \in \ker(\pi)$. So we may assume $d = 1$. There exists $\phi \in \mathrm{Aut}(\mathbb{Z}^r) = \mathrm{GL}_r(\mathbb{Z})$ such that $\phi(e_1) = x$. Then $\mathbb{Z}^r \xrightarrow{\phi} \mathbb{Z}^r \xrightarrow{\pi} A$ sends $e_1 \mapsto x \mapsto 0$. But then $\pi \circ \phi(e_i)$ for $2 \leq i \leq r$

generate A, contradicting minimality. So $A \cong \mathbb{Z}^r$. For uniqueness, if $A \cong \mathbb{Z}^r \cong \mathbb{Z}^s$, then $A/2A \cong \mathbb{F}_2^r \cong \mathbb{F}_2^s$, so $r = s$.

Let B be the torsion subgroup of A. Note that A/B is torsion-free. We get an exact sequence

$$0 \to B \to A \to \mathbb{Z}^r \to 0.$$

We want to go back from $\mathbb{Z}^r \to A$. Then for $e_i \in \mathbb{Z}^r$, there exists some $a_i \in A$ that maps to e_i. Since $\mathbb{Z}^r$ is free in Ab, there exists $\iota : \mathbb{Z}^r \to A$ such that $\iota(e_i) = a_i$ for all i. Then $A \cong B \oplus \mathbb{Z}^r$. Let n_1 be the exponent of B (lcm of orders is the highest order in this case). Choose $b_1 \in B$ of order n_1; then $A \cong \langle b_1 \rangle \oplus A/\langle b_1 \rangle \cong \mathbb{Z}/n_1\mathbb{Z} \oplus A/\langle b_1 \rangle$. Repeat with n_2, etc. We get $A \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$. Uniqueness follows from the uniqueness of the exponent of a group. □

Example 13.1. Here is an example of this decomposition.

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/360\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

13.3 Group actions

Definition 13.3. A **group action** is a map $\cdot : G \times X \to X$ such that

1. $e \cdot x = x$,
2. $g \cdot (h \cdot x) = (gh) \cdot x$.

The pair of G with the action on X is called a **G-set**.

Remark 13.1. These are left G-sets. We can define right G-sets in a similar way.

Example 13.2. S_X acts on X by $\sigma \cdot x = \sigma(x)$.

Example 13.3. D_n acts on the vertices of a regular n-gon by rotating and reflecting them.

Example 13.4. $\mathrm{GL}_n(R)$ for a ring R acts on R^n viewed as column vectors.

Definition 13.4. G-set is the category with objects a set X with a G-action $G \times X \to X$ and morphisms $f : X \to Y$ such that $f(g \cdot x) = g \cdot f(x)$ for all $x \in X$ and $g \in G$.

Definition 13.5. Te **orbit** of $x \in X$ is $G \cdot x = \{g \cdot x : g \in G\} \subseteq X$.

Remark 13.2. Being in the same orbit gives an equivalence relation on X.

Definition 13.6. The **stabilizer** is $G_x = \{g \in G : g \cdot x = x\} \subseteq G$.

Definition 13.7. G acts **transitively** on X if it has just one orbit ($G \cdot x = X$ for all $x \in X$). G acts **faithfully** if no element of $G \setminus \{e\}$ fixes all $x \in X$; i.e. $\bigcap_{x \in X} G_x = \{e\}$.

Example 13.5. S_X acts transitively and faithfully on X. The stabilizer of $x \in X$ is $S_{X \setminus \{x\}}$, viewed as a subgroup of S_X.

Example 13.6. D_n acts faithfully and transitively on vertices/edges. The stabilizer of the vertex is the subgroup generated by reflection across the axis through 0 and the vertex.

Example 13.7. G acts faithfully and transitively on G by left multiplication but not necessarily by conjugation if $G \neq \{e\}$. With the action of conjugation, the orbits are conjugacy classes $C_x = \{gxg^{-1} : g \in G\}$. $Z(G) = \bigcap_{x \in X} Z_x \neq \{e\}$, where $Z_x = \{g \in G : gxg^{-1} = x\}$, so if $Z(G) \neq \{e\}$, then this is nontrivial.

Example 13.8. G acts on subsets $S \subseteq G$ by conjugation. The orbits are conjugate subsets. The stabilizer of S is $N_G(S)$, the **normalizer** of S. $N_G(S) = \{g \in G : gSg^{-1} = S\}$. Note that $N_G(S)$ acts on S by conjugation. So $\bigcap_{x \in S} Z_x = Z_G(S) = \{g \in G : gs = sg \; \forall x \in S\}$, which is called the **centralizer** of S.

14 Orbit-Stabilizer and Symmetric Groups

14.1 The orbit-stabilizer theorem

Theorem 14.1. *Let X be a G-set. For each x, there is a bijection $\psi_x : G/G_x \to G \cdot x$ given by $gG_x \mapsto g \cdot x$ for $g \in G$.*

Proof. Exercise. $\square$

Corollary 14.1.

$$[G : G_x] = |G \cdot x|.$$

Proposition 14.1 (class equation)**.** *Let T be the set of representatives of conjugacy classes in G. If G is finite,*

$$|G| = \sum_{x \in T} [G : Z_x] = |Z(G)| + \sum_{x \in G \setminus Z(G)} [G : Z_x|.$$

Proof. G acts on itself by conjugation, and the stabilizer of $x \in G$ is Z_x. The orbit of x is C_x, the conjugacy class of x. Then

$$|G| = \sum_{x \in T} |C_x| = \sum_{x \in T} [G : Z_x].$$

$\square$

14.2 Action of symmetric groups

Let $\sigma \in S_n$. An element σ acts on $X_n = \{1, \ldots, n\}$.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Definition 14.1. A **k-cycle** ($k \leq n$) is the permutation

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}(i) = \begin{cases} a_{j+1} & i = a_j, i \leq j \leq k-1 \\ a_1 & i = a_k \\ i & \text{otherwise.} \end{cases}$$

Every permutation is a product of disjoint cycles, which commute.

Example 14.1.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 6 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 6 \end{pmatrix} \begin{pmatrix} 4 & 5 \end{pmatrix}$$

Definition 14.2. A **transposition** is a 2-cycle.

Proposition 14.2. *Every cycle can be written as a product of transpositions.*

Proof. Prove the following relationship by induction on n:

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_2 & a_3 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1} & a_{n-2} \end{pmatrix}.$$

□

How does conjugation work?

$$\sigma \begin{pmatrix} a_1 & a_2 & \cdots a_k \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_k) \end{pmatrix}.$$

Example 14.2. What is the centralizer of $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \in S_5$? This is $\left\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 5 \end{pmatrix} \right\rangle$.

Theorem 14.2. *If $\sigma = \tau_1 \cdots \tau_r = \rho_1 \cdots \rho_s$ for transpositions τ_i and ρ_i, then $r \equiv s \pmod 2$.*

Proof. Let $S_n \circlearrowright \mathbb{Z}[x_1, \ldots, x_n]$ by $\sigma \cdot f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Let

$$p(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Then $\tau \cdot p = \prod_{1 \leq i < j \leq n}(x_{\tau(i)} - x_{\tau(j)})$. If $\tau = \begin{pmatrix} k & \ell \end{pmatrix}$ with $k < \ell$, then $x_{\tau(i)} x_{\tau(j)}$ occurs with the sign in the product unless $i = k, j \leq \ell$ or $i \geq k, j = \ell$. So $\tau \cdot p = (-1)^{2(\ell - k) - 1} p = -p$.

In general, $\sigma \cdot p = \operatorname{sgn}(\sigma) p$, where $\operatorname{sgn} : S_n \to \{\pm 1\}$ is a homomorphism, and $\operatorname{sgn}(\tau) = -1$ for any transposition τ. So $\operatorname{sgn}(\sigma) = (-1)^r = (-1)^s$, so $r \equiv s \pmod 2$. □

14.3 Alternating groups

In the above proof, we defined the **sign** of a permutation, which is ± 1.

Definition 14.3. A permutation is **even/odd** if its sign is $1/-1$.

Example 14.3. What is the sign of a cycle? $\operatorname{sgn} \begin{pmatrix} 1 & \cdots & k \end{pmatrix} = (-1)^{k+1}$

Definition 14.4. The **alternating group** is $A_n = \ker(\operatorname{sgn}) = \{\sigma \in S_n : \sigma \text{ is even}\} \trianglelefteq S_n$.

Note that $|A_n| = n!/2$ for $n \geq 2$.

Definition 14.5. A group is **simple** if it has no proper, nontrivial normal subgroups (and is nontrivial).

Example 14.4. A_4 is not simple. $\{\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c & d \end{pmatrix} : \{a, b, c, d\} = \{1, 2, 3, 4\}\} \cup \{e\} \trianglelefteq A_4$

Theorem 14.3. *A_5 is simple.*

Proof. An element in A_5 must be e, a three cycle, a product of two two-cycles, or a five cycle. The centralizer of $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ in $A_5 = \left\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 5 \end{pmatrix} \right\rangle \cap A_5 = \left\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \right\rangle$. So $C_{(1\,2\,3)}$, the set of 3-cycles, has size 20. Similarly number of products of two 2-cycles is 15, and the number of five cycles is 12.

The conjugacy classes have order 1, 12, 12, 15, and 20. Every normal subgroup N is a union of conjugacy classes (including $\{e\}$) and has order dividing $|A_n| = 60$. The only way is to take $N = A_5$ or $N = e$. □

Remark 14.1. An action $G \circlearrowright X$ can be thought of as a homomorphism $\rho : G \to S_X$. Then $\ker(\rho) = \bigcap_{x \in X} G_x$ is trivial if and only if the aciton is faithful. G acting on G by left multiplication gives us that $\rho : G \to S_G$ is injective. This is Cayley's theorem.

15 Simple Groups, Burnside's Formula, and p-Groups

15.1 Simple groups

Theorem 15.1. *A_n is simple for $n \geq 5$.*

Proof. Proceed by induction on n. We know this for $n = 5$. Assume it for $n-1$ with $n \geq 6$. The intersection of the stabilizer of i and A_n is $G_i = (S_n)_i \cap A_n \cong A_{n-1}$ for $1 \leq i \leq n$, so G_i is simple. Let $N \trianglelefteq A_n$ with $N \neq \{e\}$. If there exists $i \in X_n = \{1, \ldots, n\}$ and $\tau \in N \setminus \{e\}$ with $\tau(i) = i$, then $N \cap G_i \neq \{e\}$ and $N \cap G_1 \trianglelefteq G_i$. So $N \cap G_i = G_i$; i.e. $G_i \leq N$.

For any $\sigma \in A_n$ with $\sigma(i) = j$, we have $\sigma G_i \sigma^{-1} = G_j$. Then $\sigma = \begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} k & \ell \end{pmatrix}$ works for some $\{k, \ell\} \cap \{i, j\} = \varnothing$ since $n \geq 4$. So $G_j \leq N$ since $N \trianglelefteq A_n$. So every product of 2 transpositions is in N since $n \geq 5$, so $A_n = N$.

Take $\tau \in N$. If there exists $\tau' \in N$ and $i \in X_n$ such that $\tau(i) = \tau'(i)$, then $\tau(\tau')^{-1}(i) = i$. Then $\tau = \tau'$, or $N = A_n$. Write τ as a product of disjoint cycles. There are 2 cases:

1. $\tau = \begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix} \cdots$ where $k \geq 3$: Pick $\sigma \in A_k$ such that $\sigma(a_1) = a_1, \sigma(a_2) = a_2, \sigma(a_3) \neq a_3$. Take $\tau' := \sigma\tau\sigma^{-1}$. This works.

2. $\tau = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \cdots \begin{pmatrix} a_{m-1} & a_m \end{pmatrix}$: Take $\sigma = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_3 & a_5 \end{pmatrix}$. Then $\tau' = \sigma\tau\sigma^{-1}$ works as well. So $\tau'(a_1) = \tau(a_1)$ but $\tau' \neq \tau$. $\square$

In general, the following theorem is true. We will not prove it.[3]

Theorem 15.2 (classification of finite simple groups)**.** *Every finite simple group is isomorphic to one of*

1. *$\mathbb{Z}/p\mathbb{Z}$ with p prime*
2. *(simple) group of Lie type*
3. *A_n for $n \geq 5$*
4. *one of 26 sporadic simple groups*
5. *the Tits group*

15.2 Burnside's formula

For $g \in G$ and X a G-set, denote the set of fixed points of g as $X^g = \{x \in X : g \cdot x = x\}$. If $S \subseteq G$, let $X^S = \{x \in X : g \cdot x = x \,\forall g \in S\} = \bigcap_{g \in S} X^g$. Recall that the stabilizer of x is $G_x = \{g \in G : g \cdot x = x\} \subseteq G$. Then $g \in G_x \iff x \in X^g$.

[3] The proof is thousands of pages long.

Theorem 15.3 (Burnside's formula)**.** *Suppose G is finite, and X is a finite G-set. The number r of G-orbits in X is*

$$r = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Proof. Let $S = \{(g,x) : g \in G, x \in X, g \cdot x = x\}$. On one hand,

$$S = \coprod_{g\in G}\{(g,x) : x \in X^g\},$$

which is in bijection with X^g. On the other hand,

$$S = \coprod_{x\in X}\{(g,zx) : g \in G_x\},$$

which is in bijection with G_x. So

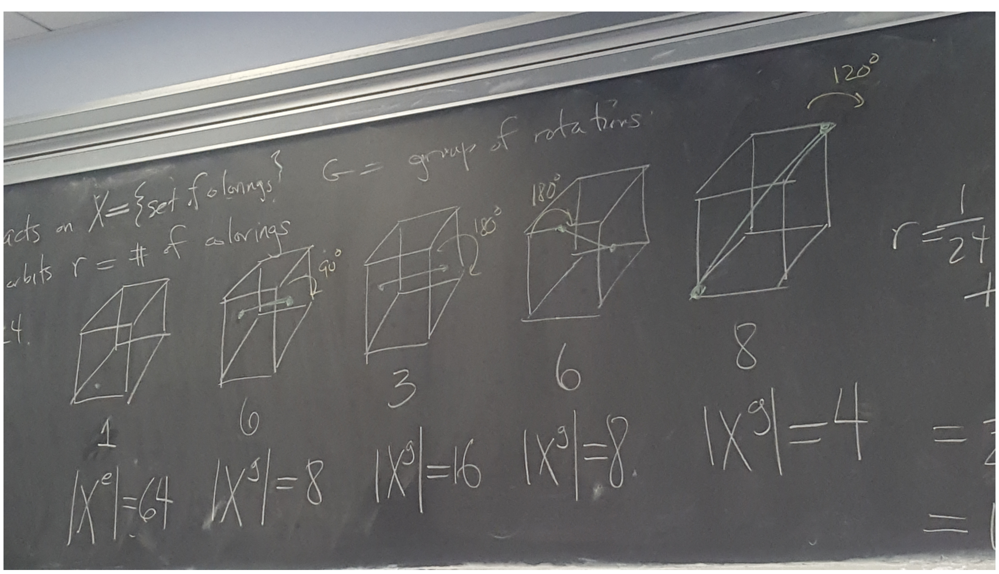
$$\sum_{g\in G}|X^g| = |S| = \sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|G\cdot x|} = |G|\sum_{x\in X}\frac{1}{|G\cdot x|}.$$

Each orbit appears $|G \cdot x|$ times in this sum. So we get

$$\sum_{g\in G}|X^g| = |G|\sum_{\text{orbit reps.}} 1 = |G|r. \qquad \square$$

This allows us to solve fun counting problems.

Example 15.1. How many ways are there to color the sides of a cube red and blue (that look different under rotations)? Let G be the group of rotations of a cube. G acts on X, the set of colorings of a cube. The number of orbits r is the number of colorings. $|G| = 24$. Let's write out what the elements are and the number of fixed points in each case.



So, by Burnside's formula,

$$r = \frac{1}{24}(64 + 6 \cdot 8 + 3 \cdot 16 + 6 \cdot 8 + 8 \cdot 4) = 10.$$

15.3 p-groups

Let p be prime.

Definition 15.1. A group G is a p**-group** if every element of G has a p-power order.

Example 15.2. $\mathbb{Z}/p^n\mathbb{Z}$ is a p-group.

Example 15.3. Q_8 and D_4 are 2-groups.

Example 15.4. Here is an infinite p-group. $\{a/p^n : 0 \leq a \leq p^n - 1, n \geq 1\} \subseteq \mathbb{Q}/\mathbb{Z}$.

Lemma 15.1. *Let G have p-power order, and let X be a finite G-set. Then*

$$|X| \equiv |X^G| \pmod{p}.$$

Proof. Let S be a set of orbit representatives in X. Then

$$|X| = \sum_{x \in S} |G \cdot x| = \sum_{x \in S} [G : G_x] \equiv \sum_{x \in X^G} 1 = |X^G| \pmod{p},$$

where $X^G \subseteq S$ is the set of singleton orbits. $\square$

Theorem 15.4 (Cauchy)**.** *Let p be prime and G a finite group with $p \mid |G|$. Then G contains an element of order p.*

Proof. Let $X = \{(a_1, \dots, a_p) \in G^p : a_1 \cdots a_p = e\}$. Then $S_p \circlearrowright X$ by permuting the indices $\sigma(a_1, \dots, a_p) = (a_{\sigma(1)}, \dots, a_{\sigma(p)})$. Let $\tau = \begin{pmatrix} 1 & 2 & \cdots & p \end{pmatrix}$. Then $H = \langle \tau \rangle$ acts on X such that $X^H = X^\tau = \{(a, a, \dots, a) \mid a^p = e\}$. Note that $X^H \neq \varnothing$ since $(e, \dots, e) \in X^H$. Also, $|X| = |G|^{p-1} \equiv 0 \pmod{p}$. By the lemma, $|X^H| \equiv 0 \pmod{p}$, so since $X^H \neq \varnothing$, X^H has another element; i.e. there exists $a \neq e$ with $a^p = e$. $\square$

Corollary 15.1. *If G is a finite p-group, then G has p-power order.*

Proposition 15.1. *If G is a nontrivial finite p-group, then $Z(G) \neq \{e\}$.*

Proof. If $Z(G) = \{e\}$, then the class equation gives

$$|G| = 1 + \sum_{x \in S} C_x = 1 + \sum_{x \in S} [G : Z_x] \equiv 1 \pmod{p},$$

where S is a set of representatives of nontrivial conjugacy classes. Since G has p-power order, we get $|G| = 1$. $\square$

Theorem 15.5. *Every group of order p^2 is abelian.*

Proof. Let $|G| = p^2$. If G is not abelian, then $Z(G)$ has order p. Then $Z(G) = \langle a \rangle$, where a has order p. Let $b \notin \langle a \rangle$. Then b has order p, and $G = \langle a, b \rangle$. Note that b commutes with a because $a \in Z(G)$. But b commutes with itself, so $b \in Z(G)$. This is a contradiction. $\square$

16 Sylow Theorems

16.1 Sylow p-subgroups

For this lecture, we will assume that a p-group is finite and of order p^k. Let G be a finite group. Take $p \mid |G|$ and say that $p^n \mid\mid |G|$ if $p^n \mid |G|$ but $p^{n+1} \nmid |G|$.

Definition 16.1. A **p-subgroup** of G is a subgroup of order p^k for some $k \leq n$.

Definition 16.2. A **Sylow p-subgroup** of G is a p-subgroup of G which is not properly contained in any other p-subgroup.

Example 16.1. The symmetric group S_5 has order $120 = 2^3 \cdot 3 \cdot 5$. For $p = 5$, a Sylow 5-subgroup will look like $\langle \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} \rangle$. There are $6 = 4!/4$ of these, For $p = 3$, a Sylow 3-subgroup will look like $\langle \begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix} \rangle$. There are 10 of these. For $p = 2$, a Sylow 2-subgroup will look like $\langle \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix}, \begin{pmatrix} a_1 & a_3 \end{pmatrix} \rangle$. There are 15 of these.

Observe that the number of each type of Sylow p-subgroup divides the order of the group. In general, this is unusual.

16.2 Sylow theorems

Let $n_p(G)$ be the number of p-Sylow subgroups of G, and let $\mathrm{Syl}_p(G)$ be the set of Sylow p-subgroups of G. Our goal will be to prove the following.

Theorem 16.1 (Sylow theorems)**.** *Let G be a finite group.*

1. *Every Sylow p-subgroup of G has order p^n, where $p^n \mid\mid |G|$.*
2. *Any two Sylow p-subgroups are conjugate.*
3. *$n_p(G) \mid |G|$, and $n_p(G) \equiv 1 \pmod{p}$.*

Recall that if P is a p-group, X is a finite set, and $P \circlearrowright X$, then $|X| \equiv |X^p| \pmod{p}$.

Lemma 16.1. *Let G be finite, and let H be a p-subgroup of G. Then*

$$[G : H] \equiv [N_G(H) : H] \pmod{p}.$$

Proof. Let $L = G/H$ be the set of right cosets of H. Then $|L| = [G : H]$. $H \circlearrowright L$ by $h \cdot (aH) = (ha)H$. If $aH \in L^H$, then for all $h \in H$, $haH = aH$, which means that $a^{-1}haH = H$, which is the same thing as $a^{-1}ha \in H$ for all $h \in H$. □

Theorem 16.2. *If $H \leq G$, and $|H| = p^k$ for $k < n$, then there is some $P \leq G$ with $H \trianglelefteq P$ and $|P| = p^{k+1}$.*

Proof. If $|H| \neq p^n$, then $p \mid [G : H]$, so $p \mid [N_G(H) : H] = |N_G(H)/H|$. So $N_G(H)/H$ has a subgroup P/H of order p. Then $P \leq N_G(H)$, and $|P| = p^{k+1} = |P/H||H|$. So $H \trianglelefteq P$. □

This proves the first Sylow theorem. Let's prove the second theorem.

Proof. Take $P, Q \in \mathrm{Sly}_p(G)$. We know that $|P| = |Q| = p^n$. Let $Q \circlearrowright G/P$. Since $p \nmid |G/P|$, $p \nmid |(G/P)^Q|$. So $(G/P)^Q \neq \varnothing$, and we get some xP such that $qxP = xP$ for all $q \in Q$. This means that $(x^{-1}qx)P = P$, so $x^{-1}qx \in P$ for all $q \in Q$. So $x^{-1}Qx \subseteq P$. Since P and $x^{-1}Qx$ have the same order, $x^{-1}Qx = P$. □

Now let's prove the third Sylow theorem.

Proof. Let $G \circlearrowright \mathrm{Syl}_p(G)$ by conjugation. By the second Sylow theorem, this action is transitive. Let P be a Sylow p-subgroup of G. By orbit-stabilizer,

$$n_p(G) = |\mathrm{Syl}_p(G)| = [G : \mathrm{Stab}(P)] = [G : N_G(P)].$$

We have that

$$[G : P] = [G : N_G(P)][N_P(G) : P]$$

and

$$[G : P] \equiv [N_G(P) : P] \not\equiv 0 \pmod{p},$$

so

$$[G : N_G(P)] \equiv 1 \pmod{p}.$$

□

Example 16.2. Let $|G| = 42$. We will show that G has a nontrivial normal subgroup. $n_7(G) \mid 42$ and $7 \nmid n_7(G)$, so $n_7(G) \mid 6$. So $n_7(G) = 1$. So if $|H| = 7$, then $H \trianglelefteq G$.

Example 16.3. Let $|G| = 30$. We show that G has a nontrivial normal subgroup. Then G has 9 nontrivial normal subgroups. $n_5(G) \mid 30$, so $n_5(G) \mid 6$. Then $n_5(G) = 1$ or 6. Similarly, $n_3(G) \mid 10$, so $n_3(G) = 1$ or 10. Assume that $n_5(G), n_3(G) > 1$. Then we have 6 5-subgroups. Each one has 4 elements of order 5. So there are 24 elements of order 5. If $n_3(G) = 10$, there are 20 different elements of order 3. This is impossible because $24 + 20 > 30$.

17 Applications of the Sylow theorems

17.1 Groups of order p^n, pq, and p^2q

Proposition 17.1. *Groups of order p^n with $n > 1$ are not simple.*

Proof. Assume for contradiction that G is simple. Note that $Z(G) \|G\|$ and is nontrivial. So $Z(G) = G$, which makes G abelian. So G has order p. $\square$

Proposition 17.2. *Groups of order pq with primes $p < q$ have a normal subgroup of order q and are cyclic if $q \not\equiv 1 \pmod{p}$.*

Proof. Note that $n_q(G) \mid p$, and $n_q(G) \equiv 1 \pmod{q}$. So $n_q(G) = 1$. By Sylow's theorem, $Q \trianglelefteq G$, where Q is a Sylow-q subgroup. So $PQ = G$, and $P \cap Q = \{e\}$, so $G = Q \rtimes P$. This gives a homomorphism $\varphi : P \to \mathrm{Aut}(Q)$. Moreover, $\mathrm{Aut}(Q) = (\mathbb{Z}.q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$. The map φ is trivial unless $q \cong 1 \pmod{p}$. If it is trivial, then $G = P \times Q = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$. $\square$

Proposition 17.3. *Groups of order 255 are cyclic.*

Proof. Factor $255 = 3 \cdot 5 \cdot 17$. By the Sylow theorems, $n_17(G) = 1$, so we hav a normal Sylow 17-subgroup P such that $G/P \cong \mathbb{Z}/15\mathbb{Z}$. Look at $n_3(G)$ and $n_5(G)$. Note that $n_3(G) = 1$ or 85, and $n_5(G) = 1$ or 51. If $n_3(G) = 85$, we get $2 \cdot 85 = 170$ elements of order 3. If $n_5(G) = 51$, we have $4 \cdot 51 = 204$ elements of order 5. We cannot have both, so we either have a normal Sylow 3-subgroup or a normal Sylow 5-subgroup Q.

Then $PQ \trianglelefteq G$, and R is a Sylow-4 or Sylow-3 subgroup. Then $G = PQ \rtimes R$, with a homomorphism $R \to \mathrm{Aut}(PQ)$. Since PQ is cyclic, $\mathrm{Aut}(PQ) \cong \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Since R has order prime to 2, this homomorphism is trivial. So we get $G = P \times Q \times R \cong \mathbb{Z}/255\mathbb{Z}$. $\square$

Proposition 17.4. *Groups of order p^2q with p, q prime are not simple.*

Proof. If $p > q$, then $n_p(G) \cong 1 \pmod{p}$ and $n_p(G) \mid q$, so $n_p(G) = 1$. If $q > p$. $n_q(G) = 1$ or p^2. Assume $n_q(G) = p^2$. Then $p^2 \cong 1 \pmod{q}$, so $q \mid (q-1)$ or $q \mid p+1$. Since $q > p$, we cannot have $q \mid (p-1)$, so we must have $q \mid (p+1)$, which gives $p = 2$ and $q = 3$. So $n_2(G) = 3$, and $n_q(G) = 4$. So there are 8 elements of order 3 and at least $3 + 2 + 1$ elements of 2-power order. But this gives 14 elements, which is greater than $12 = 2^2 \cdot 3$. $\square$

17.2 Subgroups of S_n

Proposition 17.5. *Suppose that G is finite, simple, and $p \mid |G|$ (but $p \not\|\,|G|$). Then G is isomorphic to a subgroup of S_n, where $n = n_p(G)$.*

Proof. G acts on $\mathrm{Syl}_p(G)$ by conjugation. There are n such Sylow p-subgroups, so this gives a homomorphism $\rho : G \to S_n$ such that $\ker(\rho) \trianglelefteq G$. If $\ker(\rho) = 1$, then G is isomorphic to a subgroup of S_n. If $\ker(G) = G$, the action is trivial but also transitive. So there exists a unique, therefore normal, Sylow p-subgroup. $\square$

Proposition 17.6. *There are no simple groups of order 160.*

Proof. Factor $160 = 2^5 \cdot 5$. If G is simple and $|G| = 160$, the $n_5(G) = 16$ and $n_2(G) = 5$. So G is isomorphic to a subgroup of S_5. But $|S_5| = 5! = 120$, which is a contradiction. $\square$

Proposition 17.7. *Let $H, K \leq G$ with H, K finite. Then $|HK| = |H||K|/|H \cap K|$.*

Proof. Consider the bijection $H/(H \cap K) \to HK/K$. Finish the rest for homework. $\square$

Proposition 17.8. *There are no simple groups of order 48.*

Proof. Factor $48 = 2^4 \cdot 3$. If G is simple, $n_2(G) = 3$. Let P, Q be Sylow 2-subgroups of G. Then $|P \cap Q| = |P||Q|/|PQ| = 256/|PQ|$. Since $|PQ > 48$, we get $|P \cap Q| > 4$. So $|P \cap Q| = 8$, which gives $|PQ| = 32$. Then $P \cap Q \trianglelefteq P, Q$. So $N_G(P \cap Q) \supseteq PQ$ must equal G, and we get that $P \cap Q \trianglelefteq G$. $\square$

This is a special case of the following proposition.

Proposition 17.9. *Let $p^n \mid\mid |G|$, and suppose that $|P \cap Q| \leq p^{n-r}$ for some $r \geq 1$ for all Sylow p subgroups $P \neq Q$. Then $n_p(G) \equiv 1 \pmod{p^r}$.*

Proof. The idea is to show that $P \cap Q = P \cap N_G(Q)$. We will do this next time. $\square$

18 Composition Series

18.1 Restrictions on simple groups

Lemma 18.1. *Let P, Q be Sylow p-subgroups of a group G. $P \cap Q = P \cap N_G(Q)$.*

Proof. Let $H = P \cap N_G(Q)$. We know that $H \leq N_G(Q)$, so $HQ = QH$. So $HQ \leq G$. Since $|HQ| = |H||Q|/|H \cap Q|$, HQ is a p-group. So $H \leq Q$ since Q is a Sylow p-subgroup. $\square$

Proposition 18.1. *Let G be a finite group and let $P^n \mid\mid |G|$ for $n \geq 1$. Assume that for all Sylow p subgroups $P \neq Q$, $|P \cap Q| \leq p^{n-r}$. Then $n_p(G) = 1 \pmod{p}^r$.*

Proof. $P \circlearrowright \mathrm{Syl}_p(G)$ by conjugation. Note that $p^n \mid [P : P \cap Q] = [P : P_Q] = |\text{orbit of } Q|$. We can count

$$n_p(G) = \sum_{\text{orbits}} |\text{orbit}| \equiv 1 \pmod{p^r}.$$

$\square$

Proposition 18.2. *Every simple group of order 60 is isomorphic to A_5.*

Proof. Factor $60 = 4 \cdot 3 \cdot 5$. Then $n_5(G) = 6$, $n_3(G) = 4$ or 10, and $n_2(G) = 3, 5$ or 15. We cannot have $n_3(G) = 4$ or $n_2(G) = 3$. If $n_2(G) = 5$, then G is isomorphic to a subgroup of $S_5 \cong S_{\mathrm{Syl}_2(G)}$. So the image of G has index 2. If $G \neq A_5$, then $G \cap A_5$ has index 2 in A_5. Since subgroups of index 2 are normal, we get $G \cap A_5 \trianglelefteq A_5$, contradicting the fact that A_5 is simple. So in this case, $G \cong A_5$.

If $n_2(G) = 15$, then $15 \not\equiv 2 \pmod 4$, so we have $P, Q \in \mathrm{Syl}_2(G)$ with $|P \cap Q| = 2$. Then $N_G(P \cap Q) \supseteq PQ$. So $|N_G(P \cap Q)| > 4$ and is a multiple of 4 dividing 60. So $|N_G(P \cap Q)| \in \{12, 20, 60\}$. If $|P \vee Q| = 60$, then $N_G(P \cap Q) = G$, so $P \cap Q \trianglelefteq G$. If $|M| = 12$ or 20, then G acts on G/M, of order ≤ 5. So G is isomorphic to a subgroup of S_3 or S_5. S_3 is impossible because G is too large, and we have already treated the case of S_5. $\square$

Proposition 18.3. *There are no simple groups of order* $396 = 4 \cdot 9 \cdot 11$.

Proof. If G is simple, then $n_{11}(G) = 12 = [G : N_G(P)]$, where P is a Sylow 11-subgroup. Then $|N_G(P)| = 33$. So G is isomorphic to a subgroup of S_{12}, and we get $N_G(P) \leq N_{S_{12}}(P)$. Then P is still Sylow 11 in S_12, so $n_{11}(S_{12}) \mid 12!/33 = 10! \cdot 4$. We can count $n_{11}(S_{12}) = 12!/(11 \cdot 10) = 9! \cdot 12$. But $12 \nmid 40$, so we have a contradiction. $\square$

18.2 Composition series

Definition 18.1. Let G be a group. A **series** is a collection $(H_i)_{i \in \mathbb{Z}}$ of subgroups of G such that $H_{i-1} \leq H_i$ for all i.

Definition 18.2. A series is **ascending** if $H_i = 1$ for all i sufficiently small. A series is **descending** if $H_i = G$ for all sufficiently large i. A series is **finite** if it is both ascending and descending.

In the descending case, we often take $H_i \leq H_{i-1}$ and only deal with $i \geq 0$. If the series is finite and we write

$$1 = H_0 \leq H_1 \leq \cdots \leq H_{t-1} \leq H_t = G$$

with $H_i \neq H_{i-1}$ for all i, then we say that t is the length of the series.

Definition 18.3. A finite series is **subnormal** if $H_{i-1} \trianglelefteq H_i$ for all i. A finite series is **normal** if $H_{i-1} \trianglelefteq G$ for all i.

Definition 18.4. A **composition series** is a subnormal series such that H_i/H_{i-1} are all simple or trivial. The H_i/H_{i-1} are called **composition factors**.

Example 18.1. In the composition series

$$1 \trianglelefteq A_5 \trianglelefteq S_5$$

the composition factors are S_5 and $\mathbb{Z}/2\mathbb{Z}$.

Example 18.2. In the composition series

$$1 \trianglelefteq p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \trianglelefteq p^{n-2}/p^n\mathbb{Z} \trianglelefteq \cdots \trianglelefteq p\mathbb{Z}/p^n\mathbb{Z} \trianglelefteq \mathbb{Z}/p^n\mathbb{Z}$$

the composition factors are all $\mathbb{Z}/p\mathbb{Z}$.

Example 18.3. In the composition series

$$1 \trianglelefteq \mathbb{Z}/2\mathbb{Z} \trianglelefteq (\mathbb{Z}/2\mathbb{Z})^2 \trianglelefteq A_4 \trianglelefteq S_4$$

the composition factors are $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z}$.

Lemma 18.2. *Given a composition series and $N \trianglelefteq G$,*

1. *We have a composition series $H_{f(i)} \cap N$ with $f : \{0, \ldots, s\} \to \{0, \ldots, t\}$ with $f(0) = 0$ with the i-th factor $H_{f(i)}/H_{f(i)-1} \cong H_{f(i)}/H_{f(i-1)}$*
2. *$\overline{H_i} = H_i/(H_i \cap N)$, and we have a composition series for G/N of the form $\overline{H_{f(i)}}$ with $f' : \{0, \ldots, r\} \to \{0, \ldots t\}$ increasing with $f(0) = 0$ and composition factors $H_{f'(i)}/H_{f'(i)-1}$*
3. *$\mathrm{im}(f) \cup \mathrm{im}(f') = \{0, \ldots, t\}$, and $r + s = t$.*

19 The Jordan-Hölder Theorem and Solvable Groups

19.1 The Jordan-Hölder theorem

Last time we had a lemma which said that if $N \trianglelefteq G$, then a composition series for N comes from a composition series for G by taking $H_i \cap N$ and eliminating duplicates. A composition series for G/N comes from H_iN/N and eliminating duplicates. If the composition series for N has length r, and the composition series for G/N has length s, then $r+s=t$, where t is the length of the composition series for G.

Lemma 19.1. *Let $N \trianglelefteq G$. There exists a 1 to 1 correspondence between subgroups of G containing N and subgroups of G/N.*

Lemma 19.2. *Let $N \trianglelefteq G$ have composition series $1 = H_0 \trianglelefteq \cdots \trianglelefteq H_s = N$ and G/N have composition series $1 = Q_0 \trianglelefteq \cdots \trianglelefteq Q_r = G/N$. Then let H_{s+i} be the unique subgroup of G containing N with $N_{s+i}/N = Q_i$. Then $1 = H_0 \trianglelefteq \cdots \trianglelefteq H_t = G$ for $t = r+s$ is a composition series for G, and $H_{s+i}/H_{s+i-1} \cong Q_i/Q_{i-1}$.*

Theorem 19.1 (Jordan-Hölder)**.** *Let G be a finite group.*

1. *G has a composition series.*
2. *If $G \neq 1$ with two composition series $(K_i)_{i=0}^s$ and $(H_j)_{j=0}^t$, then $s=t$, and there exists $\sigma \in S_t$ such that $H_{\sigma(i)}/H_{\sigma(i)-1} \cong K_i/K_{i-1}$.*

Proof. Proceed by induction on $|G|$. If G is simple, $1 \trianglelefteq G$ is the only composition series, and we are done. If G is not simple, there there exists a proper normal subgroup $N \trianglelefteq G$ with $N \neq 1$. By induction, N and G/N have composition series. By the lemma, G has a composition series, as well.

To prove the second statement induct on the minimal length s of a composition series $(K)_{i=0}^s$. If $s=1$, then G is simple, so this case is done. Let $N = K_{s-1} \trianglelefteq G$. N has the composition series $(K_i)_{i=0}^{s-1}$. N also has the composition series $(H_{f(i)} \cap N)_{i=0}^r$ where $f : \{0, \dots, r\} \to \{0, \dots, t\}$ is increasing with $f(0) = 0$. By induction, $r = s-1$, and there exists a $\sigma \in S_{s-1}$ such that $K_i/K_{i-1} \cong (H_{f(\sigma(i))} \cap N)/(H_{f(\sigma(i))-1} \cap N)$.

Let $k < r$ be maximal such that $H_{k-1} \leq N$. Then $H_{k-1} \cap N = H_{k-1} \trianglelefteq H_k \cap N < H_k$. So $H_{k-1} = H_k \cap N$, which implies that $k \notin \operatorname{im}(f)$. Then $H_k/H_{k-1} \cong H_k/(H_k \cap N) \cong H_kN/N = G/N$. If $(H_iN)/(H_{i-1}N) \neq 1$ for $i \neq k$, then G/N has composition series of length ≥ 2, but G/N is simple. So $r = t-1$. □

19.2 Solvable groups

Definition 19.1. Let $G_{i\geq 0}^{(i)}$ be descending. The series $G^{(0)} = G$, $G^{(1)} = G' = [G,G]$, with general term $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for all $i \geq 0$ is called the **derived series** of G.

Definition 19.2. A group G is **solvable** if it has finite derived serires.

Example 19.1. Abelian groups are solvable.

Example 19.2. Semidirect products of abelian groups are solvable. If $G = N \rtimes H$, then $G' \leq N$ and $G'' = 1$.

Example 19.3. Simple nonabelian groups are not solvable. If G is simple and nonabelian, then $G' = G$.

Example 19.4. Let R be a commutative ring. The Heisenberg group

$$H = \left\{ \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \right\} \subseteq \mathrm{GL}_3(R)$$

is solvable.

$$\left[\begin{bmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \right] = \begin{bmatrix} 1 & 0 & xy \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

so

$$H' = \left\{ \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\} = Z(H),$$

and $H'' = 1$.

Proposition 19.1. *The following are equivalent:*

1. *G is solvable.*
2. *G has a normal series with abelian composition factors.*
3. *G has a subnormal series with abelian composition factors.*

Proof. We need only show that $3 \implies 1$. Let $1 = N_t \trianglelefteq \cdots \trianglelefteq N_1 \trianglelefteq N_0$ with abelian composition factors. Then G/N_i is abelian iff $G' \leq N_i$. N_{i-1}/N_i is abelian, so $N_i \geq (N_{i-1})' \geq G^{(i+1)}$. So $G^{(t)} = 1$ so G is solvable. $\square$

Lemma 19.3. *Let G be a group.*

1. *If G is solvable, then $H \leq G$ is solvable and G/N is solvable for $N \trianglelefteq G$.*
2. *If $N \trianglelefteq G$ and G/N are both solvable, then G is solvable.*

Proposition 19.2. *A group G with a composition series is solvable if and only if it is finite and its Jordan Hölder factors are all cyclic of prime order.*

20 Schreier's Refinement Theorem and Nilpotent Groups

20.1 Schreier's refinement theorem

Definition 20.1. A **refinement** of a subnormal series $(H_i)_{i=0}^t$ os a subnormal series $(K_j)_{j=0}^s$ usch that there exists an increasing function $f : \{0, \dots, t\} \to \{0, \dots, s\}$ with $H_i = K_{f(i)}$ for all i.

Definition 20.2. Two subnormal series $(H_i)_{i=0}^t$ and $(K_j)_{j=0}^s$ are **equivalent** if $s = t$ and there exists a permutation $\sigma \in S_t$ such that $H_i/H_{i-1} \cong K_{\sigma(i)}/K_{\sigma(i)-1}$ for all $i \in \{1, \dots, t\}$

Theorem 20.1 (Schreier refinement theorem)**.** *Any two subnormal series in a group G have equivalent refinements.*

Proof. Here is the idea of the proof. If $(H_i)_{i=0}^t$ and $(K_j)_{j=0}^s$ are subnormal series, let $N_{si+j} = H_i(H_{i+1} \cap K_j)$ for all $0 \leq i < t$ and $0 \leq j < s$ and $N_{st} = G$. This refines (H_i). Do the same for (K_j). To see that they are equivalent, use the butterfly (or Zassenhaus) lemma from homework. $\square$

20.2 Nilpotent groups

Definition 20.3. The **lower central series** of a group G is $G = G$. $G_{i+1} = [G, G_i]$, where $[G, G_i]$ is the subgroup generated by commutators, $\langle \{[a, b] : a \in G, b \in G_i\} \rangle$.

Definition 20.4. A group G is **nilpotent** if $G_n = 1$ for all sufficiently large n in the lower central series. The smallest n such that $G_{n+1} = 1$ is the **nilpotence class** of G

Example 20.1. Let $E_{i,j}(\alpha)$ be the elementary matrix $I + \alpha e_{i,j}$.

1. $E_{i,j}(\alpha)E_{i,j}(\beta) = E_{i,j}(\alpha + \beta)$.
2. If $i \neq j$, $k \neq \ell$, and $i \neq \ell$, then
$$[E_{i,j}(\alpha), E_{k,\ell}(\beta)] = \begin{cases} E_{i,\ell}(\alpha\beta) & j = k \\ 0 & j \neq k. \end{cases}$$
3. Let U be the group of upper triangular matrices with 1s along the diagonal. Then $U = \langle \{E_{i,j}(\alpha) : i < j, \alpha \in F\} \rangle$. $U_2 = U'$ is the subgroup of such matrices with 0s on the diagonal above the main diagonal. U_3 is the subgroup of such matrices with 0s on the 2 diagonals above the main diagonal. Continuing like this, we get $U_n = 1$.

Example 20.2. Let
$$G = \mathrm{Aff}(F) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in F^*, b \in F \right\} \cong F \rtimes F^*,$$

where the subgroups in the direct product are the off-diagonal matrices (with 1s in the diagonal) and the subgroup of diagonal matrices.

$$\left[\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right] = \begin{bmatrix} 1 & ab \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b(a-1) \\ 0 & 1 \end{bmatrix},$$

so

$$U = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} = [G, G]$$

if $F \not\cong F_2$. $G'' = 1$, and $G_n = U$ for all $n \geq 2$. So G is solvable but not nilpotent.

Definition 20.5. The **upper central series** $(Z^i(G))_{i \geq 0}$ of a group G is $Z^0(G) = 1$, $Z^i(G) = Z(G)$, and $G^{i+1}(G)$ is the inverse simage of $Z(G/Z^i(G))$ under the quotient map $G \to G/Z^i(G)$.

Proposition 20.1. *G is nilponent if and only if the upper central series is finite. If n is minimal such that $G_{n+1} = 1$, then $G_{n+1-i} \leq Z^i(G)$ for all i, and $Z^n(G)$ is minimal such that $Z^n(G) = G$.*

Proof. This is proven by induction. Here is the idea. Let $G = G_1 > G_2 > \cdots > G_n > G_{n+1} = 1$. Then $[G, G_n] = 1$, so $G_n \leq Z(G) = Z_1(G)$. □

Example 20.3. Nilpotent groups can have different upper and lower central series. Look at $G = \mathbb{Z}/p\mathbb{Z} \times U$, where U is the set of upper triangular 4×4 matrices with 1s on the diagonal and entries in $\mathbb{F}_p$. THen $G_2 = U_2$, $G_3 = U_3$¡ and $G_4 = 1$. $Z^1(G) = Z(G) = \mathbb{Z}/p\mathbb{Z} \times U_3$, $Z^2(G) = \mathbb{Z}/p\mathbb{Z} \times U_2$, and $Z^3(G) = \mathbb{Z}/p\mathbb{Z} \times U_1 = G$.

Proposition 20.2. *Finite p-groups are nilpotent.*

Proof. Let P be a finite p-group. We induct on $|P| \neq 1$. Then $Z(P) \neq 1$, so $P/Z(P)$ is a p-group o smaller order so it is nilpotent. Say $\overline{P} = P/Z(P)$ has niltpotence class n. THen $Z^n(P/Z(P)) = P/Z(P) = \overline{P}$. Let $|pi_i : P \to P/Z^i(P)$. THen $Z^{i+1}(P) = \pi_i^{-1}(Z(P/Z^i(P))) = \pi_i^1(Z(\overline{P}/(Z^i(P)/Z(P))))$. By induction, $Z^i(P)/Z(P) = Z^{i-1}(\overline{P})$, so this is equal to $\pi_1^{-1}(Z^{i+1}(P))$. So the smallest j such that $Z^j(P) = P$ is $j = n+1$. □

21 Frattini's Argument and Characterizations of Nilpotent Groups

21.1 Frattini's argument

Theorem 21.1 (Frattini's argument)**.** *Let G be a finite group, $N \trianglelefteq G$, and let P be a Sylow p-subgroup of N. Then $G = NN_G(P)$.*

Proof. If $g \in G$, then $gPg^{-1} \leq N$ (since $N \trianglelefteq G$). So gPg^{-1} is Sylow p in N, and therefore, there exists some $n \in N$ such that $gPg^{-1}nPn^{-1}$. Then $n^{-1}g \in N_G(P)$. So $g \in NN_G(P)$. □

21.2 Characterizations of nilpotent groups

Theorem 21.2. *Let G be a finite group. The following are equivalent:*

1. *G is nilpotent.*
2. *If $H < G$, then $H < N_G(H)$.*
3. *If $P \in \mathrm{Syl}_p$, then $P \trianglelefteq G$.*
4. *$G \cong \prod_{p \text{ prime}} P_p$, where P_p is a Sylow p-subgroup.*
5. *If $M < G$ is a maximal proper subgroup (not contained in any other proper subgroup), then $M \trianglelefteq G$.*

Proof. (1) $\implies$ (2): Suppose $N < G$. If $HZ(G) = G$¡ then $G = N_G(H)$, so $H < N_G(H)$. If $HZ(G) \neq G$, $N_G(HZ(G)) = N_G(H)$, so we may assume that $Z(G) \leq H$ (replace H by $HZ(G)$). Now $H/Z(G) < G/Z(G)$. If G has nilpotence class n, then $G/Z(G)$ has nilpotence class $\leq n-1$. By induction, $H/Z(G) < N_{G/Z(G)}(H/Z(G))$. This is $N_G(H)/Z(G)$, so $H < H_G(H)$.

(2) $\implies$ (3): If G is a p-group, then $G \trianglelefteq G$, so we are done. If G is not a p-group, let $P \in \mathrm{Syl}_p(G)$ with $P < G$. Then $P \trianglelefteq N = N_G(P)$, and $P < N$. P is unique of its order, so it is characteristic in N. So $P \trianglelefteq N_G(N)$. So $N = N_G(N)$. By (2), $N = G$. So $P \trianglelefteq G$.

(3) $\implies$ (4): This is the Krull-Schmidt theorem.

(4) $\implies$ (5): Let $M < G$ be maximal, and suppose that $p_1, \dots, p_s$ are the distinct primes dividing $|G|$. If $s = 1$, then Sylow's theorems give us a subgroup of order p^{n-1} normal in G, where $|G| = p^n$. If $s > 1$, let $P_1, \dots, P_s$ be our Sylow p-subgroups. For $M < G$ is maximal, we claim that there exists a unique i such that $M \cap P_i \neq P_i$. Existence is clear, and for uniqueness, $M < MP_i = G$, which forces $M \cap P_j = P_j$ for all $j \neq i$. Then $M \cong (M \cap P_i) \times \prod_{j \neq i} P_j$. Sylow's theorems imply that $M \cap P_i \trianglelefteq P_i$, so $M \trianglelefteq G$.

(5) $\implies$ (3): Let $P \in \mathrm{Syl}_p(G)$ with $P \ntrianglelefteq G$. Then $N_G(P) \leq M < G$, where M is maximal. Then $M \trianglelefteq G$, and $P \in \mathrm{Syl}_p(M)$. By Frattini's argument, $G = MN_G(P) = M$. This is a contradiction.

(4) $\implies$ (1): $G \cong \prod_{i=1}^s P_i$. Since p-groups are nilpotent, G is nilpotent. $\square$

Proposition 21.1. *Let G be nilpotent, and let $S \subseteq G$ with image generating $G^{\mathrm{ab}} = G/[G,G]$. Then S generates G.*

Proof. Proceed by induction on the nilpotence class n. If $n = 1$, then $G = G^{\mathrm{ab}}$. If $n \geq 2$, then $(G/G_n)^{\mathrm{ab}} \cong G/(G_nG_2) \cong G^{\mathrm{ab}}$. By induction, $\mathrm{im}(S)$ generates G/G_n. If $H = \langle S\rangle \leq G$, then $G = G_nH$. $G_n \leq Z(G)$, so $N_G(H) = G$. So $H \trianglelefteq G$. Then $G_n = [G_{n-1}, G] = [G_{n-1}, G_nH] = [G_{n-1}, H] \leq H$ (since $H \trianglelefteq G$). So $G = G_nH = H = \langle S\rangle$. $\square$

Theorem 21.3. *If p is prime, then there exist exactly 2 isomorphism classes of nonabelian groups of order p^3, represented by*

1. *if $p = 2$, D_4 and Q_8,*
2. *if p is odd,* $\mathrm{Heis}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p^2\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ *and*

$$K = \left\{\begin{bmatrix} a & b \\ 0 & 1\end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) : a \equiv 1 \mod p\right\} \cong \mathbb{Z}/p^2\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z},$$

where $\varphi(1)$ is multiplication by $1 + p$.

Remark 21.1. $\mathrm{Heis}(\mathbb{Z}/2\mathbb{Z}) \cong D_4$. For p odd, $\mathrm{Heis}(\mathbb{Z}/p\mathbb{Z})$ has no elements of order p^2.

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1\end{bmatrix}^p = \begin{bmatrix} 1 & p & \binom{p}{2} \\ 0 & 1 & p \\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix} 1 & 0 & \binom{p}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1\end{bmatrix}.$$

21.3 Linear groups

Lemma 21.1.

$$|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}) = q^{n(n-1)/2}\prod_{i=1}^n (q^i - 1).$$

$$|\mathrm{SL}_n(\mathbb{F}_q)| = q^{n(n-1)/2}\prod_{i=2}^n (q^i - 1).$$

Proof. For the order of $\mathrm{GL}_n(\mathbb{F}_q)$, we have $q^n - 1$ choices for the first column, then $q^n - q$ choices for the second columns, etc. since the columns must be linearly independent.

For $\mathrm{SL}_n(\mathbb{F}_q)$, we quotient out by the determinant map, which is onto $\mathbb{F}_p^\times$. $\square$

Definition 21.1. The **projective special linear group** is $\mathrm{PSL}_n(F) = \mathrm{SL}_n(F)/Z(\mathrm{SL}_n(F))$.

Proposition 21.2.

$$\mathrm{SL}_n(F) = \langle \{E_{i,j}(\alpha) : \alpha \in F, i \neq j\}\rangle$$

22 Properties of Linear Groups

22.1 The special linear group $\mathrm{SL}_n(F)$

Let $\mathbb{F}_q$ be the field with q elements, where q is a prime power. Later on, we will prove that a unique such field exists for each q.

Proposition 22.1. $\mathrm{SL}_n(F)$ *is generated by elementary matrices* $\{\{E_{i,j}(\alpha) : i \neq j, \alpha \in F\}$.

Proof. Let U be the unipotent group of upper triangular matrices with 1s as a diagonal. $U \trianglelefteq B$, the Borel subgroup of upper triangular matrices. U is nilpotent. $U^{\mathrm{ab}} \cong \mathbb{F}$, which is generated by the images of $E_{i,i+1}(\alpha)$. So U is generated by the elementary matrices.

$\mathrm{GL}_n(F) = BWB$, where $W = \iota(S_n)$, where $\iota : S_n \to \mathrm{GL}_n(F)$ sends σ to its permutation matrix. In fact, $\mathrm{GL}_n(F) = \coprod_{w \in W} BwB$, and $G = \mathrm{SL}_n(F) = \coprod_{w \in \iota(A_n)} B'wB'$, where $B' = B \cap G$. So $B \cong U \rtimes F^n$, where F^n is thought of as the diagonal matrices.

It suffices to show that the diagonal matrices or determinant 1 and permutation matrices of determinant 1 are in the subgroup generated by elementary matrices. For diagonal matrices, it suffices to show that we can get matrices of this form:

$$\begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & x & & & & \\ & & & \ddots & & & \\ & & & & x^{-1} & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

with only 2 non-identity entries. Note that

$$[E_{1,2}(\alpha), E_{2,1}(\alpha)] = \begin{bmatrix} 1+\alpha & \alpha \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1+\alpha & -\alpha \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1+\alpha+\alpha^2 & -\alpha^2 \\ \alpha & 1-\alpha \end{bmatrix},$$

so

$$E_{1,2}\left(\frac{\alpha^2}{1-\alpha}\right) \cdot [E_{1,2}(\alpha), E_{2,1}(\alpha)] \cdot E_{2,1}\left(\frac{-\alpha}{1-\alpha}\right) = \begin{bmatrix} (1-\alpha)^{-1} & 0 \\ 0 & 1-\alpha \end{bmatrix}.$$

To get permutation matrices, we do something like this:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$$
$$\to \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & -1 & 0 \end{bmatrix} \to \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix} \to \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

∎

Proposition 22.2. *The groups $\langle\{E_{i,j}(\alpha) : \alpha \in F\}\rangle$ are all conjugate.*

Proof. Let σ be an even permutation. Then $\iota(\sigma)E_{i,j}\iota(\sigma)^{-1} = E_{\sigma(i),\sigma(j)}(\alpha)$; this is just a change of basis. The rest is an exercise. $\square$

Proposition 22.3. $\mathrm{SL}_n(F) = [\mathrm{GL}_n F, \mathrm{GL}_n(F)]$ *unless $n = 2$ and $F \cong \mathbb{F}_2$ or $\mathbb{F}_3$.*

Proof. Note that $E_{i,j}(\alpha) = [E_{i,k}(\alpha).E_{k,j}(\alpha)]$ with $k \neq i, j$ for $n \geq 3$. For $n = 2$, we have

$$\left[\begin{bmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{bmatrix}, \begin{bmatrix}1 & \beta\\ 0 & 1\end{bmatrix}\right] = \begin{bmatrix}\alpha & \alpha\beta\\ 0 & \alpha^{-1}\end{bmatrix}\begin{bmatrix}\alpha^{-1} & -\alpha^{-1}\beta\\ 0 & \alpha\end{bmatrix} = \begin{bmatrix}1 & (\alpha^2-1)\beta\\ 0 & 1\end{bmatrix}.$$

We can choose $\beta \neq 0$ and $\alpha^2 \neq 1$ with $\alpha \neq 0$ iff $F \cong \mathbb{F}_2$ or $\mathbb{F}_3$. $\square$

Proposition 22.4. $\mathrm{SL}_n(F)$ *acts doubly transitively on the set of 1-dimensional subspaces of F^n.*

Proof. Given pairs of distinct nonzero vectors $(v_1, v_2), (w_1, w_2)$ with $Fv_1 \neq Fv_2$ and $Fw_1 \neq Fw_2$, there exists an $A \in \mathrm{GL}_n(F)$ such that $Av_i = w_i$ for $i = 1, 2$. Follow this by the matrix sending $w_1 \mapsto \det(A)^{-1}w_1$, $w_2 \mapsto w_2$, and all other basis elements to themselves. $\square$

22.2 The projective special linear group $\mathrm{PSL}_n(\mathbb{F}_q)$.

Theorem 22.1. *$PSL_n(\mathbb{F}_q)$ is simple for $n \geq 2$, unless $n = 2$ and $q \in \{2, 3\}$.*

Proof. Let P be the stabilizer of $\mathbb{F}_q e_1$ in $G = \mathrm{SL}_n(\mathbb{F}_q)$. These are matrices (with determinant 1) where the first column has zeros everywhere except the top left entry. P is maximal $< G$, and $P = \coprod_{w \in P\cap\iota(A_n)} B'wB'$. Consider the subgroup $K \trianglelefteq P$ of matrices with 1s on the diagonal and 0s above the diagonal except possibly for the first row.

Suppose $N \trianglelefteq G$. If $N \leq P$, then $N = gNg^{-1}$ stabilizes $g \cdot \mathbb{F}_q e_1$ for all $g \in G$. So N stabilizes $\mathbb{F}_q e_i$ for all i. Also, N stabilizes $\mathbb{F}_q(e_i + e_j)$ for all $i \neq j$. So $N \subseteq Z(\mathrm{SL}_n(\mathbb{F}_q))$.

If $N \not\leq P$, then $PN = G$, since G is maximal. Then $KN/N \trianglelefteq PN/N = G/N$, so $KN \trianglelefteq G$. We have that $E_{1,j}(\alpha) \in K$ for all $\alpha \in \mathbb{F}_q$ and $j \geq 2$. So since KN is normal, $E_{i,j}(\alpha) \in KN$ for all $i \neq j$ and $\alpha \in F$ by our second proposition. Then $G = KN$ by the first proposition. So $G/N \cong K/(K \cap N)$ is abelian. Then $N \geq G' = \mathrm{SL}_n(\mathbb{F}_q)$ by the third proposition. So $N = G$. $\square$

23 Principal Ideal Domains, Maximal Ideals, and Prime Ideals

23.1 Group extensions

Definition 23.1. A **(short) exact sequence** of groups is a sequence

$$1 \longrightarrow N \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$$

where ι is injective, π is surjective, and $\mathrm{im}(\iota) = \ker(\pi)$.

Definition 23.2. A **group extension** of G by N is a group E, where

$$1 \longrightarrow N \xrightarrow{\iota} E \xrightarrow{\pi} G \longrightarrow 1$$

is exact. If $E = N \rtimes_\varphi G$, we call it a **split extension**.

23.2 Simple rings and ideals

Proposition 23.1. *A ring is a division ring iff it has no nonzero proper left ideals.*

Proof. ($\Longrightarrow$): Let $I \neq 0$ be a left ideal of R¿ If $r \in I \setminus \{0\}$, then $r \in R^\times$, so $1 \in I$. So $I = R$.

($\Longleftarrow$): Let $r \in R \setminus \{0\}$. $Rr = R$, so there exists some $u \in R$ such that $ur = 1$. $Ru = R$, so there exists some $s \in R$ such that $su = 1$. Then $s = sur = r$. Then r has a left and a right inverse, so $r \in R^\times$. $\square$

Definition 23.3. A ring with no nonzero proper (two-sided) ideals is called **simple**.

Example 23.1. Let D be a division ring, and let $M_n(D)$ be the ring of $n \times n$ matrices with entries in D. Let $e_{i,j}$ be the matrix with 0 in every entry but (i,j) and a 1 in the (i,j) coordinate. Then $M_n(D)e_{i,j}$ is the set of matrices which are 0 outside of the j-th column. Similarly, $e_{i,j}M_n(D)$ is the set of matrices which are 0 outside of the i-th row. So the two sided ideal $(e_{i,j}) = M_n(D)$.

To show that $M_n(D)$ is simple, let $A \in M_n(D) \setminus \{0\}$, and suppose that $a_{i,j} \neq 0$ for some i, j. Then $e_{i,i}Ae_{j,j} = a_{i,j}e_{i,j}$. Since $a_{i,j} \neq 0$, $a_{i,j} \in D^\times$,which means that $e_{i,j} \in (A)$. So $(A) = M_n(D)$.

Let I, J be ideals in a ring. Then IJ is the span of ab, with $a \in I$ and $b \in J$. In general, $IJ \subseteq I \cap J$.

Let (I_α) be a system of ideals, totally ordered under containment. Then $\bigcup_\alpha I_\alpha$ is an ideal (this is also true for left or right ideals).

Theorem 23.1 (Chinese remainder theorem)**.** *Let $I_1, \dots, I_k$ be "pairwise coprime," i.e. $I_j + I_i = R$ for $j \neq i$. Then*

$$R/\bigcap_{i=1}^{k} \cong \prod_{i=1}^{k} R/I_i.$$

Proof. The proof is basically the same as the proof that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}.m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$, where $n = m_1 \cdots m_k$ and the m_i are coprime. □

23.3 Principal ideal domains

Definition 23.4. A **(left) zero divisor** $r \in R \setminus \{0\}$ is an element such that there exists some $s \in \mathbb{R} \setminus \{0\}$ with $rs = 0$. A **zero divisor** is a left and right zero divisor.

Definition 23.5. A **domain** is a commutative ring without zero divisors.

Definition 23.6. A **principal ideal domain (PID)** is a domain in which every ideal is principal (generated by 1 element).

Example 23.2. $\mathbb{Z}$ is a PID.

Example 23.3. If F is a field, then $F[x]$ is a PID. How do we divide polynomials? There is a map $\deg : F[x] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$ such that $\deg(f) \geq 0$ if $f \neq 0$ and $\deg(f) = 0$ iff f is constant and nonzero. If $f, g \in F[x]$ with $g \neq 0$, then $= qg + r$, where $q, r \in F[x]$ and $\deg(r) < \deg(f)$.

Proposition 23.2. *If F is a field, then $F[x]$ is a PID.*

Proof. Let I be a nonzero ideal. Choose $g\ inI \setminus \{0\}$ for minimal degree. If $f \in I$, write $f = qg + r$ with $r \in I$ and $\deg(r) < \deg(g)$. Then $r = 0$, so $f \in (g)$. Hence, $I = (g)$. □

Definition 23.7. An element π of a commutative ring R is **irreducible** if whenever $\pi = ab$ with $a, b \in R$, either $a \in \mathbb{R}^\times$ or $b \in R^\times$.

Definition 23.8. Two elements $a, b \in R$ are **associate** if there exists $u \in R^\times$ such that $a = ub$.

Example 23.4. The irreducible elements in $\mathbb{Z}$ are $\pm$ primes.

Example 23.5. The irreducible elements in $F[x]$ are the (nonconstant) irreducible polynomials.

If $f \in F[x]$, we get a function $f : F \to F$. But this does not necessarily go both ways. Let $f = x^p - x = x(x^{p-1} - 1)$, where $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_p$, but $f \neq 0$ since $\deg(f) = p$.

23.4 Maximal and prime ideals

Definition 23.9. An ideal of a ring is **maximal** if it is proper and not properly contained in any proper ideal.

Definition 23.10. An ideal p of a commutative ring is **prime** if it is proper, and whenever $ab \in p$ for $a, b \in R$, then $a \in p$ or $b \in p$.

Proposition 23.3. *Principal prime ideals in a domain are generated by irreducible elements.*

Proof. If $p = (\pi)$ is prime and $ab = \pi \in (p)$, then either $a \in p$ or $b \in p$. So $a = s\pi$ or $b = t\pi$. Without loss of generality, $a = s\pi$. So $(bs - 1)\pi = 0$, which means that $b = s^{-1} \in R^\times$. □

Example 23.6. In $\mathbb{Z}$ and $F[x]$, nonzero prime and maximal ideals are the same. However, in $F[x, y]$, the ideal (x) is prime but not maximal. The ideal (x, y) is prime and maximal. In the ring $\mathbb{Z}[x]$, (p, x) is maximal if p is prime. But (p) and (x) are prime but no maximal.

Lemma 23.1. *An element $m \subsetneq R$ is maximal iff R/m is a division ring. If R is commutative, then $p \subsetneq R$ is prime iff R/p is an integral domain.*

Proof. The key is that ideals in R/I are in correspondence with ideals of R containing I. When $I = m$, if R/m is a division ring, then the ideals in R/m are $0, R/m$. Then the only ideals in R containing m are m and R.

If p is prime, then $ab \in p$ implies that $a \in p$ or $b \in p$. So $a + p = p$ or $b + p = p$. This is equivalent to $\overline{a}\overline{b} = (a+p)(b+p) = p$. If R/p is an integral domain, then $ab \in p \iff \overline{a}\overline{b} = 0$, so $\overline{a} = 0$ or $\overline{b} = 0$. This is equivalent to $a \in p$ or $b \in p$. □

Lemma 23.2 (Zorn's lemma)**.** *Let X be a partially ordered set. Suppose that every chain (totally ordered subset) in X has an upper bound (an upper bound $x \in X$ of a set $S \subseteq X$ is such that $s \leq x$ for all $s \in S$. Then X has a maximal element ($x \in X$ such that if $y \in X$ and $x \leq y$, then $y = x$).*

This is equivalent to the axiom of choice.

Theorem 23.2. *Every ring has a maximal ideal.*

Proof. Let X be the set of proper ideals in R. If $C \subseteq X$ is a chain, then $\bigcup_{N \in C} N$ is an upper bound for C. So X has a maximal element which is a maximal ideal. □

24 Artinian and Noetherian Rings

24.1 Maximal ideals

Theorem 24.1. *Let I be an ideal of a ring R. Then there exists a maximal ideal of R containing I.*

Proof. Let X be the set of proper ideals of R containing R. If C is a chain in X, $N = \bigcup_{J \in C} J$ is and ideal containing I, and $1 \notin N$, so $N \neq R$. So $\mathbb{C}$ has an upper bound. By Zorn's lemma, X has a maximal element, which is a maximal ideal containing I. □

Proposition 24.1. *Maximal ideals in a commutative ring are prime.*

Proof. We have already proved that m is maximal iff R/m is a simple ring and that in a commutative ring, p is prime iff R/p is an integral domain. If R is commutative, then R/m is a division ring. □

Remark 24.1. (0) is prime iff R is a domain.

Example 24.1. $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, and $\mathbb{Z}[x]/(p) \cong \mathbb{F}_p[x]$.

24.2 Artinian and noetherian rings

Definition 24.1. Let $(I, \leq)$ be a partially ordered set. A chain $a_1 \leq a_2 \leq a_3 \leq \cdots$ satisfies the **ascending chain condition (ACC)** if there exists some N such that $a_k = a_N$ for all $k \geq N$. A chain $a_1 \geq a_2 \geq a_3 \geq \cdots$ satisfies the **descending chain condition (DCC)** if there exists some N such that $a_k = a_N$ for all $k \geq N$.

Definition 24.2. An R-module is **noetherian** if its set of R-submodules satisfies the ACC. And R module is **artinian** if its R submodules satisfy the DCC.[4]

Definition 24.3. A ring is **left noetherian** (resp. **left artinian**) if it is noetherian (resp. artinian) as a left module over itself. A ring is **noetherian** (resp. **artinian**) if it is left and right noetherian (resp. artinian).

Example 24.2. The polynomial ring $F[x_1, x_2, x_3, \ldots]$ is not noetherian. It has the infinite ascending chain

$$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots .$$

Example 24.3. $F[x]/(x^n)$ is both artinian and noetherian. Check that all ideals of this ring have the form (x^i) for $0 \leq i \leq n$.

Proposition 24.2. *Finite products of division rings are artinian and noetherian.*

[4] Noetherian and artinian are words used so commonly that they are often not capitalized, like abelian.

Proposition 24.3. *An R-module M is noetherian iff every submodule of M is finitely generated.*

Proof. ($\Longleftarrow$): Suppose $(N_i)_{i=1}^{\infty}$ is anascending chain of R-sbumodules of M. Then $N = \bigcup_{i=1}^{\infty} N_i$ is an R-submodule of M. Then N is gnerated by $m_1, \ldots, m_k \in N$. Each $m_i \in N_{j_i}$ for some $j_i \geq 1$. Every m_i is in $N_{\max j_i}$. So $N_{\max j_i} = N$.

($\Longrightarrow$): Let M be noetherian, and let $N \subseteq M$ be a submodule. If $N \neq 0$, then take $a_1 \in N \setminus (0)$. Set $N_1 = Ra_1$. If possible, take $a_i \in N \setminus N_i$, and set $N_{i+1} = N_i + Ra_{i+1} = R(a_1, \ldots, a_{i+1})$. Then

$$(0) = N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots ,$$

so this pocess must terminate; i.e. there exists some i such that $N_i = N$, and N_i is finitely generated. □

Corollary 24.1. *PIDs are noetherian.*

Example 24.4. $F[x]$ is noetherian.

Proposition 24.4. *Let M be an R-module and N be an R-submodule of M. THen M is noetherian iff N and M/N are noetherian.*

Proof. ($\Longrightarrow$): If N is noetherian, then submodules of M are finitely generated. Then submodules of N are finitely generated, so N is Noetherian. Now let $A \subseteq M/N$ is an R-submodule and $\pi L M \to M/N$ be the quotient map. Then $\pi^{-1}(A)$ is finitely generated and π applied to the generators generate A.

($\Longleftarrow$): Let $P \subseteq M$ be an R submodule. Then $P \cap N \subseteq N$ and $(P+N)/N \subseteq M/N$ are submodules of N and M/N, so they are finitely generated. Note that $(P+N)/N \cong P/(P \cap N)$. If $p_1, \ldots, p_k$ generated $P \cap N$ and $q_1, \ldots, q_\ell$ generate $P/(P \cap N)$, then we claim that $p_1, \ldots, p_k, q_1' \in \pi_P^{-1}(\{q_1\}), \ldots, q_\ell' \in \pi_P^{-1}(\{q_\ell\})$ generate P, where $\pi_P : P \to P/(P \cap N)$. If $a \in P$, then $\pi_P(a) = \sum_{i=1}^{\ell} r_i q_i$ for $r_i \in R$, and then $a - \sum_{i=1}^{\ell} r_i q_i' \in P \cap N$. So it equals $\sum_{j=1}^{k} s_j p_j$, where $s_-j \in R$. □

Corollary 24.2. *If R is noetherian, then R^n is noetherian for $n \in N^+$.*

Proof. Induct on n. The inductive step follows form $R^{n+1}/R \cong R^n$. □

Proposition 24.5. *Every finitely generated module over a left noetherian ring is noetherian.*

Proof. Let M be a finitely generated R-module, where R is left-noetherian, and let the finite list of generators be $a_1, \ldots, a_n \in M$. R^n is a free R-module of rank n, so there exists a unique $\phi : R^n \to M$ such that $\phi(e_i) = a_i$ for all i. Then ϕ is onto. Let $N \subseteq M$ be a submodule, and consider the R-submodule $N' = \phi^{-1}(N) \subseteq R^n$. R^n is noetherian, so since N' is finitely generated, N is finitely generated. □

Definition 24.4. A domain R is a **unique factorization domain (UFD)** if every element $a \in R \setminus \{0\}$ can be written as $a = u\pi_1 \cdots \pi_k$ with $u \in R^\times$, $\pi_i \in R$ irreducible, and if $a = vp_1, \ldots p_\ell$ with $v \in R^\times$ and $p_i \in R$ irreducible, then $k = \ell$ and there exists a permutation $\sigma \in S_k$ such that $\pi \sim p_{\sigma(i)}$ for all i.

25 Localization of Rings

25.1 Construction and properties

Let's say we have a commutative ring where not every element has a multiplicative inverse. How do we add in more elements to get a larger ring with some more inverses? We may not want to add in all inverses if we want to preserve the structure of the original ring.

Definition 25.1. A subset S of a ring R is **multiplicatively closed** if it closed under multiplication, $1 \in S$, and $0 \notin S$.

Lemma 25.1. *Suppose R is commutative, and let $S \subseteq R$ be multiplicatively closed. The relation $\sim$ on $R \times S$ given by $(a, s) \sim (b, t)$ iff there exists $r \in S$ such that $rat = rbs$ is an equivalence rrelation.*

Proof. Let's verify transitivity. Suppose $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$, so there exist $r, q \in S$ such that $rat = rbs$ and $qbu = qct$. Note that $rqt \in S$ since these elements are all in S. Then

$$(rqt)au = q(rat)u = q(rbs)u = rs(qbu) = rs(qct) = (rqt)cs. \qquad \square$$

Remark 25.1. If S contains no zero divisors, then $rat = rbs \implies at = bs$. So we can replace the condition in $\sim$ with $at = bs$. his of this as $a/s = b/t$.

Definition 25.2. The equivalence class of (a, s) under $\sim$ is denoted a/s (or $\frac{a}{s}$) The set of equivalence classes is $S^{-1}R$.

Theorem 25.1. *$S^{-1}R$ is a commutative ring with addition and multiplication*

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Proof. If $(a, s) \sim (a', s')$, we want that $(at + bs)/(st) = (a't + bs')(s't)$. There exists $r \in S$ such that $ras' = ra's$. Then

$$r(st + bs)s' = rats' + rbss' = ras'ts + rbss' = r(a't + bss')s.$$

Showing multiplication is well-defined is similar (and a bit easier, actually). The additive identity is $0/1$, and the multiplicative identity is $1/1$. $\square$

Remark 25.2. We have a homomorphism $\iota : R \to S^{-1}R$ with $\iota(r) = r/1$. This is injective iff S has no zero divisors. $a/1 = b/1$ means $ra = rb$. This means $ra = rb$ if S has no zero divisors, and otherwise, we can find a, b, r such that $ra = rb$ but $a \neq b$.

Remark 25.3. If $s \in S$ is a zero divisor and $rs = 0$ with $r \in R$. then $0 = 0/s = rs/s = r/1 = s$, so $r \mapsto 0$ in $S^{-1}R$. But S maps into $(S^{-1}R)^\times$ because $s \cdot 1/s = 1$. Also, no elements get mapped to 0 because if $s/1 = 0/1 = 0$, then there exists some $r \in S$ with $rs = 0$, which is impossible because $0 \notin S$.

Remark 25.4. If $\phi : R \to R'$ is a ring homomorphism such that $\phi(S) \subseteq (R')^\times$, then there exists a unique homomorphism $\psi : S^{-1}R \to R'$ such that

$$\begin{tikzcd} R \arrow[r, "\iota"] \arrow[dr, "\phi"'] & S^{-1}R \arrow[d, "\psi"] \\ & R' \end{tikzcd}$$

given by $\psi(a/s) = \phi(a)\phi(s)^{-1}$.

25.2 Examples of localizations

Definition 25.3. Let R be a domain and $S = R \setminus \{0\}$ then $Q(R) := S^{-1}R$ is the **fraction field**, field of fractions, or **quotient field** of R. It is the "smallest" field containing R.

Example 25.1. Let F be a field. $Q(F[x]) = F(x)$, the field of rational functions over F. These are $f(x)/g(x)$ where $g \neq 0$.

Definition 25.4. Let $S = T \setminus (\{\text{zero divisors}\} \cup \{0\})$. Then $Q(R) = S^{-1}R$ is called the **total ring of fractions**.

Example 25.2. Let $R = \mathbb{Z} \times \mathbb{Z}$. You can check that $Q(R) = \mathbb{Q} \times \mathbb{Q}$. In fact, if $R = R_1 \times R_2$, then $Q(R) = Q(R_1) \times Q(R_2)$.

Example 25.3. Let $R = F[x, y]/(xy)$, and $S = \{x^n : n \geq 0\}$. Then $S^{-1}R \cong F[x, x^{-1}]$, via the isomorphism $x \mapsto x$ and $y \mapsto 0$.

Definition 25.5. Let $S_p = S \setminus p$, where p is a prime ideal. The ring $R_p = S^{-1}pR$. is the **localization of** R at p.

Note that $pR_p \subseteq R_p$, so $(R_p)^\times = R_p \setminus pR_p$. So pRp is the unique maximal ideal in R_p.

Definition 25.6. A commutative ring with a unique maximal ideal is called a **local ring**.

Example 25.4. Let $p \in \mathbb{Z}$ be prime. Then $\mathbb{Z}_{(p)} = \{a/b \in Q : p \nmid b\}$.

Example 25.5. $F[x]_{(x)} = \{f/g : x \nmid g\}$.

Example 25.6. Let $x \in R$ be not a zero-divisor. Let $S = \{x^n : n \geq 0\}$. Then $R_x = S^{-1}R = \{a/x^n : a \in R, n \geq 0\}$. If $R = F[x]$ and $x = x$, then $F[x]_x = F[x, x^{-1}] \subseteq F(x)$.

Proposition 25.1. *Let $\iota : R \to S^{-1}R$ send $r \mapsto r/1$. Let $I \subseteq R$ be an ideal.*

1. *$S^{-1}I = \{a/s : a \in I, s \in S\}$ is an ideal of $S^{-1}R$.*
2. *$\iota^{-1}(S^{-1}I) = \{a \in R : Sa \cap I \neq \varnothing\}$.*

3. If $J \subseteq S^{-1}R$*, then* $S^{-1} \cdot \iota^{-1}(J) = J$*.*

Proof. For part 1, $a/s + b/t = (at + bs)/(st)$, where $at + bs \in I$ and $st \in S$. Then $r \cdot a/s = (ra)/s$, where $r \in I$ and $s \in S$.

For part 2, let $\phi(s) = b/s$, where $b \in I$, $s\ inS$, and $a \in R$. What properties must a have? Then $a/1 = b/s$ iff there eixsts some $r \in S$ such that $ras = rb$. This is true for some b, s iff there exists some $r' \in S$ such that $r'a \in I$.

The proof of part 3 is left as an exercise. $\square$

26 Ideals of Localizations, Hilbert's Basis Theorem, and UFDs

26.1 Ideals of localizations

Let R be a commutative ring, and let S be multiplicatively closed. We have a map S^{-1} sending ideals of R to ideals of $S^{-1}R$. This is onto; that is, every ideal of $S^{-1}R$ arises this way. Suppose S has no 0-divisors. Then

$$I \mapsto S^{-1}I \iff I \in S^{-1}I \iff 1 = a/s, a \in I, s \in S \iff I \cap S = \varnothing.$$

Example 26.1. Let $S = S_p$ for p prime. Then $S_p \cap I = \varnothing \iff I \subseteq p$. This is because Rp is ocal; that is, pRp is the unique maximal ideal.

Example 26.2. Let $R = \mathbb{Z}$, and let $p \in \mathbb{Z}$ be prime. Then $\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z}, p \nmid b\} \subseteq \mathbb{Q}$. This has ideals $p^n\mathbb{Z}_{(p)}$, where $n \geq 0$.

26.2 Hilbert's basis theorem

Theorem 26.1 (Hilbert's basis theorem)**.** *Let R be a commutative noetherian ring. Then $R[x]$ is noetherian.*

Proof. Let $I \subseteq R[x]$ be an ideal. Let L be the set of leading coefficients of polynomials in I. We claim that L is an ideal of R. If $a \in L$, then a is the leading coefficient of $f \in I$. Then for $r \in R$, then $rf \in I$ has leading coefficient ra or $ra = 0 \in L$. If $a, b \in L$, then $f, g \in I$ with $f(x) = ax^n + \cdots$ and $g(x) = bx^m + \cdots$; without loss of generality, $n \geq m$, so $f + x^{n-m}g = (a+b)x^n + \cdots \in I$. So $a + b \in L$.

Since R is noetherian, $L = (a_1, \ldots, a_k)$, where $a_i \in R$. Let $f_i \in I$ have leading coefficients a_i and degree n_i, and let $n = \max\{n_i\}$. Let $L_m \subseteq R$ be the ideal of leading coefficients of polynomials of degree m and 0. Then $L_m = (b_{1,m}, \ldots, b_{\ell_m,m})$, since R is noetherian. Let $g_{i,m} \in I$ have degree m and leading coefficient $b_{i,m}$. Now let $J = (f_1, \ldots, f_k, g_{1,1} \cdots g_{\ell_0,0}, \ldots, g_{1,n}, \ldots, g_{\ell_n})$.

We claim that $J = I$. Let $h \in I$ have leading coefficient c. Write $c = \sum_{i=1}^k r_i a_i$ with $r_i \in R$. If $m = \deg(h) > n$, then set $h' = \sum_{i=1}^k r_i x^{m-n_i} f_i$. This has degree m, leading coefficient c, so $\deg(h - h') < m$. Repeat, so we can assume $\deg(h) \leq n$. Then there exist $s_1, \ldots, s_{\ell_m} \in R$ such that $c = \sum_{i=1}^{\ell_m} s_i b_{i,m}$. So $h - \sum_{i=1}^{\ell_m} s_i g_{i,m}$ has degree $< m$. Repeat until we get degree zero. $\square$

Corollary 26.1. *If R is noetherian, then $R[x_1, \ldots, x_n]$ is noetherian.*

Definition 26.1. Let R be a ring. The **center** of R is $Z(R) = \{r \in R : rs = sr\ \forall s \in R\}$.

Definition 26.2. An **algebra** A over a commutative ring R is a ring A and a nonzero homomorphism of rings $R \to Z(A)$.

If R is a field, the homomorphism $R \to Z(A)$ is injective, and A is an R-vector space.

Example 26.3. $F[x_1, \dots, x_n]$ is an algebra over R.

Example 26.4. The quaternions, $\mathbb{H} = \{a + bi + c_j + dl : a, b, c, d \in \mathbb{R}\}$ is an $\mathbb{R}$ algebra. This is not a $\mathbb{C}$-algebra, but it contains $\mathbb{C}$.

Example 26.5. A finitely generated commutative algebra over a field is isomorphic to $F[x_1, \dots, x_n]/I$, where I is an ideal.

Corollary 26.2. *Any finitely generated algebra over a field (which is noetherian) is noetherian (as a ring).*

$F[(x_i)_{i \in I}]$ is the free object on I in the category of commutative F-algebras.

26.3 Unique factorization domains

Example 26.6. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. $6 = 23 = (1 + \sqrt{-5})(1 - \sqrt{5})$. The only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so these factorizations really are different.

Definition 26.3. Let R be a UFD. An element $d \in R$ is a **gcd** of $a_1, \dots, a_r \in R$ if $d \mid a_i$ for all i and if $d' \mid a_i$ for all i, ten $d' \mid d$.

Lemma 26.1. *Let R be a UFD. Then $a_1, \dots, a_r$ have a gcd.*

Proof. Take $\pi \mid a_1, \dots, a_r$, and consider $a_1 \pi_1^{-1}, \dots, a_r \pi_1^{-1}$. Repeat until there does not exist a $\pi_k \mid a_i \pi_1^{-1} \cdots \pi_{k-1}^{-1}$ for all i. Then $\pi_1 \cdots \pi_{k-1}$ is a gcd. □

Lemma 26.2. *Let R be a UFD. If $a \in R \setminus \{0\}$. Then (a) is maximal iff (a) is prime iff (a) is irreducible.*

Proof. Let $a \notin R^x$. Then the existence of $b, c \notin R^\times$ such that $a = bc$ is equivalent to $(b) \supsetneq (a)$ for some $b \in R \setminus R^\times$. This is equivalent to $(a) \subsetneq I \subsetneq R$, which is equivalent to (a) not being maximal.

The rest is an exercise. □

Theorem 26.2. *A PID is a UFD.*

27 Unique Factorization in PIDs and Polynomials, Gauss' Lemma, and Eisenstein's Criterion

27.1 Unique factorization in PIDs

Proposition 27.1. *In a PID, every irreducible element generates a prime ideal.*

Proof. If $a \in R^\times$ is irreducible, then $b \mid a \iff (a) \subsetneq (b) \subsetneq R$. Since R is a PID, a is maximal, and so it is prime. $\square$

Theorem 27.1. *If R is a PID, R is a UFD.*

Proof. Let $a \neq 0$ with $a \notin \mathbb{R}^\times$. If a is irreducible, we are done. Otherwise, write $a = bc$, where b, c are not units. If b, c are not irreducible, break them down into smaller pieces in the same way. Keep doing this until the process stops. Why must it stop? This is because R is noetherian.

For uniqueness of factorizations, suppose that $a = b_1 b_2, \dots b_r = c_1 c_2 \cdots c_s$, where b_i, c_j are irreducible. We want to show that $r = s$, and there exists a permutation $\sigma \in S_r$ such that $b_{\sigma(i)} = c_i u_i$ for some unit u_i for each i. We know that b_1 generates a prime ideal, so $b_1 \mid c_1 \cdots c_r$. So $b_1 \mid c_i$ for some i, and we get that $c_i = b_i v$, where $v \in R^\times$ (since b_1, c_i are irreducible). By induction on r, we are done. $\square$

Is every PID a UFD?

Example 27.1. Look at $k[x, y]$, where k is a field. This is a UFD, but it is not a PID. It is not a PID because the ideal (x, y) is not principal.

27.2 Gauss' lemma and unique factorization of polynomials over a UFD

Theorem 27.2. *If R is a UFD, then so is $R[x]$.*

Corollary 27.1. *If R is a UFD, then so is $R[x_1, \dots, x_n]$.*

The idea is this: Let $Q(R)$ be the quotient field of R. Then $Q(R)[x]$ is a PID and hence a UFD. We will try to factor the polynomial in $Q(R)[x]$ and bring that factorization back down to $R[x]$.

Definition 27.1. If $f \in R[x]$, the **content** of f is the ideal generated by the gcd of its coefficients.

Example 27.2. If $f = a_0 + a_1 x + \cdots + a_n x^n$, then $c(f) = (\gcd(a_1, \dots, a_n))$.

Definition 27.2. f is **primitive** if $c(f) = R$.

Lemma 27.1. *If $f \in R[x]$, then $f(x) = cg(x)$, where $c \in R$ and $g(x)$ is primitive.*

Lemma 27.2 (Gauss)**.** *If $f(x), g(x) \in R[x]$ are primitive, so is $f(x)g(x)$.*

Proof. Take π irreducible such that $\pi \mid c(fg)$. Write $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$. Take r, s minimal such that $\pi \nmid b_r, c_s$. Then $f(x)g(x) = a_0b_0 + \cdots + (a_0b_{r+s} + a_1b_{r+s-1} + \cdots + a_rb_s + \cdots + a_{r+s}b_0)x^{r+s} + \cdots$. Then π divides all these terms in the coefficient of x^{r+s} except a_rb_s. Then $\pi \mid a_rb_s$, which is a contradiction. □

Proposition 27.2. *Let $f(x) = f(x)h(x)$ with $g, h \in Q(R)[x]$. Then $f(x) = f_1(x)h_1(x)$, where $g_1, h_1 \in R[x]$, $\deg(g_1) = \deg(g)$, and $\deg(h_1) = \deg(h)$.*

Proof. Take $r, s \in R$. Then $rg(x), sh(x) \in R[x]$. Then $rsf(x) = (rg(x))(sh(x))$. Let $g_0 = rg$ and $h - 0 = sh$. Then $f(x) = cf_2(x)$, $g_0(x) = dg_2(x)$, and $h_0(x) = eh_2(x)$, where f_2, g_2, h_2 are primitive. Then $f_2 = g_2h_2$. □

We can now prove the theorem.

Proof. If $g \in R[x] \subseteq Q(R)[x]$, factor $f(x) = g_1(x) \cdots g_r(x)$ where $g_1, \ldots, g_r \in R[x]$ are irreducible in $Q(R)[x]$. Then $f(x) = ch_1(x) \cdots h_r(x)$, where $c \in R$ and $h_1, \ldots, h_r$ are primitive. Since R is a UFD, $c = \pi_1 \cdots \pi_s$, where the π_1 are irreducibles.

To get uniqueness, let $\pi'_1 \cdots \pi'_s h'_1(x) \cdots h'_r(x)$ be another factorization. If we look at the content, we get $(\pi_1 \cdots \pi_s) = (\pi'_1 \cdots \pi'_s)$. Since R is a sUFD, s$s = s'$. So $(\pi_i) = (\pi'_{\sigma(i)})$ for some σ. We can do the same for the h'_i. □

27.3 Eisenstein's criterion

How can we tell if $f(x) \in k[x]$ is irreducible?

Theorem 27.3 (Eisenstein)**.** *Suppose $f \in R[x]$, and let $\mathfrak{p} \subseteq R$ be a prime ideal. Write $f(x) = a_0 + \cdots + a_nx^n$. Assume $a_0, \ldots, a_{n-1} \in \mathfrak{p}$ but $a_0 \notin \mathfrak{p}^2$ and $a_n \notin \mathfrak{p}$. Then f is irreducible.*

Proof. Let $\overline{f}(x) \in (R/\mathfrak{p})[x]$. Then $\overline{f}(x) = \overline{a}_nx^n$. If $g(x)h(x) = f(x)$, then $\overline{g}(x)\overline{h}(x) = \overline{f}(x) = \overline{a}_nx^n$. Then $\overline{g}(x) = \overline{b}_mx^m$ and $\overline{h}(x) = \overline{c}_kx^k$ with $m, k > 0$. This is a contradiction. □

Example 27.3. Look at the cyclotomic polynomial $\Phi_p = 1 + x + \cdots + x^{p-1} = (x^p - 1)/x - 1$. Then $\Phi_p(x + 1) = (x^{p-1} + px^{p-2} + \cdots + p$, so it is irreducible.