Mathematics

Robin Adams

May 25, 2024

Contents

Part I

Category Theory

Chapter 1

Foundations

This is a placeholder — I am not sure what foundation I want to use for this project yet. I will try to work in a way which is foundation-independent. What I do could be formalized in ZFC, ETCS, or some other system. I will assume the usual set theoretic constructions as needed. Sets will be defined up to bijection only.

Chapter 2

Categories

2.1 Categories

Definition 2.1 (Category)**.** A *category* $\mathcal{C}$ consists of:

- A class $|\mathcal{C}|$ of *objects*. We write $A \in \mathcal{C}$ for $A \in |\mathcal{C}|$.
- For any objects A, B, a set $\mathcal{C}[A, B]$ of *morphisms* from A to B. We write $f : A \to B$ for $f \in \mathcal{C}[A, B]$.
- For any object A, a morphism $\mathrm{id}_A : A \to A$, the *identity* morphism on A.
- For any morphisms $f : A \to B$ and $g : B \to C$, a morphism $g \circ f : A \to C$, the *composite* of f and g.

such that:

Associativity Given $f : A \to B$, $g : B \to C$ and $h : C \to D$, we have $h \circ (g \circ f) = (h \circ g) \circ f$

Left Unit Law For any morphism $f : A \to B$, we have $\mathrm{id}_B \circ f = f$.

Right Unit Law For any morphism $f : A \to B$, we have $f \circ \mathrm{id}_A = f$.

Example 2.2 (Category of Sets)**.** The *category of sets* **Set** has objects all sets and morphisms all functions.

Proposition 2.3. *The identity morphism on an object is unique.*

Proof: If i and j are identity morphisms on A then $i = i \circ j = j$. □

Definition 2.4 (Endomorphism)**.** In a category $\mathcal{C}$, an *endomorphism* on an object A is a morphism $A \to A$. We write $\mathrm{End}_{\mathcal{C}}(A)$ for $\mathcal{C}[A, A]$.

Definition 2.5 (Opposite Category)**.** For any category $\mathcal{C}$, the *opposite* category $\mathcal{C}^{\mathrm{op}}$ is the category with the same objects as $\mathcal{C}$ and

$$\mathcal{C}^{\mathrm{op}}[A, B] = \mathcal{C}[B, A]$$

2.2 Preorders

Definition 2.6 (Preorder)**.** A *preorder* on a set A is a relation $\leq$ on A that is reflexive and transitive.

A *preordered set* is a pair $(A, \leq)$ such that $\leq$ is a preorder on A. We usually write A for the preordered set $(A, \leq)$.

We identify any preordered set A with the category whose objects are the elements of A, with one morphism $a \to b$ iff $a \leq b$, and no morphism $a \to b$ otherwise.

Example 2.7. For any ordinal α, let α be the preorder $\{\beta : \beta < \alpha\}$ under $\leq$.

Definition 2.8 (Discrete Preorder)**.** We identify any set A with the *discrete* preorder $(A, =)$.

2.3 Monomorphisms and Epimorphisms

Definition 2.9 (Monomorphism)**.** In a category, let $f : A \to B$. Then f is a *monomorphism* or *monic* iff, for every object X and morphism $x, y : X \to A$, if $fx = fy$ then $x = y$.

Definition 2.10 (Epimorphism)**.** In a category, let $f : A \to B$. Then f is a *epimorphism* or *epi* iff, for every object X and morphism $x, y : B \to X$, if $xf = yf$ then $x = y$.

Proposition 2.11. *The composite of two monomorphism is monic.*

Proof:
$\langle 1 \rangle 1.$ Let: $f : A \rightarrowtail B$ and $g : B \rightarrowtail C$ be monic.
$\langle 1 \rangle 2.$ Let: $x, y : X \to A$
$\langle 1 \rangle 3.$ Assume: $g \circ f \circ x = g \circ f \circ y$
$\langle 1 \rangle 4.$ $f \circ x = f \circ y$
$\langle 1 \rangle 5.$ $x = y$
□

Proposition 2.12. *The composite of two epimorphisms is epi.*

Proof: Dual. □

Proposition 2.13. *Let $f : A \to B$ and $g : B \to C$. If $g \circ f$ is monic then f is monic.*

Proof: If $f \circ x = f \circ y$ then $gfx = gfy$ and so $x = y$. □

Proposition 2.14. *Let $f : A \to B$ and $g : B \to C$. If $g \circ f$ is epi then g is epi.*

Proof: Dual. □

Proposition 2.15. *A function is a monomorphism in* **Set** *iff it is injective.*

PROOF:
$\langle 1\rangle 1$. LET: $f : A \to B$
$\langle 1\rangle 2$. If f is monic then f is injective.
  $\langle 2\rangle 1$. ASSUME: f is monic.
  $\langle 2\rangle 2$. LET: $x, y \in A$
  $\langle 2\rangle 3$. ASSUME: $f(x) = f(y)$
  $\langle 2\rangle 4$. LET: $\overline{x}, \overline{y} : 1 \to A$ be the functions such that $\overline{x}(*) = x$ and $\overline{y}(*) = y$
  $\langle 2\rangle 5$. $f \circ \overline{x} = f \circ \overline{y}$
  $\langle 2\rangle 6$. $\overline{x} = \overline{y}$
    PROOF: By $\langle 2\rangle 1$.
  $\langle 2\rangle 7$. $x = y$
$\langle 1\rangle 3$. If f is injective then f is monic.
  $\langle 2\rangle 1$. ASSUME: f is injective.
  $\langle 2\rangle 2$. LET: X be a set and $x, y : X \to A$.
  $\langle 2\rangle 3$. ASSUME: $f \circ x = f \circ y$
    PROVE: $x = y$
  $\langle 2\rangle 4$. LET: $t \in X$
    PROVE: $x(t) = y(t)$
  $\langle 2\rangle 5$. $f(x(t)) = f(y(t))$
  $\langle 2\rangle 6$. $x(t) = y(t)$
    PROOF: By $\langle 2\rangle 1$.
□

Proposition 2.16. *A function is an epimorphism in* **Set** *iff it is surjective.*

PROOF:
$\langle 1\rangle 1$. LET: $f : A \to B$
$\langle 1\rangle 2$. If f is an epimorphism then f is surjective.
  $\langle 2\rangle 1$. ASSUME: f is an epimorphism.
  $\langle 2\rangle 2$. LET: $b \in B$
  $\langle 2\rangle 3$. LET: $x, y : B \to 2$ be defined by $x(b) = 1$ and $x(t) = 0$ for all other $t \in B$, $y(t) = 0$ for all $t \in B$.
  $\langle 2\rangle 4$. $x \neq y$
  $\langle 2\rangle 5$. $x \circ f \neq y \circ f$
  $\langle 2\rangle 6$. There exists $a \in A$ such that $f(a) = b$.
$\langle 1\rangle 3$. If f is surjective then f is an epimorphism.
  $\langle 2\rangle 1$. ASSUME: f is surjective.
  $\langle 2\rangle 2$. LET: $x, y : B \to X$
  $\langle 2\rangle 3$. ASSUME: $x \circ f = y \circ f$
    PROVE: $x = y$
  $\langle 2\rangle 4$. LET: $b \in B$
    PROVE: $x(b) = y(b)$
  $\langle 2\rangle 5$. PICK $a \in A$ such that $f(a) = b$
  $\langle 2\rangle 6$. $x(f(a)) = y(f(a))$
  $\langle 2\rangle 7$. $x(b) = y(b)$
□

Proposition 2.17. *In a preorder, every morphism is monic and epi.*

PROOF: Immediate from definitions. ∎

2.4 Sections and Retractions

Definition 2.18 (Section, Retraction)**.** In a category, let $r : A \to B$ and $s : B \to A$. Then r is a *retraction* of s, and s is a *section* of r, iff $r \circ s = \mathrm{id}_B$.

Proposition 2.19. *Every identity morphism is a section and retraction of itself.*

PROOF: Immediate from definitions. ∎

Proposition 2.20. *Let $r, r' : A \to B$ and $s : B \to A$. If r is a retraction of s and r' is a section of s then $r = r'$.*

PROOF:

$$\begin{aligned} r &= r \circ \mathrm{id}_A \\ &= r \circ s \circ r' \\ &= \mathrm{id}_B \circ r' \\ &= r' \end{aligned}$$

∎

Proposition 2.21. *Let $r_1 : A \to B$, $r_2 : B \to C$, $s_1 : B \to A$ and $s_2 : C \to B$. If r_1 is a retraction of s_1 and r_2 is a retraction of s_2 then $r_2 \circ r_1$ is a retraction of $s_1 \circ s_2$.*

PROOF:

$$\begin{aligned} r_2 \circ r_1 \circ s_1 \circ s_2 &= r_2 \circ \mathrm{id}_B \circ s_2 \\ &= r_2 \circ s_2 \\ &= \mathrm{id}_C \end{aligned}$$

∎

Proposition 2.22. *Every section is monic.*

PROOF:
⟨1⟩1. LET: $s : A \to B$ be a section of $r : B \to A$.
⟨1⟩2. LET: $x, y : X \to A$ satisfy $sx = sy$.
⟨1⟩3. $rsx = rsy$
⟨1⟩4. $x = y$
∎

Proposition 2.23. *Every retraction is epi.*

PROOF: Dual. ∎

Proposition 2.24. *In* **Set***, every epimorphism has a retraction.*

PROOF: By the Axiom of Choice. ∎

Example 2.25. It is not true in general that every monomorphism in any category has a section. nor that every epimorphism in any category has a retraction.

In the category **2**, the morphism $0 \leq 1$ is monic and epi but has no retraction or section.

2.5 Isomorphisms

Definition 2.26 (Isomorphism)**.** In a category $\mathcal{C}$, a morphism $f : A \to B$ is an *isomorphism*, denoted $f : A \cong B$, iff there exists a morphism $f^{-1} : B \to A$, the *inverse* of f, such that $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$.

An *automorphism* on an object A is an isomorphism between A and itself. We write $\mathrm{Aut}_{\mathcal{C}}(A)$ for the set of all automorphisms on A.

Objects A and B are *isomorphic*, $A \cong B$, iff there exists an isomorphism between them.

Proposition 2.27. *The inverse of an isomorphism is unique.*

PROOF: Proposition 2.20. □

Proposition 2.28. *For any object A we have $\mathrm{id}_A : A \cong A$ and $\mathrm{id}_A^{-1} = \mathrm{id}_A$.*

PROOF: Since $\mathrm{id}_A \circ \mathrm{id}_A = \mathrm{id}_A$ by the Unit Laws. □

Proposition 2.29. *If $f : A \cong B$ then $f^{-1} : B \cong A$ and $(f^{-1})^{-1} = f$.*

PROOF: Immediate from definitions. □

Proposition 2.30. *If $f : A \cong B$ and $g : B \cong C$ then $g \circ f : A \cong C$ and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

PROOF: From Proposition 2.21. □

Definition 2.31 (Groupoid)**.** A *groupoid* is a category in which every morphism is an isomorphism.

2.6 Initial and Terminal Objects

Definition 2.32 (Initial Object)**.** An object I in a category is *initial* iff, for any object X, there is exactly one morphism $I \to X$.

Example 2.33. The empty set is the initial object in **Set**.

Definition 2.34 (Terminal Object)**.** An object T in a category is *terminal* iff, for any object X, there is exactly one morphism $X \to T$.

Example 2.35. Every singleton is terminal in **Set**.

Proposition 2.36. *If I and J are initial in a category, then there exists a unique isomorphism $I \cong J$.*

PROOF:
$\langle 1 \rangle 1$. LET: i be the unique morphism $I \to J$.
$\langle 1 \rangle 2$. LET: i^{-1} be the unique morphism $J \to I$.
$\langle 1 \rangle 3$. $i \circ i^{-1} = \mathrm{id}_J$
  PROOF: Since there is only one morphism $J \to J$.
$\langle 1 \rangle 4$. $i^{-1} \circ i = \mathrm{id}_I$

PROOF: Since there is only one morphism $I \to I$.
□

Proposition 2.37. *If S and T are terminal in a category, then there exists a unique isomorphism $S \cong T$.*

PROOF: Dual. □

Chapter 3

Functors

Definition 3.1 (Functor)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A *functor* $F : \mathcal{C} \to \mathcal{D}$ consists of:

- for every object $A \in \mathcal{C}$, an object $FA \in \mathcal{D}$
- for any morphism $f : A \to B : \mathcal{C}$, a morphism $Ff : FA \to FB : \mathcal{D}$

such that:

- $F\mathrm{id}_A = \mathrm{id}_{FA}$
- $F(g \circ f) = Fg \circ Ff$

Definition 3.2 (Identity Functor)**.** For any category $\mathcal{C}$, the *identity functor* $1_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ is defined by

$$1_{\mathcal{C}} A = A$$
$$1_{\mathcal{C}} f = f$$

Definition 3.3 (Constant Functor)**.** Given categories $\mathcal{C}$, $\mathcal{D}$ and an object $D \in \mathcal{D}$, the *constant functor* $K^{\mathcal{C}} D : \mathcal{C} \to \mathcal{D}$ is the functor defined by

$$K^{\mathcal{C}} DC = D$$
$$K^{\mathcal{C}} Df = \mathrm{id}_D$$

3.1 Comma Categories

Definition 3.4 (Comma Category)**.** Let $F : \mathcal{C} \to \mathcal{E}$ and $G : \mathcal{D} \to \mathcal{E}$ be functors. The *comma category* $F \downarrow G$ is the category with:

- objects all pairs (C, D, f) where $C \in \mathcal{C}$, $D \in \mathcal{D}$ and $f : FC \to GD : \mathcal{E}$

- morphisms $(u, v) : (C, D, f) \to (C', D', g)$ all pairs $u : C \to C' : \mathcal{C}$ and $v : D \to D' : \mathcal{D}$ such that the following diagram commutes:

$$\begin{array}{ccc} FC & \xrightarrow{f} & GD \\ \downarrow{\scriptstyle Fu} & & \downarrow{\scriptstyle Gv} \\ FC' & \xrightarrow{g} & GD' \end{array}$$

Definition 3.5 (Slice Category)**.** Let $\mathcal{C}$ be a category and $A \in \mathcal{C}$. The *slice category* over A, denoted $\mathcal{C}/A$, is the comma category $1_{\mathcal{C}} \downarrow K^{\mathbf{1}}A$.

Definition 3.6 (Coslice Category)**.** Let $\mathcal{C}$ be a category and $A \in \mathcal{C}$. The *coslice category* over A, denoted $\mathcal{C}\backslash A$, is the comma category $K^{\mathbf{1}}A \downarrow 1_{\mathcal{C}}$.

Definition 3.7 (Pointed Sets)**.** The *category of pointed sets* $\mathbf{Set}_*$ is the coslice category $\mathbf{Set}\backslash 1$.

Part II

Number Theory

Definition 3.8 (Partition)**.** A *partition* of a natural number n is a nonincreasing sequence of positive integers whose sum is n.

Part III

Group Theory

Chapter 4

Semigroups

Definition 4.1 (Semigroup)**.** A *semigroup* consists of a set S and an associative binary operation $\cdot$ on S.

Chapter 5

Monoids

Definition 5.1 (Monoid)**.** A *monoid* consists of a semigroup M such that there exists $e \in M$, the *unit*, such that, for all $x \in M$, we have $xe = ex = x$.

We identify a monoid M with the category with one object whose morphisms are the elements of M, with composition given by $\cdot$.

Proposition 5.2. *The identity in a group is unique.*

PROOF: Proposition 2.3.

Chapter 6

Groups

Definition 6.1 (Group)**.** Let $\mathcal{C}$ be a category with finite products. A *group (object)* in $\mathcal{C}$ consists of an object $G \in \mathcal{C}$ and morphisms

$$m : G^2 \to G, e : 1 \to G, i : G \to G$$

such that the following diagrams commute.

$$\begin{tikzcd}
G^3 \arrow[r, "m\times\mathrm{id}_G"] \arrow[d, "\mathrm{id}_G\times m"] & G^2 \arrow[d, "m"] \\
G^2 \arrow[r, "m"] & G
\end{tikzcd}$$

$$\begin{tikzcd}
1\times G \arrow[r, "e\times\mathrm{id}_G"] \arrow[dr, "\cong"] & G^2 \arrow[d, "m"] \\
& G
\end{tikzcd}
\qquad
\begin{tikzcd}
G\times 1 \arrow[r, "\mathrm{id}_G\times e"] \arrow[dr, "\cong"] & G^2 \arrow[d, "m"] \\
& G
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "\Delta"] \arrow[d] & G^2 \arrow[r, "\mathrm{id}_G\times i"] & G^2 \arrow[d, "m"] \\
1 \arrow[rr, "e"] & & G
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "\Delta"] \arrow[d] & G^2 \arrow[r, "i\times\mathrm{id}_G"] & G^2 \arrow[d, "m"] \\
1 \arrow[rr, "e"] & & G
\end{tikzcd}$$

Definition 6.2 (Group)**.** We write just 'group' for 'group in **Set**. Thus, a *group* G consists of a set G and a binary operation $\cdot : G^2 \to G$ such that $\cdot$ is associative, and there exists $e \in G$, the *identity* element of the group, such that:

- For all $x \in G$ we have $xe = ex = x$
- For all $x \in G$, there exists $x^{-1} \in G$, the *inverse* of x, such that $xx^{-1} = x^{-1}x = e$.

The *order* of a group G, denoted $|G|$, is the number of elements in G if G is finite; otherwise we write $|G| = \infty$.

Proposition 6.3. *The inverse of an element is unique.*

Proof: If i and j are inverses of x then $i = ixj = j$. □

Example 6.4.

- The *trivial* group is $\{e\}$ under $ee = e$.
- $\mathbb{Z}$ is a group under addition
- $\mathbb{Q}$ is a group under addition
- $\mathbb{Q} - \{0\}$ is a group under multiplication
- $\mathbb{R}$ is a group under addition
- $\mathbb{R} - \{0\}$ is a group under multiplication
- $\mathbb{C}$ is a group under addition
- $\mathbb{C} - \{0\}$ is a group under multiplication
- $\{-1, 1\}$ is a group under multiplication
- For any category $\mathcal{C}$ and object $A \in \mathcal{C}$, we have $\mathrm{Aut}_{\mathcal{C}}(A)$ is a group under $gf = f \circ g$.

  For A a set, we call $S_A = \mathrm{Aut}_{\mathbf{Set}}(A)$ the *symmetric group* or *group of permutations* of A.
- For $n \geq 3$, the *dihedral group* D_{2n} consists of the set of rigid motions that map the regular n-gon onto itself under composition.
- Let $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$ under matrix multiplication.
- The quaternionic group Q_8 is the group

  $$\{1, -1, i, -i, j, -j, k, -k\}$$

  with multiplication table

  $$\begin{array}{cccccccc} 1 & -1 & i & -i & j & -j & k & -k \\ -1 & 1 & -i & i & -j & j & -k & k \\ i & -i & -1 & 1 & k & -k & -j & j \\ -i & i & 1 & -1 & -k & k & j & -j \\ j & -j & -k & k & -1 & 1 & i & -i \\ -j & j & k & -k & 1 & -1 & -i & i \\ k & -k & j & -j & -i & i & -1 & 1 \\ -k & k & -j & j & i & -i & 1 & -1 \end{array}$$

Example 6.5.

- The only group of order 1 is the trivial group.
- The only group of order 2 is $\mathbb{Z}_2$.

- The only group of order 3 is $\mathbb{Z}_3$.
- There are exactly two groups of order 4: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ under $(a,b)(c,d) = (ac, bd)$.

Proposition 6.6 (Cancellation)**.** *Let G be a group. Let $a, g, h \in G$. If $ag = ah$ or $ga = ha$ then $g = h$.*

Proof: If $ag = ah$ then $g = a^{-1}ag = a^{-1}ah = h$. Similarly if $ga = ha$. □

Proposition 6.7. *Let G be a group and $g, h \in G$. Then $(gh)^{-1} = h^{-1}g^{-1}$.*

Proof: Since $ghh^{-1}g^{-1} = e$. □

Definition 6.8. Let G be a group. Let $g \in G$. We define $g^n \in G$ for all $n \in \mathbb{Z}$ as follows:

$$\begin{aligned} g^0 &= e \\ g^{n+1} &= g^n g && (n \geq 0) \\ g^{-n} &= (g^{-1})^n && (n > 0) \end{aligned}$$

Proposition 6.9. *Let G be a group. Let $g \in G$ and $m, n \in \mathbb{Z}$. Then*

$$g^{m+n} = g^m g^n \ .$$

Proof:
⟨1⟩1. For all $k \in \mathbb{Z}$ we have $g^{k+1} = g^k g$
⟨2⟩1. For all $k \geq 0$ we have $g^{k+1} = g^k g$
Proof: Immediate from definition.
⟨2⟩2. $g^{-1+1} = g^{-1}g$
Proof: Both are equal to e.
⟨2⟩3. For all $k > 1$ we have $g^{-k+1} = g^{-k}g$
Proof:

$$\begin{aligned} g^{-k+1} &= (g^{-1})^{k-1} \\ &= (g^{-1})^{k-1}g^{-1}g \\ &= (g^{-1})^k g \\ &= g^{-k}g \end{aligned}$$

⟨1⟩2. For all $k \in \mathbb{Z}$ we have $g^{k-1} = g^k g^{-1}$
Proof: Substitute $k = k - 1$ above and multiply by g^{-1}.
⟨1⟩3. $g^{m+0} = g^m g^0$
Proof: Since $g^m g^0 = g^m e = g^m$.
⟨1⟩4. If $g^{m+n} = g^m g^n$ then $g^{m+n+1} = g^m g^{n+1}$
Proof:

$$\begin{aligned} g^{m+n+1} &= g^{m+n}g && (\langle 1\rangle 1) \\ &= g^m g^n g \\ &= g^m g^{n+1} && (\langle 1\rangle 1) \end{aligned}$$

⟨1⟩5. If $g^{m+n} = g^m g^n$ then $g^{m+n-1} = g^m g^{n-1}$

Proof:

$$\begin{aligned} g^{m+n-1} g &= g^{m+n} && (\langle 1\rangle 1) \\ &= g^m g^n \\ \therefore g^{m+n-1} &= g^m g^n g^{-1} \\ &= g^m g^{n-1} && (\langle 1\rangle 2) \end{aligned}$$

□

Proposition 6.10. *Let G be a group. Let $g \in G$ and $m, n \in \mathbb{Z}$. Then*

$$(g^m)^n = g^{mn} \quad .$$

Proof:

⟨1⟩1. $(g^m)^0 = g^0$

Proof: Both sides are equal to e.

⟨1⟩2. If $(g^m)^n = g^{mn}$ then $(g^m)^{n+1} = g^{m(n+1)}$.

Proof:

$$\begin{aligned} (g^m)^{n+1} &= (g^m)^n g^m && \text{(Proposition 6.9)} \\ &= g^{mn} g^m \\ &= g^{mn+m} && \text{(Proposition 6.9)} \end{aligned}$$

⟨1⟩3. If $(g^m)^n = g^{mn}$ then $(g^m)^{n-1} = g^{m(n-1)}$.

Proof:

$$\begin{aligned} (g^m)^n &= g^{mn} \\ \therefore (g^m)^{n-1} g^m &= g^{mn-m} g^m && \text{(Proposition 6.9)} \\ \therefore (g^m)^{n-1} &= g^{mn-m} && \text{(Cancellation)} \end{aligned}$$

□

Definition 6.11 (Commute)**.** Let G be a group and $g, h \in G$. We say g and h *commute* iff $gh = hg$.

Definition 6.12. Let G be a group. Given $g \in G$ and $A \subseteq G$, we define

$$gA = \{ga : a \in A\}, \qquad Ag = \{ag : a \in A\} \quad .$$

Given sets $A, B \subseteq G$, we define

$$AB = \{ab : a \in A, b \in B\} \quad .$$

6.1 Symmetric Groups

Definition 6.13. Let n be a natural number and $a_1, \ldots, a_r \in \{1, \ldots, n\}$ be distinct. The *cycle* or *r-cycle*

$$(a_1 \ a_2 \ \cdots \ a_r) \in S_n$$

is the permutation that sends a_i to a_{i+1} $(1 \leq i < r)$ and a_r to a_1.

We call r the *length* of the cycle.

A *transposition* is a 2-cycle.

Proposition 6.14. *Disjoint cycles commute.*

PROOF: Easy. ∎

Proposition 6.15. *For any cycle $(a_1\ a_2\ \cdots\ a_r)$ in S_n and $\tau \in S_n$ we have*

$$\tau(a_1\ a_2\ \cdots\ a_n)\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \cdots\ \tau(a_n))\ .$$

PROOF: Easy. ∎

6.2 Order of an Element

Definition 6.16 (Order)**.** Let G be a group. Let $g \in G$. Then g has *finite order* iff there exists a positive integer n such that $g^n = e$. In this case, the *order* of g, denoted $|g|$, is the least positive integer n such that $g^n = e$.

If g does not have finite order, we write $|g| = \infty$.

Proposition 6.17. *Let G be a group. Let $g \in G$ and n be a positive integer. If $g^n = e$ then $|g| \mid n$.*

PROOF:
⟨1⟩1. LET: $n = q|g| + d$ where $0 \leq d < |g|$
PROOF: Division Algorithm.
⟨1⟩2. $g^d = e$
PROOF:

$$\begin{aligned} e &= g^n \\ &= g^{q|g|+d} \\ &= (g^{|g|})^q g^d && \text{(Propositions 6.9, 6.10)} \\ &= e^q g^d \\ &= g^d \end{aligned}$$

⟨1⟩3. $d = 0$
PROOF: By minimality of $|g|$.
⟨1⟩4. $n = q|g|$
∎

Corollary 6.17.1. *Let G be a group. Let $g \in G$ have finite order and $n \in \mathbb{Z}$. Then $g^n = e$ if and only if $|g| \mid n$.*

Proposition 6.18. *Let G be a group and $g \in G$. Then $|g| \leq |G|$.*

PROOF:
⟨1⟩1. ASSUME: w.l.o.g. G is finite.
⟨1⟩2. PICK i, j with $0 \leq i < j \leq |G|$ such that $g^i = g^j$.
PROOF: Otherwise $g^0, g^1, \ldots, g^{|G|}$ would be $|G| + 1$ distinct elements of G.
⟨1⟩3. $g^{j-i} = e$
⟨1⟩4. g has finite order and $|g| \leq |G|$
PROOF: Since $|g| \leq j - i \leq j \leq |G|$.

∎

Proposition 6.19. *Let G be a group. Let $g \in G$ have finite order. Let $m \in \mathbb{N}$. Then*

$$|g^m| = \frac{\mathrm{lcm}(m, |g|)}{m} = \frac{|g|}{\gcd(m, |g|)}$$

Proof: Since for any integer d we have

$$\begin{aligned} g^{md} = e &\Leftrightarrow |g| \mid md && \text{(Corollary 6.17.1)} \\ &\Leftrightarrow \mathrm{lcm}(m, |g|) \mid md \\ &\Leftrightarrow \frac{\mathrm{lcm}(m, |g|)}{m} \mid d && \square \end{aligned}$$

and so $|g^m| = \frac{\mathrm{lcm}(m,|g|)}{m}$ by Corollary 6.17.1. ∎

Corollary 6.19.1. *If g has odd order then $|g^2| = |g|$.*

Proposition 6.20. *Let G be a group. Let $g, h \in G$ have finite order. Assume $gh = hg$. Then $|gh|$ has finite order and*

$$|gh| \mid \mathrm{lcm}(|g|, |h|)$$

Proof: Since $(gh)^{\mathrm{lcm}(|g|,|h|)} = g^{\mathrm{lcm}(|g|,|h|)} h^{\mathrm{lcm}(|g|,|h|)} = e$. ∎

Example 6.21. This example shows that we cannot remove the hypothesis that $gh = hg$.

In $\mathrm{GL}_2(\mathbb{R})$, take

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} .$$

Then $|g| = 4$, $|h| = 3$ and $|gh| = \infty$.

Proposition 6.22. *Let G be a group and $g, h \in G$ have finite order. If $gh = hg$ and $\gcd(|g|, |h|) = 1$ then $|gh| = |g||h|$.*

Proof:
$\langle 1 \rangle$1. Let: $N = |gh|$
$\langle 1 \rangle$2. $g^N = (h^{-1})^N$
$\langle 1 \rangle$3. $g^{N|g|} = e$
$\langle 1 \rangle$4. $|g^N| \mid |g|$
$\langle 1 \rangle$5. $h^{-N|h|} = e$
$\langle 1 \rangle$6. $|g^N| \mid |h|$
$\langle 1 \rangle$7. $|g^N| = 1$
Proof: Since $\gcd(|g|, |h|) = 1$.
$\langle 1 \rangle$8. $g^N = e$
$\langle 1 \rangle$9. $|g| \mid N$
$\langle 1 \rangle$10. $h^{-N} = e$
$\langle 1 \rangle$11. $|h| \mid N$
$\langle 1 \rangle$12. $N = |g||h|$

PROOF: Using Proposition 6.20.
∎

Proposition 6.23. *Let G be a finite group. Assume there is exactly one element $f \in G$ of order 2. Then the product of all the elements of G is f.*

PROOF: Let the elements of G be $g_1, g_2, \ldots, g_n$. Apart from e and f, every element and its inverse are distinct elements of the list. Hence the product of the list is $ef = f$. ∎

Proposition 6.24. *Let G be a finite group of order n. Let m be the number of elements of G of order 2. Then $n - m$ is odd.*

PROOF: In the list of all elements that are not of order 2, every element and its inverse are distinct except for e. Hence the list has odd length. ∎

Corollary 6.24.1. *If a finite group has even order, then it contains an element of order 2.*

Proposition 6.25. *Let G be a group and $a, g \in G$. Then $|aga^{-1}| = |g|$.*

PROOF: Since

$$\begin{aligned}(aga^{-1})^n = e &\Leftrightarrow ag^n a^{-1} = e \\ &\Leftrightarrow g^n = e\end{aligned}$$

∎

Proposition 6.26. *Let G be a group and $g, h \in G$. Then $|gh| = |hg|$.*

PROOF: Since $|gh| = |ghgg^{-1}| = |hg|$. ∎

Proposition 6.27. *Let G be a group of order n. Let k be relatively prime to n. Then every element in G has the form x^k for some x.*

⟨1⟩1. PICK integers a and b such that $an + bk = 1$.
⟨1⟩2. LET: $g \in G$
⟨1⟩3. $g = (g^b)^k$
PROOF:

$$\begin{aligned} g &= g.(g^n)^{-a} && (g^n = e) \\ &= g^{1-an} \\ &= g^{bk} \end{aligned}$$

∎

6.3 Generators

Definition 6.28 (Generator)**.** Let G be a group and $a \in G$. We say *a generates* the group iff, for all $x \in G$, there exists an integer n such that $x^n = a$.

Example 6.29. $\mathrm{SL}_2(\mathbb{Z})$ is generated by

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

PROOF:

⟨1⟩1. LET: $H = \langle s, t \rangle$

⟨1⟩2. For all $q \in \mathbb{Z}$ we have $\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \in H$.

PROOF: It is t^q.

⟨1⟩3. For all $q \in \mathbb{Z}$ we have $\begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} \in H$.

PROOF:

$$\begin{aligned} st^{-q}s^{-1} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} \end{aligned}$$

⟨1⟩4.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & qa+b \\ c & qc+d \end{pmatrix}$$

⟨1⟩5.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} = \begin{pmatrix} a+qb & b \\ c+qd & d \end{pmatrix}$$

⟨1⟩6. For any $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, if c and d are both nonzero, then there exists $N \in H$ such that the bottom row of MN has one entry the same as M and one entry with smaller absolute value.

PROOF: From ⟨1⟩4 and ⟨1⟩5 taking $q = -1$.

⟨1⟩7. For any $M \in \mathrm{SL}_2(\mathbb{Z})$, there exists $N \in H$ such that MN has a zero on the bottom row.

PROOF: Apply ⟨1⟩6 repeatedly.

⟨1⟩8. Any matrix in $\mathrm{SL}_2(\mathbb{Z})$ with a zero on the bottom row is in H.

⟨2⟩1. $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H$

PROOF: ⟨1⟩2

⟨2⟩2. $\begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} \in H$

PROOF: It is $s^2 \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ since $s^2 = -I$.

⟨2⟩3. $\begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix} \in H$

PROOF: It is $\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} s$.

⟨2⟩4. $\begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \in H$

PROOF: It is $s^2 \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} s$.

⟨1⟩9. Every matrix in $\mathrm{SL}_2(\mathbb{Z})$ is in H.

□

6.4 p-groups

Definition 6.30 (p-group)**.** Let p be a prime. A *p-group* is a finite group whose order is a power of p.

Chapter 7

Group Homomorphisms

Definition 7.1 (Homomorphism)**.** Let G and H be groups. A *(group) homomorphism* $\phi : G \to H$ is a function such that, for all $x, y \in G$,

$$\phi(xy) = \phi(x)\phi(y) \ .$$

Proposition 7.2. *Let G and H be groups with identities e_G and e_H. Let $\phi : G \to H$ be a group homomorphism. Then $\phi(e_G) = e_H$.*

PROOF: Since $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$ and so $\phi(e_G) = e_H$ by Cancellation. □

Proposition 7.3. *Let $\phi : G \to H$ be a group homomorphism. For all $x \in G$ we have $\phi(x^{-1}) = \phi(x)^{-1}$.*

PROOF: Since $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(e_G) = e_H$. □

Proposition 7.4. *Let G, H and K be groups. If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms then $\psi \circ \phi : G \to K$ is a homomorphism.*

PROOF: For $x, y \in G$ we have

$$\psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\psi(\phi(y)) \ .$$

Proposition 7.5. *Let G be a group. Then $\mathrm{id}_G : G \to G$ is a group homomorphism.*

PROOF: For $x, y \in G$ we have $\mathrm{id}_G(xy) = xy = \mathrm{id}_G(x)\mathrm{id}_G(y)$. □

Proposition 7.6. *Let $\phi : G \to H$ be a group homomorphism. Let $g \in G$ have finite order. Then $|\phi(g)|$ divides $|g|$.*

PROOF: Since $\phi(g)^{|g|} = \phi(g^{|g|}) = e$. □

Definition 7.7 (Category of Groups)**.** Let **Grp** be the category of groups and group homomorphisms.

Example 7.8. There are 49487365402 groups of order 1024 up to isomorphism.

Proposition 7.9. *A group homomorphism $\phi : G \to H$ is an isomorphism in* **Grp** *if and only if it is bijective.*

PROOF:
$\langle 1\rangle 1$. ASSUME: ϕ is bijective.
PROVE: ϕ^{-1} is a group homomorphism.
$\langle 1\rangle 2$. LET: $h, h' \in H$
$\langle 1\rangle 3$. $\phi(\phi^{-1}(hh')) = \phi(\phi^{-1}(h)\phi^{-1}(h'))$
PROOF: Both are equal to hh'.
$\langle 1\rangle 4$. $\phi^{-1}(hh') = \phi^{-1}(h)\phi^{-1}(h')$
$\square$

Corollary 7.9.1.
$$D_6 \cong C_3$$

PROOF: The canonical homomorphism $D_6 \to C_3$ is bijective. $\square$

Corollary 7.9.2.
$$(\mathbb{R}, +) \cong (\{x \in \mathbb{R} : x > 0\}, \cdot)$$

PROOF: The function that maps x to e^x is a bijective homomorphism. $\square$

Proposition 7.10. *The trivial group is the zero object in* **Grp**.

PROOF: For any group G, the unique function $G \to \{e\}$ is a group homomorphism, and the only group homomorphism $\{e\} \to G$ maps e to e_G. $\square$

Proposition 7.11. *For any groups G and H, the set $G \times H$ under $(g, h)(g', h') = (gg', hh')$ is the product of G and H in* **Grp**.

PROOF:
$\langle 1\rangle 1$. $G \times H$ is a group.
$\langle 2\rangle 1$. The multiplication is associative.
PROOF: Since $(g_1, h_1)((g_2, h_2)(g_3, h_3)) = ((g_1, h_1)(g_2, h_2))(g_3, h_3) = (g_1g_2g_3, h_1h_2h_3)$.
$\langle 2\rangle 2$. (e_G, e_H) is the identity.
PROOF: Since $(g, h)(e_G, e_H) = (e_G, e_H)(g, h) = (g, h)$.
$\langle 2\rangle 3$. The inverse of (g, h) is (g^{-1}, h^{-1}).
PROOF: Since $(g, h)(g^{-1}, h^{-1}) = (g^{-1}, h^{-1})(g, h) = (e_G, e_H)$.
$\langle 1\rangle 2$. $\pi_1 : G \times H \to G$ is a group homomorphism.
PROOF: Immediate from definitions.
$\langle 1\rangle 3$. $\pi_2 : G \times H \to H$ is a group homomorphism.
PROOF: Immediate from definitions.
$\langle 1\rangle 4$. For any group homomorphism $\phi : K \to G$ and $\psi : K \to H$, the function $\langle \phi, \psi\rangle : K \to G \times H$ where $\langle \phi, \psi\rangle(k) = (\phi(k), \psi(k))$ is a group homomorphism.
PROOF:
$$\begin{aligned}
\langle \phi, \psi\rangle(kk') &= (\phi(kk'), \psi(kk')) \\
&= (\phi(k)\phi(k'), \psi(k)\psi(k')) \\
&= (\phi(k), \psi(k))(\phi(k'), \psi(k')) \\
&= \langle \phi, \psi\rangle(k)\langle \phi, \psi\rangle(k')
\end{aligned}$$

$\square$

7.1 Subgroups

Definition 7.12 (Subgroup)**.** Let $(G, \cdot)$ and $(H, *)$ be groups such that H is a subset of G. Then H is a *subgroup* of G iff the inclusion $i : H \hookrightarrow G$ is a group homomorphism.

Proposition 7.13. *If $(H, *)$ is a subgroup of $(G, \cdot)$ then $*$ is the restriction of $\cdot$ to H.*

PROOF: Given $x, y \in H$ we have
$$x * y = i(x * y) = i(x) \cdot i(y) = x \cdot y \ . \qquad \square$$

Example 7.14. For any group G we have $\{e\}$ is a subgroup of G.

Proposition 7.15. *Let G be a group. Let H be a subset of G. Then H is a subgroup of G iff H is nonempty and, for all $x, y \in H$, we have $xy^{-1} \in H$.*

PROOF:
$\langle 1\rangle 1$. If H is a subgroup of G then H is nonempty.
  PROOF: Since every group has an identity element and so is nonempty.
$\langle 1\rangle 2$. If H is a subgroup of G then, for all $x, y \in H$, we have $xy^{-1} \in H$.
  PROOF: Easy.
$\langle 1\rangle 3$. If H is nonempty and, for all $x, y \in H$, we have $xy^{-1} \in H$, then H is a subgroup of G.
  $\langle 2\rangle 1$. ASSUME: H is nonempty.
  $\langle 2\rangle 2$. ASSUME: $\forall x, y \in H . xy^{-1} \in H$
  $\langle 2\rangle 3$. $e \in H$
    PROOF: Pick $x \in H$. We have $e = xx^{-1} \in H$.
  $\langle 2\rangle 4$. $\forall x \in H . x^{-1} \in H$
    PROOF: Given $x \in H$ we have $x^{-1} = ex^{-1} \in H$.
  $\langle 2\rangle 5$. H is closed under the restriction of $\cdot$
    PROOF: Given $x, y \in H$ we have $xy = x(y^{-1})^{-1} \in H$.
  $\langle 2\rangle 6$. H is a group under the restriction of $\cdot$
    PROOF: Associativity is inherited from G and the existence of an identity element and inverses follows from $\langle 2\rangle 3$ and $\langle 2\rangle 4$.
  $\langle 2\rangle 7$. The inclusion $H \hookrightarrow G$ is a group homomorphism.
    PROOF: For $x, y \in H$ we have $i(xy) = i(x)i(y) = xy$.
$\square$

Corollary 7.15.1. *The intersection of a set of subgroups of G is a subgroup of G.*

Corollary 7.15.2. *Let $\phi : G \to H$ be a group homomorphism. Let K be a subgroup of H. Then $\phi^{-1}(K)$ is a subgroup of G.*

PROOF:
$\langle 1\rangle 1$. $\phi^{-1}(K)$ is nonempty.
  PROOF: Since $e \in \phi^{-1}(K)$.
$\langle 1\rangle 2$. LET: $x, y \in \phi^{-1}(K)$

$\langle 1 \rangle 3.$ $\phi(x), \phi(y) \in K$
$\langle 1 \rangle 4.$ $\phi(x)\phi(y)^{-1} \in K$
$\langle 1 \rangle 5.$ $\phi(xy^{-1}) \in K$
$\langle 1 \rangle 6.$ $xy^{-1} \in \phi^{-1}(K)$
$\square$

Corollary 7.15.3. *Let $\phi : G \to H$ be a group homomorphism. Let K be a subgroup of G. Then $\phi(K)$ is a subgroup of H.*

PROOF:
$\langle 1 \rangle 1.$ LET: $x, y \in \phi(K)$
$\langle 1 \rangle 2.$ PICK $a, b \in K$ such that $x = \phi(a)$ and $y = \phi(b)$
$\langle 1 \rangle 3.$ $xy^{-1} = \phi(ab^{-1})$
$\langle 1 \rangle 4.$ $xy^{-1} \in \phi(K)$
$\square$

Proposition 7.16. *Let G be a subgroup of $\mathbb{Z}$. Then there exists $d \geq 0$ such that $G = d\mathbb{Z}$.*

PROOF:
$\langle 1 \rangle 1.$ ASSUME: w.l.o.g. $G \neq \{0\}$
PROOF: Since $\{0\} = 0\mathbb{Z}$.
$\langle 1 \rangle 2.$ LET: d be the least positive element of G.
PROVE: $G = d\mathbb{Z}$
PROOF: If $n \in G$ then $-n \in G$ so G must contain a positive element.
$\langle 1 \rangle 3.$ $G \subseteq d\mathbb{Z}$
$\langle 2 \rangle 1.$ LET: $n \in G$
$\langle 2 \rangle 2.$ LET: q and r be the integers such that $n = qd + r$ and $0 \leq r < d$.
$\langle 2 \rangle 3.$ $r \in G$
PROOF: Since $r = n - qd$.
$\langle 2 \rangle 4.$ $r = 0$
PROOF: By minimality of d.
$\langle 2 \rangle 5.$ $n = qd \in d\mathbb{Z}$
$\langle 1 \rangle 4.$ $d\mathbb{Z} \subseteq G$
$\square$

7.2 Kernel

Definition 7.17 (Kernel)**.** Let $\phi : G \to H$ be a group homomorphism. The *kernel* of ϕ is

$$\ker \phi = \{g \in G : \phi(g) = e\} .$$

Proposition 7.18. *Let $\phi : G \to H$ be a group homomorphism. Then* $\ker \phi$ *is a subgroup of G.*

PROOF: Corollary 7.15.2. $\square$

Proposition 7.19. *Let $\phi : G \to H$ be a group homomorphism. Then the inclusion $i : \ker\phi \hookrightarrow G$ is terminal in the category of pairs $(K, \alpha : K \to G)$ such that $\phi \circ \alpha = 0$.*

PROOF:
⟨1⟩1. $\phi \circ i = 0$
⟨1⟩2. For any group K and homomorphism $\alpha : K \to G$ such that $\phi \circ \alpha = 0$, there exists a unique homomorphism $\beta : K \to \ker\phi$ such that $i \circ \beta = \alpha$.
□

Proposition 7.20. *Let $\phi : G \to H$ be a group homomorphism. Then the following are equivalent:*

1. *ϕ is monic.*
2. $\ker\phi = \{e\}$
3. *ϕ is injective.*

PROOF:
⟨1⟩1. $1 \Rightarrow 2$
⟨2⟩1. ASSUME: ϕ is monic.
⟨2⟩2. LET: $i : \ker\phi \hookrightarrow G$, $j : \{e\} \hookrightarrow \ker\phi \hookrightarrow G$ be the inclusions.
⟨2⟩3. $\phi \circ i = \phi \circ j$
⟨2⟩4. $i = j$
⟨1⟩2. $2 \Rightarrow 3$
⟨2⟩1. ASSUME: $\ker\phi = \{e\}$
⟨2⟩2. LET: $x, y \in G$
⟨2⟩3. ASSUME: $\phi(x) = \phi(y)$
⟨2⟩4. $\phi(xy^{-1}) = e$
⟨2⟩5. $xy^{-1} \in \ker\phi$
⟨2⟩6. $xy^{-1} = e$
⟨2⟩7. $x = y$
⟨1⟩3. $3 \Rightarrow 1$
PROOF: Easy.
□

Proposition 7.21. *A group homomorphism is an epimorphism if and only if it is surjective.*

7.3 Inner Automorphisms

Proposition 7.22. *Let G be a group and $g \in G$. The function $\gamma_g : G \to G$ defined by $\gamma_g(a) = gag^{-1}$ is an automorphism on G.*

PROOF:
⟨1⟩1. γ_g is a homomorphism.

PROOF:
$$\begin{aligned}\gamma_g(ab) &= gabg^{-1} \\ &= gag^{-1}gbg^{-1} \\ &= \gamma_g(a)\gamma_g(b)\end{aligned}$$
⟨1⟩2. γ_g is injective.
PROOF: By Cancellation.
⟨1⟩3. γ_g is surjective.
PROOF: Given $b \in G$, we have $\gamma_g(g^{-1}bg) = b$.
□

Definition 7.23 (Inner Automorphism)**.** Let G be a group. An *inner automorphism* on G is a function of the form $\gamma_g(a) = gag^{-1}$ for some $g \in G$.

We write $\mathrm{Inn}(G)$ for the set of inner automorphisms of G.

Proposition 7.24. *Let G be a group. The function $\gamma : G \to \mathrm{Aut}_{\mathbf{Grp}}(G)$ that maps g to γ_g is a group homomorphism.*

PROOF: Since $\gamma_{gh}(a) = ghah^{-1}g^{-1} = \gamma_g(\gamma_h(a))$. □

Corollary 7.24.1. $\mathrm{Inn}(G)$ *is a subgroup of* $\mathrm{Aut}_{\mathbf{Grp}}(G)$.

7.4 Direct Products

Definition 7.25 (Direct Product)**.** The *direct product* of groups G and H is their product in **Grp**.

7.5 Free Groups

Proposition 7.26. *Let A be a set. Let $\mathcal{F}^A$ be the category whose objects are pairs (G, j) where G is a group and j is a function $A \to G$, with morphisms $f : (G, j) \to (H, k)$ the group homomorphisms $f : G \to H$ such that $f \circ j = k$. Then $\mathcal{F}^A$ has an initial object.*

PROOF:
⟨1⟩1. LET: $W(A)$ be the set of words in the alphabet whose elements are the elements of A together with $\{a^{-1} : a \in A\}$.
⟨1⟩2. LET: $r : W(A) \to W(A)$ be the function that, given a word w, removes the first pair of letters of the form aa^{-1} or $a^{-1}a$; if there is no such pair, then $r(w) = w$.
⟨1⟩3. Let us say that a word w is a *reduced word* iff $r(w) = w$.
⟨1⟩4. For any word w of length n, we have $r^{\lceil \frac{n}{2} \rceil}(w)$ is a reduced word.
PROOF: Since we cannot remove more than $n/2$ pairs of letters from w.
⟨1⟩5. LET: $R : W(A) \to W(A)$ be the function $R(w) = r^{\lceil \frac{n}{2} \rceil}(w)$, where n is the length of w.
⟨1⟩6. LET: $F(A)$ be the set of reduced words.
⟨1⟩7. Define $\cdot : F(A)^2 \to F(A)$ by $w \cdot w' = R(ww')$

$\langle 1\rangle 8.$ $\cdot$ is associative.

PROOF: Both $w_1 \cdot (w_2 \cdot w_3)$ and $(w_1 \cdot w_2) \cdot w_3$ are equal to $R(w_1 w_2 w_3)$.

$\langle 1\rangle 9.$ The empty word is the identity element in $F(A)$

$\langle 1\rangle 10.$ The inverse of $a_1^{\pm 1} a_2^{\pm 1} \cdots a_n^{\pm 1}$ is $a_n^{\mp 1} \cdots a_2^{\mp 1} a_1^{\mp 1}$.

$\langle 1\rangle 11.$ LET: $j : A \to F(A)$ be the function that maps a to the word a of length
.

$\langle 1\rangle 12.$ LET: G be any group and $k : A \to G$ any function.

$\langle 1\rangle 13.$ The only morphism $f : (F(A), j) \to (G, k)$ in $\mathcal{F}^A$ is $f(a_1^{\pm 1} a_2^{\pm 1} \cdots a_n^{\pm 1}) = k(a_1)^{\pm 1} k(a_2)^{\pm 1} \cdots k(a_n)^{\pm 1}$.

□

Definition 7.27 (Free Group)**.** For any set A, the *free group* on A is the initial object $(F(A), i)$ in $\mathcal{F}^A$.

Proposition 7.28. *$i : A \to F(A)$ is injective.*

PROOF:

$\langle 1\rangle 1.$ LET: $x, y \in A$

$\langle 1\rangle 2.$ ASSUME: $x \neq y$
PROVE: $i(x) \neq i(y)$

$\langle 1\rangle 3.$ LET: $f : A \to C_2$ be the function that maps x to 0 and all other elements of A to 1.

$\langle 1\rangle 4.$ LET: $\phi : F(A) \to C_2$ be the group homomorphism such that $f = \phi \circ i$.

$\langle 1\rangle 5.$ $f(x) \neq f(y)$

$\langle 1\rangle 6.$ $\phi(i(x)) \neq \phi(i(y))$

$\langle 1\rangle 7.$ $i(x) \neq i(y)$

□

Proposition 7.29.

$$F(0) \cong \{e\}$$

PROOF: For any set A, the unique group homomorphism $\{e\} \to A$ makes the following diagram commute.

$$\begin{tikzcd}
\{e\} \arrow[r] & A \\
\emptyset \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Proposition 7.30. *The free group on 1 is $\mathbb{Z}$ with the injection mapping 0 to* 1.

PROOF: Given any group G and function $a : 1 \to G$, the required unique homomorphism $\phi : \mathbb{Z} \to G$ is defined by $\phi(n) = a(0)^n$. □

Proposition 7.31. *For any sets A and B, we have that $F(A + B)$ is the coproduct of $F(A)$ and $F(B)$ in* **Grp**.

$$\begin{tikzcd}
 & G & \\
F(A) \arrow[ur, "f"] \arrow[r, "\kappa_1"] & F(A+B) \arrow[u, "k"'] & F(B) \arrow[l, "\kappa_2"] \arrow[ul, "g"'] \\
A \arrow[u, "i_A"] \arrow[r, "k_1"] & A+B \arrow[u, "j"] & B \arrow[u, "i_B"] \arrow[l, "k_2"]
\end{tikzcd}$$

Proof:
⟨1⟩1. Let: $i_A : A \to F(A)$, $i_B : B \to F(B)$, $j : A + B \to F(A + B)$ be the canonical injections.
⟨1⟩2. Let: κ_1, κ_2 be the unique group homomorphisms that make the diagram above commute.
⟨1⟩3. Let: G be any group and $f : F(A) \to G$, $g : F(B) \to G$ any group homomorphisms.
⟨1⟩4. Let: $h : A+B \to G$ be the unique function such that $h \circ k_1 = f \circ i_A$ and $h \circ k_2 = g \circ i_B$.
⟨1⟩5. Let: $k : F(A + B) \to G$ be the unique group homomorphism such that $k \circ j = h$.
⟨1⟩6. k is the unique group homomorphism such that $k \circ \kappa_1 \circ i_A = f \circ i_A$ and $k \circ \kappa_2 \circ i_B = g \circ i_B$.
⟨1⟩7. k is the unique group homomorphism such that $k \circ \kappa_1 = f$ and $k \circ \kappa_2 = g$.
□

Definition 7.32 (Subgroup Generated by a Group)**.** Let G be a group and A a subset of G. Let $\phi : F(A) \to G$ be the unique group homomorphism such that $\phi(a) = a$ for all $a \in A$. The subgroup *generated* by A is

$$\langle A \rangle := \operatorname{im} \phi$$

$$\begin{tikzcd}
F(A) \arrow[r, "\phi"] & G \\
A \arrow[u] \arrow[ur] &
\end{tikzcd}$$

Proposition 7.33. *Let G be a group and A a subset of G. Then $\langle A \rangle$ is the set of all elements of the form $a_1^{\pm 1} a_2^{\pm 1} \cdots a_n^{\pm 1}$ (where $n \geq 0$) such that $a_1, \ldots, a_n \in A$.*

Proof: Immediate from definitions. □

Corollary 7.33.1. *Let G be a group and $g \in G$. Then*

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \ .$$

Proposition 7.34. *Let G be a group and A a subset of G. Then $\langle A \rangle$ is the intersection of all the subgroups of G that include A.*

PROOF: Easy. □

Definition 7.35 (Finitely Generated)**.** Let G be a group. Then G is *finitely generated* iff there exists a finite subset A of G such that $G = \langle A \rangle$.

Proposition 7.36. *Every subgroup of a finitely generated free group is free.*

PROOF: TODO.

Proposition 7.37. $F(2)$ *includes subgroups isomorphic to the free group on arbitrarily many generators.*

PROOF: TODO

Proposition 7.38.

$$[F(2), F(2)] \cong F(\mathbb{Z})$$

PROOF: TODO

7.6 Normal Subgroups

Definition 7.39 (Normal Subgroup)**.** A subgroup N of G is *normal* iff, for all $g \in G$ and $n \in N$, we have $gng^{-1} \in N$.

Example 7.40. Every subgroup of Q_8 is normal.

Proposition 7.41. *Let G be a group and N a subgroup of G. Then the following are equivalent.*

1. *N is normal.*
2. $\forall g \in G. gNg^{-1} \subseteq N$
3. $\forall g \in G. gNg^{-1} = N$
4. $\forall g \in G. gN \subseteq Ng$
5. $\forall g \in G. gN = Ng$

PROOF:
⟨1⟩1. $1 \Leftrightarrow 2$
PROOF: Immediate from definitions.
⟨1⟩2. $2 \Rightarrow 3$
PROOF: If 2 holds then we have $gNg^{-1} \subseteq N$ and $g^{-1}Ng \subseteq N$ hence $N = gNg^{-1}$.
⟨1⟩3. $3 \Rightarrow 2$
PROOF: Trivial.
⟨1⟩4. $2 \Leftrightarrow 4$
PROOF: Easy.
⟨1⟩5. $3 \Leftrightarrow 5$
PROOF: Easy.

$\square$

Proposition 7.42. *Let $\phi : G \to H$ be a group homomorphism. Then $\ker \phi$ is a normal subgroup of G.*

PROOF: Given $g \in G$ and $n \in \ker \phi$ we have

$$\begin{aligned}\phi(gng^{-1}) &= \phi(g)\phi(n)\phi(g)^{-1} \\ &= \phi(g)\phi(g)^{-1} \\ &= e\end{aligned}$$

and so $gng^{-1} \in \ker \phi$. $\square$

Proposition 7.43. *If H and K are normal subgroups of a group G then HK is normal in G.*

PROOF: For $g \in G$, $h \in H$ and $k \in K$ we have $ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$. $\square$

7.7 Quotient Groups

Definition 7.44. Let G be a group. Let $\sim$ be an equivalence relation on G. Then we say that $\sim$ is *compatible* with the group operation on G iff, for all $a, a', g \in G$, if $a \sim a'$ then $ga \sim ga'$ and $ag \sim a'g$.

Proposition 7.45. *Let G be a group. Let $\sim$ be an equivalence relation on G. Then there exists an operation $\cdot : (G/\sim)^2 \to G/sim$ such that*

$$\forall a, b \in G.[a][b] = [ab]$$

iff $\sim$ is compatible with the group operation on G. In this case, $G/\sim$ is a group under $\cdot$ and the canonical function $\pi : G \to G/\sim$ is a group homomorphism, and is universal with respect to group homomorphisms $\phi : G \to G'$ such that if $a \sim a'$ then $\phi(a) = \phi(a')$.

PROOF: Easy. $\square$

Definition 7.46 (Quotient Group)**.** Let G be a group. Let $\sim$ be an equivalence relation on G that is compatible with the group operation on G. Then $G/\sim$ is the *quotient group* of G by $\sim$ under $[a][b] = [ab]$.

Proposition 7.47. *Let G be a group and H a subgroup of G. Then H is normal if and only if there exists a group K and homomorphism $\phi : G \to K$ such that $H = \ker \phi$.*

PROOF: One direction is given by Proposition 7.42. For the other direction, take $K = G/H$ and ϕ to be the canonical map $G \to G/H$. $\square$

Definition 7.48 (Modular Group)**.** The *modular group* $\mathrm{PSL}_2(\mathbb{Z})$ is $\mathrm{SL}_2(\mathbb{Z})/\{I, -I\}$.

Proposition 7.49. $\mathrm{PSL}_2(\mathbb{Z})$ *is generated by* $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *and* $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$.

PROOF: By Example 6.29.

Proposition 7.50 (Roger Alperin)**.** $\mathrm{PSL}_2(\mathbb{Z})$ *is presented by* $(x, y | x^2, y^3)$.

PROOF:
$\langle 1\rangle 1$. LET: $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
$\langle 1\rangle 2$. LET: $y = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$
$\langle 1\rangle 3$. Define an action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathbb{R} - \mathbb{Q}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} r = \frac{ar+b}{cr+d} \enspace .$$

$\langle 2\rangle 1$. Given $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$ and r irrational we have $\frac{ar+b}{cr+d}$ is irrational.
$\langle 3\rangle 1$. ASSUME: for a contradiction $\frac{ar+b}{cr+d} = \frac{p}{q}$ where p and q are integers with $q > 0$.
$\langle 3\rangle 2$. $aqr + bq = cpr + dp$
$\langle 3\rangle 3$. $(aq - cp)r = dp - bq$
$\langle 3\rangle 4$. $aq = cp = dp - bq = 0$
$\langle 3\rangle 5$. $adq - cdp = 0$
$\langle 3\rangle 6$. $cdp - cbq = 0$
$\langle 3\rangle 7$. $(ad - cb)q = 0$
PROOF: Since $ad - cb = 1$.
$\langle 3\rangle 8$. $q = 0$
$\langle 3\rangle 9$. Q.E.D.
PROOF: This contradicts $\langle 3\rangle 1$.
$\langle 2\rangle 2$. $-Ir = r$
PROOF: Since $-Ir = \frac{-r}{-1} = r$.
$\langle 2\rangle 3$. Given $A, B \in \mathrm{PSL}_2(\mathbb{Z})$ we have $A(Br) = (AB)r$.
PROOF:

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} r \right] &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{er+f}{gr+h} \\ &= \frac{a\frac{er+f}{gr+h} + b}{c\frac{er+f}{gr+h} + d} \\ &= \frac{a(er+f) + b(gr+h)}{c(er+f) + d(gr+h)} \\ &= \frac{(ae+bg)r + (af+bh)}{(ce+dg)r + (cf+dh)} \\ &= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} r \\ &= \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] r \end{aligned}$$

$\langle 1\rangle 4$.

$$yr = 1 - \frac{1}{r}$$

$\langle 1 \rangle 5.$

$$y^{-1}r = \frac{1}{1-r}$$

PROOF: Since $y^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$

$\langle 1 \rangle 6.$

$$yxr = 1 + r$$

PROOF: Since $yx = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$.

$\langle 1 \rangle 7.$

$$y^{-1}xr = \frac{r}{1+r}$$

PROOF: Since $y^{-1}x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

$\langle 1 \rangle 8.$ If $r > -1$ is positive then yxr is positive.
$\langle 1 \rangle 9.$ If r is positive then $y^{-1}xr$ is positive.
$\langle 1 \rangle 10.$ If $r < -1$ then $y^{-1}xr$ is positive.
$\langle 1 \rangle 11.$ If r is negative then yr is positive.
$\langle 1 \rangle 12.$ If r is negative then $y^{-1}r$ is positive.
$\langle 1 \rangle 13.$ No product of the form

$$(y^{\pm 1}x)(y^{\pm 1}x) \cdots (y^{\pm 1}x)$$

with one or more factors can equal the identity.

PROOF: If the last factor is (yx), then the product maps numbers in $(-1, 0)$ to positive numbers. If the last factor is $(y^{-1}x)$, then the product maps numbers < -1 to positive numbers.

$\langle 1 \rangle 14.$ No product of the form

$$(y^{\pm 1}x)(y^{\pm 1}x) \cdots (y^{\pm 1}x)y^{\pm 1}$$

with one or more factors can equal the identity.

PROOF: The product maps negative numbers to positive numbers.

$\langle 1 \rangle 15.$ $\mathrm{PSL}_2(\mathbb{Z})$ is presented by $(x, y | x^2, y^3)$.

□

Corollary 7.50.1. $\mathrm{PSL}_2(\mathbb{Z})$ *is the coproduct of* C_2 *and* C_3 *in* **Grp**.

Theorem 7.51. *Every group homomorphism* $\phi : G \to H$ *may be decomposed as*

$$G \longrightarrow G/\ker\phi \xrightarrow{\cong} \mathrm{im}\,\phi \longrightarrow H$$

PROOF: Easy. □

Corollary 7.51.1 (First Isomorphism Theorem)**.** *Let* $\phi : G \to H$ *be a surjective group homomorphism. Then* $H \cong G/\ker\phi$.

Proposition 7.52. *Let* H_1 *be a normal subgroup of* G_1 *and* H_2 *a normal subgroup of* G_2*. Then* $H_1 \times H_2$ *is a normal subgroup of* $G_1 \times G_2$*, and*

$$\frac{G_1 \times G_2}{H_1 \times H_2} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2} \quad .$$

PROOF: $\pi \times \pi : G_1 \times G_2 \twoheadrightarrow G_1/H_1 \times G_2/H_2$ is a surjective homomorphism with kernel $H_1 \times H_2$. ∎

Example 7.53.

$$\mathbb{R}/\mathbb{Z} \cong S^1$$

PROOF: Map a real number r to $(\cos r, \sin r)$. The result is a surjective group homomorphism with kernel $\mathbb{Z}$. ∎

Proposition 7.54. *Let H be a normal subgroup of a group G. For every subgroup K of G that includes H, we have H is a normal subgroup of K, and K/H is a subgroup of G/H. The mapping*

$$u : \{\textit{subgroups of } G \textit{ including } H\} \to \{\textit{subgroups of } G/H\}$$

with $u(K) = K/H$ is a poset isomorphism.

PROOF:
⟨1⟩1. If K is a subgroup of G that includes H then H is normal in K.
⟨1⟩2. If K is a subgroup of G that includes H then K/H is a subgroup of G/H.
⟨1⟩3. If $H \subseteq K_1 \subseteq K_2$ then $K_1/H \subseteq K_2/H$.
⟨1⟩4. If $K_1/H = K_2/H$ then $K_1 = K_2$
⟨2⟩1. ASSUME: $K_1/H = K_2/H$
⟨2⟩2. $K_1 \subseteq K_2$
⟨3⟩1. LET: $k \in K_1$
⟨3⟩2. $kH \in K_2/H$
⟨3⟩3. PICK $k' \in K_2$ such that $kH = k'H$
⟨3⟩4. $kk'^{-1} \in H$
⟨3⟩5. $kk'^{-1} \in K_2$
⟨3⟩6. $k \in K_2$
⟨2⟩3. $K_2 \subseteq K_1$
PROOF: Similar.
⟨1⟩5. For any subgroup L of G/H, there exists a subgroup K of G that includes H such that $L = K/H$.
⟨2⟩1. LET: L be a subgroup of G/H.
⟨2⟩2. LET: $K = \{k \in G : kH \in L\}$
⟨2⟩3. K is a subgroup of G.
PROOF: Given $k, k' \in K$ we have $kH, k'H \in L$ hence $kk'^{-1}H \in L$ and so $kk'^{-1} \in K$.
⟨2⟩4. $H \subseteq K$
PROOF: For all $h \in H$ we have $hH = H \in L$.
⟨2⟩5. $L = K/H$
PROOF: By definition.
∎

Proposition 7.55 (Third Isomorphism Theorem)**.** *Let H be a normal subgroup of a group G. Let N be a subgroup of G that includes H. Then N/H is normal* *in G/H if and only if N is normal in G, in which case*

$$\frac{G/H}{N/H} \cong \frac{G}{N}$$

PROOF:
⟨1⟩1. If N/H is normal in G/H then N is normal in G.
⟨2⟩1. ASSUME: N/H is normal in G/H.
⟨2⟩2. LET: $g \in G$ and $n \in N$.
⟨2⟩3. $gng^{-1}H \in N/H$
⟨2⟩4. PICK $n' \in N$ such that $gng^{-1}H = n'H$
⟨2⟩5. $gng^{-1}n'^{-1} \in H$
⟨2⟩6. $gng^{-1}n'^{-1} \in N$
⟨2⟩7. $gng^{-1} \in N$
⟨1⟩2. If N is normal in G then N/H is normal in G/H and $(G/H)/(N/H) \cong G/N$.
⟨2⟩1. ASSUME: N is normal in G.
⟨2⟩2. LET: $\phi : G/H \to G/N$ be the homomorphism $\phi(gH) = gN$
⟨3⟩1. If $gH = g'H$ then $gN = g'N$
PROOF: If $gg'^{-1} \in H$ then $gg'^{-1} \in N$.
⟨3⟩2. $\phi((gH)(g'H)) = \phi(gH)\phi(g'H)$
PROOF: Both are $gg'N$.
⟨2⟩3. ϕ is surjective.
⟨2⟩4. $\ker \phi = N/H$
⟨2⟩5. $(G/H)/(N/H) \cong G/N$
PROOF: By the First Isomorphism Theorem.
□

Proposition 7.56 (Second Isomorphism Theorem)**.** *Let H and K be subgroups of a group G. Assume that H is normal in G. Then:*

1. *HK is a subgroup of G, and H is normal in HK.*
2. *$H \cap K$ is normal in K, and*

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

PROOF:
⟨1⟩1. HK is a subgroup of G.
PROOF: Since $hkh'k' = hh'(h'^{-1}kh')k' \in HK$.
⟨1⟩2. H is normal in HK.
⟨1⟩3. $H \cap K$ is normal in K and $HK/H \cong K/(H \cap K)$
PROOF: The function that maps k to kH is a surjective homomorphism $K \twoheadrightarrow HK/H$ with kernel $H \cap K$. Surjectivity follows because $hkH = hkh^{-1}H$.
□

See also Proposition 7.71 for a result that holds even if H is not normal.

7.8 Cosets

Proposition 7.57. *Let G be a group. Let $\sim$ be an equivalence relation on G such that, for all $a, b, g \in G$, if $a \sim b$ then $ga \sim gb$. Let $H = \{h \in G : h \sim e\}$. Then H is a subgroup of G and, for all $a, b \in G$, we have*

$$a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH \quad .$$

PROOF:
$\langle 1 \rangle 1.$ $e \in H$
$\langle 1 \rangle 2.$ For all $x, y \in H$ we have $xy^{-1} \in H$.
  $\langle 2 \rangle 1.$ ASSUME: $x \sim e$ and $y \sim e$.
  $\langle 2 \rangle 2.$ $e \sim y^{-1}$
    PROOF: Since $yy^{-1} \sim ey^{-1}$.
  $\langle 2 \rangle 3.$ $xy^{-1} \sim e$
    PROOF: Since $xy^{-1} \sim ey^{-1} \sim e$.
$\langle 1 \rangle 3.$ If $a \sim b$ then $a^{-1}b \in H$.
  PROOF: If $a \sim b$ then $a^{-1}b \sim a^{-1}a = e$.
$\langle 1 \rangle 4.$ If $a^{-1}b \in H$ then $aH = bH$.
  $\langle 2 \rangle 1.$ ASSUME: $a^{-1}b \in H$
  $\langle 2 \rangle 2.$ $bH \subseteq aH$
    PROOF: For any $h \in H$ we have $bh = aa^{-1}bh \in aH$.
  $\langle 2 \rangle 3.$ $aH \subseteq bH$
    PROOF: Similar since $b^{-1}a \in H$.
$\langle 1 \rangle 5.$ If $aH = bH$ then $a \sim b$.
  $\langle 2 \rangle 1.$ ASSUME: $aH = bH$
  $\langle 2 \rangle 2.$ PICK $h \in H$ such that $a = bh$.
  $\langle 2 \rangle 3.$ $b^{-1}a = h$
  $\langle 2 \rangle 4.$ $b^{-1}a \in H$
  $\langle 2 \rangle 5.$ $b^{-1}a \sim e$
  $\langle 2 \rangle 6.$ $a \sim b$
    PROOF: $a = bb^{-1}a \sim be = b$.
$\square$

Definition 7.58 (Coset)**.** Let G be a group and H a subgroup of G. A *left coset* of H is a set of the form aH for $a \in G$. A *right coset* of H is a set of the form Ha for some $a \in G$.

We write G/H for the set of all left cosets of H, and $G \backslash H$ for the set of all right cosets of H.

Proposition 7.59.

$$G/H \cong G \backslash H$$

PROOF: The function that maps aH to Ha^{-1} is a bijection. $\square$

Proposition 7.60. *Let G be a group and H a subgroup of G. Define $\sim_H$ on G by: $a \sim b$ iff $a^{-1}b \in H$. This defines a one-to-one correspondence between the subgroups of G and the equivalence relations $\sim$ on G such that, for all $a, b, g \in G$, if $a \sim b$, then $ga \sim gb$. The equivalence class of a is aH.*

PROOF:
⟨1⟩1. For any subgroup H, we have $\sim_H$ is an equivalence relation on G.
⟨2⟩1. $\sim$ is reflexive.
PROOF: For any $a \in G$ we have $a^{-1}a = e \in H$.
⟨2⟩2. $\sim$ is symmetric.
PROOF: If $a^{-1}b \in H$ then $b^{-1}a \in H$.
⟨2⟩3. $\sim$ is transitive.
PROOF: If $a^{-1}b \in H$ and $b^{-1}c \in H$ then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.
⟨1⟩2. If $a \sim_H b$ then $ga \sim_H gb$.
PROOF: If $a^{-1}b \in H$ then $(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b \in H$.
⟨1⟩3. For any equivalence relation $\sim$ on G such that, whenever $a \sim b$, then $ga \sim gb$, there exists a subgroup H such that $\sim = \sim_H$.
PROOF: Proposition 7.57.
⟨1⟩4. The $\sim_H$-equivalence class of a is aH.
PROOF:
$$\begin{aligned} a \sim b &\Leftrightarrow a^{-1}b \in H \\ &\Leftrightarrow \exists h \in H.a^{-1}b = h \\ &\Leftrightarrow \exists h \in H.b = aH \\ &\Leftrightarrow b \in aH \end{aligned}$$
□

Proposition 7.61. *Let G be a group and H a subgroup of G. Define $\sim_H$ on G by: $a \sim b$ iff $ab^{-1} \in H$. This defines a one-to-one correspondence between the subgroups of G and the equivalence relations $\sim$ on G such that, for all $a, b, g \in G$, if $a \sim b$, then $ag \sim bg$. The equivalence class of a is Ha.*

PROOF: Similar. □

Proposition 7.62. *Let G be a group and H be a subgroup of G. Define $\sim_L$ and $\sim_R$ on G by:*

$$a \sim_L b \Leftrightarrow a^{-1}b \in H, \qquad a \sim_R b \Leftrightarrow ab^{-1} \in H \ .$$

Then $\sim_L = \sim_R$ if and only if H is normal.

PROOF:
⟨1⟩1. If $\sim_L = \sim_R$ then H is normal.
⟨2⟩1. ASSUME: $\sim_L = \sim_R$
⟨2⟩2. LET: $h \in H$ and $g \in G$
⟨2⟩3. $g \sim_L gh^{-1}$
⟨2⟩4. $g \sim_R gh^{-1}h$
⟨2⟩5. $ghg^{-1} \in H$
⟨1⟩2. If H is normal then $\sim_L = \sim_R$.
⟨2⟩1. ASSUME: H is normal.
⟨2⟩2. If $a \sim_L b$ then $a \sim_R b$.
⟨3⟩1. ASSUME: $a \sim_L b$
⟨3⟩2. $a^{-1}b \in H$

⟨3⟩3. $aa^{-1}ba^{-1} \in H$
⟨3⟩4. $ba^{-1} \in H$
⟨3⟩5. $a \sim_R b$
⟨2⟩3. If $a \sim_R b$ then $a \sim_L b$.
PROOF: Similar.
□

Corollary 7.62.1. *Let G be a group and H be a normal subgroup of G. Define $\sim$ on G by $a \sim b$ iff $a^{-1}b \in H$. Then $G/\sim$ is a group under $[a][b] = [ab]$.*

Definition 7.63 (Quotient Group)**.** Let G be a group and H be a normal subgroup of G. The *quotient group* G/H is $G/\sim$ where $a \sim b$ iff $a^{-1}b \in H$, under $[a][b] = [ab]$ or $(aH)(bH) = abH$.

Corollary 7.63.1. *Let H be a normal subgroup of a group G. For every group homomorphism $\phi : G \to G'$ such that $H \subseteq \ker \phi$, there exists a unique group homomorphism $\overline{\phi} : G/H \to G'$ such that the following diagram commutes.*

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, "\pi"'] & & G' \\ & G/H \arrow[ur, "\overline{\phi}"'] & \end{tikzcd}$$

Proposition 7.64. *$\mathbb{Z}/n\mathbb{Z}$ has exactly n elements.*

PROOF: Every integer is congruent to one of $0, 1, \ldots, n-1$ by the division algorithm, and no two of them are conguent to one another, since if $0 \leq i < j < n$ then $0 < j - i < n$. □

Proposition 7.65. *Let m and n be integers with $n > 0$. The order of m in $\mathbb{Z}/n\mathbb{Z}$ is $\frac{n}{\gcd(m,n)}$.*

PROOF: By Proposition 6.19 since the order of 1 is n. □

Proposition 7.66. *The integer m generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m, n) = 1$.*

PROOF: By Proposition 7.65. □

Corollary 7.66.1. *If p is prime then every non-zero element in $\mathbb{Z}/p\mathbb{Z}$ is a generator.*

Proposition 7.67.

$$\mathrm{Aut}_{\mathbf{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$$

PROOF: Every permutation of $\{(1,0), (0,1), (1,1)\}$ gives an automorphism of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Example 7.68. Not all monomorphisms split in **Grp**.
Define $\phi : \mathbb{Z}/3\mathbb{Z} \to S_3$ by

$$\phi(0) = \mathrm{id}_3, \qquad \phi(1) = (1\ 3\ 2), \qquad \phi(2) = (1\ 2\ 3)\ .$$

Then ϕ is monic but has no retraction.

For if $r : S_3 \to \mathbb{Z}/3\mathbb{Z}$ is a retraction, then we would have

$$r(1\ 2) + r(2\ 3) = 1, \qquad r(2\ 3) + r(1\ 2) = 2$$

which is impossible.

Proposition 7.69. *Let G be a group, H a subgroup of G, and $g \in G$. The function that maps h to gh is a bijection $H \cong gH$.*

PROOF: By Cancellation. □

Proposition 7.70. *Let G be a group, H a subgroup of G, and $g \in G$. The function that maps h to hg is a bijection $H \cong Hg$.*

PROOF: By Cancellation. □

Proposition 7.71. *Let H and K be finite subgroups of a group G. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|} \ .$$

PROOF:

$\langle 1 \rangle 1$. LET: $f : \{hK : h \in H\} \to H/(H \cap K)$ be the function $f(hK) = h(H \cap K)$

PROOF: This is well-defined because if $hK = h'K$ then $h^{-1}h' \in H \cap K$ so $h(H \cap K) = h'(H \cap K)$.

$\langle 1 \rangle 2$. f is injective.

PROOF: If $h(H \cap K) = h'(H \cap K)$ then $hK = h'K$.

$\langle 1 \rangle 3$. f is surjective.

PROOF: Clear.

$\langle 1 \rangle 4$.

$$\frac{|HK|}{|K|} = \frac{|H|}{|H \cap K|}$$

□

7.9 Congruence

Definition 7.72 (Congruence)**.** Given integers a, b, n with n positive, we say a is *congruent* to b *modulo* n, and write $a \equiv b (\operatorname{mod} n)$, iff $a + n\mathbb{Z} = b + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$.

Proposition 7.73. *Given integers a, b, n with n positive, we have $a \equiv b (\operatorname{mod} n)$ iff $n \mid a - b$.*

PROOF: By Proposition 7.57. □

Proposition 7.74. *If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$ then $a + b \equiv a' + b' \bmod n$.*

PROOF: If $n \mid a' - a$ and $n \mid b' - b$ then $n \mid (a' + b') - (a + b)$. □

Proposition 7.75. *If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$ then $ab \equiv a'b' \bmod n$.*

PROOF: If $n \mid a' - a$ and $n \mid b' - b$ then $n \mid a'b' - ab = a'(b' - b) + (a' - a)b$. □

7.10 Cyclic Groups

Definition 7.76 (Cyclic Group)**.** The *cyclic* groups are $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ for positive integers n.

Proposition 7.77. *If m and n are positive integers with $\gcd(m, n) = 1$ then $C_{mn} \cong C_m \times C_n$.*

PROOF: The function that maps x to $(x \bmod m, x \bmod n)$ is an isomorphism. □

Proposition 7.78. *Let G be a group and $g \in G$. Then $\langle g \rangle$ is cyclic.*

PROOF: If g has finite order then $\langle g \rangle \cong C_{|g|}$, otherwise $\langle g \rangle \cong \mathbb{Z}$. □

Proposition 7.79. *Every finitely generated subgroup of $\mathbb{Q}$ is cyclic.*

PROOF:
$\langle 1 \rangle 1$. LET: $G = \langle a_1/b, \ldots, a_n/b \rangle$ where $a_1, \ldots, a_n, b$ are integers with $b > 0$
$\langle 1 \rangle 2$. LET: $a = \gcd(a_1, \ldots, a_n)$
$\langle 1 \rangle 3$. $G = \langle a/b \rangle$
□

Corollary 7.79.1. *$\mathbb{Q}$ is not finitely generated.*

7.11 Commutator Subgroup

Definition 7.80 (Commutator)**.** Let G be a group and $g, h \in G$. The *commutator* of g and h is

$$[g, h] = ghg^{-1}h^{-1} \quad .$$

Definition 7.81 (Commutator Subgroup)**.** Let G be a group. The *commutator subgroup*, denoted $[G, G]$ or G', is the subgroup generated by the elements of the form $aba^{-1}b^{-1}$.

We write $G^{(i)}$ for the result of taking the commutator subgroup i times starting with G.

Lemma 7.82. *Let $\phi : G_1 \to G_2$ be a group homomorphism. Then, for all $g, h \in G_1$, we have*

$$\phi([g, h]) = [\phi(g), \phi(h)]$$

and so $\phi(G_1') \subseteq G_2'$.

PROOF: Easy. □

7.12 Presentations

Definition 7.83 (Presentation)**.** A *presentation* of a group G is a pair (A, R) where A is a set and $R \subseteq F(A)$ is a set of words such that

$$G \cong F(A)/N(R)$$

where $N(R)$ is the smallest normal subgroup of $F(A)$ that includes R.

Example 7.84.

- The free group on a set A is presented by $(A, \emptyset)$.
- S_3 is presented by $(x, y|x^2, y^3, xyxy)$.
- $(a, b \mid a^2, b^2, (ab)^n)$ is a presentation of D_{2n}.
- $(x, y \mid x^2y^{-2}, y^4, xyx^{-1}y)$ is a presentation of Q_8.

Proposition 7.85 (Word Problem)**.** *Let (A, R) be a presentation of the group G. Let $w_1, w_2 \in F(A)$ be two words. Then it is undecidable in general if $w_1N(R) = w_2N(R)$ in G.*

Definition 7.86 (Finitely Presented)**.** A group is *finitely presented* iff it has a presentation (A, R) where both A and R are finite.

Proposition 7.87. *Let $(A|R)$ be a presentation of G and $(A'|R')$ a presentation of H. Assume w.l.o.g. A and A' are disjoint. Then the group $G * G'$ presented by $(A \cup A'|R \cup R')$ is the coproduct of G and G' in* **Grp**.

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & A \cup A' \arrow[d] & A' \arrow[l] \arrow[d] \\
F(A) \arrow[r] \arrow[d] & F(A \cup A') \arrow[d] & F(A') \arrow[l] \arrow[d] \\
G \arrow[r, "\kappa_1"] & G * G' & G' \arrow[l, "\kappa_2"']
\end{tikzcd}$$

Proof:
⟨1⟩1. Let: $\kappa_1 : G \to G*G'$ and $\kappa_2 : G' \to G*G'$ be the unique homomorphisms that make the diagram above commute.
⟨1⟩2. Let: $\phi : G \to H$ and $\psi : G' \to H$ be any homomorphisms.
⟨1⟩3. Let: $[\phi, \psi] : F(A \cup A') \to H$ be the unique homomorphism such that ...
⟨1⟩4. $R \cup R' \subseteq \ker[\phi, \psi]$
⟨1⟩5. $[\phi, \psi]$ factors uniquely through the morphism $F(A \cup A') \to G * G'$
□

7.13 Index of a Subgroup

Definition 7.88 (Index)**.** Let G be a group and H a subgroup of G. The *index* of H in G, denoted $|G : H|$, is the number of left cosets of H in G if this is finite, otherwise ∞.

Theorem 7.89 (Lagrange's Theorem)**.** *Let G be a finite group and H a subgroup of G. Then*

$$|G| = |G : H||H| \ .$$

Proof: G/H is a partition of G into $|G : H|$ subsets, each of size $|H|$. □

Corollary 7.89.1. *For p a prime number, the only group of order p is C_p.*

PROOF: Let G be a group of order p and $g \in G$ with $g \neq e$. Then $|\langle g \rangle|$ divides p and is not 1, hence is p, that is, $G = \langle g \rangle$. □

Theorem 7.90 (Cauchy's Theorem)**.** *Let G be a finite group. If p is prime and $p \mid |G|$ then the number of cyclic subgroups of order p is congruent to 1 modulo p. In particular, there exists an element of order p.*

PROOF:
$\langle 1 \rangle 1$. LET: $S = \{(a_1, a_2, \ldots, a_p) \in G^p : a_1 a_2 \cdots a_p = e\}$
$\langle 1 \rangle 2$. $|S| = |G|^{p-1}$
PROOF: Given any $a_1, \ldots, a_{p-1} \in G$, there exists a unique a_p such that $(a_1, \ldots, a_p) \in S$, namely $a_p = (a_1 \cdots a_{p-1})^{-1}$.
$\langle 1 \rangle 3$. $p \mid |S|$
$\langle 1 \rangle 4$. Define an action of $\mathbb{Z}/p\mathbb{Z}$ on S by

$$m \cdot (a_1, \ldots, a_p) = (a_m, a_{m+1}, \ldots, a_p, a_1, a_2, \ldots, a_{m-1}) \ .$$

PROOF: If $(a_1, \ldots, a_p) \in S$ then $(a_2, a_3, \ldots, a_p, a_1) \in S$ since $a_1 = (a_2 \cdots a_p)^{-1}$.
$\langle 1 \rangle 5$. LET: Z be the set of fixed points of this action.
$\langle 1 \rangle 6$. $|Z| \equiv 0 (\bmod p)$
PROOF: Corollary 9.18.1, $\langle 1 \rangle 3$.
$\langle 1 \rangle 7$. $Z = \{(a, a, \ldots, a) : a^p = e\}$
$\langle 1 \rangle 8$. $Z \neq \emptyset$
PROOF: Since $(e, e, \ldots, e) \in Z$.
$\langle 1 \rangle 9$. An element a has order p iff $(a, a, \ldots, a) \in Z$ and $a \neq e$.
$\langle 1 \rangle 10$. LET: N be the number of cyclic subgroups of order p.
$\langle 1 \rangle 11$. The number of elements of order p is $N(p-1)$
$\langle 1 \rangle 12$. $|Z| = N(p-1) + 1$
$\langle 1 \rangle 13$. $-N + 1 \equiv 0 (\bmod p)$
PROOF: From $\langle 1 \rangle 6$.
$\langle 1 \rangle 14$. $N \equiv 1 (\bmod p)$
□

Proposition 7.91. *Let G be a group. Let K be a subgroup of G and H a subgroup of K. If $|G : H|$, $|G : K|$ and $|K : H|$ are all finite then*

$$|G : H| = |G : K||K : H| \ .$$

PROOF:
$\langle 1 \rangle 1$. LET: $G/K = \{g_1 K, g_2 K, \ldots, g_m K\}$
$\langle 1 \rangle 2$. LET: $K/H = \{k_1 H, k_2 H, \ldots, k_n H\}$
$\langle 1 \rangle 3$. $G/H = \{g_i k_j H : 1 \leq i \leq m, 1 \leq j \leq n\}$
$\langle 2 \rangle 1$. LET: $g \in G$
$\langle 2 \rangle 2$. PICK i such that $gK = g_i K$
$\langle 2 \rangle 3$. $g^{-1} g_i \in K$
$\langle 2 \rangle 4$. PICK j such that $g^{-1} g_i H = k_j H$
$\langle 2 \rangle 5$. $g^{-1} g_i k_j \in H$
$\langle 2 \rangle 6$. $gH = g_i k_j H$
$\langle 1 \rangle 4$. If $g_i k_j H = g_{i'} k_{j'} H$ then $i = i'$ and $j = j'$.

$\langle 2 \rangle 1$. ASSUME: $g_i k_j H = g_{i'} k_{j'} H$
$\langle 2 \rangle 2$. $g_i K = g_{i'} K$
$\langle 2 \rangle 3$. $i = i'$
$\langle 2 \rangle 4$. $k_j H = k_{j'} H$
$\langle 2 \rangle 5$. $j = j'$
□

7.14 Cokernels

Proposition 7.92. *Let $\phi : G \to H$ be a homomorphism between groups. Then there exists a group K and homomorphism $\pi : H \to K$ that is initial with respect to all homomorphism $\alpha : H \to L$ such that $\alpha \circ \phi = 0$.*

PROOF:
$\langle 1 \rangle 1$. LET: N be the intersection of all the normal subgroups of H that include $\operatorname{im} \phi$.
$\langle 1 \rangle 2$. LET: $K = H/N$ and π be the canonical homomorphism.
$\langle 1 \rangle 3$. LET: $\pi \circ \phi = 0$
$\langle 1 \rangle 4$. LET: $\alpha : H \to L$ satisfy $\alpha \circ \phi = 0$
$\langle 1 \rangle 5$. $\operatorname{im} \phi \subseteq \ker \alpha$
$\langle 1 \rangle 6$. $N \subseteq \ker \alpha$
$\langle 1 \rangle 7$. There exists a unique $\overline{\alpha} : H/\operatorname{im} \phi \to L$ such that $\overline{\alpha} \circ \pi = \alpha$
□

Definition 7.93 (Cokernel)**.** For any homomorphism $\phi : G \to H$ in **Grp**, the *cokernel* of ϕ is the group $\operatorname{coker} \phi$ and homomorphism $\pi : H \to \operatorname{coker} \phi$ that is initial among homomorphisms $\alpha : H \to L$ such that $\alpha \circ \phi = 0$.

Example 7.94. It is not true that a homomorphism with trivial cokernel is epi. The inclusion $\langle (1\ 2) \rangle \hookrightarrow S_3$ has trivial cokernel but is not epi.

7.15 Cayley Graphs

Definition 7.95 (Cayley Graph)**.** Let G be a finitely generated group. Let A be a finite set of generators for G. The *Cayley graph* of G with respect to A is the directed graph whose vertices are the elements of G, with an edge $g_1 \to g_2$ labelled by $a \in A$ iff $g_2 = g_1 a$.

Proposition 7.96. *G is the free group on A iff the Cayley graph with respect to A is a tree.*

PROOF: Both are equivalent to saying that the product of two different strings of elements of A and/or their inverses are not equal. □

7.16 Characteristic Subgroups

Definition 7.97 (Characteristic Subgroup)**.** Let G be a group. Let H be a subgroup of G. Then H is a *characteristic* subgroup of G iff, for every automorphism ϕ of G, we have $\phi(H) \subseteq H$.

Proposition 7.98. *Characteristic subgroups are normal.*

PROOF: Take ϕ to be conjugation with respect to an arbitrary element. □

Proposition 7.99. *Let G be a group. Let K be a normal subgroup of G and H a characteristic subgroup of K. Then H is normal in G.*

PROOF: For any $a \in G$ we have conjugation by a is an automorphism on K, hence H is closed under it. □

Proposition 7.100. *Let G be a group. Let H be a subgroup of G. Suppose there is no other subgroup of G isomorphic to H. Then H is characteristic, hence normal.*

PROOF: For any automorphism ϕ on G, we have $\phi(H)$ is isomorphic to H, hence $\phi(H) = H$. □

Proposition 7.101. *Let G be a finite group. Let K be a normal subgroup of G. Assume $|K|$ and $|G/K|$ are relatively prime. Then K is characteristic.*

PROOF:
$\langle 1 \rangle$1. LET: K' be a subgroup of G isomorphic to K.
PROVE: $K' = K$
$\langle 1 \rangle$2. $|K'/(K \cap K')|$ divides both $|K'| = |K|$ and $|G/K|$
$\langle 1 \rangle$3. $|K'/(K \cap K')| = 1$
$\langle 1 \rangle$4. $K' = K \cap K'$
$\langle 1 \rangle$5. $K' = K$
□

Proposition 7.102. *The commutator subgroup of a group is characteristic.*

PROOF: Lemma 7.82. □

7.17 Simple Groups

Definition 7.103 (Simple Group)**.** A group G is *simple* iff its only normal subgroups are $\{e\}$ and G.

Proposition 7.104. *Let G be a group. Then G is simple if and only if the only homomorphic images of G are* 1 *and G.*

PROOF: Both are equivalent to saying that, for any surjective homomorphism $\phi : G \to G'$, either ϕ has kernel $\{e\}$ (in which case it is an isomorphism) or ϕ has kernel G (in which case $G' = 1$.) □

7.18 Sylow Subgroups

Definition 7.105 (Sylow Subgroup)**.** Let p be a prime number. Let G be a finite group. A *p-Sylow subgroup* of G is a subgroup of order p^r, where r is the largest integer such that p^r divides $|G|$.

Proposition 7.106. *Let p be prime. Let G be a finite group. Let P be a p-Sylow subgroup of G. If P is normal then P is characteristic.*

Proof: Proposition 7.101. □

Corollary 7.106.1. *Let p be prime. Let G be a finite group. Let P be a p-Sylow subgroup of G. Let H be a subgroup of G that includes P. If P is normal in H and H is normal in G then P is normal in G.*

7.19 Series of Subgroups

Definition 7.107 (Series of Subgroups)**.** Let G be a group. A *series* of subgroups of G is a sequence (G_n) of subgroups of G such that

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots$$

It is a *normal* series iff G_{n+1} is normal in G_n for all n.

Proposition 7.108. *The maximal length of a normal series in G is 0 iff G is trivial.*

Proof: Since 1 is normal in G for every G. □

Proposition 7.109. *The maximal length of a normal series in G is 1 iff G is non-trivial and simple.*

Proof: Immediate from definitions. □

Example 7.110. $\mathbb{Z}$ has normal series of arbitrary length.

Proof: We have $\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq \cdots$. □

Example 7.111. The maximal length of a normal series in $\mathbb{Z}/n\mathbb{Z}$ is the number of primes in the prime factorization of n.

Proof: Let $n = p_1 p_2 \cdots p_k$. A normal series of maximal length is
$$\mathbb{Z}/p_1p_2\cdots p_k\mathbb{Z} \supsetneq \mathbb{Z}/p_1p_2\cdots p_{k-1}\mathbb{Z} \supsetneq \cdots \supsetneq \mathbb{Z}/p_1\mathbb{Z} \supsetneq \{e\}$$.□

Definition 7.112 (Equivalent Normal Series)**.** Let

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = \{e\}$$
$$G = G'_0 \supsetneq G'_1 \supsetneq G'_2 \supsetneq \cdots \supsetneq G'_m = \{e\}$$

be two normal series in a group G. Then the two series are *equivalent* iff $m = n$ and there exists a permutation $\sigma \in S_n$ such that, for all i, we have $G_i/G_{i+1} \cong G'_{\sigma(i)}/G'_{\sigma(i)+1}$.

Definition 7.113 (Composition Series)**.** Let G be a group. A *composition series* for G is a series of subgroups in G

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = \{e\}$$

such that, for all i, we have G_i / G_{i+1} is simple.

Proposition 7.114. *A normal series of maximal length in a group is a composition series.*

Proof: Easy. $\square$

Corollary 7.114.1. *Every finite group has a composition series.*

Corollary 7.114.2. *If a group has a composition series then every normal subgroup has a composition series.*

Definition 7.115 (Refinement)**.** A series of subgroups S_1 is a *refinement* of the series S_2 iff every subgroup in S_2 appears in S_1.

Lemma 7.116. *Let G be a group. Let Q, N and L be subgroups of G. Assume L is a normal subgroup of Q and $qN = Nq$ for all $q \in Q$. Then*

$$\frac{QN}{LN} \cong \frac{Q}{L(Q \cap N)} \quad .$$

Proof:
⟨1⟩1. QN is a subgroup of G.
  Proof: Since $QN = NQ$.
⟨1⟩2. LN is a subgroup of G.
  Proof: Since $LN = NL$.
⟨1⟩3. LN is normal in QN.
  ⟨2⟩1. Let: $l \in L$, $q \in Q$, and $n, n' \in N$.
    Prove: $qnln'n^{-1}q^{-1} \in LN$
  ⟨2⟩2. Pick $n_1 \in N$ such that $nl = ln_1$
  ⟨2⟩3. Pick $n_2 \in N$ such that $n_1 n' n^{-1} q^{-1} = q^{-1} n_2$
  ⟨2⟩4. $qnln'n^{-1}q^{-1} = qlq^{-1}n_2 \in LN$
    Proof: Since L is normal in Q.
⟨1⟩4. The function $f : Q \to QN/LN$ that maps q to qLN is a surjective homomorphism.
⟨1⟩5. $\ker f = L(Q \cap N)$
  ⟨2⟩1. $\ker f \subseteq L(Q \cap N)$
    ⟨3⟩1. Let: $x \in \ker f$
    ⟨3⟩2. $x \in LN$
    ⟨3⟩3. Pick $l \in L$ and $n \in N$ such that $x = ln$
    ⟨3⟩4. $n = l^{-1}x \in Q \cap N$
    ⟨3⟩5. $x \in L(Q \cap N)$
  ⟨2⟩2. $L(Q \cap N) \subseteq \ker f$
    Proof: Since $L(Q \cap N) \subseteq Q$ and $L(Q \cap N) \subseteq LN$.

⟨1⟩6. Q.E.D.
 PROOF: First Isomorphism Theorem.
□

Theorem 7.117 (Schreier)**.** *Any two normal series in a group have equivalent refinements.*

PROOF:
⟨1⟩1. LET: G be a group.
⟨1⟩2. LET: $S_1 : G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_m = \{e\}$ and $S_2 : G = H_0 \supsetneq H_1 \supsetneq H_2 \supsetneq \cdots \supsetneq H_n = \{e\}$ be two normal series in G.
⟨1⟩3. For each i, we have
$$G_i = G_i \cap H_0 \supseteq G_i \cap H_1 \supseteq \cdots \supseteq G_i \cap H_n = \{e\}$$
is a series of subgroups in G_i.
⟨1⟩4. For each i, we have
$$G_i = (G_i \cap H_0)G_{i+1} \supseteq (G_i \cap H_1)G_{i+1} \supseteq \cdots \supseteq (G_i \cap H_n)G_{i+1} = G_{i+1}$$
is a normal series in G_i.
 ⟨2⟩1. LET: $0 \leq i < m$ and $0 \leq j < n$
  PROVE: $(G_i \cap H_{j+1})G_{i+1}$ is normal in $(G_i \cap H_j)G_{i+1}$
 ⟨2⟩2. LET: $x \in G_i \cap H_{j+1}$, $y \in G_{i+1}$, $a \in G_i \cap H_j$ and $b \in G_{i+1}$
  PROVE: $abxyb^{-1}a^{-1} \in (G_i \cap H_{j+1})G_{i+1}$
 ⟨2⟩3. $axa^{-1} \in G_i \cap H_{j+1}$
  PROOF: Since $a, x \in G_i$ and H_{j+1} is normal in H_j.
 ⟨2⟩4. $ax^{-1}bxa^{-1} \in G_{i+1}$
  PROOF: Since G_{i+1} is normal in G_i.
 ⟨2⟩5. $yb^{-1} \in G_{i+1}$
 ⟨2⟩6. $ayb^{-1}a^{-1} \in G_{i+1}$
  PROOF: Since G_{i+1} is normal in G_i.
 ⟨2⟩7. $abxyb^{-1}a^{-1} = (axa^{-1})(ax^{-1}bxa^{-1}ayb^{-1}a^{-1}) \in (G_i \cap H_{j+1})G_{i+1}$
⟨1⟩5. Let S be the series obtained by concatenating the series ⟨1⟩4 for G_0 to G_1, G_1 to G_2, …, G_{m-1} to G_m
⟨1⟩6. S is a refinement of S_1.
⟨1⟩7. S is normal.
⟨1⟩8. LET: T be the similarly constructed normal refinement of S_2.
⟨1⟩9. For all i, j we have
$$\frac{(G_i \cap H_j)G_{i+1}}{(G_i \cap H_{j+1})G_{i+1}} \cong \frac{G_i \cap H_j}{(G_i \cap H_{j+1})(G_{i+1} \cap H_j)}$$
 ⟨2⟩1. $G_i \cap H_{j+1}$ is normal in $G_i \cap H_j$
 ⟨2⟩2. For all $q \in G_i \cap H_j$ we have $qG_{i+1} = G_{i+1}q$
  PROOF: Since for all $q \in G_i$ we have $qG_{i+1} = G_{i+1}q$.
 ⟨2⟩3. Q.E.D.
  PROOF: Lemma 7.116
⟨1⟩10. For all i, j we have
$$\frac{(G_i \cap H_j)H_{j+1}}{(G_{i+1} \cap H_j)H_{j+1}} \cong \frac{G_i \cap H_j}{(G_{i+1} \cap H_j)(G_i \cap H_{j+1})}$$
 PROOF: Lemma 7.116

⟨1⟩11. For all i, j we have
$$\frac{(G_i \cap H_j)G_{i+1}}{(G_i \cap H_{j+1})G_{i+1}} \cong \frac{(G_i \cap H_j)H_{j+1}}{(G_{i+1} \cap H_j)H_{j+1}}$$
⟨1⟩12. S and T are equivalent.
□

Corollary 7.117.1 (Jordan-Hölder)**.** *Any two composition series for a group are equivalent.*

Definition 7.118 (Composition Factors)**.** Let G be a group that has a composition series. The multiset of *composition factors* of G is the multiset of quotients of any composition series.

Example 7.119. Non-isomorphic groups can have the same composition factors. For example, $C_2 \times C_2$ and C_4 both have composition factors $\{|C_2, C_2|\}$.

Proposition 7.120. *Let G be a group. Let N be a normal subgroup of G. Then G has a composition series if and only if N and G/N both have composition series, in which case the composition factors of G are the union of the composition factors of N and the composition factors of G/N.*

Proof:
⟨1⟩1. If G has a composition series then N and G/N have composition series.
⟨2⟩1. Let: $G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = \{e\}$ be a composition series for G.
⟨2⟩2. N has a composition series.
⟨3⟩1. For all i, we have $\frac{G_i \cap N}{G_{i+1} \cap N}$ is either trivial or isomorphic to G_i/G_{i+1}.
⟨4⟩1. The homomorphism $G_i \cap N \hookrightarrow G_i \twoheadrightarrow G_i/G_{i+1}$ has kernel $G_{i+1} \cap N$.
⟨4⟩2. There is an injective homomorphism $(G_i \cap N)/(G_{i+1} \cap N) \to G_i/G_{i+1}$.
Proof: First Isomorphism Theorem.
⟨4⟩3. $(G_i \cap N)/(G_{i+1} \cap N)$ is either trivial or isomorphic to G_i/G_{i+1}.
Proof: Since G_i/G_{i+1} is simple.
⟨3⟩2. Eliminating all duplicates from the series $N = G_0 \cap N \supseteq G_1 \cap N \supseteq G_2 \cap N \supseteq \cdots \supseteq G_n \cap N = \{e\}$ gives a composition series for N.
⟨2⟩3. G/N has a composition series.
⟨3⟩1. For all i we have $\frac{(G_i N)/N}{(G_{i+1} N)/N}$ is either trivial or isomorphic to G_i/G_{i+1}.
⟨4⟩1. Let: $0 \leq i < n$
⟨4⟩2. $\frac{(G_i N)/N}{(G_{i+1} N)N} \cong G_i N / G_{i+1} N$
Proof: Third Isomorphism Theorem.
⟨4⟩3. There exists a surjective homomorphism
$$\frac{G_i}{G_{i+1}} \twoheadrightarrow \frac{G_i N}{G_{i+1} N} .$$
⟨5⟩1. Let: f be the homomorphism $G_i \hookrightarrow G_i N \twoheadrightarrow G_i N / G_{i+1} N$
⟨5⟩2. f is surjective.
⟨5⟩3. $f(G_{i+1}) = \{e\}$
⟨5⟩4. Q.E.D.
Proof: By the universal property of quotient groups.

⟨4⟩4. $G_iN/G_{i+1}N$ is either trivial or isomorphic to G_i/G_{i+1}.
PROOF: Proposition 7.104.
⟨3⟩2. Eliminating all duplicates from the series $G/N = G_0N/N \supseteq G_1N/N \supseteq G_2N/N \supseteq \cdots \supseteq G_nN/N = \{e\}$ gives a composition series for G/N.
⟨1⟩2. If N and G/N have composition series, then G has a composition series, and the composition factors of G are the union of the composition factors of N and the composition factors of G/N.
⟨2⟩1. LET: $N = N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_n = \{e\}$ be a composition series for N.
⟨2⟩2. LET: $G/N = H_0 \supsetneq H_1 \supsetneq H_2 \supsetneq \cdots \supsetneq H_m = \{e\}$ be a composition series for G/N.
⟨2⟩3. $G = \pi^{-1}(H_0) \supsetneq \pi^{-1}(H_1) \supsetneq \cdots \pi^{-1}(H_m) = N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_n$ is a composition series for G.
□

Proposition 7.121. *Let G_1 and G_2 be groups. Then $G_1 \times G_2$ has a composition series if and only if G_1 and G_2 both have composition series.*

PROOF:
⟨1⟩1. If $G_1 \times G_2$ has a composition series then G_1 has a composition series.
⟨2⟩1. LET: $G_1 \times G_2 = A_0 \supsetneq A_1 \supsetneq \cdots \supsetneq A_n = \{e\}$ be a composition series.
⟨2⟩2. For each i, we have $\pi_1(A_i)/\pi_1(A_{i+1})$ is either isomorphic to A_i/A_{i+1} or trivial.
⟨2⟩3. Eliminating duplicates from $G_1 = \pi_1(A_0) \supseteq \pi_1(A_1) \supseteq \cdots \supseteq \pi_1(A_n) = \{e\}$ gives a composition series for G_1.
⟨1⟩2. If $G_1 \times G_2$ has a composotion series then G_2 has a composition series.
PROOF: Similar.
⟨1⟩3. If G_1 and G_2 have composition series then $G_1 \times G_2$ has a composition series.
⟨2⟩1. LET: $G_1 = H_0 \supsetneq H_1 \supsetneq \cdots \supsetneq H_m = \{e\}$ be a composition series for G_1.
⟨2⟩2. LET: $G_2 = K_0 \supsetneq K_1 \supsetneq \cdots \supsetneq K_n = \{e\}$ be a composition series for G_2.
⟨2⟩3. $G_1 \times G_2 = H_0 \times K_0 \supsetneq H_1 \times K_0 \supsetneq \cdots \supsetneq H_m \times K_0 \supsetneq H_m \times K_1 \supsetneq \cdots \supsetneq H_m \times K_n = \{e\}$ is a composition series for $G_1 \times G_2$.
□

Definition 7.122 (Cyclic Series)**.** A normal series of subgroups is *cyclic* iff every quotient is cyclic.

Chapter 8

Abelian Groups

Definition 8.1 (Abelian Group)**.** A group is *Abelian* iff any two elements commute.

In an Abelian group G, we often denote the group operation by $+$, the identity element by 0 and the inverse of an element g by $-g$. We write ng for g^n ($g \in G$, $n \in \mathbb{Z}$).

Example 8.2. Every group of order ≤ 4 is Abelian.

Example 8.3. For any positive integer n, we have $\mathbb{Z}/n\mathbb{Z}$ is an Abelian group under addition.

Example 8.4. S_n is not Abelian for $n \geq 3$. If $x = \begin{pmatrix} 1 & 2 \end{pmatrix}$ and $y = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$ then $xy = \begin{pmatrix} 2 & 3 \end{pmatrix}$ and $yx = \begin{pmatrix} 1 & 3 \end{pmatrix}$.

Example 8.5. There are 42 Abelian groups of order 1024 up to isomorphism.

Proposition 8.6. *Let G be a group. If $g^2 = e$ for all $g \in G$ then G is Abelian.*

Proof: For any $g, h \in G$ we have

$$\begin{aligned} ghgh &= e \\ \therefore hgh &= g \qquad \text{(multiplying on the left by } g\text{)} \\ \therefore hg &= gh \qquad \text{(multiplying on the right by } h\text{)} \square \end{aligned}$$

Proposition 8.7. *Let G be a group. Then G is Abelian if and only if the function that maps g to g^{-1} is a group homomorphism.*

Proof:

⟨1⟩1. If G is Abelian then the function that maps g to g^{-1} is a group homomorphism.

Proof: Since $(gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1}$.

⟨1⟩2. If the function that maps g to g^{-1} is a group homomorphism then G is Abelian.

PROOF: Since $gh = (g^{-1})^{-1}(h^{-1})^{-1} = (g^{-1}h^{-1})^{-1} = hg$.
□

Proposition 8.8. *Let G be a group. Then G is Abelian if and only if the function that maps g to g^2 is a group homomorphism.*

PROOF:
⟨1⟩1. If G is Abelian then the function that maps g to g^2 is a group homomorphism.
PROOF: Since $(gh)^2 = g^2h^2$.
⟨1⟩2. If the function that maps g to g^2 is a group homomorphism then G is Abelian.
PROOF: Since we have $(gh)^2 = ghgh = g^2h^2$ and so $hg = gh$.
□

Proposition 8.9. *Let G be a group. Then G is Abelian if and only if the homomorphism $\gamma : G \to \mathrm{Aut}_{\mathbf{Grp}}(G)$ is the trivial homomorphism.*

PROOF:
⟨1⟩1. If G is Abelian then γ is trivial.
PROOF: Since $\gamma_g(a) = gag^{-1} = a$.
⟨1⟩2. If γ is trivial then G is Abelian.
PROOF: If $\gamma_g(a) = gag^{-1} = a$ for all g and a then $ga = ag$ for all g, a.
□

Proposition 8.10. *Let G be an Abelian group. Let $g, h \in G$. If g has maximal finite order in G, and h has finite order, then $|h| \mid |g|$.*

PROOF:
⟨1⟩1. ASSUME: for a contradiction $|h| \nmid |g|$.
⟨1⟩2. PICK a prime p such that $|g| = p^m r$, $|h| = p^n s$ where $p \nmid r$, $p \nmid s$ and $m < n$.
⟨1⟩3. $|g^{p^m} h^s| = p^n r$
PROOF: Proposition 6.22.
⟨1⟩4. $|g| < |g^{p^m} h^s|$
⟨1⟩5. Q.E.D.
PROOF: This contradicts the maximality of $|g|$.
□

Proposition 8.11. *Given a set A and an Abelian group H, the set H^A is an Abelian group under*

$$(\phi + \psi)(a) = \phi(a) + \psi(a) \qquad (\phi, \psi \in H^A, a \in A) \ .$$

PROOF:
⟨1⟩1. $\phi + (\psi + \chi) = (\phi + \psi) + \chi$
⟨1⟩2. $\phi + \psi = \psi + \phi$
⟨1⟩3. LET: $0 : A \to H$ be the function $0(a) = 0$.
⟨1⟩4. $\phi + 0 = 0 + \phi = \phi$

$\langle 1 \rangle 5$. Given $\phi : A \to H$, define $-\phi : A \to H$ by $(-\phi)(a) = -(\phi(a))$.
$\langle 1 \rangle 6$. $\phi + (-\phi) = (-\phi) + \phi = 0$
□

Proposition 8.12. *Given a group G and an Abelian group H, the set $\mathbf{Grp}[G, H]$ is a subgroup of H^G.*

PROOF:
$\langle 1 \rangle 1$. Given $\phi, \psi : G \to H$ group homomorphisms, we have $\phi - \psi$ is a group homomorphism.
PROOF:

$$\begin{aligned}(\phi - \psi)(g + g') &= \phi(g + g') - \psi(g + g') \\ &= \phi(g) + \phi(g') - \psi(g) - \psi(g') \\ &= \phi(g) - \psi(g) + \phi(g') - \psi(g') \\ &= (\phi - \psi)(g) + (\phi - \psi)(g')\end{aligned}$$

□

Proposition 8.13. *Let G be a group. The following are equivalent.*

1. $\mathrm{Inn}(G)$ *is cyclic.*
2. $\mathrm{Inn}(G)$ *is trivial.*
3. G *is Abelian.*

PROOF:
$\langle 1 \rangle 1$. $1 \Rightarrow 2$
$\langle 2 \rangle 1$. ASSUME: $\mathrm{Inn}(G) = \langle \gamma_g \rangle$
$\langle 2 \rangle 2$. g commutes with every element of G
$\langle 3 \rangle 1$. LET: $x \in G$
$\langle 3 \rangle 2$. PICK $n \in \mathbb{Z}$ such that $\gamma_x = \gamma_g^n$
$\langle 3 \rangle 3$. $\forall y \in G. xyx^{-1} = g^n y g^{-n}$
$\langle 3 \rangle 4$. $xgx^{-1} = g$
$\langle 2 \rangle 3$. $\gamma_g = \mathrm{id}_G$
$\langle 1 \rangle 2$. $2 \Rightarrow 3$
$\langle 2 \rangle 1$. ASSUME: $\forall g \in G. \gamma_g = \mathrm{id}_G$
$\langle 2 \rangle 2$. LET: $x, y \in G$
$\langle 2 \rangle 3$. $\gamma_x(y) = y$
$\langle 2 \rangle 4$. $xyx^{-1} = y$
$\langle 2 \rangle 5$. $xy = yx$
$\langle 1 \rangle 3$. $3 \Rightarrow 2$
PROOF: If $xy = yx$ for all x, y then $\gamma_x(y) = y$ for all x, y.
$\langle 1 \rangle 4$. $2 \Rightarrow 1$
PROOF: Easy.
□

Corollary 8.13.1. *If $\mathrm{Aut}_{\mathbf{Grp}}(G)$ is cyclic then G is Abelian.*

Proposition 8.14. *Every subgroup of an Abelian group is normal.*

PROOF: Let G be an Abelian group and N a subgroup of G. Given $g \in G$ and $n \in N$ we have $gng^{-1} = n \in N$. $\square$

Proposition 8.15. *For any group G, the group $G/[G,G]$ is Abelian.*

PROOF: For any $g, h \in G$ we have

$$gh(hg)^{-1} \in [G,G]$$
$$\therefore gh[G,G] = hg[G,G] \qquad \square$$

Proposition 8.16. *Let G be a finite Abelian group. Let p be a prime divisor of $|G|$. Then G has an element of order p.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: as induction hypothesis the result holds for all groups smaller than G.
$\langle 1 \rangle 2$. PICK $g \in G - \{0\}$.
$\langle 1 \rangle 3$. PICK an element $h \in \langle g \rangle$ with prime order q.
$\langle 1 \rangle 4$. CASE: $q = p$
  PROOF: h is the required element.
$\langle 1 \rangle 5$. CASE: $q \neq p$
  $\langle 2 \rangle 1$. PICK $r \in G$ such that $r + \langle h \rangle$ has order p in $G/\langle h \rangle$.
    PROOF: By induction hypothesis since $|G/\langle h \rangle| = |G|/q$.
  $\langle 2 \rangle 2$. $pr \in \langle h \rangle$
  $\langle 2 \rangle 3$. PICK k such that $pr = kh$
  $\langle 2 \rangle 4$. $pqr = e$
  $\langle 2 \rangle 5$. qr has order p.
$\square$

Corollary 8.16.1. *For n an odd integer, any Abelian group of order $2n$ has exactly one element of order 2.*

PROOF: If x and y are distinct elements of order 2 then $\langle x, y \rangle = \{e, x, y, xy\}$ has size 4 and so $4 \mid 2n$ which is a contradiction. $\square$

Example 8.17. It is not true that, if G is a finite group and $d \mid |G|$, then G has an element of order d. The quaternionic group has no element of order 4.

Proposition 8.18. *If G is a finite Abelian group and $d \mid |G|$ then G has a subgroup of size d.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: as induction hypothesis the result is true for all $d' < d$.
$\langle 1 \rangle 2$. ASSUME: w.l.o.g. $d \neq 1$.
$\langle 1 \rangle 3$. PICK a prime p such that $p \mid d$.
$\langle 1 \rangle 4$. PICK an element $g \in G$ of order p.
$\langle 1 \rangle 5$. $d/p \mid |G/\langle g \rangle|$
$\langle 1 \rangle 6$. PICK a subgrop H of $G/\langle g \rangle$ of size d/p.
$\langle 1 \rangle 7$. $\pi^{-1}(H)$ is a subgroup of G of size d.
$\square$

Proposition 8.19. *Let $(G, \cdot)$ be a group. Let $\circ : G^2 \to G$ be a group homomorphism such that $(G, \circ)$ is a group. Then $\circ$ and $\cdot$ coincide, and G is Abelian.*

Proof:
⟨1⟩1. For all $g_1, g_2, h_1, h_2 \in G$ we have
$$(g_1 g_2) \circ (h_1 h_2) = (g_1 \circ h_1)(g_2 \circ h_2)$$
⟨1⟩2. $e \circ e = e$
Proof:
$$\begin{aligned} e \circ e &= (ee) \circ (ee) \\ &= (e \circ e)(e \circ e) \end{aligned}$$
Hence $e \circ e = e$ by Cancellation.
⟨1⟩3. e is the identity of $(G, \circ)$
⟨1⟩4. For all $g, h \in G$ we have
$$g \circ h = gh$$
Proof:
$$\begin{aligned} g \circ h &= (ge) \circ (eh) \\ &= (g \circ e)(e \circ h) \\ &= gh \end{aligned}$$
⟨1⟩5. For all $g, h \in G$ we have $gh = hg$.
Proof:
$$\begin{aligned} gh &= (e \circ g)(h \circ e) \\ &= (eh) \circ (ge) \\ &= h \circ g \\ &= hg \end{aligned}$$
□

Corollary 8.19.1. *If $(G, m : G^2 \to G, e : 1 \to G, i : G \to G)$ is a group object in* **Grp** *then m is the multiplication of G, $e(*)$ is the identity of G, $i(g) = g^{-1}$, and G is Abelian.*

Conversely, if (G, m) is any Abelian group, then (G, m, e, i) is a group object in **Grp** *where $e(*) = e$ and $i(g) = g^{-1}$.*

Proposition 8.20. *Let G be a group. If every element of G has order ≤ 2 then G is Abelian.*

Proof:
⟨1⟩1. Let: $x, y \in G$
Prove: $xy = yx$
⟨1⟩2. Assume: w.l.o.g. $x \neq e \neq y$.
⟨1⟩3. $x^2 = e = y^2$
⟨1⟩4. $x^{-1} = x$ and $y^{-1} = y$.
⟨1⟩5. Case: $xy = e$
Proof: Then $y = x^{-1}$ and so $xy = yx = e$.
⟨1⟩6. Case: $xy \neq e$
⟨2⟩1. $(xy)^2 = e$
⟨2⟩2. $xyxy = e$

⟨2⟩3. $xy = y^{-1}x^{-1}$
⟨2⟩4. $xy = yx$
□

Proposition 8.21. *Every Abelian group is solvable.*

PROOF: If G is Abelian then $G' = \{e\}$. □

Proposition 8.22. *The only non-trivial simple finite Abelian groups are $\mathbb{Z}/p\mathbb{Z}$ for p a prime.*

PROOF:
⟨1⟩1. LET: G be a non-trivial simple finite Abelian group.
⟨1⟩2. PICK a prime p that divides $|G|$.
⟨1⟩3. PICK an element $a \in G$ of order p.
PROOF: Cauchy's Theorem.
⟨1⟩4. $\langle a \rangle = G$
□

8.1 The Category of Abelian Groups

Definition 8.23 (Category of Abelian Groups)**.** Let **Ab** be the full subcategory of **Grp** whose objects are the Abelian groups.

Proposition 8.24. *If $(G, m : G^2 \to G, e : 1 \to G, i : G \to G)$ is a group object in* **Ab** *then m is the multiplication of G, $e(*)$ is the identity of G, $i(g) = g^{-1}$, and G is Abelian.*

Conversely, if (G, m) is any Abelian group, then (G, m, e, i) is a group object in **Ab** *where $e(*) = e$ and $i(g) = g^{-1}$.*

PROOF: Immediate from Corollary 8.19.1. □

Definition 8.25 (Direct Sum)**.** Given Abelian groups G and H, we also call the direct product of G and H the *direct sum* and denote it $G \oplus H$.

Proposition 8.26. *Given Abelian groups G and H, the direct sum $G \oplus H$ is the coproduct of G and H in* **Ab**.

PROOF:
⟨1⟩1. LET: $\kappa_1 : G \to G \oplus H$ be the group homomorphism $\kappa_1(g) = (g, e_H)$.
⟨1⟩2. LET: $\kappa_2 : H \to G \oplus H$ be the group homomorphism $\kappa_2(h) = (e_G, h)$.
⟨1⟩3. Given group homomorphism $\phi : G \to K$ and $\psi : H \to K$, define $[\phi, \psi] : G \oplus H \to K$ by $[\phi, \psi](g, h) = \phi(g) + \psi(h)$.
⟨1⟩4. $[\phi, \psi]$ is a group homomorphism.
PROOF:

$$\begin{aligned}
[\phi, \psi]((g, h) + (g', h')) &= [\phi, \psi](g + g', h + h') \\
&= \phi(g + g') + \psi(h + h') \\
&= \phi(g) + \phi(g') + \psi(h) + \psi(h') \\
&= \phi(g) + \psi(h) + \phi(g') + \psi(h') \\
&= [\phi, \psi](g, h) + [\phi, \psi](g', h')
\end{aligned}$$

$\langle 1\rangle 5.$ $[\phi, \psi] \circ \kappa_1 = \phi$
PROOF:

$$\begin{aligned}[\phi, \psi](\kappa_1(g)) &= [\phi, \psi](g, e_h) \\ &= \phi(g) + \psi(e_H) \\ &= \phi(g) + e_K \\ &= \phi(g)\end{aligned}$$

$\langle 1\rangle 6.$ $[\phi, \psi] \circ \kappa_2 = \psi$
PROOF: Similar.
$\langle 1\rangle 7.$ If $f : G \oplus H \to K$ is a group homomorphism with $f \circ \kappa_1 = \phi$ and $f \circ \kappa_2 = \psi$ then $f = [\phi, \psi]$.
PROOF:

$$\begin{aligned}f(g, h) &= f((g, e_H) + (e_G, h)) \\ &= f(\kappa_1(g)) + f(\kappa_2(h)) \\ &= \phi(g) + \psi(h)\end{aligned}$$

□

Theorem 8.27. *Every finitely generated Abelian group is a direct sum of cyclic groups.*

PROOF: TODO □

8.2 Free Abelian Groups

Proposition 8.28. *Let A be a set. Let $\mathcal{F}^A$ be the category whose objects are pairs (G, j) where G is an Abelian group and j is a function $A \to G$, with morphisms $f : (G, j) \to (H, k)$ the group homomorphisms $f : G \to H$ such that $f \circ j = k$. Then $\mathcal{F}^A$ has an initial object.*

PROOF:
$\langle 1\rangle 1.$ LET: $\mathbb{Z}^{\oplus A}$ be the subgroup of $\mathbb{Z}^A$ consisting of all functions $\alpha : A \to \mathbb{Z}$ such that $\alpha(a) = 0$ for only finitely many $a \in A$.
$\langle 1\rangle 2.$ LET: $i : A \to \mathbb{Z}^{\oplus A}$ be the function such that $i(a)(b) = 1$ if $a = b$ and 0 if $a \neq b$.
$\langle 1\rangle 3.$ LET: G be any Abelian group and $j : A \to G$ any function.
$\langle 1\rangle 4.$ The unique homomorphism $\phi : \mathbb{Z}^{\oplus A} \to G$ required is defined by $\phi(\alpha) = \sum_{a \in A} \alpha(a) j(a)$
□

Definition 8.29 (Free Abelian Group)**.** For any set A, the *free Abelian group* on A is the initial object $(F^{ab}(A), i)$ in $\mathcal{F}^A$.

Proposition 8.30. *For any sets A and B, we have that $F^{ab}(A + B)$ is the coproduct of $F^{ab}(A)$ and $F^{ab}(B)$ in* **Grp**.

$$\begin{tikzcd}
& G & \\
F^{ab}(A) \arrow[ur, "f"] \arrow[r, "\kappa_1"] & F^{ab}(A+B) \arrow[u, "k"] & F^{ab}(B) \arrow[ul, "g"'] \arrow[l, "\kappa_2"] \\
A \arrow[u, "i_A"] \arrow[r, "k_1"] & A+B \arrow[u, "j"] & B \arrow[u, "i_B"] \arrow[l, "k_2"]
\end{tikzcd}$$

PROOF:
⟨1⟩1. LET: $i_A : A \to F^{ab}(A)$, $i_B : B \to F^{ab}(B)$, $j : A + B \to F^{ab}(A + B)$ be the canonical injections.
⟨1⟩2. LET: κ_1, κ_2 be the unique group homomorphisms that make the diagram above commute.
⟨1⟩3. LET: G be any group and $f : F^{ab}(A) \to G$, $g : F^{ab}(B) \to G$ any group homomorphisms.
⟨1⟩4. LET: $h : A + B \to G$ be the unique function such that $h \circ k_1 = f \circ i_A$ and $h \circ k_2 = g \circ i_B$.
⟨1⟩5. LET: $k : F^{ab}(A + B) \to G$ be the unique group homomorphism such that $k \circ j = h$.
⟨1⟩6. k is the unique group homomorphism such that $k \circ \kappa_1 \circ i_A = f \circ i_A$ and $k \circ \kappa_2 \circ i_B = g \circ i_B$.
⟨1⟩7. k is the unique group homomorphism such that $k \circ \kappa_1 = f$ and $k \circ \kappa_2 = g$.
$\square$

Proposition 8.31. *For A and B finite sets, if $F^{\mathrm{ab}}(A) \cong F^{\mathrm{ab}}(B)$ then $A \cong B$.*

PROOF:
⟨1⟩1. For any set C, define $\sim$ on $F^{\mathrm{ab}}(C)$ by: $f \sim f'$ iff there exists $g \in F^{\mathrm{ab}}(C)$ such that $f - f' = 2g$.
⟨1⟩2. For any set C, $\sim$ is an equivalence relation on $F^{\mathrm{ab}}(C)$.
⟨1⟩3. For any set C, we have $F^{\mathrm{ab}}(C) / \sim$ is finite if and only if C is finite, in which case $|F^{\mathrm{ab}}(C) / \sim| = 2^{|C|}$.
PROOF: There is a bijection between $F^{\mathrm{ab}}(C) / \sim$ and the finite subsets of C, which maps f to $\{c \in C : f(c) \text{ is odd}\}$.
⟨1⟩4. If $F^{\mathrm{ab}}(A) \cong F^{\mathrm{ab}}(B)$ then $A \cong B$.
PROOF: If $|F^{\mathrm{ab}}(A) / \sim| = |F^{\mathrm{ab}}(B) / \sim|$ then $2^{|A|} = 2^{|B|}$ and so $|A| = |B|$.
$\square$

Proposition 8.32. *Let G be an Abelian group. Then G is finitely generated if and only if there exists a surjective homomorphism $\mathbb{Z}^{\oplus n} \twoheadrightarrow G$ for some n.*

PROOF:
⟨1⟩1. If G is finitely generated then there exists a surjective homomorphism $\mathbb{Z}^{\oplus n} \twoheadrightarrow G$ for some n.
PROOF: Let $G = \langle a_1, \ldots, a_n \rangle$. Define $\phi : \mathbb{Z}^{\oplus n} \twoheadrightarrow G$ by $\phi(i_1, \ldots, i_n) = i_1 \cdot a_1 + \cdots + i_n \cdot a_n$.

⟨1⟩2. If there exists a surjective homomorphism $\phi : \mathbb{Z}^{\oplus n} \twoheadrightarrow G$ for some n then G is finitely generated.
Proof: G is generated by $\phi(1, 0, \ldots, 0)$, $\phi(0, 1, 0, \ldots, 0)$, $\ldots$, $\phi(0, \ldots, 0, 1)$.
$\square$

Proposition 8.33. *Let A be a set. Let $i : A \hookrightarrow F(A)$ be the free group on A. Then $\pi \circ i : A \to F(A)/[F(A), F(A)]$ is the free Abelian group on A.*

$$\begin{tikzcd}
F(A)/[F(A),F(A)] \arrow[drr, "h"] & & \\
F(A) \arrow[u, "\pi"] \arrow[rr, "g"] & & G \\
A \arrow[u, "i"] \arrow[urr, "f"'] & &
\end{tikzcd}$$

Proof:
⟨1⟩1. Let: G be an Abelian group and $f : A \to G$ a function.
⟨1⟩2. Let: $g : F(A) \to G$ be the unique group homomorphism such that $g \circ i = f$.
⟨1⟩3. $[F(A), F(A)] \subseteq \ker g$
Proof: For all $x, y \in F(A)$ we have $g(xyx^{-1}y^{-1}) = g(x)+g(y)-g(x)-g(y) = 0$.
⟨1⟩4. Let: $h : F(A)/[F(A), F(A)]$ be the unique group homomorphism such that $h \circ \pi = g$.
⟨1⟩5. h is the unique group homomorphism such that $h \circ \pi \circ i = f$.
$\square$

Corollary 8.33.1. *Let A and B be sets. Let $F(A)$ and $F(B)$ be the free groups on A and B respectively. If $F(A) \cong F(B)$ then $A \cong B$.*

Proof: Proposition 8.31. $\square$

8.3 Cokernels

Proposition 8.34. *Let $\phi : G \to H$ be a homomorphism between Abelian groups. Then there exists an Abelian group K and homomorphism $\pi : H \to K$ that is initial with respect to all homomorphism $\alpha : H \to L$ such that $\alpha \circ \phi = 0$.*

Proof:
⟨1⟩1. Let: $K = H/\operatorname{im}\phi$ and π be the canonical homomorphism.
⟨1⟩2. Let: $\pi \circ \phi = 0$
⟨1⟩3. Let: $\alpha : H \to L$ satisfy $\alpha \circ \phi = 0$
⟨1⟩4. $\operatorname{im}\phi \subseteq \ker \alpha$
⟨1⟩5. There exists a unique $\overline{\alpha} : H/\operatorname{im}\phi \to L$ such that $\overline{\alpha} \circ \pi = \alpha$
$\square$

Definition 8.35 (Cokernel)**.** For any homomorphism $\phi : G \to H$ in **Ab**, the *cokernel* of ϕ is the Abelian group $\operatorname{coker}\phi$ and homomorphism $\pi : H \to \operatorname{coker}\phi$ that is initial among homomorphisms $\alpha : H \to L$ such that $\alpha \circ \phi = 0$.

Proposition 8.36. *$\pi : H \to \operatorname{coker}\phi$ is initial among functions $f : H \to X$ such that, for all $x, y \in H$, if $x + \operatorname{im}\phi = y + \operatorname{im}\phi$ then $f(x) = f(y)$.*

PROOF: Easy. □

Proposition 8.37. *Let $\phi : G \to H$ be a homomorphism of Abelian groups. Then the following are equivalent.*

- *ϕ is an epimorphism.*
- *$\operatorname{coker}\phi$ is trivial.*
- *ϕ is surjective.*

PROOF:
⟨1⟩1. $1 \Rightarrow 2$
  ⟨2⟩1. ASSUME: ϕ is epi.
  ⟨2⟩2. LET: $\pi : H \to \operatorname{coker}\phi$ be the canonical homomorphism.
  ⟨2⟩3. $\pi \circ \phi = 0 \circ \phi$
  ⟨2⟩4. $\pi = 0$
  ⟨2⟩5. $\operatorname{coker}\phi = \operatorname{im}\pi$ is trivial.
⟨1⟩2. $2 \Rightarrow 3$
  PROOF: If $\operatorname{coker}\phi = H/\operatorname{im}\phi$ is trivial then $\operatorname{im}\phi = H$.
⟨1⟩3. $3 \Rightarrow 1$
  PROOF: If it is surjective then it is epi in **Set**.
□

8.4 Commutator Subgroups

Proposition 8.38. *Let G be a group. Let G' be the commutator subgroup of G. Then G/G' is Abelian.*

PROOF: Since $ghg^{-1}h^{-1}G' = G'$ so $ghG' = hgG'$. □

Proposition 8.39. *Let G be a group and A an Abelian group. Let $\alpha : G \to A$ be a homomorphism. Then $G' \subseteq \ker\alpha$.*

PROOF: Since $\phi([g, h]) = \phi(g)\phi(h)\phi(g)^{-1}\phi(h)^{-1} = e$. □

Corollary 8.39.1. *Let G be a group. The canonical projection $G \twoheadrightarrow G/G'$ is initial in the category of homomorphisms from G to an Abelian group.*

Definition 8.40 (Abelian Series)**.** A normal series of subgroups is *Abelian* iff every quotient is Abelian.

Lemma 8.41. *Let G be a group. Let H be a normal subgroup of G. If G/H is Abelian then $G' \subseteq G/H$.*

PROOF: Given $g, h \in G$ we have

$$ghH = hgH$$

$$\therefore ghg^{-1}h^{-1} \in H$$ □

Proposition 8.42. *Let G be a finite group. The following are equivalent.*

1. *All composition factors of G are cyclic.*
2. *G has a cyclic series of subgroups ending in $\{e\}$.*
3. *G has an Abelian series of subgroups ending in $\{e\}$.*
4. *G is solvable.*

PROOF:
⟨1⟩1. $1 \Rightarrow 2$
PROOF: Trivial.
⟨1⟩2. $2 \Rightarrow 3$
PROOF: Trivial.
⟨1⟩3. $3 \Rightarrow 4$
⟨2⟩1. LET: $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$ be an Abelian series of subgroups.
⟨2⟩2. For all i we have $G^{(i)} \subseteq G_i$.
PROOF: Lemma 8.41.
⟨2⟩3. $G^{(n)} = \{e\}$
⟨1⟩4. $4 \Rightarrow 1$
PROOF: Extend the derived series of G to a composition series, using the fact that every simple Abelian group is cyclic.
□

Corollary 8.42.1. *All p-groups are solvable.*

PROOF: Their composition factors are simple p-groups, hence cyclic. □

Corollary 8.42.2. *Let G be a group and N a normal subgroup. Then G is solvable if and only if both N and G/N are solvable.*

PROOF: By Proposition 7.120. □

Corollary 8.42.3. *Let G be a finite solvable group. Then the composition factors of G are exactly C_p for p a prime factor of G (with the same multiplicities).*

PROOF: Since each composition factor is simple and cyclic hence removes one prime factor in $|G|$. □

8.5 Derived Series

Definition 8.43 (Derived Series)**.** Let G be a group. The *derived series* of G is the series of subgroups

$$G \supseteq G' \supseteq G'' \supseteq G''' \supseteq \cdots$$

where G' is the commutator subgroup of G.

We write $G^{(i)}$ for the $i + 1$st entry in the derived series

Proposition 8.44. *Each $G^{(i)}$ is characteristic.*

PROOF:
⟨1⟩1. G is characteristic in G.
PROOF: Trivial.
⟨1⟩2. If $G^{(i)}$ is characteristic in G then $G^{(i+1)}$ is characteristic in G.
⟨2⟩1. ASSUME: $G^{(i)}$ is characteristic.
⟨2⟩2. LET: $\phi : G \cong G$ be an automorphism of G.
⟨2⟩3. For all $g, h \in G^{(i)}$ we have $\phi([g, h]) \in G^{(i+1)}$.
PROOF: Since $\phi([g, h]) = [\phi(g), \phi(h)]$ and $\phi(g), \phi(h) \in G^{(i)}$.
⟨2⟩4. $\phi(G^{(i+1)}) \subseteq G^{(i+1)}$
□

8.6 Solvable Groups

Definition 8.45 (Solvable)**.** A group is *solvable* iff its derived series terminates in $\{e\}$.

Theorem 8.46 (Feit-Thompson)**.** *Every finite group of odd order is solvable.*

Corollary 8.46.1. *Every non-Abelian finite simple group has even order.*

PROOF: A non-Abelian finite simple group of odd order is solvable, hence its composition factors are all Abelian. But a simple group is its own only composition factor. □

Proposition 8.47. *Let H be a nontrivial normal subgroup of a solvable group G. Then H contains a nontrivial Abelian subgroup that is normal in G.*

PROOF:
⟨1⟩1. LET: r be the largest number such that $H \cap G^{(r)}$ is non-trivial.
⟨1⟩2. LET: $K = H \cap G^{(r)}$
⟨1⟩3. K is Abelian.
PROOF: Since $[K, K] \subseteq G^{(r+1)} = \{e\}$.
⟨1⟩4. K is normal.
PROOF: Proposition 8.44.
□

Theorem 8.48 (Burnside)**.** *Let p and q be primes. Every group of order $p^a q^b$ is solvable.*

Chapter 9

Group Actions

9.1 Group Actions

Definition 9.1 (Action)**.** Let G be a group. Let A be an object of a category $\mathcal{C}$. A *(left) action* of G on A is a group homomorphism $G \to \mathrm{Aut}_{\mathcal{C}}(A)$.

It is *faithful* or *effective* iff it is injective.

Proposition 9.2. *Let A be a set. An action of the group G on the set A is given by a function $\cdot : G \times A \to A$ such that*

- $\forall a \in A. ea = a$
- $\forall g, h \in G. \forall a \in A. (gh)a = g(ha)$

Proof: Just unfolding definitions. ∎

Example 9.3. Left multiplication defines a faithful action of any group on its own underlying set.

In fact, for any subgroup H of a group G, left multiplication defines an action of G on G/H.

Corollary 9.3.1 (Cayley's Theorem)**.** *Every group G is a subgroup of a symmetric group, namely* $\mathrm{Aut}_{\mathbf{Set}}(G)$.

Example 9.4. Conjugation $g * h = ghg^{-1}$ is an action of any group on its own underlying set.

Definition 9.5 (Transitive)**.** An action of a group G on a set A is *transitive* iff, for all $a, b \in A$, there exists $g \in G$ such that $ga = b$.

Example 9.6. Left multiplication of a group G is a transitive action of G on G.

Definition 9.7 (Orbit)**.** Given an action of a group G on a set A and $a \in A$, the *orbit* of a is

$$\mathrm{O}_G(a) := \{ga : g \in G\} \ .$$

Proposition 9.8. *Given an action of a group G on a set A, the orbits form a partition of A.*

PROOF:
$\langle 1 \rangle 1$. Every element of A is in some orbit.
  PROOF: Since $a \in \mathrm{O}_G(a)$.
$\langle 1 \rangle 2$. Distinct orbits are disjoint.
  $\langle 2 \rangle 1$. LET: $a \in \mathrm{O}_G(b) \cap \mathrm{O}_G(c)$
  $\langle 2 \rangle 2$. PICK $g, h \in G$ such that $a = gb = hc$.
  $\langle 2 \rangle 3$. $\mathrm{O}_G(b) \subseteq \mathrm{O}_G(c)$
    PROOF: For all $k \in G$ we have $kb = kg^{-1}hc$.
  $\langle 2 \rangle 4$. $\mathrm{O}_G(c) \subseteq \mathrm{O}_G(b)$
    PROOF: Similar.
$\square$

Proposition 9.9. *Given an action of a group G on a set A and $a \in A$, the action is transitive on $\mathrm{O}_G(a)$.*

PROOF:
$\langle 1 \rangle 1$. The restriction of the action is an action on $\mathrm{O}_G(a)$.
  PROOF: Since $g(ha) = (gh)a$, the action maps $\mathrm{O}_G(a)$ to itself.
$\langle 1 \rangle 2$. The restricted action is transitive.
  PROOF: Given $ga, ha \in \mathrm{O}_G(a)$, we have $ha = (hg^{-1})(ga)$.
$\square$

Definition 9.10 (Stabilizer Subgroup)**.** Given an action of a group G on a set A and $a \in A$, the *stabilizer subgroup* of a is

$$\mathrm{Stab}_G(a) := \{g \in G : ga = a\} \quad .$$

Proposition 9.11. *Stabilizer subgroups are subgroups.*

PROOF: If $g, h \in \mathrm{Stab}_G(a)$ then $gh^{-1}a = a$ so $gh^{-1} \in \mathrm{Stab}_G(a)$. $\square$

Proposition 9.12. *Let G act on a set A. Let $a \in A$ and $g \in G$. Then*

$$\mathrm{Stab}_G(ga) = g\mathrm{Stab}_G(a)\,g^{-1} \quad .$$

PROOF:

$$\begin{aligned} h \in \mathrm{Stab}_G(ga) &\Leftrightarrow hga = ga \\ &\Leftrightarrow g^{-1}hga = a \\ &\Leftrightarrow g^{-1}hg \in \mathrm{Stab}_G(a) \\ &\Leftrightarrow h \in g\mathrm{Stab}_G(a)\,g^{-1} \end{aligned} \qquad \square$$

Corollary 9.12.1. *Let G be an action on a set A and $a \in A$. If $\mathrm{Stab}_G(a)$ is normal in G, then for any $b \in \mathrm{O}_G(a)$ we have $\mathrm{Stab}_G(a) = \mathrm{Stab}_G(b)$.*

Definition 9.13 (Free)**.** An action of a group G on a set A is *free* iff, whenever $ga = a$, then $g = e$.

Example 9.14. The action of left multiplication is free.

Proposition 9.15. *Let G be a group. Let H be a subgroup of G of finite index n. Then H includes a subgroup K that is normal in G and such that $|G : K|$ divides* $\gcd(|G|, n!)$.

PROOF:
$\langle 1 \rangle 1$. LET: $\sigma : G \to \mathrm{Aut}_{\mathbf{Set}}(G/H)$ be the action of left multiplication.
$\langle 1 \rangle 2$. LET: $K = \ker \sigma$
$\langle 1 \rangle 3$. $K \subseteq H$
  $\langle 2 \rangle 1$. LET: $g \in K$
  $\langle 2 \rangle 2$. $\sigma(g)(H) = H$
  $\langle 2 \rangle 3$. $gH = H$
  $\langle 2 \rangle 4$. $g \in H$
$\langle 1 \rangle 4$. K is normal in G.
  PROOF: Proposition 7.42.
$\langle 1 \rangle 5$. $|G : K| \mid |G|$
  PROOF: Lagrange's Theorem.
$\langle 1 \rangle 6$. $|G : K| \mid n!$
  PROOF: Since G/K is a subgroup of $\mathrm{Aut}_{\mathbf{Set}}(G/H)$.
$\square$

Corollary 9.15.1. *Let G be a finite group. Let H be a subgroup of G of index p where p is the smallest prime that divides $|G|$. Then H is normal in G.*

PROOF:
$\langle 1 \rangle 1$. PICK a subgroup K of H normal in G such that $|G : K|$ divides $\gcd(|G|, p!)$.
$\langle 1 \rangle 2$. $|G : K|$ divides p.
$\langle 1 \rangle 3$. $|G : H||H : K|$ divides p.
$\langle 1 \rangle 4$. $|H : K| = 1$
$\langle 1 \rangle 5$. $H = K$
$\langle 1 \rangle 6$. H is normal.
$\square$

Corollary 9.15.2. *Any subgroup of index 2 is normal.*

Proposition 9.16. *Let G be a group with finite set of generators A. Then left multiplication defines a free action of G on its Cayley graph.*

PROOF: Easy since if $g_2 = g_1 a$ then $hg_2 = hg_1 a$. $\square$

Corollary 9.16.1. *A free group acts freely on a tree.*

Theorem 9.17. *If a group G acts freely on a tree then G is free.*

Corollary 9.17.1. *Every subgroup of the free group on a finite set is free.*

PROOF: If H is a subgroup of $F(A)$ then left multiplication defines a free action of H on the Cayley graph of $F(A)$, which is a tree. $\square$

Proposition 9.18. *Let S be a finite set. Let G be a group acting on S. Let Z be the set of fixed points of the action:*

$$Z = \{a \in S : \forall g \in G . ga = a\} \enspace .$$

Let A be a set of representatives for the nontrivial orbits of the action. Then

$$|S| = |Z| + \sum_{a \in A} [G : \mathrm{Stab}_G (a)] \enspace .$$

PROOF: Immediate from the fact that the orbits partition S. □

Corollary 9.18.1. *Let p be a prime. Let S be a finite set. Let G be a p-group acting on S. Let Z be the set of fixed points of the action. Then $|Z| \cong |S| (\mathrm{mod}\, p)$.*

Corollary 9.18.2. *Let p be a prime. Let S be a finite set. Let G be a p-group acting on S. If p does not divide $|S|$ then the action has a fixed point.*

9.2 Category of G-Sets

Definition 9.19. Given a group G, let $G - \mathbf{Set}$ be the category with:

- objects all pairs (A, ρ) such that A is a set and $\rho : G \times A \to A$ is an action of G on A;
- morphisms $f : (A, \rho) \to (B, \sigma)$ are functions $f : A \to B$ that are *(G-)equivariant*, i.e.

$$\forall g \in G . \forall a \in A . f(\rho(g, a)) = \sigma(g, f(a)) \enspace .$$

Proposition 9.20. *A G-equivariant function $f : A \to B$ is an isomorphism in $G - \mathbf{Set}$ if and only if it is bijective.*

PROOF:
⟨1⟩1. LET: $f : A \to B$ be G-equivariant and bijective.
PROVE: f^{-1} is G-equivariant.
⟨1⟩2. LET: $g \in G$ and $b \in B$
⟨1⟩3. $f^{-1}(gb) = gf^{-1}(b)$
PROOF:

$$\begin{aligned} f(f^{-1}(gb)) &= gb \\ &= gf(f^{-1}(b)) \\ &= f(gf^{-1}(b)) \end{aligned}$$

□

Proposition 9.21. *Let G be a group and A a transitive G-set. Let $a \in A$. Then A is isomorphic to $G/\mathrm{Stab}_G (a)$ under left multiplication.*

PROOF:
⟨1⟩1. LET: $f : G/\mathrm{Stab}_G(a) \to A$ be the function $f(g\mathrm{Stab}_G(a)) = ga$.
⟨2⟩1. ASSUME: $g\mathrm{Stab}_G(a) = h\mathrm{Stab}_G(a)$
PROVE: $ga = ha$
⟨2⟩2. $g^{-1}h \in \mathrm{Stab}_G(a)$
⟨2⟩3. $g^{-1}ha = a$
⟨2⟩4. $ha = ga$
⟨1⟩2. f is G-equivariant.
PROOF: Since $f(gh\mathrm{Stab}_G(a)) = gha = gf(h\mathrm{Stab}_G(a))$.
⟨1⟩3. f is injective.
PROOF: If $ga = ha$ then $g^{-1}h \in \mathrm{Stab}_G(a)$ so $g\mathrm{Stab}_G(a) = h\mathrm{Stab}_G(a)$.
⟨1⟩4. f is surjective.
PROOF: Since for all $b \in A$ there exists $g \in G$ such that $ga = b$.
□

Corollary 9.21.1. *If O is an orbit of the action of a finite group G on a set A, then O is finite and $|O|$ divides $|G|$.*

Corollary 9.21.2. *Let H be a subgroup of G and $g \in G$. Then*

$$G/H \cong G/(gHg^{-1})$$

in $G - \mathbf{Set}$.

PROOF: Taking $A = G/H$ and $a = gH$. □

Proposition 9.22. *Given a family of G-sets $\{A_i\}_{i\in I}$, we have $\prod_{i\in I} A_i$ is their product in $G - \mathbf{Set}$ under*

$$g\{a_i\}_{i\in I} = \{ga_i\}_{i\in I} \quad .$$

PROOF: Easy. □

Proposition 9.23. *Given a family of G-sets $\{A_i\}_{i\in I}$, we have $\coprod_{i\in I} A_i$ is their product in $G - \mathbf{Set}$ under*

$$g(i, a_i) = (i, ga_i) \quad .$$

PROOF: Easy. □

Proposition 9.24. *Every finite G-set is a coproduct of G-sets of the form G/H.*

PROOF: If $O(a_1)$, ..., $O(a_n)$ are the orbits of the G-set A, then G is the coproduct of $G/\mathrm{Stab}_G(a_1)$, ..., $G/\mathrm{Stab}_G(a_n)$. □

Proposition 9.25. *For any group G we have $G \cong \mathrm{Aut}_{G-\mathbf{Set}}(G)$ (considering G as a G-set under left multiplication).*

PROOF:
⟨1⟩1. Define $\phi : G \to \mathrm{Aut}_{G-\mathbf{Set}}(G)$ by $\phi(g)(g') = g'g^{-1}$.

⟨2⟩1. LET: $g \in G$
PROVE: $\lambda g' \in G.g'g^{-1}$ is an automorphism of G in $G - \mathbf{Set}$.
⟨2⟩2. $\phi(g)$ is G-equivariant.
PROOF: Since $\phi(g)(h_1 h_2) = h_1 h_2 g^{-1} = h_1 \phi(g)(h_2)$.
⟨2⟩3. $\phi(g)$ is injective.
PROOF: By Cancellation.
⟨2⟩4. $\phi(g)$ is surjective.
PROOF: For any $h \in G$ we ahev $h = \phi(g)(hg)$.
⟨1⟩2. ϕ is a group homomorphism.
PROOF: $\phi(g_1 g_2)(h) = h{g_2}^{-1}{g_1}^{-1} = \phi(g_1)(\phi(g_2)(h))$.
⟨1⟩3. ϕ is injective.
PROOF: If $\phi(g) = \phi(g')$ then $g = \phi(g)(e) = \phi(g')(e) = g'$.
⟨1⟩4. ϕ is surjective.
⟨2⟩1. LET: $\sigma \in \mathrm{Aut}_{G-\mathbf{Set}}(G)$
⟨2⟩2. LET: $g = \sigma(e)$
PROVE: $\sigma = \phi(g^{-1})$
⟨2⟩3. $\sigma(h) = hg$
PROOF: $\sigma(h) = \sigma(he) = h\sigma(e) = hg$.
□

9.3 Center

Definition 9.26 (Center)**.** The *center* of a group G, $Z(G)$, is the kernel of the conjugation action $\sigma : G \to S_G$.

Proposition 9.27. *The center of a group G is*

$$Z(G) = \{g \in G : \forall a \in G.ag = ga\} \ .$$

PROOF: Immediate from definitions. □

Lemma 9.28. *Let G be a finite group. Assume $G/Z(G)$ is cyclic. Then G is Abelian and so $G/Z(G)$ is trivial.*

PROOF:
⟨1⟩1. PICK $g \in G$ such that $gZ(G)$ generates $G/Z(G)$.
⟨1⟩2. LET: $a, b \in G$
⟨1⟩3. PICK $r, s \in \mathbb{Z}$ such that $aZ(G) = g^r Z(G)$ and $bZ(G) = g^s Z(G)$
⟨1⟩4. LET: $z = g^{-r} a \in Z(G)$ and $w = g^{-s} b \in Z(G)$
⟨1⟩5. $a = g^r z$ and $b = g^s w$
⟨1⟩6. $ab = ba$
PROOF:

$$\begin{aligned} ab &= g^r z g^s w \\ &= g^{r+s} z w \\ &= g^s w g^r z \\ &= ba \end{aligned}$$

∎

Proposition 9.29. *Let G be a group. Let N be a subgroup of $Z(G)$. Then N is normal in G.*

Proof: For all $n \in N$ and $g \in G$ we have $gng^{-1} = ngg^{-1} = n \in N$ since $n \in Z(G)$. ∎

Proposition 9.30. *For any group G we have $G/Z(G) \cong \mathrm{Inn}\,(G)$.*

Proof: The homomorphism $g \mapsto \gamma_g$ is a surjective homomorphism with kernel $Z(G)$. ∎

Proposition 9.31. *Let p and q be prime integers. Let G be a group of order pq. Then either G is Abelian or the center of G is trivial.*

Proof: Otherwise we would have $|Z(G)| = p$ say and so $|\mathrm{Inn}\,(G)\,| = q$, meaning $\mathrm{Inn}\,(G)$ is cyclic, hence trivial, which is a contradiction. ∎

Theorem 9.32 (First Sylow Theorem)**.** *Let p be a prime and $k \in \mathbb{N}$. Let G be a finite group. If p^k divides $|G|$ then G has a subgroup of order p^k.*

Proof:
$\langle 1\rangle$1. Assume: as induction hypothesis the statement is true for all groups smaller than G.
$\langle 1\rangle$2. Assume: w.l.o.g. $k \neq 0$ and $|G| \neq p$
$\langle 1\rangle$3. Case: There exists a proper subgroup H of G such that p does not divide $[G : H]$.
  Proof: Then H has a subgroup of order p^k by induction hypothesis $\langle 1\rangle$1.
$\langle 1\rangle$4. Case: For every proper subgroup H of G we have p divides $[G : H]$.
  $\langle 2\rangle$1. p divides $|Z(G)|$.
    Proof: By the Class Formula.
  $\langle 2\rangle$2. Pick $a \in Z(G)$ that has order p.
    Proof: Cauchy's Theorem.
  $\langle 2\rangle$3. Let: $N = \langle a\rangle$
  $\langle 2\rangle$4. N is normal.
    Proof: Proposition 9.29.
  $\langle 2\rangle$5. p^{k-1} divides $|G/N|$.
  $\langle 2\rangle$6. Pick a subgroup Q of G/N of order p^{k-1}.
    Proof: Induction hypothesis $\langle 1\rangle$1.
  $\langle 2\rangle$7. Let: $P = \pi^{-1}(Q)$
  $\langle 2\rangle$8. $|P| = p^k$

∎

Theorem 9.33 (Second Sylow Theorem)**.** *Let G be a finite group. Let p be a prime. Let P be a p-Sylow subgroup of G. Let H be a subgroup of G that is a p-group. Then H is a subgroup of a conjugate of P.*

Proof:

$\langle 1 \rangle 1$. PICK a fixed point gP for the action of H on the set of left cosets of P by left multiplication.

PROOF: Corollary 9.18.2.

$\langle 1 \rangle 2$. For all $h \in H$ we have $hgP = gP$

$\langle 1 \rangle 3$. $H \subseteq gPg^{-1}$

□

9.4 Centralizer

Definition 9.34 (Centralizer)**.** Let G be a group. Let $a \in G$. The *centralizer* or *normalizer* of a, denoted $Z_G(a)$, is the stabilizer of a under the action of conjugation.

Proposition 9.35.

$$Z_G(a) = \{g \in G : ga = ag\}$$

PROOF: Immediate from definitions. □

9.5 Conjugacy Class

Definition 9.36 (Conjugacy Class)**.** Let G be a group. Let $a \in G$. The *conjugacy class* of a, denoted $[a]$, is the orbit of a under the action of conjugation.

Proposition 9.37 (Class Formula)**.** *Let G be a finite group. Let A be a set of representatives of the non-trivial conjugacy classes. Then*

$$|G| = |Z(G)| + \sum_{a \in A} [G : Z(a)] \enspace .$$

PROOF: Proposition 9.18. □

Corollary 9.37.1. *Let p be a prime. Let G be a p-group and H a nontrivial normal subgroup of G. Then $H \cap Z(G) \neq \{e\}$.*

PROOF: Let A be a set of representatives of the non-trivial conjugacy classes. Let $A \cap H = \{a_1, \ldots, a_n\}$. Then

$$|H| = |H \cap Z(G)| + \sum_{i=1}^{n} [G : Z(a_i)] \enspace .$$

Since $p \mid |H|$ and $p \mid [G : Z(a_i)]$ for all i, we have $p \mid |H \cap Z(G)|$. □

Corollary 9.37.2. *Let p be a prime. Every p-group has a non-trivial center.*

Corollary 9.37.3. *Let p be a prime. Every group G of order p^2 is Abelian.*

PROOF: By Proposition 9.31. □

Proposition 9.38. *Let p be a prime and r a non-negative integer. Let G be a group of order p^r. Then, for $k = 0, 1, \ldots, r$, we have G has a normal subgroup of order p^k.*

PROOF:
$\langle 1\rangle 1$. ASSUME: as induction hypothesis the result holds for $r' < r$.
$\langle 1\rangle 2$. ASSUME: w.l.o.g. $k > 0$
PROOF: Since $\{e\}$ is a normal subgroup of order p^0.
$\langle 1\rangle 3$. PICK a subgroup N of $Z(G)$ of order p.
$\langle 2\rangle 1$. $p \mid |Z(G)|$
PROOF: From Corollary 9.37.2.
$\langle 2\rangle 2$. $Z(G)$ has a subgroup of order p.
PROOF: Cauchy's Theorem.
$\langle 1\rangle 4$. N is normal.
PROOF: Proposition 9.29.
$\langle 1\rangle 5$. PICK a normal subgroup M of G/N of order p^{k-1}.
PROOF: From the induction hypothesis $\langle 1\rangle 1$.
$\langle 1\rangle 6$. $\pi^{-1}(M)$ is a normal subgroup of G of order p^k.
□

Example 9.39. The only non-Abelian group of order 6 is S_3.

PROOF:
$\langle 1\rangle 1$. LET: G be a non-Adelian group of order 6.
$\langle 1\rangle 2$. $Z(G) = \{e\}$
PROOF: Otherwise $Z(G)$ has order 2 or 3 and is cyclic, contradicting Lemma 9.28.
$\langle 1\rangle 3$. G has three conjugacy classes: $Z(G)$, a class of size 2 and a class of size 3.
PROOF: By the Class Formula since the only way to make 5 using non-trivial factors of 6 is $2 + 3$.
$\langle 1\rangle 4$. PICK an element $y \in G$ of order 3.
PROOF: It cannot be that every element is of order ≤ 2 by Proposition 8.20.
$\langle 1\rangle 5$. $\langle y\rangle$ is normal in G.
PROOF: Since it has index 2.
$\langle 1\rangle 6$. The conjugacy class y is $\{y, y^2\}$.
PROOF: Since $\langle y\rangle$ must be a union of conjugacy classes.
$\langle 1\rangle 7$. The conjugacy class of size 2 is $\{y, y^2\}$.
PROOF: Since y^2 has order 3 and so its conjugacy class is of size 2 similarly, and there is only one conjugacy class of size 2.
$\langle 1\rangle 8$. PICK $x \in G$ such that $yx = xy^2$.
PROOF: y^2 is conjugate to y so there exists x such that $x^{-1}yx = y^2$.
$\langle 1\rangle 9$. x has order 2.
PROOF: x is not in the conjugacy class of size 2 so its order cannot be 3.
$\langle 1\rangle 10$. x and y generate G.
PROOF: Since e, y, y^2, x, xy, xy^2 are all distinct.
$\langle 1\rangle 11$. $G \cong S_3$
PROOF: We now know the entire multiplication table of G.
□

Proposition 9.40. *Let G be a finite group. Let H be a subgroup of G of order 2. Let $a \in H$. Let $[a]_H$ be the conjugacy class of a in H, and $[a]_G$ the conjugacy* *class of a in G. If $Z_G(a) \subseteq H$ then $[a]_H$ is half the size of $[a]_G$; otherwise, $[a]_H = [a]_G$.*

PROOF:
$\langle 1 \rangle 1$. H is normal in G.
  PROOF: Corollary 9.15.2.
$\langle 1 \rangle 2$. $HZ_G(a)$ is a subgroup of G.
$\langle 1 \rangle 3$. H is normal in $HZ_G(a)$.
$\langle 1 \rangle 4$. $H \cap Z_G(a)$ is normal in $Z_G(a)$.
$\langle 1 \rangle 5$.

$$\frac{HZ_G(a)}{H} \cong \frac{Z_G(a)}{H \cap Z_G(a)}$$

$\langle 1 \rangle 6$. If $Z_G(a) \subseteq H$ then $|[a]_H| = |[a]_G|/2$.
  PROOF: In this case we have $Z_H(a) = Z_G(a)$ and so $|[a]_H| = |H|/|Z_H(a)| = (|G|/2)/|Z_G(a)| = |[a]_G|/2$.
$\langle 1 \rangle 7$. If $Z_G(a) \nsubseteq H$ then $[a]_H = [a]_G$.
  PROOF:
  $\langle 2 \rangle 1$. PICK $b \in Z_G(a) - H$
  $\langle 2 \rangle 2$. $Hb^{-1} = G - H$
  $\langle 2 \rangle 3$. $G = HZ_G(a)$
    PROOF: For $x \in H$ we have $x = xe$ and for $x \notin H$ we have $x \in Hb^{-1}$ hence $xb \in H$ and $x = (xb)b$.
  $\langle 2 \rangle 4$. $|[a]_H| = |[a]_G|$
    PROOF:

$$\begin{aligned} |[a]_H| &= \frac{|H|}{|Z_H(a)|} \\ &= \frac{|H|}{|H \cap Z_G(a)|} \\ &= \frac{|Z_G(a)||H|}{|Z_G(a)||H \cap Z_G(a)|} \\ &= \frac{|HZ_G(a)|}{|Z_G(a)|} \\ &= \frac{|G|}{|Z_G(a)|} \\ &= |[a]_G| \end{aligned}$$

□

9.6 Conjugation on Sets

Definition 9.41 (Conjugation)**.** Let G be a group. Define an action of G on $\mathcal{P}G$ called *conjugation* that takes g and A to

$$gAg^{-1} = \{gag^{-1} : a \in A\} .$$

Proposition 9.42. *The conjugate of a subgroup is a subgroup.*

PROOF: Let H be a subgroup of G. Given $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$, we have
$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1{h_2}^{-1}g^{-1} \in gHg^{-1} \ . \qquad \square$$

Definition 9.43 (Normalizer)**.** Let G be a group and $A \subseteq G$. The *normalizer* of A, denoted $N_G(A)$, is its stabilizer under conjugation.

Proposition 9.44. *Let G be a group, $g \in G$ and A a finite subset of G. If $gAg^{-1} \subseteq A$ then $gAg^{-1} = A$ and so $g \in N_G(A)$.*

PROOF: Conjugation by g is an injection from A into A, hence a bijection. $\square$

Proposition 9.45. *Let G be a group and H a subgroup of G. Then $N_G(H)$ is the largest subgroup of G that includes H such that H is normal in $N_G(H)$.*

PROOF:
⟨1⟩1. $N_G(H)$ is a subgroup of G.
  PROOF: If $a, b \in N_G(H)$ then $ab^{-1}Hba^{-1} = aHa^{-1} = H$ so $ab^{-1} \in N_G(H)$.
⟨1⟩2. $H \subseteq N_G(H)$
  PROOF: Easy.
⟨1⟩3. H is normal in $N_G(H)$.
  PROOF: If $a \in N_G(H)$ then $aHa^{-1} = H$ by definition.
⟨1⟩4. For any subgroup K of G, if $H \subseteq K$ and H is normal in K then $K \subseteq N_G(H)$.
  PROOF: H is normal in K means that, for all $a \in K$, we have $aHa^{-1} = H$ and so $a \in N_G(H)$.
$\square$

Corollary 9.45.1. *Let G be a group and H a subgroup of G. Then H is normal if and only if $G = N_G(H)$.*

Proposition 9.46. *Let G be a group and H a subgroup of G. If $[G : N_G(H)]$ is finite, then it is the number of subgroups conjugate to H.*

PROOF: By the Orbit-Stabilizer Theorem. $\square$

Corollary 9.46.1. *Let G be a group and H a subgroup of G. If $[G : H]$ is finite, the the number of subgroups conjugate to H is finite and divides $[G : H]$.*

Lemma 9.47. *Let H be a p-group that is a subgroup of a finite group G. Then*
$$[N_G(H) : H] \equiv [G : H] \pmod p \ .$$

PROOF:
⟨1⟩1. ASSUME: w.l.o.g. H is non-trivial.
⟨1⟩2. gH is a fixed point of the action of H on the set of left cosets of H by left multiplication if and only if $g \in N_G(H)$.
  PROOF:
$$\begin{aligned} gH \text{ is a fixed point} &\Leftrightarrow \forall h \in H. hgH = gH \\ &\Leftrightarrow H \subseteq gHg^{-1} \\ &\Leftrightarrow H = gHg^{-1} && (|gHg^{-1}| = |H|) \\ &\Leftrightarrow g \in N_G(H) \end{aligned}$$

$\langle 1 \rangle 3$. The number of fixed points in $[N_G(H) : H]$.
$\langle 1 \rangle 4$. Q.E.D.
PROOF: Corollary 9.18.1.
□

Proposition 9.48. *Let H be a p-subgroup of a finite group G that is not a p-Sylow subgroup. Then there exists a p-subgroup H' of G such that H is a normal subgroup of H' and $[H' : H] = p$.*

PROOF:
$\langle 1 \rangle 1$. p divides $[N_G(H) : H]$.
PROOF: Lemma 9.47.
$\langle 1 \rangle 2$. PICK $gH \in N_G(H)/H$ of order p.
PROOF: Cauchy's Theorem.
$\langle 1 \rangle 3$. LET: $H' = \pi^{-1}(\langle gH \rangle)$
$\langle 1 \rangle 4$. H is a normal subgroup of H'.
$\langle 1 \rangle 5$. $[H' : H] = p$
□

Corollary 9.48.1. *No p-group of order $\geq p^2$ is simple.*

Lemma 9.49. *Let p be a prime. Let G be a finite group. Let P be a p-Sylow subgroup of G. Every p-subgroup of $N_G(P)$ is a subgroup of P.*

PROOF:
$\langle 1 \rangle 1$. LET: H be a p-subgroup of $N_G(P)$.
$\langle 1 \rangle 2$. P is normal in $N_G(P)$.
PROOF: Proposition 9.45.
$\langle 1 \rangle 3$. PH is a subgroup of $N_G(P)$.
PROOF: Second Isomorphism Theorem.
$\langle 1 \rangle 4$. $|PH/P| = |H/(P \cap H)|$
PROOF: Second Isomorphism Theorem.
$\langle 1 \rangle 5$. PH is a p-group.
$\langle 2 \rangle 1$. ASSUME: for a contradiction q is prime, $q \mid |PH|$ and $q \neq p$
$\langle 2 \rangle 2$. $q \mid |PH/P|$
$\langle 2 \rangle 3$. $q \mid |H/(P \cap H)|$
$\langle 2 \rangle 4$. $q \mid |H|$
$\langle 2 \rangle 5$. Q.E.D.
PROOF: This contradicts the fact that H is a p-group, $\langle 1 \rangle 1$.
$\langle 1 \rangle 6$. $PH = P$
PROOF: By maximality of P.
$\langle 1 \rangle 7$. $H \subseteq P$
□

Lemma 9.50. *Let p be a prime. Let G be a finite group. Let P be a p-Sylow subgroup of G. Let P act by conjugation on the set of p-Sylow subgroups of G. Then P is the unique fixed point of this action.*

PROOF:

$\langle 1\rangle 1.$ P is a fixed point of this action.
PROOF: For any $x \in P$ we have $xPx^{-1} = P$.
$\langle 1\rangle 2.$ If Q is any fixed point of the action then $Q = P$.
$\langle 2\rangle 1.$ LET: Q be a fixed point of the action.
$\langle 2\rangle 2.$ For all $x \in P$ we have $xQx^{-1} = Q$.
$\langle 2\rangle 3.$ $P \subseteq N_G(Q)$
$\langle 2\rangle 4.$ $P \subseteq Q$
PROOF: Lemma 9.49.
$\langle 2\rangle 5.$ $P = Q$
PROOF: Since $|P| = |Q|$.
□

Theorem 9.51 (Third Sylow Theorem)**.** *Let p be a prime. Let G be a finite group of order $p^r m$ where p does not divide m. Then the number of p-Sylow subgroups of G divides m and is congruent to 1 modulo p.*

PROOF:
$\langle 1\rangle 1.$ LET: N_p be the number of p-Sylow subgroups of G.
$\langle 1\rangle 2.$ PICK a p-Sylow subgroup P.
PROOF: One exists by the First Sylow Theorem.
$\langle 1\rangle 3.$ The p-Sylow subgroups of G are exactly the conjugates of P.
PROOF: Second Sylow Theorem
$\langle 1\rangle 4.$ $m = N_p[N_G(P) : P]$
PROOF: Since $N_p = [G : N_G(P)]$ by Proposition 9.46.
$\langle 1\rangle 5.$ N_p divides m.
$\langle 1\rangle 6.$ $mN_p \equiv m (\mathrm{mod}\, p)$
$\langle 2\rangle 1.$ $m \equiv [N_G(P) : P] (\mathrm{mod}\, p)$
PROOF: Lemma 9.47.
$\langle 2\rangle 2.$ $mN_p \equiv m (\mathrm{mod}\, p)$
PROOF: By $\langle 1\rangle 4$.
$\langle 1\rangle 7.$ $N_p \equiv 1 (\mathrm{mod}\, p)$
□

PROOF:
$\langle 1\rangle 1.$ LET: N_p be the number of p-Sylow subgroups of G.
$\langle 1\rangle 2.$ PICK a p-Sylow subgroup P of G.
PROOF: First Sylow Theorem.
$\langle 1\rangle 3.$ N_p is the number of conjugates of P.
PROOF: Second Sylow Theorem.
$\langle 1\rangle 4.$ $N_p \mid m$
PROOF: Corollary 9.46.1.
$\langle 1\rangle 5.$ P acts on the set of conjugates of P with one fixed point.
PROOF: Lemma 9.50.
$\langle 1\rangle 6.$ $N_p \equiv 1 (\mathrm{mod}\, p)$
PROOF: Corollary 9.18.1.
□

Corollary 9.51.1. *Let G be a finite group. Let p be a prime number. If $|G| = mp^r$ and the only divisor d of m such that $d \equiv 1 (\bmod p)$ is $d = 1$, then G is not simple.*

PROOF: There must be 1 p-Sylow subgroup, which has order p^r and is normal. ∎

Corollary 9.51.2. *Let G be a finite group. Let p be a prime number. If $|G| = mp^r$ where $1 < m < p$ then G is not simple.*

Proposition 9.52. *Let p and q be prime numbers with $p < q$. Let G be a group of order pq with a normal subgroup H of order p. Then G is cyclic.*

PROOF:
$\langle 1 \rangle 1$. LET: $\gamma : G \to \mathrm{Aut}_{\mathbf{Grp}}(H)$ be the action of conjugation.
$\langle 1 \rangle 2$. H is cyclic of order p.
$\langle 1 \rangle 3$. $|\mathrm{Aut}_{\mathbf{Grp}}(H)| = p - 1$
$\langle 1 \rangle 4$. $|\operatorname{im} \gamma| \mid pq$
  PROOF: Since $\operatorname{im} \gamma$ is a quotient group of G.
$\langle 1 \rangle 5$. $|\operatorname{im} \gamma| \mid p - 1$
$\langle 1 \rangle 6$. $|\operatorname{im} \gamma| = 1$
$\langle 1 \rangle 7$. $\gamma = 0$
$\langle 1 \rangle 8$. $H \subseteq Z(G)$
$\langle 1 \rangle 9$. G is Abelian.
  PROOF: Lemma 9.28.
$\langle 1 \rangle 10$. PICK an element g of order p.
  PROOF: Cauchy's Theorem.
$\langle 1 \rangle 11$. PICK an element g of order q.
  PROOF: Cauchy's Theorem.
$\langle 1 \rangle 12$. $|gh| = pq$
  PROOF: Proposition 6.22.
∎

Corollary 9.52.1. *Let p and q be prime numbers with $p < q$ and $q \not\equiv 1 (\bmod p)$. Then the only group of order pq is the cyclic group.*

PROOF: By the Third Sylow Theorem, such a group must have exactly one p-Sylow subgroup, which is therefore normal. ∎

Proposition 9.53. *Let p be prime. Let G be a finite group. Let P be a p-Sylow subgroup of G. Then*
$$N_G(N_G(P)) = N_G(P) \ .$$

PROOF:
$\langle 1 \rangle 1$. P is normal in $N_G(P)$.
  PROOF: Proposition 9.45.
$\langle 1 \rangle 2$. $N_G(P)$ is normal in $N_G(N_G(P))$.
  PROOF: Proposition 9.45.
$\langle 1 \rangle 3$. P is normal in $N_G(N_G(P))$.

PROOF: Corollary 7.106.1.
⟨1⟩4. $N_G(N_G(P)) \subseteq N_G(P)$
PROOF: Proposition 9.45.
⟨1⟩5. $N_G(N_G(P)) = N_G(P)$
□

Proposition 9.54. *Let p, q and r be three distinct prime numbers. Then there is no simple group of order pqr.*

PROOF:
⟨1⟩1. LET: G be a group of order pqr.
⟨1⟩2. ASSUME: w.l.o.g. $p < q < r$
⟨1⟩3. ASSUME: for a contradiction G is simple.
⟨1⟩4. The number of subgroups of order p is at least $p + 1$.
PROOF: Third Sylow Theorem
⟨1⟩5. The number of subgroups of order q is at least $q + 1$.
PROOF: Third Sylow Theorem
⟨1⟩6. The number of subgroups of order r is pq.
PROOF: By the Third Sylow Theorem, the number divides pq, and it cannot be 1 (lest that subgroup be normal) or p or q (as these are less than r hence not congruent to 1 modulo r).
⟨1⟩7. There are at least $p^2 - 1$ elements of order p.
⟨1⟩8. There are at least $q^2 - 1$ elements of order q.
⟨1⟩9. There are at least $pqr - pq$ elements of order r.
⟨1⟩10. Q.E.D.
PROOF: This is a contradiction as the total number of elements of order 1, p, q and r is

$$\begin{aligned} 1 + (p^2 - 1) + (q^2 - 1) + (pqr - pq) &= p^2 + q^2 + pqr - pq - 1 \\ &> pqr + p^2 - 1 \\ &> pqr \end{aligned}$$

□

Proposition 9.55. *Let G be a finite simple group. Let H be a subgroup of G of index $N > 1$. Then $|G|$ divides $N!$.*

PROOF:
⟨1⟩1. PICK a subgroup K of H that is normal in G such that $[G : K]$ divides $\gcd(|G|, N!)$.
⟨1⟩2. $K = \{e\}$
⟨1⟩3. $[G : K] = |G|$
⟨1⟩4. $|G|$ divides $N!$
□

Corollary 9.55.1. *Let G be a finite simple group. Let p be a prime factor of $|G|$. Let N_p be the number of p-Sylow subgroups of G. Then $|G|$ divides $N_p!$.*

PROOF: Since $N_p = [G : N_G(P)]$ and $N_p > 1$ since G is simple. □

Definition 9.56 (Centralizer)**.** Let G be a group and $A \subseteq G$. The *centralizer* of A is

$$Z_G(A) := \{g \in G : \forall a \in A. gag^{-1} = a\} \ .$$

Proposition 9.57. *Let H and K be subgroups of G with $H \subseteq N_G(K)$. Then the function $\gamma : H \to \mathrm{Aut}_{\mathbf{Grp}}(K)$ defined by conjugation*

$$\gamma_h(k) = hkh^{-1}$$

is a homomorphism of groups with $\ker \gamma = H \cap Z_G(K)$.

PROOF:
⟨1⟩1. For all $g, h \in H$ we have $\gamma_{gh} = \gamma_g \circ \gamma_h$.
PROOF: Since $\gamma_{gh}(k) = \gamma_g(\gamma_h(k)) = ghkh^{-1}g^{-1}$.
⟨1⟩2. For all $h \in H$ we have $\gamma_h = \mathrm{id}_K$ iff $h \in Z_G(K)$.
PROOF: Both are equivalent to $\forall k \in K. hkh^{-1} = k$, i.e. $\forall k \in K. hk = kh$.
□

9.7 Nilpotent Groups

Definition 9.58 (Nilpotent)**.** Let G be a group. Define inductively a sequence (Z_n) of subgroups of G by $Z_0 = \{e\}$, and Z_{i+1} is the inverse image under π of the center of G/Z_i.

Then G is *nilpotent* iff $Z_n = G$ for some n.

We prove this is well-defined by proving that, for all i, we have Z_i is normal in G.

PROOF:
⟨1⟩1. ASSUME: as induction hypothesis Z_i is normal in G.
PROVE: Z_{i+1} is normal in G.
⟨1⟩2. LET: $x \in Z_{i+1}$ and $g \in G$
PROVE: $gxg^{-1} \in Z_{i+1}$
PROVE: For all $h \in G$ we have $gxg^{-1}hZ_i = hgxg^{-1}Z_i$
⟨1⟩3. LET: $h \in G$
⟨1⟩4. $gxg^{-1}hZ_i = hgxg^{-1}Z_i$
PROOF:

$$\begin{aligned} gxg^{-1}hZ_i &= gg^{-1}hxZ_i \\ &= hxZ_i \\ &= hgg^{-1}xZ_i \\ &= hgxg^{-1}Z_i \end{aligned}$$

□

Proposition 9.59. *Every Abelian group is nilpotent.*

PROOF: Let G be an Abelian group. The center of G/Z_0 is G/Z_0, hence $Z_1 = G$.
□

Proposition 9.60. *Let G be a group. Then G is nilpotent if and only if $G/Z(G)$ is nilpotent.*

PROOF:
$\langle 1 \rangle 1$. LET: (Z_n) be the sequence of subgroups of G where $Z_0 = \{e\}$ and Z_{n+1} is the inverse image of the center of G/Z_n.
$\langle 1 \rangle 2$. $G/Z_0 \cong G$
$\langle 1 \rangle 3$. $Z_1 = Z(G)$
$\langle 1 \rangle 4$. The corresponding sequence of subgroups for $G/Z(G)$ is $G/Z(G)$, $Z_2/Z(G)$, $Z_3/Z(G)$, ...
$\langle 1 \rangle 5$. G is nilpotent iff $G/Z(G)$ is nilpotent.
PROOF: Both are equivalent to $\exists n. Z_n = g$ and to $\exists n. Z_n/Z(G) = G/Z(G)$.
□

Proposition 9.61. *Every p-group is nilpotent.*

PROOF: Each Z_n is a p-group and so has non-trivial center, hence each Z_{n+1} is larger than Z_n and so the sequence must terminate. □

Proposition 9.62. *Every nilpotent group is solvable.*

PROOF: Let (Z_n) be the defining sequence of subgroups. Then $Z_{n+1}/Z_n = Z(G/Z_n)$ is Abelian for all n, hence the group is solvable by Proposition 8.42.
□

Example 9.63. The converse is not true — S_3 is solvable but not nilpotent.

Proposition 9.64. *Let G be a nilpotent group. Then every nontrivial normal subgroup of G intersects $Z(G)$ non-trivially.*

PROOF:
$\langle 1 \rangle 1$. LET: H be a nontrivial normal subgroup of G.
$\langle 1 \rangle 2$. LET: (Z_n) be the sequence of subgroups with $Z_0 = \{e\}$ and Z_{n+1} the inverse image of $Z(G/Z_n)$.
$\langle 1 \rangle 3$. LET: r be least such that $H \cap Z_r \neq \{e\}$.
$\langle 1 \rangle 4$. PICK $h \in H \cap Z_r$ with $h \neq e$.
$\langle 1 \rangle 5$. $hZ_{r-1} \in Z(G/Z_{r-1})$
$\langle 1 \rangle 6$. For all $g \in G$ we have $ghZ_{r-1} = hgZ_{r-1}$
$\langle 1 \rangle 7$. For all $g \in G$ we have $ghg^{-1}h^{-1} \in Z_{r-1}$
$\langle 1 \rangle 8$. For all $g \in G$ we have $ghg^{-1}h^{-1} = e$
PROOF: Since $ghg^{-1}h^{-1} \in H$ and $H \cap Z_{r-1} = \{e\}$.
$\langle 1 \rangle 9$. For all $g \in G$ we have $gh = hg$
$\langle 1 \rangle 10$. $h \in H \cap Z(G)$
□

Example 9.65. We cannot weaken the hypothesis to G being solvable. S_3 is solvable and $\mathbb{Z}/2\mathbb{Z}$ is a nontrivial normal subgroup but its intersection with $Z(S_3)$ is just $\{e\}$.

Proposition 9.66. *Let G be a finite nilpotent group. Let H be a proper subgroup of G. Then $H \subsetneq N_G(H)$.*

PROOF:
⟨1⟩1. ASSUME: as induction hypothesis the theorem holds for all groups smaller than G.
⟨1⟩2. $Z(G)$ is non-trivial.
⟨1⟩3. CASE: $Z(G) \nsubseteq H$
⟨2⟩1. PICK $g \in Z(G) - H$
⟨2⟩2. $g \in N_G(H) - H$
⟨1⟩4. CASE: $Z(G) \subseteq H$
⟨2⟩1. $H/Z(G) \subsetneq N_{G/Z(G)}(H/Z(G))$
PROOF: By induction hypothesis ⟨1⟩1.
⟨2⟩2. PICK g such that $gZ(G) \in N_{G/Z(G)}(H/Z(G)) - H/Z(G)$
⟨2⟩3. $g \in N_G(H)$
⟨3⟩1. LET: $h \in H$
PROVE: $ghg^{-1} \in H$
⟨3⟩2. $ghg^{-1}Z(G) \in H/Z(G)$
⟨3⟩3. PICK $h_1 \in H$ such that $ghg^{-1}Z(G) = h_1Z(G)$
⟨3⟩4. $ghg^{-1}{h_1}^{-1} \in Z(G)$
⟨3⟩5. $ghg^{-1}{h_1}^{-1} \in H$
PROOF: ⟨1⟩4
⟨3⟩6. $ghg^{-1} \in H$
⟨2⟩4. $g \notin H$
□

Corollary 9.66.1. *Every Sylow subgroup of a finite nilpotent group is normal.*

PROOF:
⟨1⟩1. LET: G be a finite nilpotent group.
⟨1⟩2. LET: P be Sylow subgroup of G
⟨1⟩3. $N_G(P) = N_G(N_G(P))$
PROOF: Proposition 9.53.
⟨1⟩4. $N_G(P) = G$
PROOF: Proposition 9.66.
⟨1⟩5. P is normal.
□

9.8 Symmetric Groups

Proposition 9.67. *Every permutation in S_n is the product of a unique set of disjoint cycles.*

PROOF: Since any permutation acts as a cycle on any of its orbits. □

Corollary 9.67.1. *The transpositions generate S_n.*

PROOF: Since any cycle is a product of transpositions:
$$(a_1\ a_2\ \cdots\ a_n) = (a_1\ a_n) \circ \cdots \circ (a_1\ a_3) \circ (a_1\ a_2)\ .$$ □

Definition 9.68 (Type)**.** For any $\sigma \in S_n$, the *type* of σ is the partition of n consisting of the sizes of the orbits of σ.

Proposition 9.69. *Two permutations in S_n are conjugate if and only if they have the same type.*

PROOF:
⟨1⟩1. Two permutations that are conjugate have the same type.
PROOF: Since
$\tau(a_1\, a_2\, \cdots\, a_r)(b_1\, b_2\, \cdots\, b_s)\cdots(c_1\, c_2\, \cdots\, c_t)tau^{-1} = (\tau(a_1)\, \tau(a_2)\, \cdots\, \tau(a_r))(\tau(b_1)\, \tau(b_2)\, \cdots\, \tau(b_s))\cdots(\tau(c_1)\, \tau(c_2)\, \cdots$
⟨1⟩2. Two permutaitons with the same type are conjugate.
⟨2⟩1. LET: $\rho = (a_1\ a_2\ \cdots\ a_r)(b_1\ b_2\ \cdots\ b_s)\cdots(c_1\ c_2\ \cdots\ c_t)$ and $\sigma = (a'_1\, a'_2\, \cdots\, a'_r)(b'_1\, b'_2\, \cdots\, b'_s)\cdots(c'_1\, c'_2\, \cdots\, c'_t)$
⟨2⟩2. LET: τ be the permutation $\tau(a_i) = a'_i$, $\tau(b_i) = b'_i$, …, $\tau(c_i) = c'_i$
⟨2⟩3. $\sigma = \tau\rho\tau^{-1}$
□

Corollary 9.69.1. *The number of conjugacy classes in S_n equals the number of permutations of n.*

Definition 9.70 (Sign)**.** Define $\Delta_n \in \mathbb{Z}[x_1, \ldots, x_n]$ by

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

Define an action of S_n on $\mathbb{Z}[x_1, \ldots, x_n]$ by

$$\sigma p(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \enspace .$$

The *sign* of a permutation $\sigma \in S_n$ is the number $\epsilon(\sigma) \in \{1, -1\}$ such that

$$\sigma\Delta_n = \epsilon(\sigma)\Delta_n \enspace .$$

We say σ is *even* if $\epsilon(\sigma) = 1$ and *odd* if $\epsilon(\sigma) = -1$.

Proposition 9.71. *ϵ is a group homomorphism $S_n \to \mathbb{Z}^*$.*

PROOF:
⟨1⟩1. LET: $\rho, \sigma \in S_n$
⟨1⟩2. $(\rho \circ \sigma)\Delta_n = \rho(\sigma\Delta_n)$
⟨1⟩3. $\epsilon(\rho \circ \sigma)\Delta_n = \epsilon(\rho)\epsilon(\sigma)\Delta_n$
⟨1⟩4. $\epsilon(\rho \circ \sigma) = \epsilon(\rho)\epsilon(\sigma)$
□

Proposition 9.72. *Let $\sigma = \tau_1 \cdots \tau_r$ where each τ_i is a transposition. Then σ is even if and only if r is even.*

PROOF: Since every transposition is odd and ϵ is a homomorphism, we have $\epsilon(\tau_1 \cdots \tau_r) = (-1)^r$. □

Corollary 9.72.1. *A cycle is even if and only if its length is odd.*

9.9 Alternating Groups

Definition 9.73. Let $n \in \mathbb{N}$. The *alternating group* A_n is the subgroup of S_n consisting of the even permutations.

Proposition 9.74. *For $n \geq 2$ we have A_n is normal in S_n and*

$$[S_n : A_n] = 2 \ .$$

PROOF: Since $\epsilon : S_n \to \{1, -1\}$ is a homomorphism with kernel A_n. □

Proposition 9.75. *j6FAK Let $n \geq 2$ and $\sigma \in A_n$. Let $[\sigma]_{A_n}$ be the conjugacy class of σ in A_n, and $[\sigma]_{S_n}$ the conjugacy class of σ is S_n. Then:*

1. *If $Z_{S_n}(\sigma) \subseteq A_n$ then $|[\sigma]_{S_n}| = 2|[\sigma]_{A_n}|$.*
2. *If not then $[\sigma]_{S_n} = [\sigma]_{A_n}$.*

PROOF:
$\langle 1 \rangle 1.$ $Z_{A_n}(\sigma) = A_n \cap Z_{S_n}(\sigma)$
$\langle 1 \rangle 2.$ $|[\sigma]_{S_n}| = [S_n : Z_{S_n}(\sigma)]$
PROOF: Orbit-Stabilizer Theorem.
$\langle 1 \rangle 3.$ $|[\sigma]_{A_n}| = [A_n : Z_{A_n}(\sigma)]$
PROOF: Orbit-Stabilizer Theorem.
$\langle 1 \rangle 4.$ If $Z_{S_n}(\sigma) \subseteq A_n$ then $|[\sigma]_{S_n}| = 2|[\sigma]_{A_n}|$.
PROOF:

$$\begin{aligned} |[\sigma]_{S_n}| &= [S_n : Z_{S_n}(\sigma)] \\ &= [S_n : A_n][A_n : Z_{S_n}(\sigma)] \\ &= 2|[\sigma]_{A_n}| \end{aligned}$$

$\langle 1 \rangle 5.$ If $Z_{S_n}(\sigma) \nsubseteq A_n$ then $[\sigma]_{S_n} = [\sigma]_{A_n}$.
$\langle 2 \rangle 1.$ ASSUME: $Z_{S_n}(\sigma) \nsubseteq A_n$
$\langle 2 \rangle 2.$ $A_n Z_{S_n}(\sigma) = S_n$
PROOF: Since $A_n \subseteq A_n Z_{S_n}(\sigma)$ and $[S_n : A_n] = 2$.
$\langle 2 \rangle 3.$ $|[\sigma]_{S_n}| = |[\sigma]_{A_n}|$
PROOF:

$$\begin{aligned} |[\sigma]_{S_n}| &= [S_n : Z_{S_n}(\sigma)] \\ &= [A_n Z_{S_n}(\sigma) : Z_{S_n}(\sigma)] \\ &= [A_n : A_n \cap Z_{S_n}(\sigma)] && \text{(Second Isomorphism Theorem)} \\ &= [A_n : Z_{A_n}(\sigma)] \\ &= |[\sigma]_{A_n}| \end{aligned}$$

□

Proposition 9.76. *Let $n \geq 2$. Let $\sigma \in A_n$. Then $|[\sigma]_{S_n}| = 2|[\sigma]_{A_n}|$ if and only if the type of σ consists of distinct odd numbers.*

PROOF:
$\langle 1 \rangle 1.$ If $|[\sigma]_{S_n}| = 2|[\sigma]_{A_n}|$ then the type of σ consists of distinct odd numbers.

⟨2⟩1. If the type of σ has an even number then $Z_{S_n}(\sigma) \nsubseteq A_n$.
PROOF: If $(a_1\ a_2\ \cdots\ a_n)$ is an even cycle that is a factor of σ then $(1\ 2\ \cdots\ n)$ is an odd permutation in $Z_{S_n}(\sigma)$.

⟨2⟩2. If the type of σ has an odd number repeated then $Z_{S_n}(\sigma) \nsubseteq A_n$.
PROOF: If $(a_1\ a_2\ \cdots\ a_n)$ and $(b_1\ b_2\ \cdots\ b_n)$ are two distinct odd factors of σ then $(a_1\ b_1)(a_2\ b_2)\cdots(a_n\ b_n)$ is an odd permutation in $Z_{S_n}(\sigma)$.

⟨2⟩3. Q.E.D.
PROOF: Proposition 9.75

⟨1⟩2. If the type of σ consists of distinct odd numbers then $|[\sigma]_{S_n}| = 2|[\sigma]_{A_n}|$.

⟨2⟩1. LET: $\sigma = (a_{11}\ \cdots\ a_{1\lambda_1})(b_{21}\ \cdots\ b_{2\lambda_2})\cdots(c_{n1}\ \cdots\ c_{n\lambda_n})$ where the λ_i are all odd and distinct.

⟨2⟩2. LET: $\tau \in Z_{S_n}(\sigma)$
PROVE: τ is even.

⟨2⟩3. $(\tau(a_{i1})\ \cdots\ \tau(a_{i\lambda_i})) = (\tau_{i1}\ \cdots\ \tau_{i\lambda_i})$

⟨2⟩4. The action of τ on $\{a_{i1}, \ldots, a_{i\lambda_i}\}$ is $(a_{i1}\ \cdots\ a_{i\lambda_i})^{r_i}$ for some r_i

⟨2⟩5. $\tau = \prod_{i=1}^{n}(a_{i1}\ \cdots\ a_{i\lambda_i})^{r_i}$

⟨2⟩6. τ is even.

$\square$

Chapter 10

Classification of Groups

Example 10.1.

- The only group of order 1 is the trivial group.
- The only group of order 2 is C_2.
- The only group of order 3 is C_3.
- There are two groups of order 4: C_4 and $C_2 \times C_2$.
- The only group of order 5 is C_5.
- There are two groups of order 6: C_6 and S_3.
- The only group of order 7 is C_7.
- There are two groups of order 9: C_9 and $C_3 \times C_3$.
- There are two groups of order 10: C_{10} and D_{10}.
- The only group of order 11 is C_{11}.
- The only group of order 13 is C_{13}.
- There are two groups of order 14: C_{14} and D_{14}.
- The only group of order 15 is C_{15}.

Proposition 10.2. *The only non-Abelian groups of order 8 are D_8 and Q_8.*

PROOF:
$\langle 1 \rangle 1$. LET: G be a non-Abelian group of order 8.
$\langle 1 \rangle 2$. G has no element of order 8.
  PROOF: If it does then it is C_8 and hence Abelian.
$\langle 1 \rangle 3$. PICK an element y of order 4.
  $\langle 2 \rangle 1$. PICK an element a of order 2.
  $\langle 2 \rangle 2$. $G/\langle a \rangle$ is isomorphic to C_4 or $C_2 \times C_2$.
  $\langle 2 \rangle 3$. PICK an element $y\langle a \rangle$ of order 2 in $G/\langle a \rangle$

⟨2⟩4. $y^2 \in \langle a \rangle$
⟨2⟩5. Case:
$y^2 = a$
Proof: In this case y is of order 4.
⟨2⟩6. Case:
$y^2 = e$
Proof: In this case $G \cong C_2^3$ which is Abelian.
⟨1⟩4. Pick $x \notin \langle y \rangle$ such that $x^2 = e$ or $x^2 = y^2$
⟨2⟩1. $G/\langle y \rangle \cong C_2$
⟨2⟩2. Pick $x\langle y \rangle \in G/\langle y \rangle$ of order 2.
⟨2⟩3. $x^2 \in \langle y \rangle$
⟨2⟩4. $x^2 \neq y$ and $x^2 \neq y^3$
⟨2⟩5. $x^2 = e$ or $x^2 = y^2$
⟨1⟩5. $xy = y^3 x$
⟨2⟩1. $xy \neq e$
Proof: Since $y^{-1} = y^3 \neq x$.
⟨2⟩2. $xy \neq y$
Proof: $xy = y$ implies $x = e$.
⟨2⟩3. $xy \neq y^2$
Proof: $xy = y^2$ implies $x = y$.
⟨2⟩4. $xy \neq y^3$
Proof: $xy = y^3$ implies $x = y^2$.
⟨2⟩5. $xy \neq x$
Proof: $xy = x$ implies $y = e$.
⟨2⟩6. $xy \neq yx$
Proof: $xy = yx$ implies G is Abelian.
⟨2⟩7. $xy \neq y^2 x$
⟨3⟩1. Assume: for a contradiction $xy = y^2 x$
⟨3⟩2. $xy^2 = x$
Proof:

$$\begin{aligned} xy^2 &= y^2 xy \\ &= y^4 x \\ &= x \end{aligned}$$

⟨3⟩3. $y^2 = e$
⟨1⟩6. The multiplication table of G is one of the following.

e	y	y^2	y^3	x	yx	y^2x	y^3x
y	y^2	y^3	e	yx	y^2x	y^3x	x
y^2	y^3	e	y	y^2x	y^3x	x	yx
y^3	e	y	y^2	y^3x	x	yx	y^2x
x	y^3x	y^2x	yx	e	y^3	y^2	y
yx	x	y^3x	y^2x	y	e	y^3	y^2
y^2x	yx	x	y^3x	y^2	y	e	y^3
y^3x	y^2x	yx	x	y^3	y^2	y	e

e	y	y^2	y^3	x	yx	y^2x	y^3x
y	y^2	y^3	e	yx	y^2x	y^3x	x
y^2	y^3	e	y	y^2x	y^3x	x	yx
y^3	e	y	y^2	y^3x	x	yx	y^2x
x	y^3x	y^2x	yx	y^2	y	e	y^3
yx	x	y^3x	y^2x	y^3	y^2	y	e
y^2x	yx	x	y^3x	e	y^3	y^2	y
y^3x	y^2x	yx	x	y	e	y^3	y^2

$\langle 1\rangle 7.$ $G \cong D_8$ or $G \cong Q_8$.
$\square$

Proposition 10.3. *Let q be an odd prime. Then D_{2q} is the only non-Abelian group of order $2q$.*

PROOF:
$\langle 1\rangle 1.$ LET: G be a non-Abelian group of order $2q$.
$\langle 1\rangle 2.$ PICK $y \in G$ of order q.
PROOF: Cauchy's Theorem
$\langle 1\rangle 3.$ $\langle y\rangle$ is the only subgroup of order q.
PROOF: Third Sylow Theorem
$\langle 1\rangle 4.$ $\langle y\rangle$ is normal.
$\langle 1\rangle 5.$ PICK $x \in G - \langle y\rangle - \{e\}$
$\langle 1\rangle 6.$ $|x| = 2$
PROOF: We cannot have $|x| = 2q$ since G is not cyclic, and $|x| \neq q$ since $\langle x\rangle$ is not the subgroup of order q.
$\langle 1\rangle 7.$ $xyx^{-1} \in \langle y\rangle$
PROOF: Since $x\langle y\rangle x^{-1} = \langle y\rangle$ by $\langle 1\rangle 3$.
$\langle 1\rangle 8.$ PICK r such that $0 \leq r < q$ and $xyx^{-1} = y^r$.
$\langle 1\rangle 9.$ $y^{r^2} = y$
PROOF:

$$\begin{aligned} y^{r^2} &= (xyx^{-1})^r && (\langle 1\rangle 8) \\ &= xy^r x^{-1} \\ &= x^2 y x^{-2} && (\langle 1\rangle 8) \\ &= y && (\langle 1\rangle 6) \end{aligned}$$

$\langle 1\rangle 10.$ $q \mid (r-1)(r+1)$
PROOF: Since $y^{(r-1)(r+1)} = e$ and $|y| = q$ by $\langle 1\rangle 2$.
$\langle 1\rangle 11.$ $r = 1$ or $r = q-1$
PROOF: Since $0 \leq r < q$ by $\langle 1\rangle 8$.
$\langle 1\rangle 12.$ $r \neq 1$
$\langle 2\rangle 1.$ ASSUME: for a contradiction $r = 1$.
$\langle 2\rangle 2.$ $xy = yx$
PROOF: $\langle 1\rangle 8$
$\langle 2\rangle 3.$ $|xy| = 2q$
PROOF: Proposition 6.22
$\langle 2\rangle 4.$ G is cyclic.
$\langle 2\rangle 5.$ Q.E.D.

PROOF: This contradicts ⟨1⟩1.
⟨1⟩13. $x^2 = e$ and $y^q = e$ and $yx = xy^{q-1}$
⟨1⟩14. $G \cong D_{2q}$
□

Corollary 10.3.1. *For q an odd prime, the only groups of order $2q$ are C_{2q} and D_{2q}.*

Proposition 10.4. *There is no non-Abelian simple group of order less than 60.*

PROOF:We rule out the other sizes as follows:

- 1 — Only group is the trivial group.
- 2 — Prime therefore cyclic
- 3 — Prime therefore cyclic
- 4 — Corollary 9.48.1
- 5 — Prime therefore cyclic
- 6 — Corollary 9.51.2
- 7 — Prime therefore cyclic
- 8 — Corollary 9.48.1
- 9 — Corollary 9.48.1
- 10 — Corollary 9.51.2
- 11 — Prime therefore cyclic
- 12 —

  ⟨1⟩1. There is no simple non-Abelian group of order 12.
  ⟨2⟩1. ASSUME: for a contradiction G is a simple non-Abelian group of order 12.
  ⟨2⟩2. G has 4 3-Sylow subgroups.
  ⟨2⟩3. G has 8 elements of order 3.
  ⟨2⟩4. G has 3 elements of order 2 or 4.
  ⟨2⟩5. G has one 2-Sylow subgroup.
  ⟨2⟩6. The 2-Sylow subgroup of G is normal.
  ⟨2⟩7. Q.E.D.
  PROOF: This contradicts ⟨2⟩1.

- 13 — Prime therefore cyclic
- 14 — Corollary 9.51.2
- 15 — Corollary 9.51.2

- 16 — Corollary 9.48.1
- 17 — Prime therefore cyclic
- 18 — Corollary 9.51.2
- 19 — Prime therefore cyclic
- 20 — Corollary 9.51.2
- 21 — Corollary 9.51.2
- 22 — Corollary 9.51.2
- 23 — Prime therefore cyclic
- 24 —

  $\langle 1\rangle 2$. There is no simple non-Abelian group of order 24.

  $\langle 2\rangle 1$. Assume: for a contradiction G is a simple non-Abelian group of order 24.
  $\langle 2\rangle 2$. G has 3 2-Sylow subgroups.
  $\langle 2\rangle 3$. Let: $\gamma : G \to S_3$ be the action of conjugation of G on the set of 2-Sylow subgroups.
  $\langle 2\rangle 4$. $\ker \gamma \neq \{e\}$
  Proof: γ cannot be injective since $|G| > |S_3|$.
  $\langle 2\rangle 5$. $\ker \gamma \neq G$
  $\langle 2\rangle 6$. $\ker \gamma$ is a proper non-trivial normal subgroup of G.
  $\langle 2\rangle 7$. Q.E.D.
  Proof: This contradicts $\langle 2\rangle 1$.

- 25 — Corollary 9.48.1
- 26 — Corollary 9.51.2
- 27 — Corollary 9.48.1
- 28 — Corollary 9.51.2
- 29 — Prime therefore cyclic
- 30 — Proposition 9.54
- 31 — Prime therefore cyclic
- 32 — Corollary 9.48.1
- 33 — Corollary 9.51.2
- 34 — Corollary 9.51.2
- 35 — Corollary 9.51.2

- 36 —

  ⟨1⟩3. There is no simple non-Abelian group of order 36.

  ⟨2⟩1. Assume: for a contradiction G is a simple non-Abelian group of order 36.
  ⟨2⟩2. G has 4 3-Sylow subgroups.
  ⟨2⟩3. Let: $\gamma : G \to S_4$ be the action of conjugation of G on the set of 2-Sylow subgroups.
  ⟨2⟩4. $\ker \gamma \neq \{e\}$
  Proof: γ cannot be injective since $|G| > |S_4|$.
  ⟨2⟩5. $\ker \gamma \neq G$
  ⟨2⟩6. $\ker \gamma$ is a proper non-trivial normal subgroup of G.
  ⟨2⟩7. Q.E.D.
  Proof: This contradicts ⟨2⟩1.

- 37 — Prime therefore cyclic
- 38 — Corollary 9.51.2
- 39 — Corollary 9.51.2
- 40 — There can be only 1 5-Sylow subgroup.
- 41 — Prime therefore cyclic
- 42 — Proposition 9.54
- 43 — Prime therefore cyclic
- 44 — Corollary 9.51.2
- 45 — There can be only 1 5-Sylow subgroup.
- 46 — Corollary 9.51.2
- 47 — Prime therefore cyclic
- 48 —

  ⟨1⟩4. There is no simple non-Abelian group of order 48.

  ⟨2⟩1. Assume: for a contradiction G is a simple non-Abelian group of order 48.
  ⟨2⟩2. G has 3 2-Sylow subgroups.
  ⟨2⟩3. Let: $\gamma : G \to S_3$ be the action of conjugation of G on the set of 2-Sylow subgroups.
  ⟨2⟩4. $\ker \gamma \neq \{e\}$
  Proof: γ cannot be injective since $|G| > |S_3|$.
  ⟨2⟩5. $\ker \gamma \neq G$
  ⟨2⟩6. $\ker \gamma$ is a proper non-trivial normal subgroup of G.
  ⟨2⟩7. Q.E.D.
  Proof: This contradicts ⟨2⟩1.

- 49 — Corollary 9.48.1
- 50 — Corollary 9.51.2
- 51 — Corollary 9.51.2
- 52 — Corollary 9.51.2
- 53 — Prime therefore cyclic
- 54 — Corollary 9.51.2
- 55 — Corollary 9.51.2
- 56 — Corollary 9.51.2
- 57 — Corollary 9.51.2
- 58 — Corollary 9.51.2
- 59 — Prime therefore cyclic

Proposition 10.5. *Every simple group of order 60 has a subgroup of index 5.*

Proof:
⟨1⟩1. Let: G be a simple group of order 60.
⟨1⟩2. The number of 2-Sylow subgroups of G is either 5 or 15.
⟨2⟩1. Let: n be the number of 2-Sylow subgroups.
⟨2⟩2. $60|n!$
Proof: Corollary 9.55.1.
⟨2⟩3. $n \geq 5$
⟨2⟩4. $n \mid 15$
Proof: Third Sylow Theorem
⟨2⟩5. $n = 5$ or $n = 15$
⟨1⟩3. Assume: w.l.o.g. G has 15 2-Sylow subgroups.
⟨1⟩4. G has 4 or 10 3-Sylow subgroups.
⟨1⟩5. G has 10 3-Sylow subgroups.
Proof: Corollary 9.55.1.
⟨1⟩6. G has exactly 6 5-Sylow subgroups.
⟨1⟩7. The number of elements of order 3 is 20.
⟨1⟩8. The number of elements of order 5 is 24.
⟨1⟩9. The number of elements of order 2 or 4 is 15.
⟨1⟩10. Pick two 2-Sylow subgroups H_1 and H_2 with non-trivial intersection.
⟨1⟩11. Let: $g \in G$ be such that $H_1 \cap H_2 = \{e, g\}$.
⟨1⟩12. Let: $K = Z_G(H_1 \cap H_2)$
⟨1⟩13. $|K| = 12$ or $|K| = 20$
Proof: We have $4 \mid |K|$ since $H_1 \leq K$, and $|K| \geq 6$ since $H_1 \cup H_2 \subseteq K$. We also have $|K| \mid 60$.
⟨1⟩14. $[G : K] \neq 3$
Proof: There cannot be an embedding of G in S_3.

⟨1⟩15. $[G : K] = 5$
□

Proposition 10.6. *There is no non-Abelian simple group of order between 60 and 168.*

Proof: We rule out the other sizes as follows:

- 61 — prime therefore cyclic
- 62 — Corollary 9.51.2
- 63 — Corollary 9.51.1
- 64 — Corollary 9.48.1
- 65 — Corollary 9.51.2
- 66 — Corollary 9.51.2
- 67 — prime therefore cyclic
- 68 — Corollary 9.51.2
- 69 — Corollary 9.51.2
- 70 — Proposition 9.54
- 71 — prime therefore cyclic
- 72

  ⟨1⟩1. There is no simple non-Abelian group of order 72

  Proof:
  ⟨2⟩1. Assume: for a contradiction G is a simple non-Abelian group of order 72.
  ⟨2⟩2. G has 4 3-Sylow subgroups.
  ⟨2⟩3. Let: $\gamma : G \to S_4$ be the action of conjugation on the set of 3-Sylow subgroups.
  ⟨2⟩4. $\ker \gamma \neq 1$
  Proof: Since $|G| > |S_4|$.
  ⟨2⟩5. $\ker \gamma$ is a non-trivial proper subgroup of G.
  ⟨2⟩6. Q.E.D.
  Proof: This is a contradiction.

- 73 — prime therefore cyclic
- 74 — Corollary 9.51.2
- 75 — Corollary 9.51.2
- 76 — Corollary 9.51.2

- 77 — Corollary 9.51.2
- 78 — Corollary 9.51.2
- 79 — prime therefore cyclic
- 80

  ⟨1⟩2. There is no simple non-Abelian group of order 80.

  Proof:
  ⟨2⟩1. Assume: for a contradiction G is a simple non-Abelian group of order 80.
  ⟨2⟩2. G has 5 2-Sylow subgroups.
  ⟨2⟩3. Let: $\gamma : G \to S_5$ be the action of conjugation on the set of 2-Sylow subgroups.
  ⟨2⟩4. $\ker \gamma \neq 1$
  Proof: Otherwise $\operatorname{im} \gamma$ would be a subgroup of S_5 of order 80, contradicting Lagrange's Theorem.
  ⟨2⟩5. $\ker \gamma$ is a non-trivial normal subgroup of G.
  ⟨2⟩6. Q.E.D.
  Proof: This is a contradiction.

- 81 — Corollary 9.48.1
- 82 — Corollary 9.51.2
- 83 — prime therefore cyclic
- 84 — Corollary 9.51.1
- 85 — Corollary 9.51.2
- 86 — Corollary 9.51.2
- 87 — Corollary 9.51.2
- 88 — Corollary 9.51.2
- 89 — prime therefore cyclic
- 90 — Corollary 9.51.1
- 91 — Corollary 9.51.2
- 92 — Corollary 9.51.2
- 93 — Corollary 9.51.2
- 94 — Corollary 9.51.2
- 95 — Corollary 9.51.2

- 96 — There are 3 2-Sylow subgroups. The kernel of the action of conjugation $G \to S_3$ is a non-trivial normal subgroup of G.
- 97 — prime therefore cyclic
- 98 — Corollary 9.51.2
- 99 — Corollary 9.51.2
- 100 — Corollary 9.51.2
- 101 — prime therefore cyclic
- 102 — Proposition 9.54
- 103 — prime therefore cyclic
- 104 — Corollary 9.51.2
- 105 — Proposition 9.54
- 106 — Corollary 9.51.2
- 107 — prime therefore cyclic
- 108 — There are 4 3-Sylow subgroups. The kernel of the action of conjugation $G \to S_4$ is a non-trivial normal subgroup of G.
- 109 — prime therefore cyclic
- 110 — Proposition 9.54
- 111 — Corollary 9.51.2
- 112

  $\langle 1 \rangle 3.$ There is no simple non-Abelian group of order 112.

  $\langle 2 \rangle 1.$ Assume: for a contradiction G is a simple non-Abelian group of order 112.

  $\langle 2 \rangle 2.$ G has exactly 7 2-Sylow subgroups.

  $\langle 2 \rangle 3.$ Let: $\gamma : G \to A_7$ be the action of conjugation of G on the set of 2-Sylow subgroups.

  Proof: $\gamma(g)$ is always an even permutation since G has no subgroup of index 2.

  $\langle 2 \rangle 4.$ $\ker \gamma \neq 1$

  Proof: Since $|G|$ does not divide $|A_7| = 7!/2$.

  $\langle 2 \rangle 5.$ $\ker \gamma$ is a non-trivial normal subgroup of G.

  $\langle 2 \rangle 6.$ Q.E.D.
- 113 — prime therefore cyclic
- 114 — Proposition 9.54

- 115 — Corollary 9.51.2
- 116 — Corollary 9.51.2
- 117 — Corollary 9.51.2
- 118 — Corollary 9.51.2
- 119 — Corollary 9.51.2
- 120

  ⟨1⟩4. There is no simple non-Abelian group of order 120.

  Proof:
  ⟨2⟩1. Assume: for a contradiction G is a simple non-Abelian group of order 120.
  ⟨2⟩2. There are exactly 6 5-Sylow subgroups.
  ⟨2⟩3. Let: $\gamma : G \to A_6$ be the action of conjugation on the set of 5-Sylow subgroups.
  ⟨2⟩4. $\operatorname{im}\gamma$ is a subgroup of A_6 of order 120.
  ⟨2⟩5. Q.E.D.
  Proof: This is a contradiction by inspection of the list of subgroups of A_6.

- 121 — Corollary 9.48.1
- 122 — Corollary 9.51.2
- 123 — Corollary 9.51.2
- 124 — Corollary 9.51.2
- 125 — Corollary 9.48.1
- 126 — Corollary 9.51.1
- 127 — prime therefore cyclic
- 128 — Corollary 9.48.1
- 129 — Corollary 9.51.2
- 130 — Proposition 9.54
- 131 — prime therefore cyclic
- 132

  ⟨1⟩5. There is no simple non-Abelian group of order 132.

  ⟨2⟩1. Assume: for a contradiction G is a simple non-Abelian group of order 132.
  ⟨2⟩2. There are at least 4 3-Sylow subgroups.

⟨2⟩3. There are at least 8 elements of order 3.
⟨2⟩4. There are exactly 12 11-Sylow subgroups.
⟨2⟩5. There are exactly 120 elements of order 11.
⟨2⟩6. There are exactly 3 elements of order 2.
⟨2⟩7. There is a unique 2-Sylow subgroups.
⟨2⟩8. Q.E.D.
PROOF: This is a contradiction.

- 133 — Corollary 9.51.2
- 134 — Corollary 9.51.2
- 135 — Corollary 9.51.1
- 136 — Corollary 9.51.2
- 137 — prime therefore cyclic
- 138 — Proposition 9.54
- 139 — prime therefore cyclic
- 140 — Corollary 9.51.1
- 141 — Corollary 9.51.2
- 142 — Corollary 9.51.2
- 143 — Corollary 9.51.2
- 144 — Burnside's Theorem
- 145 — Burnside's Theorem
- 146 — Burnside's Theorem
- 147 — Burnside's Theorem
- 148 — Burnside's Theorem
- 149 — prime therefore cyclic
- 150 — There are exactly 6 5-Sylow subgroups. The kernel of the action of conjugation $G \to A_5$ is a non-trivial normal subgroup since 150 does not divide $|A_5| = 60$.
- 151 — prime therefore cyclic
- 152 — Burnside's Theorem
- 153 — Burnside's Theorem
- 154 — Proposition 9.54

- 155 — Burnside's Theorem
- 156 — Corollary 9.51.2
- 157 — prime therefore cyclic
- 158 — Burnside's Theorem
- 159 — Burnside's Theorem
- 160 — Burnside's Theorem
- 161 — Burnside's Theorem
- 162 — Burnside's Theorem
- 163 — prime therefore cyclic
- 164 — Burnside's Theorem
- 165 — Proposition 9.54
- 166 — Burnside's Theorem
- 167 — prime therefore cyclic

Proposition 10.7. *Every group of order* < 120 *and* $\neq 60$ *is solvable.*

PROOF:
⟨2⟩1. LET: G be a group of order n where $n < 120$ and $n \neq 60$.
⟨2⟩2. If n is odd then G is solvable.
PROOF: Feit-Thompson Theorem
⟨2⟩3. If n has at most two prime factors then G is solvable.
PROOF: Burnside's Theorem
⟨2⟩4. CASE: $n = pqr$ for some primes p, q, r
PROOF: Its composition factors must be C_p, C_q and C_r.
⟨2⟩5. CASE: $n = 84$
PROOF: By the Third Sylow Theorem, the 7-Sylow subgroup is normal. Since every group of order 12 is solvable, so is every group of order 84.
□

Part IV

Ring Theory

Chapter 11

Rngs

Definition 11.1 (Ring)**.** A *rng* consists of a set R and binary operations $+, \cdot :$ $R^2 \to R$ such that:

- $(R, +)$ is an Abelian group
- $\cdot$ is associative.
- The *distributive properties* hold: for all $r, s, t \in R$ we have

$$(r+s)t = rt + st, \qquad r(s+t) = rs + rt \ .$$

Example 11.2.

- The *zero rng* is $\{0\}$.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are rngs.
- $2\mathbb{Z}$ is a rng.
- Given a rng R and natural number n, then the set $\mathfrak{gl}_n(R)$ of all $n \times n$ matrices with entries in R is a rng under matrix addition and matrix multiplication.
- For any set S, the power set $\mathcal{P}S$ is a rng under $A+B = (A \cup B) - (A \cap B)$ and $AB = A \cap B$.
- Given a rng R and a set S, then R^S is a rng under $(f+g)(s) = f(s)+g(s)$ and $(fg)(s) = f(s)g(s)$ for all $f, g \in R^S$ and $s \in S$.
- The set $\mathfrak{sl}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) : \operatorname{tr} M = 0\}$ is a rng.
- The set $\mathfrak{sl}_n(\mathbb{C}) = \{M \in \mathfrak{gl}_n(\mathbb{C}) : \operatorname{tr} M = 0\}$ is a rng.
- $\mathbb{Z}/n\mathbb{Z}$ is a rng.

- The ring $\mathbb{H}$ of *quaternions* is $\mathbb{R}^4$ under the following operations, where we write (a, b, c, d) as $a + bi + cj + dk$:

$$\begin{aligned}(a+bi+cj+dk)+(a'+b'i+c'j+d'k) &= (a+a')+(b+b')i \\ &\quad + (c+c')j+(d+d')k \\ (a+bi+cj+dk)(a'+b'i+c'j+d'k) &= (aa'-bb'-cc'-dd') \\ &\quad + (ab'+ba'+cd'-dc')i \\ &\quad + (ac'-bd'+ca'+db')j \\ &\quad + (ad'+bc'-cb'+da')k\end{aligned}$$

- For any Abelian group G, the set $\mathrm{End}_{\mathbf{Ab}}(G)$ is a ring under pointwise addition and composition.

Proposition 11.3. *In any rng R we have*

$$\forall x \in R. x0 = 0x = 0 \enspace .$$

Proof:

$$\begin{aligned} x0 &= x(0+0) \\ &= x0 + x0 \end{aligned}$$

and so $x0 = 0$ by Cancellation. Similarly $0x = 0$. ∎

Definition 11.4 (Zero Divisor)**.** Let R be a rng and $a \in R$.

Then a is a *left-zero-divisor* iff there exists $b \in R - \{0\}$ such that $ab = 0$.

The element a is a *right-zero-divisor* iff there exists $b \in R - \{0\}$ such that $ba = 0$.

Example 11.5. 0 is a left- and right-zero-divisor in every non-zero rng.

The zero rng is the only ring with no zero-divisors.

Proposition 11.6. *Let R be a rng and $a \in R$. Then a is not a left-zero-divisor if and only if left multiplication by a is an injective function $R \to R$.*

Proof:

$\langle 1 \rangle 1.$ If a is not a left-zero-divisor then left multiplication by a is injective.
  $\langle 2 \rangle 1.$ Assume: a is not a left-zero-divisor.
  $\langle 2 \rangle 2.$ Let: $ab = ac$
  $\langle 2 \rangle 3.$ $a(b - c) = 0$
  $\langle 2 \rangle 4.$ $b - c = 0$
  $\langle 2 \rangle 5.$ $b = c$
$\langle 1 \rangle 2.$ If a is a left-zero-divisor then left multiplication by a is not injective.
  $\langle 2 \rangle 1.$ Pick $b \neq 0$ such that $ab = 0$.
  $\langle 2 \rangle 2.$ $ab = a0$ but $b \neq 0$

∎

11.1 Commutative Rngs

Definition 11.7 (Commutative)**.** A rng R is *commutative* iff $\forall x, y \in R. xy = yx$.

Example 11.8.

- The zero rng is commutative.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are commutative.
- $2\mathbb{Z}$ is commutative.
- $\mathfrak{gl}_2(\mathbb{R})$ is not commutative.
- For any set S, the rng $\mathcal{P}S$ is commutative.
- If R is commutative then R^S is commutative.

11.2 Rng Homomorphisms

Definition 11.9. Let R and S be rngs. A *rng homomorphism* $\phi : R \to S$ is a function such that, for all $x, y \in R$, we have

$$\phi(x+y) = \phi(x) + \phi(y)$$
$$\phi(xy) = \phi(x)\phi(y)$$

Let **Rng** be the category of rngs and rng homomorphisms.

11.3 Quaternions

Definition 11.10 (Norm)**.** The *norm* of a quaternion is defined by

$$N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2 \quad .$$

Chapter 12

Rings

Definition 12.1 (Ring)**.** A *ring* R is a rng such that there exists $1 \in R$, the *multiplicative identity*, such that

$$\forall x \in R . x1 = 1x = x \ .$$

Example 12.2.

- The zero rng is a ring with $1 = 0$.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are rngs.
- $2\mathbb{Z}$ is not a ring.
- If R is a ring then $\mathfrak{gl}_n(R)$ is a ring.
- For any set S, the rng $\mathcal{P}S$ is a ring with $1 = S$.
- If R is a ring then R^S is a ring.
- $\mathfrak{sl}_n(\mathbb{R})$ is not a ring for $n > 0$.
- $\mathfrak{sl}_n(\mathbb{C})$ is not a ring for $n > 0$.
- $\mathfrak{so}_n(\mathbb{R}) = \{M \in \mathfrak{sl}_n(\mathbb{R}) : M + M^T = 0\}$ is not a ring.
- $\mathbb{Z}/n\mathbb{Z}$ is a ring.

Proposition 12.3. *In any ring R, if $0 = 1$ then R is the zero ring.*

Proof: For any $x \in R$ we have $x = 1x = 0x = 0$. ∎

Proposition 12.4. *In any ring we have $(-1)x = -x$.*

Proof: Since

$$\begin{aligned} x + (-1)x &= 1x + (-1)x \\ &= (1 + (-1))x \\ &= 0x \\ &= 0 \end{aligned}$$ ∎

12.1 Units

Definition 12.5 (Left-Unit, Right-Unit)**.** Let R be a ring and $a \in R$. Then a is a *left-unit* iff there exists $b \in R$ such that $ab = 1$. The element a is a *right-unit* iff there exists $b \in R$ such that $ba = 1$.

An element is a *unit* iff it is a left-unit and a right-unit.

Proposition 12.6. *Let R be a ring and $a \in R$. Then a is a left-unit iff left multiplication by a is a surjective function $R \to R$.*

PROOF:
$\langle 1 \rangle 1$. If a is a left-unit then left multiplication by a is surjective.
  $\langle 2 \rangle 1$. PICK $b \in R$ such that $ab = 1$.
  $\langle 2 \rangle 2$. For all $c \in R$ we have $c = a(bc)$.
$\langle 1 \rangle 2$. If left multiplication by a is surjective then a is a left-unit.
  PROOF: Immediate.
□

Proposition 12.7. *Let R be a ring and $a \in R$. Then a is a right-unit iff right multiplication by a is a surjective function $R \to R$.*

PROOF: Similar. □

Proposition 12.8. *No left-unit is a right-zero-divisor.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: for a contradiction $ab = 1$ and $ca = 0$ where $c \neq 0$.
$\langle 1 \rangle 2$. $c = 0$
  PROOF:

$$\begin{aligned} 0 &= 0b \\ &= cab \\ &= c1 \\ &= c \end{aligned}$$

$\langle 1 \rangle 3$. Q.E.D.
  PROOF: This is a contradiction.
□

Proposition 12.9. *No right-unit is a left-zero-divisor.*

PROOF: Similar. □

Proposition 12.10. *The inverse of a unit is unique.*

PROOF: If $ba = 1$ and $ac = 1$ then $b = bac = c$. □

Proposition 12.11. *The units of a ring form a group under multiplication.*

PROOF:
$\langle 1 \rangle 1$. If a and b are units then ab is a unit.
  PROOF: We have $b^{-1}a^{-1}ab = 1$ and $abb^{-1}a^{-1} = 1$.

$\langle 1 \rangle 2$. 1 is a unit.
 PROOF: Since $1 \cdot 1 = 1$.
$\langle 1 \rangle 3$. If a is a unit then its inverse is a unit.
 PROOF: Immediate from definitions.
□

Definition 12.12 (Group of Units)**.** For any ring R, we write R^* for the group of the units of R under multiplication.

Example 12.13. The quaternionic group is a subgroup of $\mathbb{H}^*$.

Example 12.14. The norm is a group homomorphism $\mathbb{H}^* \rightarrow \mathbb{R}^+$ where $\mathbb{R}^+$ is the group of positive real numbers under multiplication with kernel isomorphic to $\mathrm{SU}_2(\mathbb{C})$. The isomorphism maps a quaternion $a + bi + cj + dk$ to $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$.

Theorem 12.15 (Fermat's Little Theorem)**.** *Let p be a prime number and a any integer. Then $a^p \equiv a (\bmod p)$.*

PROOF: If $p \mid a$ then $a^p \equiv a \equiv 0 (\bmod p)$. Otherwise, we have $a^{p-1} \equiv 1 (\bmod p)$ by applying Lagrange's Theorem to $(\mathbb{Z}/p\mathbb{Z})^*$. □

Example 12.16. It is not true that, if $n \mid |G|$, then G has a subgroup of order n. The group A_4 has order 12 but no subgroup of order 6.

Proposition 12.17. *If p is prime then $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.*

PROOF:
$\langle 1 \rangle 1$. LET: g be an element of maximal order in $(\mathbb{Z}/p\mathbb{Z})^*$.
$\langle 1 \rangle 2$. For all $h \in (\mathbb{Z}/p\mathbb{Z})^*$ we have $h^{|g|} = 1$.
 PROOF: Proposition 8.10.
$\langle 1 \rangle 3$. There are at most $|g|$ elements x such that $x^{|g|} = 1$ in $\mathbb{Z}/p\mathbb{Z}$
$\langle 1 \rangle 4$. $p - 1 \leq |g|$
$\langle 1 \rangle 5$. $|g| = p - 1$
$\langle 1 \rangle 6$. g generates $(\mathbb{Z}/p\mathbb{Z})^*$.
□

Example 12.18. $(\mathbb{Z}/12\mathbb{Z})^*$ is not cyclic. Its elements are 1, 5, 7 and 11 with orders 1, 2, 2 and 2.

Theorem 12.19 (Wilson's Theorem)**.** *A positive integer p is prime if and only if $(p-1)! \equiv 1 (\bmod p)$.*

$\langle 1 \rangle 1$. If p is prime then $(p-1)! \equiv 1 (\bmod p)$.
 $\langle 2 \rangle 1$. ASSUME: p is prime.
 $\langle 2 \rangle 2$. $(p-1)!$ is the product of all the elements of $(\mathbb{Z}/p\mathbb{Z})^*$
 $\langle 2 \rangle 3$. The only element of $(\mathbb{Z}/p\mathbb{Z})^*$ with order 2 is -1.
 $\langle 2 \rangle 4$. $(p-1)! \equiv -1 (\bmod p)$
  PROOF: Proposition 6.23.

$\langle 1\rangle 2$. If $(p-1)! \equiv -1 (\bmod p)$ then p is prime.
$\langle 2\rangle 1$. ASSUME: (
$(p-1)! \equiv -1 (\bmod p)$)
$\langle 2\rangle 2$. LET: d be a proper divisor of p.
PROVE: $d = 1$
$\langle 2\rangle 3$. $d \mid (p-1)!$
$\langle 2\rangle 4$. $d \mid 1$
PROOF: Since $d \mid p \mid (p-1)! + 1$.
$\langle 2\rangle 5$. $d = 1$
□

Proposition 12.20. *If p and q are distinct odd primes then $(\mathbb{Z}/pq\mathbb{Z})^*$ is not cyclic.*

PROOF:
$\langle 1\rangle 1$. $|(\mathbb{Z}/pq\mathbb{Z})^*| = (p-1)(q-1)$
$\langle 1\rangle 2$. LET: $g \in (\mathbb{Z}/pq\mathbb{Z})^*$
PROVE: g does not have order $(p-1)(q-1)$
$\langle 1\rangle 3$. $g^{(p-1)(q-1)/2} \equiv 1 (\bmod p)$
$\langle 1\rangle 4$. $g^{(p-1)(q-1)/2} \equiv 1 (\bmod q)$
$\langle 1\rangle 5$. $pq \mid g^{(p-1)(q-1)/2} - 1$
$\langle 1\rangle 6$. $g^{(p-1)(q-1)/2} \equiv 1 (\bmod pq)$
$\langle 1\rangle 7$. $|g| \mid (p-1)(q-1)/2$
□

Proposition 12.21. *For any prime p, we have $\mathrm{Aut}_{\mathbf{Grp}}(C_p) \cong C_{p-1}$.*

PROOF:
$\langle 1\rangle 1$. LET: $\phi : \mathrm{Aut}_{\mathbf{Grp}}(C_p) \to (\mathbb{Z}/p\mathbb{Z})^*$ be the function $\phi(\alpha) = \alpha(1)$.
PROOF: $\alpha(1)$ has order p in C_p and so is coprime with p.
$\langle 1\rangle 2$. ϕ is a homomorphism.
PROOF: $\phi(\alpha \circ \beta) = \alpha(\beta(1)) = \alpha(\beta(1)1) = \beta(1)\alpha(1) = \phi(\alpha)\phi(\beta)$
$\langle 1\rangle 3$. ϕ is injective.
PROOF: If $\phi(\alpha) = \phi(\beta)$ then for any n we have $\alpha(n) = n\alpha(1) = n\phi(\alpha) = n\phi(\beta) = n\beta(1) = \beta(n)$.
$\langle 1\rangle 4$. ϕ is surjective.
PROOF: For any $r \in (\mathbb{Z}/p\mathbb{Z})^*$ we have $r = \phi(\alpha)$ where $\alpha(n) = nr \bmod p$.
$\langle 1\rangle 5$. $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$
□

12.2 Euler's ϕ-function

Proposition 12.22. *For n a positive integer, we have $(\mathbb{Z}/n\mathbb{Z})^* = \{m \in \mathbb{Z}/n\mathbb{Z} : \gcd(m, n) = 1\}$.*

PROOF:

$$\begin{aligned} m \in (\mathbb{Z}/n\mathbb{Z})^* &\Leftrightarrow \exists a.am \equiv 1 (\operatorname{mod} n) \\ &\Leftrightarrow \exists a, b.am + bn = 1 \\ &\Leftrightarrow \gcd(m, n) = 1 \end{aligned} \qquad \square$$

Definition 12.23 (Euler's Totient Function)**.** For n a positive integer, let $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.

Proposition 12.24. *If n is an odd positive integer then $\phi(2n) = \phi(n)$.*

PROOF:
⟨1⟩1. LET: n be an odd positive integer.
⟨1⟩2. For any integer m, if $\gcd(m, n) = 1$ then $\gcd(2m + n, 2n) = 1$
PROOF: For p a prime, if $p \mid 2m + n$ and $p \mid 2n$ then $p \neq 2$ (since $2m + n$ is odd) so $p \mid n$ and hence $p \mid m$, which is a contradiction.
⟨1⟩3. For any integer r, if $\gcd(r, 2n) = 1$ then $\gcd(\frac{r+n}{2}, n) = 1$
PROOF: If $p \mid n$ and $p \mid \frac{r+n}{2}$ then $p \mid r + n$ so $p \mid r$ which is a contradiction.
⟨1⟩4. The function that maps m to $2m + n$ is a bijection between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$.
$\square$

Theorem 12.25. *For any positive integer n we have*

$$\sum_{m>0, m|n} \phi(m) = n \enspace .$$

PROOF:
⟨1⟩1. Define $\chi : \{0, 1, \dots, n-1\} \to \{(m, d) : m > 0, m \mid n, d \text{ generates } \langle n/m \rangle\}$ by: $\chi(x) = (\gcd(x, n), x)$.
⟨1⟩2. χ is injective.
⟨1⟩3. χ is surjective.
PROOF: Given (m, d) such that d generates $\langle n/m \rangle$ we have $\chi(d) = (m, d)$.
⟨1⟩4. $n = \sum_{m>0, m|n} \phi(m)$
PROOF: Since $\langle n/m \rangle \cong C_m$ and so has $\phi(m)$ generators.
$\square$

Proposition 12.26. *For any positive integers a and n, we have $n \mid \phi(a^n - 1)$.*

PROOF: Since the order of a is n in $(\mathbb{Z}/(a^n - 1)\mathbb{Z})^*$. $\square$

Theorem 12.27 (Euler's Theorem)**.** *For any coprime integers a and n we have $a^{\phi(n)} \equiv a (\operatorname{mod} n)$.*

PROOF: Immediate from Lagrange's Theorem. $\square$

Proposition 12.28.

$$|\mathrm{Aut}_{\mathbf{Grp}}(C_n)| = \phi(n)$$

PROOF: An automorphism α is determined by $\alpha(1)$ which is any element of order n, and g has order n iff $\gcd(g, n) = 1$. $\square$

Example 12.29.

$$\mathrm{Aut}_{\mathbf{Grp}}(\mathbb{Z}) \cong C_2$$

PROOF: The only automorphisms are the identity and multiplication by -1. □

12.3 Nilpotent Elements

Definition 12.30 (Nilpotent)**.** Let R be a ring and $a \in R$. Then a is *nilpotent* iff there exists n such that $a^n = 0$.

Proposition 12.31. *Let R be a ring and $a, b \in R$. If a and b are nilpotent and $ab = ba$ then $a + b$ is nilpotent.*

PROOF:
⟨1⟩1. PICK m and n such that $a^m = b^n = 0$.
⟨1⟩2. $(a + b)^{m+n} = 0$

PROOF: Since $(a+b)^{m+n} = \sum_k \left(\begin{array}{c} m+n \\ k \end{array} \right) a^k b^{m+n-k}$ and every term in this sum is 0 since, for every k, either $k \geq m$ or $m + n - k \geq n$.

□

Proposition 12.32. *m is nilpotent in $\mathbb{Z}/n\mathbb{Z}$ if and only if m is divisible by all the prime factors of n.*

PROOF:
⟨1⟩1. If m is nilpotent then m is divisible by all the prime factors of n.
  ⟨2⟩1. ASSUME: $m^a \equiv 0 (\bmod n)$
  ⟨2⟩2. For every prime p, if $p \mid n$ then $p \mid m^a$.
  ⟨2⟩3. For every prime p, if $p \mid n$ then $p \mid m$.
⟨1⟩2. If m is divisible by all the prime factors of n then m is nilpotent in $\mathbb{Z}/n\mathbb{Z}$.
  ⟨2⟩1. ASSUME: m is divisible by all the prime factors of n.
  ⟨2⟩2. LET: a be the largest number such that $p^a \mid n$ for some prime p.
  ⟨2⟩3. For every prime p that divides n we have $p^a \mid m^a$
  ⟨2⟩4. $n \mid m^a$
  ⟨2⟩5. $m^a \equiv 0 (\bmod n)$
  ⟨2⟩6. m is nilpotent in $\mathbb{Z}/n\mathbb{Z}$.

□

Chapter 13

Ring Homomorphisms

Definition 13.1 (Ring Homomorphism)**.** Let R and S be rings. A *ring homomorphism* $\phi : R \to S$ is a rng homomorphism such that $\phi(1) = 1$.

Proposition 13.2. *The zero-ring is terminal in* **Ring**.

Proof: Easy. $\square$

Proposition 13.3. *The ring* $\mathbb{Z}$ *is initial in* **Ring**.

Proof: Easy. $\square$

Proposition 13.4. *Let R and S be rings and $\phi : R \to S$ be a rng homomorphism. If ϕ is surjective, then ϕ is a ring homomorphism.*

Proof:
$\langle 1 \rangle 1$. Pick $a \in R$ such that $\phi(a) = 1$
$\langle 1 \rangle 2$. $\phi(1) = 1$
Proof:

$$\begin{aligned} \phi(1) &= \phi(1)\phi(a) \\ &= \phi(1a) \\ &= \phi(a) \\ &= 1 \end{aligned}$$

$\square$

Example 13.5. For any set S we have $\mathcal{P}S \cong (\mathbb{Z}/2\mathbb{Z})^S$ in **Ring** with the isomorphism

$$\phi : \mathcal{P}S \cong (\mathbb{Z}/2\mathbb{Z})^S$$
$$\phi(A)(s) = \begin{cases} 1 & \text{if } s \in A \\ 0 & \text{if } s \notin A \end{cases}$$

Example 13.6. The function $\mathbb{H} \to \mathfrak{gl}_4(\mathbb{R})$ that maps $a + bi + cj + dk$ to

$$\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

is a monomorphism in **Ring**, as is the function $\mathbb{H} \to \mathfrak{sl}_2(\mathbb{C})$ that maps $a + bi + cj + dk$ to

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} .$$

Proposition 13.7. *Ring homomorphisms preserve units.*

PROOF: If $uv = 1$ then $\phi(u)\phi(v) = 1$. □

Proposition 13.8. *Let $\phi : R \to S$ be a ring homomorphism. Then the following are equivalent.*

1. *ϕ is a monomorphism.*
2. $\ker \phi = \{0\}$
3. *ϕ is injective.*

PROOF:
⟨1⟩1. $1 \Rightarrow 2$
  ⟨2⟩1. ASSUME: ϕ is a monomorphism.
  ⟨2⟩2. LET: $r \in \ker \phi$
  ⟨2⟩3. LET: $\mathrm{ev}_r : \mathbb{Z}[x] \to R$ be the unique ring homomorphism such that $\mathrm{ev}_r(x) = r$.
  ⟨2⟩4. LET: $\mathrm{ev}_0 : \mathbb{Z}[x] \to R$ be the unique ring homomorphism such that $\mathrm{ev}_0(x) = 0$.
  ⟨2⟩5. $\phi \circ \mathrm{ev}_r = \phi \circ \mathrm{ev}_0$
  ⟨2⟩6. $\mathrm{ev}_r = \mathrm{ev}_0$
  ⟨2⟩7. $r = 0$
⟨1⟩2. $2 \Rightarrow 3$
  PROOF: Proposition 7.20.
⟨1⟩3. $3 \Rightarrow 1$
  PROOF: Easy.
□

Example 13.9. It is not true that every epimorphism in **Ring** is surjective. The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism but not surjective.

The same example shows that a ring homomorphism may be a monomorphism and an epimorphism but not be an isomorphism.

Example 13.10.

$$\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$$

The isomorphism maps any group endomorphism $\phi : \mathbb{Z} \to \mathbb{Z}$ to $\phi(1)$.

Example 13.11. The group of units of $\mathrm{End}_{\mathbf{Ab}}(G)$ is $\mathrm{Aut}_{\mathbf{Ab}}(G)$.

Example 13.12. Let R be a ring. Then the function $\lambda : R \to \mathrm{End}_{\mathbf{Ab}}(R)$ defined by

$$\lambda(a)(b) = ab$$

is a ring monomorphism.

PROOF: Easy. □

13.1 Products

Proposition 13.13. *Let R and S be rings. Then $R \times S$ is a ring under componentwise addition and multiplication, and this ring is the product of R and S in* **Ring**.

PROOF: Easy. □

Chapter 14

Subrings

Definition 14.1 (Subring)**.** Let S be a ring. A *subring* of S is a ring R such that R is a subset of S and the inclusion $R \hookrightarrow S$ is a ring homomorphism.

Proposition 14.2. *Let R and S be rings. Then R is a subring of S if and only if R is a subset of S, the unit 1 of S is an element of R, and the operations of R are the restrictions of the operations of S to R.*

Proof: Easy. $\square$

Corollary 14.2.1. *The zero ring is not a subring of any non-zero ring.*

Proposition 14.3. *Let $\phi : R \to S$ be a ring homomorphism. Then $\phi(R)$ is a subring of S.*

Proof: Easy. $\square$

14.1 Centralizer

Definition 14.4 (Centralizer)**.** Let R be a ring and $a \in R$. The *centralizer* of a is $\{r \in R : ar = ra\}$.

Proposition 14.5. *The centralizer of a is a subring of R.*

Proof: Easy. $\square$

14.2 Center

Definition 14.6 (Center)**.** The *center* of a ring R is $\{x \in R : \forall y \in R.xy = yx\}$.

Proposition 14.7. *The center of a ring is a subring.*

Proof: Easy. $\square$

Proposition 14.8. *Let R be a ring. The center of* $\mathrm{End}_{\mathbf{Ab}}(R)$ *is isomorphic to the center of R.*

PROOF:
⟨1⟩1. LET: $\lambda : R \to \mathrm{End}_{\mathbf{Ab}}(R)$ be left multiplication.
⟨1⟩2. λ maps $Z(R)$ to $Z(\mathrm{End}_{\mathbf{Ab}}(R))$.
⟨2⟩1. LET: $a \in Z(R)$
⟨2⟩2. LET: $\phi \in \mathrm{End}_{\mathbf{Ab}}(R)$
PROVE: $\lambda(a) \circ \phi = \phi \circ \lambda(a)$
⟨2⟩3. LET: $x \in R$
⟨2⟩4. $a + \phi(x) = \phi(a + x)$
⟨1⟩3. $\lambda(Z(R)) = Z(\mathrm{End}_{\mathbf{Ab}}(R))$
⟨2⟩1. LET: $\phi \in Z(\mathrm{End}_{\mathbf{Ab}}(R))$
⟨2⟩2. For all $r \in R$,
LET: $\mu_r \in \mathrm{End}_{\mathbf{Ab}}(R)$ be right multiplication by r.
⟨2⟩3. For all $r \in R$ we have $\phi \circ \mu_r = \mu_r \circ \phi$.
⟨2⟩4. For all $r, x \in R$ we have $\phi(xr) = \phi(x)r$
⟨2⟩5. For all $r \in R$ we have $\phi(r) = \phi(1)r$
⟨2⟩6. $\phi = \lambda(\phi(1))$
□

Corollary 14.8.1. *If R is a commutative ring then R is isomorphic to the center of* $\mathrm{End}_{\mathbf{Ab}}(R)$.

Example 14.9. For n a positive integer we have $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{End}_{\mathbf{Ab}}(\mathbb{Z}/n\mathbb{Z})$.

Since, for any $\phi \in \mathrm{End}_{\mathbf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ we have $\phi(m) = m\phi(1)$ and so the whole of $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ is the image of λ.

Chapter 15

Monoid Rings

Definition 15.1 (Monoid Ring)**.** Let R be a ring and M a monoid. Define $R[M]$ to be the ring whose elements are the families $\{a_m\}_{m \in M}$ such that $a_m = 0$ for all but finitely many $m \in M$, written

$$\sum_{m \in M} a_m m \quad ,$$

under

$$\sum_m a_m m + \sum_m b_m m = \sum_m (a_m + b_m) m$$

$$\left(\sum_m a_m m \right) \left(\sum_m b_m m \right) = \sum_{m \in M} \sum_{m_1 m_2 = m} a_{m_1} b_{m_2} m$$

Example 15.2. Ring homomorphisms do not necessarily preserve zero-divisors. The canonical homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ maps the non-zero-divisor 2 to a zero-divisor.

15.1 Polynomials

Definition 15.3 (Polynomial)**.** Let R be a ring. The ring of *polynomials* $R[x]$ is $R[\mathbb{N}]$. We write

$$\sum_n a_n x^n \text{ for } \sum_n a_n n \quad .$$

Concretely, a *polynomial* in R is a sequence (a_n) in R such that there exists N such that $\forall n \geq N . a_n = 0$. We write the polynomial as

$$\sum_{n=0}^{N-1} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1} \quad .$$

We write $R[x]$ for the set of all polynomials in R.

Define addition and multiplication on $R[x]$ by

$$\sum_n a_n x^n + \sum_n b_n x^n = \sum_n (a_n + b_n) x^n$$
$$\left(\sum_n a_n x^n\right)\left(\sum_n b_n x^n\right) = \sum_n \sum_{i+j=n} a_i b_j x^n$$

A *constant* is a polynomial of the form $a + 0x + 0x^2 + \cdots$ for some $a \in R$. We write $R[x_1, \ldots, x_n]$ for $R[x_1][x_2] \cdots [x_n]$.

Proposition 15.4. *For any ring R, the set of polynomials $R[x]$ is a ring.*

PROOF: Easy. □

Definition 15.5 (Degree)**.** The *degree* of a polynomial $\sum_n a_n x^n$ is the largest integer d such that $a_d \neq 0$. We take the degree of the zero polynomial to be $-\infty$.

Proposition 15.6. *Let R be a ring and $f, g \in R[x]$ be nonzero polynomials. Then*

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

PROOF: If $a_n + b_n \neq 0$ then $a_n \neq 0$ or $b_n \neq 0$. □

Proposition 15.7. *The function $i : n \to \mathbb{Z}[x_1, \ldots, x_n]$ that maps k to x_k is initial in the category with:*

- *objects all pairs $j : n \to R$ where R is a commutative ring and j a function*
- *morphisms $\phi : (j_1, R_1) \to (j_2, R_2)$ are ring homomorphisms $\phi : R_1 \to R_2$ such that $\phi \circ j_1 = j_2$.*

PROOF: The unique morphism $(i, \mathbb{Z}[x_1, \ldots, x_n]) \to (j, R)$ maps a polynomial p to $p(j(0), j(1), \ldots, j(n-1))$. □

Proposition 15.8. *Let $\alpha : R \to S$ be a ring homomorphism. Let $s \in S$ commute with $\alpha(r)$ for all $r \in R$. Then there exists a unique ring homomorphism $\overline{\alpha} : R[x] \to S$ such that $\overline{\alpha}(x) = s$ and the following diagram commutes:*

$$\begin{tikzcd}
R[x] \arrow[r, "\overline{\alpha}"] & S \\
R \arrow[u] \arrow[ur, "\alpha"] &
\end{tikzcd}$$

PROOF: The map $\overline{\alpha}$ is given by
$$\overline{\alpha}(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n) = \alpha(a_0) + \alpha(a_1) s + \alpha(a_2) s^2 + \cdots + \alpha(a_n) s^n \ .$$
□

Definition 15.9. Let R be a commutative ring. Given a polynomial $p \in R[x]$, the *polynomial function* $p : R \to R$ is the function given by: $p(r) = \alpha_r(p)$, where $\alpha_r : R[x] \to R$ is the unique ring homomorphism such that the following diagram commutes.

$$\begin{tikzcd} R[x] \arrow[r, "\alpha_r"] & R \\ 1 \arrow[u, "x"] \arrow[ur, "r"'] & \end{tikzcd}$$

Proposition 15.10. *$\mathbb{Z}[x, y]$ is the coproduct of $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ in the category of commutative rings.*

Proof: Given ring homomorphisms $f : \mathbb{Z}[x] \to R$ and $g : \mathbb{Z}[y] \to R$, the required morphism $\mathbb{Z}[x, y] \to R$ maps $p(x, y)$ to $p(f(x), g(y))$. $\square$

Example 15.11. $\mathbb{Z}[x, y]$ is not the coproduct of $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ in **Ring**. Given $f : \mathbb{Z}[x] \to R$ and $g : \mathbb{Z}[y] \to R$ with $f(x) \neq g(y)$, the mediating morphism $\mathbb{Z}[x, y] \to R$ cannot exist since it must map xy to both $f(x)g(y)$ and $g(y)f(x)$. $\square$

Definition 15.12. A polynomial is *monic* iff its last non-zero coefficient is 1.

Proposition 15.13. *A monic polynomial is not a left- or right-zero-divisor.*

Proof: Easy. $\square$

Proposition 15.14. *Let R be a ring. Let $f, g \in R[x]$ with f monic. Then there exist unique polynomials $q, r \in R[x]$ with $\deg r < \deg f$ such that*

$$g = qf + r \ .$$

Proof:
⟨1⟩1. Let: $d = \deg f$
⟨1⟩2. For all $a \in R$ and $n > d$, there exists $h \in R[x]$ with $\deg h < n$ such that
$$ax^n = ax^{n-d} f + h \ .$$
Proof: Take $h = ax^n - ax^{n-d} f$.
⟨1⟩3. For all $a \in R$ and $n > d$, there exists $q, h \in R[x]$ with $\deg h \leq d$ such that
$$ax^n = qf + h \ .$$
Proof: Repeating ⟨1⟩2 by induction.
⟨1⟩4. Let: $g = \sum_{i=0}^{n} a_i x^i$
⟨1⟩5. For $i > d$, Pick $q_i h_i \in R[x]$ with $\deg h < \deg f$ such that $a_i x^i = q_i f + h_i$
⟨1⟩6. $g = \left(\sum_{i=d+1}^{n} q_i \right) f + \sum_{i=d+1}^{n} h_i$
⟨1⟩7. q and r are unique.
Proof: If $q_1 f + r_1 = q_2 f + r_2$ then $r_1 - r_2 = (q_2 - q_1) f$ and so $r_1 - r_2 = (q_2 - q_1) f = 0$ since $\deg(r_1 - r_2) < \deg f$.
$\square$

15.2 Laurent Polynomials

Definition 15.15 (Laurent Polynomial)**.** Let R be a ring. The ring of *Laurent polynomials* is the group ring $R[\mathbb{Z}]$. We write $\sum_{n \in \mathbb{Z}} a_n x^n$ for $\sum_n a_n n$.

15.3 Power Series

Definition 15.16 (Power Series)**.** Let R be a ring. A *power series* in R is a sequence (a_n) in R. We write the power series as

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots \ .$$

We write $R[[x]]$ for the set of all power series in R.

Define addition and multiplication on $R[[x]]$ by

$$\sum_n a_n x^n + \sum_n b_n x^n = \sum_n (a_n + b_n) x^n$$

$$\left(\sum_n a_n x^n\right)\left(\sum_n b_n x^n\right) = \sum_n \sum_{i+j=n} a_i b_j x^n$$

Proposition 15.17. *For any ring R, the set of power series $R[[x]]$ is a ring.*

Proof: Easy. □

Proposition 15.18. *A power series $\sum_n a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.*

Proof:
⟨1⟩1. If $\sum_n a_n x^n$ is a unit then a_0 is a unit.
 ⟨2⟩1. Let: $\sum_n b_n x^n$ be the inverse of $\sum_n a_n x^n$.
 ⟨2⟩2. $a_0 b_0 = b_0 a_0 = 1$
⟨1⟩2. If a_0 is a unit then $\sum_n a_n x^n$ is a unit.
 Proof: Define the sequence (b_n) in R by

$$b_n = -{a_0}^{-1} \sum_{i=1}^{n} a_i b_{n-i}$$

 Then $\sum_n b_n x^n$ is the inverse of $\sum_n a_n x^n$.

□

Chapter 16

Ideals

Definition 16.1 (Left-Ideal)**.** Let R be a ring.

A subgroup I of R is a *left-ideal* iff, for all $r \in R$, we have $rI \subseteq I$.

A subgroup I of R is a *right-ideal* iff, for all $r \in R$, we have $Ir \subseteq I$.

A subgroup I of R is a *(two-sided) ideal* iff it is a left-ideal and a right-ideal.

Example 16.2. Let R be a ring and $a \in R$. Then Ra is a left-ideal and aR is a right-ideal.

In particular, $\{0\}$ is always a two-sided ideal.

Example 16.3. Let S be a set and $T \subseteq S$. Then $\{X \in \mathcal{P}S : X \subseteq T\}$ is an ideal in $\mathcal{P}S$.

Proposition 16.4. *Let S be a finite set. Then every ideal in $\mathcal{P}S$ is of the form $\{X \in \mathcal{P}S : X \subseteq T\}$ for some $T \subseteq S$.*

Proof:

$\langle 1 \rangle 1$. Let: I be an ideal in $\mathcal{P}S$.

$\langle 1 \rangle 2$. Let: $T = \bigcup I$

$\langle 1 \rangle 3$. For all $i \in T$ we have $\{i\} \in I$.

  $\langle 2 \rangle 1$. Let: $i \in T$

  $\langle 2 \rangle 2$. Pick $X \in I$ such that $i \in X$

  $\langle 2 \rangle 3$. $\{i\} = \{i\} \cap X \in I$

$\langle 1 \rangle 4$. For all $X \subseteq T$ we have $X \in I$.

  Proof: If $X = \{x_1, \ldots, x_n\}$ then $X = \{x_1\} + \cdots + \{x_n\} \in I$.

$\square$

Example 16.5. If S is an infinite set, then there is always an ideal in $\mathcal{P}S$ that is not of the form $\{X \in \mathcal{P}S : X \subseteq T\}$ for some $T \subseteq S$, namely the set of all finite subsets of S.

Proposition 16.6. *Let $\phi : R \twoheadrightarrow S$ be a surjective ring homomorphism. Let J be an ideal in R. Then $\phi(J)$ is an ideal in S.*

Proof:

⟨1⟩1. LET: $j \in J$ and $s \in S$
PROVE: $s\phi(j), \phi(j)s \in \phi(J)$
⟨1⟩2. PICK $r \in R$ such that $\phi(r) = s$
⟨1⟩3. $rj, jr \in J$
⟨1⟩4. $s\phi(j), \phi(j)s \in \phi(J)$
□

Example 16.7. We cannot remove the hypothesis that ϕ is surjective.

Let $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ be the inclusion. Then $i(2\mathbb{Z}) = 2\mathbb{Z}$ is not an ideal in $\mathbb{Q}$.

Proposition 16.8. *Let $\phi : R \to S$ be a ring homomorphism and I a (left-, right-)ideal in S. Then $\phi^{-1}I$ is a (left-, right-)ideal in R.*

PROOF: Easy. □

Corollary 16.8.1. *Let $\phi : R \to S$ be a ring homomorphism. Then $\ker\phi$ is an ideal in R.*

Definition 16.9 (Quotient Ring)**.** Let I be an ideal in R. The *quotient ring* R/I is the quotient group R/I under

$$(a + I)(b + I) = ab + I \ .$$

This is well-defined as, if $a + I = a' + I$ and $b + I = b' + I$ then

$$\begin{aligned} a - a' &\in I \\ b - b' &\in I \\ \therefore ab - a'b &\in I \\ a'b - a'b' &\in I \\ \therefore ab - a'b' &\in I \end{aligned}$$

Proposition 16.10. *Let I be an ideal in R. Then the canonical group homomorphism $\pi : R \to R/I$ is a ring homomorphism.*

PROOF: By construction. □

Proposition 16.11. *Let I be an ideal in a ring R. For every ring homomorphism $\phi : R \to S$ such that $I \subseteq \ker\phi$, there exists a unique ring homomorphism $\overline{\phi} : R/I \to S$ such that the following diagram commutes.*

$$\begin{tikzcd} R \arrow[rr, "\phi"] \arrow[dr, two heads, "\pi"'] & & S \\ & R/I \arrow[ur, "\overline{\phi}"'] & \end{tikzcd}$$

PROOF: Easy. □

Corollary 16.11.1. *Every ring homomorphism $\phi : R \to S$ decomposes as follows.*

$$\begin{tikzcd} R \arrow[r, two heads] \arrow[rrr, bend left, "\phi"] & R/\ker\phi \arrow[r, "\cong"] & \operatorname{im}\phi \arrow[r, hook] & S \end{tikzcd}$$

Corollary 16.11.2 (First Isomorphism Theorem)**.** *Let $\phi : R \twoheadrightarrow S$ be a surjective ring homomorphism. Then*

$$S \cong R/\ker\phi \ .$$

Theorem 16.12 (Third Isomorphism Theorem)**.** *Let I and J be ideals in R with $I \subseteq J$. Then J/I is an ideal in R/I, and*

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

Proof: Since the function $R/I \to R/J$ that maps $r + I$ to $r + J$ is a surjective ring homomorphism with kernel J/I. □

Corollary 16.12.1. *Let $\phi : R \twoheadrightarrow S$ be a surjective ring homomorphism. Let J be an ideal in R. Then*

$$\frac{S}{\phi(J)} \cong \frac{R}{\ker S + J}$$

Proposition 16.13. *Let R be a ring and J an ideal in $\mathfrak{gl}_n(R)$. Let $A \in \mathfrak{gl}_n(R)$. Then $A \in J$ if and only if the matrices obtained by placing any entry of A in any position and zeros elsewhere all belong to J.*

Proof: Each such matrix can be obtained by pre- and post-multiplying A by matrices which have a single 1 and 0s elsewhere. Conversely, A is a sum of such matrices. □

Corollary 16.13.1. *Let R be a ring. Let J be an ideal in $\mathfrak{gl}_n(R)$. Let I be the set of all entries of elements of J. Then I is an ideal in R, and J is the set of all matrices whose entries are in I.*

Proposition 16.14. *Let R be a ring. Let $\{I_\alpha\}_{\alpha \in A}$ be a family of ideals in R. Let*

$$\sum_{\alpha \in A} I_\alpha = \{\sum_{\alpha \in A} r_\alpha : \forall \alpha . r_\alpha \in I_\alpha, r_\alpha = 0 \text{ for all but finitely many } \alpha \in A\} \ .$$

Then $\sum_{\alpha \in A} I_\alpha$ is an ideal, and is the smallest ideal that includes every I_α.

Proof: Easy. □

Proposition 16.15. *The intersection of a set of ideals is an ideal.*

Proof: Easy. □

16.1 Characteristic

Definition 16.16 (Characteristic)**.** The *characteristic* of a ring R is the non-negative integer n such that $n\mathbb{Z}$ is the kernel of the unique ring homomorphism $\mathbb{Z} \to R$.

Proposition 16.17. *Let R be a ring. If the unit 1 has finite order in R, then its order is the characteristic of R; otherwise, the characteristic of R is 0.*

Proof: Easy. □

Example 16.18. The zero ring is the only ring with characteristic 1.

16.2 Nilradical

Definition 16.19 (Nilradical)**.** Let R be a commutative ring. The *nilradical* of R is the set of all nilpotent elements.

Proposition 16.20. *Let R be a commutative ring. The nilradical of R is an ideal in R.*

Proof: If $a^n = 0$ then for any b we have $(ba)^n = 0$. □

Example 16.21. We cannot remove the assumption that R is commutative. In $\mathfrak{gl}_2(\mathbb{R})$ we have that $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nilpotent but $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ is not.

16.3 Principal Ideals

Definition 16.22 (Principal Ideal)**.** Let R be a commutative ring and $a \in R$. The *principal ideal* generated by a is $(a) = Ra = aR$.

Example 16.23. $\{0\} = (0)$ and $R = \{1\}$ are principal ideals.

Definition 16.24. Let R be a commutative ring and $\{a_\alpha\}_{\alpha \in A}$ be a family of elements of R. The *ideal generated by the elements a_α* is

$$(a_\alpha)_{\alpha \in A} := \sum_{\alpha \in A} (a_\alpha) \ .$$

An ideal is *finitely generated* iff it is generated by a finite family of elements.

Definition 16.25. Let R be a commutative ring and I, J be ideals in R. Then IJ is the ideal generated by $\{ij\}_{i \in I, j \in J}$.

Proposition 16.26.

$$IJ \subseteq I \cap J$$

PROOF: Easy. $\square$

Proposition 16.27. *Let R be a commutative ring. Let I and J be ideals in R. If $I + J = R$ then $IJ = I \cap J$.*

PROOF:
$\langle 1 \rangle 1$. LET: $r \in I \cap J$
$\langle 1 \rangle 2$. PICK $i \in I$ and $j \in J$ such that $i + j = 1$.
$\langle 1 \rangle 3$. $ri, rj \in IJ$
$\langle 1 \rangle 4$. $r = ri + rj \in IJ$
$\square$

Proposition 16.28. *Let R be a commutative ring. Let $f \in R[x]$ be a monic polynomial of degree d. Then the function*

$$\phi : R[x] \to R^{\oplus d}$$

that sends a polynomial g to the remainder of the division of g by f induces an isomorphism of Abelian groups

$$\frac{R[x]}{(f(x))} \cong R^{\oplus d} \quad .$$

PROOF: It is clearly a group homomorphism; it is surjective since it maps any polynomial of degree $< d$ to itself, and its kernel is $(f(x))$ since these are the polynomials with remainder 0. $\square$

Corollary 16.28.1. *Let R be a commutative ring and $a \in R$. Then we have*

$$\frac{R[x]}{(x - a)} \cong R$$

PROOF:
$\langle 1 \rangle 1$. LET: $\phi : R[x] \to R$ be evaluation at a.
$\langle 1 \rangle 2$. $\phi(g)$ is the remainder when dividing g by $x - a$.
PROOF: If $g = (x - a)q + r$ then $g(a) = (a - a)q(a) + r = r$.
$\langle 1 \rangle 3$. ϕ induces a group isomorphism $R[x]/(x - a) \cong R$
PROOF: By the theorem.
$\langle 1 \rangle 4$. This isomorphism is a ring isomorphism.
PROOF: Since evaluation at a is a ring homomorphism.
$\square$

Example 16.29. We have

$$\frac{\mathbb{R}[x]}{(x^2 + 1)} \cong \mathbb{C}$$

as rings.

16.4 Maximal Ideals

Definition 16.30 (Maximal Ideal)**.** Let R be a ring and I an ideal in R. Then I is a *maximal ideal* iff $I \neq R$ and, whenever J is an ideal with $I \subseteq J$, then either $I = J$ or $J = R$.

Chapter 17

Integral Domains

Definition 17.1 (Integral Domain)**.** An *integral domain* is a non-trivial commutative ring with no nonzero zero-divisors.

Example 17.2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are integral domains.

Proposition 17.3. *$\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime.*

PROOF:

$$\begin{aligned} n \text{ is prime} &\Leftrightarrow \forall a, b \in \mathbb{Z}(n \mid ab \Rightarrow n \mid a \vee n \mid b) \\ &\Leftrightarrow \forall a, b \in \mathbb{Z}/n\mathbb{Z}(ab \cong 0 (\operatorname{mod} n) \Rightarrow a \cong 0 (\operatorname{mod} n) \vee b \cong 0 (\operatorname{mod} n)) \\ &\Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ is an integral domain} \end{aligned}$$

□

Proposition 17.4. *In an integral domain, if $x^2 = 1$ then $x = \pm 1$.*

PROOF: We have $x^2 - 1 = (x-1)(x+1) = 0$ so $x - 1 = 0$ or $x + 1 = 0$. □

Proposition 17.5. *Let R be an integral domain and $f, g \in R[x]$. Then*

$$\deg(fg) = \deg f + \deg g$$

PROOF:

⟨1⟩1. LET: $f = \sum_n a_n x^n$ and $g = \sum_n b_n x^n$.

⟨1⟩2. LET: $d = \deg f$ and $e = \deg g$.

⟨1⟩3. The $d+e$th term of fg is

$$a_d b_e x^{d+e}$$

which is non-zero.

⟨1⟩4. For $n > d + e$ the nth term of fg is 0.

□

Corollary 17.5.1. *Let R be a ring. Then $R[x]$ is an integral domain if and only if R is an integral domain.*

Proposition 17.6. *Let R be a ring. Then $R[[x]]$ is an integral domain if and only if R is an integral domain.*

PROOF:
⟨1⟩1. If $R[[x]]$ is an integral domain then R is an integral domain.
  PROOF: Easy.
⟨1⟩2. If R is an integral domain then $R[[x]]$ is an integral domain.
  ⟨2⟩1. ASSUME: R is an integral domain.
  ⟨2⟩2. LET: $\left(\sum_n a_n x^n\right)\left(\sum_n b_n x^n\right) = 0$
  ⟨2⟩3. $a_0 b_0 = 0$
  ⟨2⟩4. $a_0 = 0$ or $b_0 = 0$
  ⟨2⟩5. ASSUME: w.l.o.g. $b_0 \neq 0$
     PROVE: For all n we have $a_n = 0$
  ⟨2⟩6. ASSUME: as induction hypothesis $a_0 = a_1 = \cdots = a_{n-1} = 0$
  ⟨2⟩7. $\sum_{i=0}^{n} a_i b_{n-i} = 0$
  ⟨2⟩8. $a_n b_0 = 0$
  ⟨2⟩9. $a_n = 0$
□

Proposition 17.7. *Let R be a ring and S an integral domain. Every rng homomorphism $\phi : R \to S$ is a ring homomorphism.*

PROOF:
$$\begin{aligned}\phi(1) &= \phi(1 \cdot 1) \\ &= \phi(1)\phi(1)\end{aligned}$$
and so $\phi(1) = 1$ by Cancellation. □

Proposition 17.8. *The characteristic of an integral domain is either 0 or a prime number.*

PROOF:
⟨1⟩1. LET: D be an integral domain.
⟨1⟩2. LET: n be the characteristic of D
⟨1⟩3. ASSUME: $n \neq 0$
⟨1⟩4. ASSUME: $n = ab$
⟨1⟩5. $ab = 0$ in D
⟨1⟩6. $a = 0$ or $b = 0$ in D
⟨1⟩7. $n \mid a$ or $n \mid b$
⟨1⟩8. One of a, b is 1 and the other is n.
□

17.1 Prime Ideals

Definition 17.9 (Prime Ideal)**.** Let I be an ideal in a commutative ring R. Then I is a *prime ideal* iff R/I is an integral domain.

Example 17.10. Let R be a commutative ring and $a \in R$. Then $(x - a)$ is a prime ideal in R iff R is an integral domain.

Proposition 17.11. *Let R be a commutative ring and I a proper ideal in R. Then I is prime iff, whenever $ab \in I$, then $a \in I$ or $b \in I$.*

PROOF: The condition is the same as saying that, if $(a+I)(b+I) = I$, then $a + I = I$ or $b + I = I$. □

Definition 17.12 (Spectrum)**.** The *spectrum* of a commutative ring R, $\operatorname{Spec} R$, is the set of prime ideals.

Proposition 17.13. *Let $\phi : R \to S$ be a ring homomorphism. If I is a prime ideal in S then $\phi^{-1}(I)$ is a prime ideal in R.*

PROOF:If $ab \in \phi^{-1}(I)$ then $\phi(a)\phi(b) \in I$ so either $\phi(a) \in I$ or $\phi(b) \in I$, i.e. either $a \in \phi^{-1}(I)$ or $b \in \phi^{-1}(I)$. □

Proposition 17.14. *Let R be a commutative ring. Suppose there exists a prime ideal P in R such that the only zero-divisor in P is 0. Then R is an integral domain.*

PROOF:
$\langle 1 \rangle$1. ASSUME: $ab = 0$ in R
$\langle 1 \rangle$2. $ab \in P$
$\langle 1 \rangle$3. $a \in P$ or $b \in P$
$\langle 1 \rangle$4. $a = 0$ or $b = 0$
□

Proposition 17.15. *Let R be a commutative ring. The nilradical of R is included in every prime ideal of R.*

PROOF: Let P be a prime ideal. If $a^n = 0$ then $a^n \in P$ hence $a \in P$. □

Definition 17.16 (Krull Dimension)**.** The *(Krull) dimension* of a commutative ring R is the length of the longest chain of prime ideals in R.

Example 17.17. $\mathbb{Z}[x]$ has Krull dimension 2.

Chapter 18

Unique Factorization Domains

Example 18.1. $\mathbb{Z}$ is a UFD.

Chapter 19

Noetherian Rings

Definition 19.1 (Noetherian Ring)**.** A commutative ring is *Noetherian* iff every ideal is finitely generated.

Proposition 19.2. *The homomorphic image of a Noetherian ring is Noetherian.*

PROOF:
$\langle 1 \rangle 1$. LET: R be a Noetherian ring, S be a commutative ring, and $\phi : R \to S$ a surjective ring homomorphism.
$\langle 1 \rangle 2$. LET: I be an ideal in S.
$\langle 1 \rangle 3$. LET: $\phi^{-1}(I) = (a_1, \ldots, a_n)$
$\langle 1 \rangle 4$. $I = (\phi(a_1), \ldots, \phi(a_n))$
$\square$

Chapter 20

Principal Ideal Domains

Definition 20.1 (Principal Ideal Domain)**.** A commutative ring is a *principal ideal domain* (*PID*) iff every ideal is principal.

Example 20.2. $\mathbb{Z}$ is a PID by Proposition 7.16.

Example 20.3. $\mathbb{Z}[x]$ is not a PID. The ideal $(2, x)$ is not principal.

Proposition 20.4. *Every PID is Noetherian.*

Proof: Trivial. □

Proposition 20.5. *Every nonzero prime ideal in a PID is maximal.*

Proof:
⟨1⟩1. Let: R be a PID.
⟨1⟩2. Let: I be a nonzero prime ideal in R.
⟨1⟩3. Pick $a \in R$ such that $I = (a)$.
⟨1⟩4. Let: J be an ideal such that $I \subseteq J$
⟨1⟩5. Pick $b \in R$ such that $J = (b)$.
⟨1⟩6. Pick $t \in R$ such that $a = bt$.
⟨1⟩7. $b \in I$ or $t \in I$
⟨1⟩8. Case: $b \in I$
  Proof: Then $J \subseteq I$ so $I = J$.
⟨1⟩9. Case: $t \in I$
  ⟨2⟩1. Pick $s \in R$ such that $t = as$.
  ⟨2⟩2. $a = ast$
  ⟨2⟩3. $st = 1$
    Proof: Since R is an integral domain.
  ⟨2⟩4. $1 \in I$
  ⟨2⟩5. $I = R$
□

Corollary 20.5.1. *Any PID has Krull dimension 1.*

Chapter 21

Euclidean Domains

Example 21.1. $\mathbb{Z}$ is a Euclidean domain.

Chapter 22

Division Rings

Definition 22.1 (Division Ring)**.** A *division ring* is a ring in which every nonzero element is a two-sided unit.

Example 22.2. The quaternions form a division ring, with the inverse of a non-zero element $a + bi + cj + dk$ being

$$\frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk) \ .$$

Example 22.3. For any ring R, the ring of polynomials $R[x]$ is not a division ring, since x has no inverse.

Proposition 22.4. *Every centralizer in a division ring is a division ring.*

PROOF: If $ar = ra$ then $ra^{-1} = a^{-1}r$. □

Proposition 22.5. *A non-trivial ring R is a division ring if and only if its only left-ideals and right-ideals are $\{0\}$ and R.*

PROOF:
⟨1⟩1. If R is a division ring then the only left-ideals and right-ideals are $\{0\}$ and R.
  ⟨2⟩1. ASSUME: R is a division ring.
  ⟨2⟩2. The only left-ideals are $\{0\}$ and R.
    ⟨3⟩1. LET: I be a left-ideal that is not $\{0\}$.
      PROVE: $I = R$
    ⟨3⟩2. PICK $a \in I - \{0\}$
    ⟨3⟩3. PICK a left inverse b for a
    ⟨3⟩4. $1 \in I$
      PROOF: Since $1 = ba$.
    ⟨3⟩5. $I = R$
      PROOF: For any $r \in R$ we have $r = r1 \in I$.
  ⟨2⟩3. The only right-ideals are $\{0\}$ and R.

PROOF: Similar.

$\langle 1 \rangle 2$. If the only left-ideals and right-ideals are $\{0\}$ and R then R is a division ring.

□

Proposition 22.6. *Let K be a division ring and R a non-trivial ring. Every ring homomorphism $K \to R$ is injective.*

PROOF:

$\langle 1 \rangle 1$. LET: $\phi : K \to R$ be a ring homomorphism.
PROVE: $\ker \phi = \{0\}$

$\langle 1 \rangle 2$. LET: $x \in \ker \phi$

$\langle 1 \rangle 3$. ASSUME: for a contradiction $x \neq 0$.

$\langle 1 \rangle 4$. $\phi(xx^{-1}) = 1$

$\langle 1 \rangle 5$. $0 = 1$

$\langle 1 \rangle 6$. Q.E.D.

PROOF: This contradicts the assumption that R is non-trivial.

□

Chapter 23

Simple Rings

Definition 23.1 (Simple Ring)**.** A non-trivial ring is R *simple* iff its only two-sided ideals are $\{0\}$ and R.

Example 23.2. For any simple ring R we have $\mathfrak{gl}_n(R)$ is simple, by Corollary 16.13.1.

Proposition 23.3. *Let R be a ring and I an ideal in R. Then I is maximal iff R/I is simple.*

Proof:

$$\begin{aligned} R/I \text{ is simple} &\Leftrightarrow \text{the only ideals in } R/I \text{ are } \{I\} \text{ and } R/I \\ &\Leftrightarrow \text{the only ideals in } R \text{ that include } I \text{ are } I \text{ and } R \\ &\Leftrightarrow I \text{ is maximal} \end{aligned}$$

$\square$

Chapter 24

Reduced Rings

Definition 24.1 (Reduced Ring)**.** A ring is *reduced* iff it has no non-zero nilpotent elements.

Proposition 24.2. *Let R be a commutative ring. Let N be its nilradical. Then R/N is reduced.*

PROOF:
$\langle 1 \rangle 1$. LET: $r + N$ be nilpotent.
$\langle 1 \rangle 2$. PICK n such that $(r + N)^n = N$
$\langle 1 \rangle 3$. $r^n \in N$
$\langle 1 \rangle 4$. PICK k such that $(r^n)^k = 0$
$\langle 1 \rangle 5$. $r^{nk} = 0$
$\langle 1 \rangle 6$. $r \in N$
$\langle 1 \rangle 7$. $r + N = N$
$\square$

Proposition 24.3. *Let R be a commutative ring. Let I and J be ideals in R. If R/IJ is reduced then $IJ = I \cap J$.*

PROOF:
$\langle 1 \rangle 1$. LET: $r \in I \cap J$
PROVE: $r \in IJ$
$\langle 1 \rangle 2$. $r^2 \in IJ$
$\langle 1 \rangle 3$. $(r + IJ)^2 = IJ$
$\langle 1 \rangle 4$. $r + IJ = IJ$
PROOF: Since R/IJ is reduced.
$\langle 1 \rangle 5$. $r \in IJ$
$\square$

Chapter 25

Boolean Rings

Definition 25.1 (Boolean)**.** A ring is *Boolean* iff $a^2 = a$ for every element a.

Example 25.2. For any set S, the ring $\mathcal{P}S$ is Boolean.

Proposition 25.3. *Every non-trivial Boolean ring has characteristic 2.*

PROOF: We have $4 = 2$ and so $2 = 0$. □

Proposition 25.4. *Every Boolean ring is commutative.*

PROOF:

$$\begin{aligned}
(a+b)^2 &= a+b \\
\therefore a^2 + ab + ba + b^2 &= a+b \\
\therefore a + ab + ba + b &= a+b \\
\therefore ab + ba &= 0 \\
\therefore ab &= -ba \\
&= ba \qquad \text{(Proposition 25.3)}
\end{aligned}$$

Example 25.5. The only Boolean integral domain is $\mathbb{Z}/2\mathbb{Z}$. For, if D is a Boolean integral domain and $x \in D$, we have $x^2 = x$, so $x^2 - x = x(x-1) = 0$ and so $x = 0$ or $x = 1$, i.e. $D = \{0, 1\}$.

Proposition 25.6. *Every Boolean ring has Krull dimension 0.*

PROOF:
$\langle 1 \rangle 1$. LET: R be a Boolean ring.
$\langle 1 \rangle 2$. LET: I be a prime ideal in R.
PROVE: I is maximal.
$\langle 1 \rangle 3$. LET: J be an ideal with $I \subsetneq J$
$\langle 1 \rangle 4$. PICK $a \in J$ with $a \notin I$
$\langle 1 \rangle 5$. $a^2 - a = 0 \in I$
$\langle 1 \rangle 6$. $a(a-1) \in I$

$\langle 1\rangle 7.$ $a - 1 \in I$
$\langle 1\rangle 8.$ $a - 1 \in J$
$\langle 1\rangle 9.$ $1 \in J$
$\langle 1\rangle 10.$ $J = R$
$\square$

Chapter 26

Modules

Definition 26.1 (Left Module)**.** Let R be a ring and M an Abelian group. A *left-action* of R on M is a ring homomorphism

$$R \to \mathrm{End}_{\mathbf{Ab}}(M) \quad .$$

A *left R-module* consists of an Abelian group M and a left-action of R on M.

Proposition 26.2. *Let R be a ring and M an Abelian group. Let $\cdot : R \times M \to M$. Then $\cdot$ defines a left-action of R on M if and only if, for all $r, s \in R$ and $m, n \in M$:*

- $r(m + n) = rm + rn$
- $(r + s)m = rm + sm$
- $(rs)m = r(sm)$
- $1m = m$

Proof: Immediate from definitions. □

Proposition 26.3. *In any R-module M we have $0m = 0$ for all $m \in M$.*

Proof: Since $0m = (0 + 0)m = 0m + 0m$ and so $0m = 0$ by cancellation in M. □

Proposition 26.4. *In any R-module M we have $(-1)m = -m$ for all $m \in M$.*

Proof: Since $m + (-1)m = 1m + (-1)m = (1 + (-1))m = 0m = 0$. □

Proposition 26.5. *Every Abelian group is a $\mathbb{Z}$-module in exactly one way.*

Proof: Since $\mathbb{Z}$ is initial in **Ring**. □

Definition 26.6 (Right Module)**.** Let R be a ring. A *right R-module* consists of an Abelian group M and a function $\cdot : M \times R \to M$ such that, for all $r, s \in R$ and $m, n \in M$:

- $(m+n)r = mr + nr$
- $m(r+s) = mr + ms$
- $m(rs) = (mr)s$
- $m1 = m$

26.1 Homomorphisms

Definition 26.7 (Homomorphism of Left-Modules)**.** Let R be a ring. Let M and N be left-R-modules. A *homomorphism of left-R-modules* $\phi : M \to N$ is a group homomorphism such that, for all $r \in R$ and $m \in M$, we have $\phi(rm) = r\phi(m)$.

Let $R - \mathbf{Mod}$ be the category of left-R-modules and left-R-module homomorphisms.

Example 26.8.

$$\mathbb{Z} - \mathbf{Mod} \cong \mathbf{Ab}$$

Example 26.9. The trivial group 0 is the zero object in $R - \mathbf{Mod}$.

Proposition 26.10. *Every bijective R-module homomorphism is an isomorphism.*

Proof: Easy. □

Proposition 26.11. *Let R be a ring. Let M be an R-module. Then*

$$M \cong R - \mathbf{Mod}[R, M]$$

as R-modules.

Proof: The isomorphism maps m to the function $\lambda r.rm$. Its inverse maps an R-module homomorphism α to $\alpha(1)$. □

Proposition 26.12. *Let R be a commutative ring. Let M be an R-module. Then there is a bijection between the set of $R[x]$-module structures on M that extend the given R-module structure and* $\mathrm{End}_{R-\mathbf{Mod}}(M)$*.*

Proof:

⟨1⟩1. Let: $\alpha : R \to \mathrm{End}_{\mathbf{Ab}}(M)$ be the given R-module structure on M.

⟨1⟩2. An $R[x]$-module structure on M that extends α is a ring homomorphism $\beta : R[x] \to \mathrm{End}_{\mathbf{Ab}}(M)$ such that $\beta \circ i = \alpha$, where i is the inclusion $R \to R[x]$.

⟨1⟩3. There is a bijection between the $R[x]$-module structures on M that extend α and the elements $s \in \mathrm{End}_{\mathbf{Ab}}(M)$ that commute with $\alpha(r)$ for all $r \in R$.

Proof: By the universal property for polynomials.

⟨1⟩4. There is a bijection between the $R[x]$-module structures on M that extend α and the R-module homomorphisms $(M, \alpha) \to (M, \alpha)$.

∎

Proposition 26.13. *Let R be a commutative ring. Let M and N be R-modules. Then $R - \mathbf{Mod}[M, N]$ is an R-module under*

$$(\phi + \psi)(m) = \phi(m) + \psi(m)$$
$$(r\phi)(m) = r\phi(m)$$

PROOF: Easy. ∎

Proposition 26.14. *Let R be an integral domain. Let I be a nonzero principal ideal of R. Then $I \cong R$ in $R - \mathbf{Mod}$.*

PROOF:
$\langle 1 \rangle 1$. PICK $a \in R$ such that $I = (a)$.
$\langle 1 \rangle 2$. LET: $\phi : R \to I$ be the map $\phi(r) = ra$.
$\langle 1 \rangle 3$. ϕ is an R-module homomorphism.
  PROOF: Since $(r + s)a = ra + sa$ and $(rs)a = r(sa)$.
$\langle 1 \rangle 4$. ϕ is surjective.
$\langle 1 \rangle 5$. ϕ is injective.
  PROOF: If $ra = sa$ then $(r - s)a = 0$ so $r - s = 0$ and $r = s$.
$\langle 1 \rangle 6$. $\phi : R \cong I$
∎

26.2 Submodules

Definition 26.15 (Submodule)**.** Let M be a left-R-module and $N \subseteq M$. Then N is a *submodule* of M iff N is a subgroup of M and $\forall r \in R. \forall n \in N. rn \in N$.

Proposition 26.16. *Let R be a ring and $I \subseteq R$. Then I is a left-ideal in R iff I is a submodule of R as an R-module.*

PROOF: Immediate from definitions. ∎

Proposition 26.17. *Let R be a ring. Let M and N be left-R-modules and $\phi : M \to N$ an R-module homomorphism. Then $\ker \phi$ is a submodule of M and $\operatorname{im} \phi$ is a submodule of N.*

PROOF: Easy. ∎

Proposition 26.18. *Let R be a commutative ring. Let M be a left-R-module. Let $r \in R$. Then $rM = \{rm : m \in M\}$ is a submodule of M.*

PROOF: Easy. ∎

Proposition 26.19. *Let R be a ring. Let M be a left-R-module. Let I be a left-ideal in R. Then $IM = \{rm : r \in I, m \in M\}$ is a submodule of M.*

PROOF:

$\langle 1\rangle 1.$ IM is a subgroup of M.
  $\langle 2\rangle 1.$ LET: $r, s \in I$ and $m, n \in M$.
    PROVE: $rm + sn \in IM$
  $\langle 2\rangle 2.$ $rm + sn = r(m - n) + (s - r)n$
$\langle 1\rangle 2.$ For all $r \in R$ and $x \in IM$ we have $rx \in IM$.
$\square$

26.3 Quotient Modules

Definition 26.20 (Quotient Module)**.** Let R be a ring. Let M be a left-R-module. Let N be a submodule of M. Then the *quotient module* M/N is the quotient group M/N under

$$r(m + N) = rm + N \enspace .$$

Proposition 26.21. *Let R be a ring. Let M and P be left-R-modules. Let N be a submodule of M. Let $\phi : M \to P$ be an R-module homomorphism. If $N \subseteq \ker \phi$, then there exists a unique R-module homomorphism $\overline{\phi} : M/N \to P$ such that the following diagram commutes.*

$$\begin{tikzcd}
M \arrow[rr, "\phi"] \arrow[dr] & & P \\
& M/N \arrow[ur, "\overline{\phi}"] &
\end{tikzcd}$$

PROOF: Easy. $\square$

Theorem 26.22. *Every R-module homomorphism $\phi : M \to M'$ may be decomposed as:*

$$M \longrightarrow M/\ker\phi \xrightarrow{\cong} \operatorname{im}\phi \longrightarrow N$$

PROOF: Easy. $\square$

Corollary 26.22.1 (First Isomorphism Theorem)**.** *Let $\phi : M \to M'$ be a surjective R-module homomorphism. Then*

$$M' \cong \frac{M}{\ker\phi} \enspace .$$

Proposition 26.23 (Second Isomorphism Theorem)**.** *Let R be a ring. Let M be a left-R-module. Let N and P be submodules of M. Then $N + P$ is a submodule of M, $N \cap P$ is a submodule of P, and*

$$\frac{N + P}{N} \cong \frac{P}{N \cap P}$$

PROOF: The function that maps P to $p + N$ is a surjective homomorphism $P \to (N + P)/N$ with kernel $N \cap P$. $\square$

Proposition 26.24 (Third Isomorphism Theorem)**.** *Let R be a ring. Let M be a left-R-module. Let N be a submodule of M and P a submodule of N. Then N/P is a submodule of M/P and*

$$\frac{M/P}{N/P} \cong \frac{M}{N}$$

PROOF: The canonical map $M \to M/N$ induces a surjective homomorphism $M/P \to M/N$ which has kernel N/P. □

Proposition 26.25. *Let R be a ring. Let M be a left-R-module. The sum and intersection of a family of submodules of M are submodules of M.*

PROOF: Easy. □

26.4 Products

Proposition 26.26. $R-\textbf{Mod}$ *has products.*

PROOF: Given a family $\{M_\alpha\}_{\alpha\in A}$ of left-R-modules, we make $\prod_{\alpha\in A} M_\alpha$ into a left-R-module by

$$\begin{aligned}(f+g)(\alpha) &= f(\alpha)+g(\alpha)\\ (rf)(\alpha) &= rf(\alpha)\end{aligned}$$

□

26.5 Coproducts

Proposition 26.27. $R-\textbf{Mod}$ *has coproducts.*

PROOF: Given a family $\{M_\alpha\}_{\alpha\in A}$ of left-R-modules, take $\bigoplus_{\alpha\in A} M_\alpha$ to be $\{f \in \prod_{\alpha\in A} M_\alpha : f(\alpha) = 0$ for all but finitely many $\alpha \in A\}$. □

26.6 Direct Sum

Definition 26.28 (Direct Sum)**.** Let R be a ring. Let M and N be left-R-modules. Then the direct sum $M \oplus N$ is an R-module under

$$r(m,n) = (rm, rn)\ \ .$$

Proposition 26.29. *$M \oplus N$ is the biproduct of M and N in* $R-\textbf{Mod}$.

PROOF: Easy. □

Example 26.30. Infinite products and coproducts are in general different. We have $\mathbb{Z}^{\mathbb{N}} \not\cong \mathbb{Z}^{\oplus\mathbb{N}}$ since $\mathbb{Z}^{\mathbb{N}}$ is uncountable but $\mathbb{Z}^{\oplus\mathbb{N}}$ is countable.

26.7 Kernels and Cokernels

Proposition 26.31. *Let R be a ring. Let $\phi : M \to N$ be a left-R-module homomorphism. Then $\ker\phi \hookrightarrow M$ is terminal in the category of left-R-module homomorphisms $\alpha : P \to M$ such that $\phi \circ \alpha = 0$.*

Proof: Easy. □

Proposition 26.32. *Let R be a ring. Let $\phi : M \to N$ be a left-R-module homomorphism. Then $N \twoheadrightarrow \operatorname{coker}\phi$ is initial in the category of left-R-module homomorphisms $\alpha : N \to P$ such that $\alpha \circ \phi = 0$.*

Proof: Easy. □

Proposition 26.33. *Let R be a ring. Let $\phi : M \to N$ be a left-R-module homomorphism. Then the following are equivalent.*

- *ϕ is a monomorphism.*
- *$\ker\phi$ is trivial.*
- *ϕ is injective.*

Proof: Easy. □

Proposition 26.34. *Let R be a ring. Let $\phi : M \to N$ be a left-R-module homomorphism. Then the following are equivalent.*

- *ϕ is an epimorphism.*
- *$\operatorname{coker}\phi$ is trivial.*
- *ϕ is surjective.*

Proof: Easy. □

Proposition 26.35. *Every monomorphism in $R-\mathbf{Mod}$ is the kernel of some homomorphism.*

Proof: If $\phi : M \to N$ is a monomorphism then it is the kernel of $N \twoheadrightarrow N/\operatorname{im}\phi$. □

Proposition 26.36. *Every epimorphism in $R-\mathbf{Mod}$ is the cokernel of some homomorphism.*

Proof: If $\phi : M \to N$ is epi then it is the cokernel of $\ker\phi \hookrightarrow M$. □

Example 26.37. Monomorphisms do not split in $R-\mathbf{Mod}$. Multiplication by 2 is a monomorphism $\mathbb{Z} \to \mathbb{Z}$ but has no left inverse.

Example 26.38. Epimorphisms do not split in $R-\mathbf{Mod}$. The canonical map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is an epimorphism without a right inverse.

26.8 Free Modules

Proposition 26.39. *Let R be a ring and A a set. Then there exists a left-R-module $F^R(A)$ and function $j : A \to F^R(A)$ such that, for any left-R-module M and function $f : A \to M$, there exists a unique left-R-module homomorphism $\overline{f} : F^R(A) \to M$ such that the following diagram commutes.*

$$\begin{tikzcd} F^R(A) \arrow[r, "\overline{f}"] & M \\ A \arrow[u, "j"] \arrow[ur, "f"'] & \end{tikzcd}$$

Proof:
⟨1⟩1. Let: $R^{\oplus A} = \{\alpha : A \to R : \alpha(a) = 0$ for all but finitely many $a \in A\}$ under the operations
$$(\alpha + \beta)(a) = \alpha(a) + \beta(a)$$
$$(r\alpha)(a) = r\alpha(a)$$
⟨1⟩2. $R^{\oplus A}$ is a left-R-module.
⟨1⟩3. Let: $j : A \to R^{\oplus A}$ be the function
$$j(a)(a') = \begin{cases} 1 & \text{if } a = a' \\ 0 & \text{if } a \neq a' \end{cases}$$
⟨1⟩4. Let: M be any left-R-module.
⟨1⟩5. Let: $f : A \to M$ be a function.
⟨1⟩6. Let: $\overline{f} : R^{\oplus A} \to M$ be the function
$$\overline{f}(\alpha) = \sum_{a \in A, \alpha(a) \neq 0} \alpha(a) f(a)$$
⟨1⟩7. $\overline{f}$ is a left-R-module homomorphism.
⟨1⟩8. $\overline{f} \circ j = f$
⟨1⟩9. $\overline{f}$ is unique.

Definition 26.40. We call $j : A \to F^R(A)$ the *free* left-R-module over A.

Proposition 26.41. *j is injective.*

Proof: By the proof of the previous proposition. □

Proposition 26.42. *Let R be a ring. Let F be a non-zero free left-R-module. Let $\phi : M \to N$ be a left-R-module homomorphism. Then ϕ is onto if and only if, for every left-R-module homomorphism $\alpha : F \to N$, there exists a left-R-module homomorphism $\beta : F \to M$ such that the diagram below commutes.*

$$\begin{tikzcd} M \arrow[r, "\phi"] & N \\ F \arrow[u, "\beta"] \arrow[ur, "\alpha"'] & \end{tikzcd}$$

Proof:

⟨1⟩1. Let: F be the free left-R-module over A with injection $j : A \to F$.
⟨1⟩2. If ϕ is onto then, for every homomorphism $\alpha : F \to N$, there exists a homomorphism $\beta : F \to M$ such that $\phi \circ \beta = \alpha$.
⟨2⟩1. Assume: ϕ is onto.
⟨2⟩2. Let: $\alpha : F \to N$ be a homomorphism.
⟨2⟩3. For $a \in A$, Pick $f(a) \in M$ such that $\phi(f(a)) = \alpha(j(a))$
⟨2⟩4. Let: $\beta : F \to M$ be the unique homomorphism such that $\beta \circ j = f$
⟨2⟩5. $\phi \circ \beta = \alpha$
Proof: Each is the unique homomorphism such that $\alpha \circ j = \phi \circ f$.
□

$$\begin{tikzcd} & M \arrow[r, "\phi"] & N \\ A \arrow[ur, "f"] \arrow[r, "j"] & F \arrow[u, "\beta"] \arrow[ur, "\alpha"] & \end{tikzcd}$$

⟨1⟩3. If, for every homomorphism $\alpha : F \to N$, there exists a homomorphism $\beta : F \to M$ such that $\phi \circ \beta = \alpha$, then ϕ is onto.
⟨2⟩1. Assume: For every homomorphism $\alpha : F \to N$ there exists a homomorphism $\beta : F \to M$ such that $\phi \circ \alpha = \beta$.
⟨2⟩2. Let: $n \in N$
⟨2⟩3. Let: $\alpha : F \to N$ be the unique homomorphism such that, for all $a \in A$, we have $\alpha(j(a)) = n$
⟨2⟩4. Pick a homomorphism $\beta : F \to M$ such that $\phi \circ \beta = \alpha$
⟨2⟩5. Pick $a \in A$
⟨2⟩6. $\phi(\beta(j(a))) = n$
□

26.9 Generators

Definition 26.43 (Submodule Generated by a Set)**.** Let R be a ring. Let M be a left-R-module. Let A be a subset of M. Let $\phi_A : F^R(A) \to M$ be the unique left-R-module homomorphism such that the following diagram commutes.

$$\begin{tikzcd} F^R(A) \arrow[r, "\phi_A"] & M \\ A \arrow[u] \arrow[ur, hook] & \end{tikzcd}$$

The submodule of M *generated* by A, denoted $\langle A \rangle$, is defined to be $\operatorname{im} \phi_A$.

Definition 26.44 (Finitely Generated)**.** Let R be a ring. Let M be a left-R-module. Then M is *finitely generated* iff there exists a finite set $A \subseteq M$ such that $M = \langle A \rangle$.

Example 26.45. A submodule of a finitely generated module is not necessarily finitely generated.

Let $R = \mathbb{Z}[x_1, x_2, \ldots]$. Then R is finitely generated as an R-module, but $(x_1, x_2, \ldots)$ is not.

Proposition 26.46. *The homomorphic image of a finitely generated module is finitely generated.*

PROOF: Easy. □

Proposition 26.47. *Let R be a ring. Let M be a left-R-module. Let N be a submodule of M. If N and M/N are finitely generated then M is finitely generated.*

PROOF:
⟨1⟩1. PICK $a_1, \ldots, a_n$ that generate N.
⟨1⟩2. PICK $b_1, \ldots, b_m$ such that $b_1 + N, \ldots, b_m + N$ generate M/N.
PROVE: $a_1, \ldots, a_n, b_1, \ldots, b_m$ generate M.
⟨1⟩3. LET: $m \in M$
⟨1⟩4. PICK $r_1, \ldots, r_m \in R$ such that $m + N = r_1 b_1 + \cdots + r_m b_m + N$
⟨1⟩5. $m - r_1 b_1 - \cdots - r_m b_m \in N$
⟨1⟩6. PICK $s_1, \ldots, s_n \in R$ such that $m - r_1 b_1 - \cdots - r_m b_m = s_1 a_1 + \cdots + s_n a_n$
⟨1⟩7. $m = r_1 b_1 + \cdots + r_m b_m + s_1 a_1 + \cdots + s_n a_n$
□

26.10 Projections

Definition 26.48 (Projection)**.** Let R be a ring. Let M be a left-R-module. Let $p : M \to M$ be a left-R-module homomorphism. Then p is a *projection* iff $p^2 = p$.

Proposition 26.49. *Let R be a ring. Let M be a left-R-module. Let $p : M \to M$ be a projection. Then*
$$M \cong \ker p \oplus \operatorname{im} p \enspace .$$

PROOF:
⟨1⟩1. LET: $\phi : M \to \ker p \oplus \operatorname{im} p$ be the map $\phi(m) = (m - p(m), p(m))$
⟨1⟩2. ϕ is a left-R-module homomorphism.
⟨1⟩3. ϕ is injective.
⟨1⟩4. ϕ is surjective.
□

26.11 Pullbacks

Proposition 26.50. $R-\mathbf{Mod}$ *has pullbacks.*

PROOF:
⟨1⟩1. LET: $\mu : M \to Z$, $\nu : N \to Z$ be left-R-module homomorphisms.
⟨1⟩2. LET: $M \times_Z N = \{(m, n) \in M \times N : \mu(m) = \nu(n)\}$ under
$$(m, n) + (m', n') = (m + m', n + n')$$
$$r(m, n) = (rm, rn)$$
⟨1⟩3. $M \times_Z N$ is the pullback of M and N.
□

26.12 Pushouts

Proposition 26.51. $R - \mathbf{Mod}$ *has pushouts.*

PROOF:
⟨1⟩1. LET: $\mu : A \to M$ and $\nu : A \to N$ be left-R-module homomorphisms.

Chapter 27

Cyclic Modules

Definition 27.1 (Cyclic Module)**.** Let R be a ring. Let M be a left-R-module. Then M is *cyclic* iff there exists $m \in M$ such that $M = \langle m \rangle$.

Proposition 27.2. *Let R be a ring. Let M be a left-R-module. Then M is cyclic if and only if there exists a left-ideal I in R such that $M \cong R/I$.*

PROOF:
$\langle 1 \rangle 1$. If M is cyclic then there exists a left-ideal I in R such that $M \cong R/I$.
  $\langle 2 \rangle 1$. ASSUME: M is cyclic.
  $\langle 2 \rangle 2$. PICK $m \in M$ such that $M = \langle m \rangle$
  $\langle 2 \rangle 3$. LET: $\phi : R \to M$ be the left-R-module homomorphism $\phi(r) = rm$.
  $\langle 2 \rangle 4$. ϕ is surjective.
  $\langle 2 \rangle 5$. $M \cong R/ \ker \phi$
$\langle 1 \rangle 2$. For every left-ideal I in R, we have that R/I is cyclic.
  PROOF: R/I is generated by $1 + I$.
$\square$

Proposition 27.3. *A quotient of a cyclic module is cyclic.*

PROOF: If M is generated by m then M/N is generated by $m + N$. $\square$

Proposition 27.4. *Let R be a ring. For any left-ideal I in R and any left-R-module N, we have*

$$R - \mathbf{Mod}[R/I, N] \cong \{n \in N : \forall a \in I.an = 0\} \ .$$

PROOF:
$\langle 1 \rangle 1$. LET: $\Phi : R - \mathbf{Mod}[R/I, N] \to \{n \in N : \forall a \in I.an = 0\}$ be the function $\Phi(\alpha) = \alpha(1 + I)$
  PROOF: For all $a \in I$ we have $a\alpha(1 + I) = \alpha(a + I) = \alpha(I) = 0$.
$\langle 1 \rangle 2$. Φ is injective.
  PROOF: If $\alpha(1+I) = \beta(1+I)$ then $\alpha(r+I) = r\alpha(1+I) = r\beta(1+I) = \beta(r+I)$ for all $r \in R$, hence $\alpha = \beta$.

$\langle 1 \rangle 3.$ Φ is surjective.

PROOF: Given $n \in N$ such that $\forall a \in I.an = 0$, define $\alpha : R/I \to N$ by $\alpha(r + I) = rn$.

$\langle 1 \rangle 4.$ If R is commutative then Φ is an R-module homomorphism.

$\square$

Corollary 27.4.1. *For all $a, b \in \mathbb{Z}$ we have $\mathbf{Ab}[\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}] \cong \mathbb{Z}/\gcd(a,b)\mathbb{Z}$.*

PROOF:

$$\begin{aligned}
\mathbf{Ab}[\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}] &\cong \mathbb{Z} - \mathbf{Mod}[\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}] \\
&\cong \{n \in \mathbb{Z}/b\mathbb{Z} : \forall x \in a\mathbb{Z}.xn \cong 0 (\operatorname{mod} b)\} \\
&\cong \{n \in \mathbb{Z}/b\mathbb{Z} : \forall x \in \mathbb{Z}.b \mid xan\} \\
&= \{n \in \mathbb{Z}/b\mathbb{Z} : b \mid an\}
\end{aligned}$$

Chapter 28

Simple Modules

Definition 28.1 (Simple Module)**.** Let R be a ring. An R-module M is *simple* or *irreducible* iff its only submodules are $\{0\}$ and M.

Proposition 28.2 (Schur's Lemma)**.** *Let R be a ring. Let M and N be simple R-modules. Let $\phi : M \to N$ be an R-module homomorphism. Then either $\phi = 0$ or ϕ is an isomorphism.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: $\phi \neq 0$
$\langle 1 \rangle 2$. $\ker \phi = 0$
PROOF: Since $\ker \phi$ is a submodule of M that is not M.
$\langle 1 \rangle 3$. $\operatorname{im} \phi = N$
PROOF: Since $\operatorname{im} \phi$ is a submodule of N that is not $\{0\}$.
∎

Proposition 28.3. *Every simple module is cyclic.*

PROOF:
$\langle 1 \rangle 1$. LET: M be a simple module.
$\langle 1 \rangle 2$. ASSUME: w.l.o.g. $M \neq \{0\}$
PROOF: $\{0\} = \langle 0 \rangle$ is cyclic.
$\langle 1 \rangle 3$. PICK $m \in M$ with $m \neq 0$
$\langle 1 \rangle 4$. $\langle m \rangle = M$
PROOF: Since $\langle m \rangle$ is a submodule of M that is not $\{0\}$.
∎

Chapter 29

Noetherian Modules

Definition 29.1 (Noetherian Module)**.** Let R be a ring. A left-R-module is *Noetherian* iff every submodule is finitely generated.

Proposition 29.2. *Let R be a ring. Let M be a left-R-module and N a submodule of M. Then M is Noetherian if and only if N and M/N are Noetherian.*

PROOF:
$\langle 1\rangle 1$. If M is Noetherian then N is Noetherian.
  PROOF: Every submodule of N is a submodule of M, hence finitely generated.
$\langle 1\rangle 2$. If M is Noetherian then M/N is Noetherian.
  $\langle 2\rangle 1$. ASSUME: M is Noetherian.
  $\langle 2\rangle 2$. LET: $\pi : M \twoheadrightarrow M/N$ be the canonical epimorphism.
  $\langle 2\rangle 3$. LET: P be a submodule of M/N.
  $\langle 2\rangle 4$. PICK $a_1, \ldots, a_n \in M$ that generate $\pi^{-1}(P)$.
  $\langle 2\rangle 5$. $a_1 + N, \ldots, a_n + N$ generate P.
$\langle 1\rangle 3$. If N and M/N are Noetherian then M is Noetherian.
  $\langle 2\rangle 1$. ASSUME: N and M/N are Noetherian.
  $\langle 2\rangle 2$. LET: P be a submodule of M.
  $\langle 2\rangle 3$. PICK $a_1, \ldots, a_m \in P$ such that $a_1 + N, \ldots, a_m + N$ generate $\pi(P)$.
  $\langle 2\rangle 4$. PICK $b_1, \ldots, b_n \in M$ that generated $P \cap N$.
    PROVE: $a_1, \ldots, a_m, b_1, \ldots, b_n$ generate P.
  $\langle 2\rangle 5$. LET: $p \in P$
  $\langle 2\rangle 6$. PICK $r_1, \ldots, r_m \in R$ such that $p + N = r_1 a_1 + \cdots + r_m a_m + N$
  $\langle 2\rangle 7$. $p - r_1 a_1 - \cdots - r_m a_m \in P \cap N$
  $\langle 2\rangle 8$. PICK $s_1, \ldots, s_n \in R$ such that $p - r_1 a_1 - \cdots - r_m a_m = s_1 b_1 + \cdots + s_n b_n$
  $\langle 2\rangle 9$. $p = r_1 a_1 + \cdots + r_m a_m + s_1 b_1 + \cdots + s_n b_n$
□

Corollary 29.2.1. *If R is a Noetherian ring then $R^{\oplus n}$ is a Noetherian left-R-module.*

PROOF: The proof is by induction on n. The case $n = 1$ is immediate.
The induction step holds since $R^{\oplus(n+1)}/R^{\oplus n} \cong R$. □

Corollary 29.2.2. *If R is a Noetherian ring and M is a finitely generated left-R-module then M is Noetherian.*

Proof: There is a surjective homomorphism $R^{\oplus n} \twoheadrightarrow M$ for some n, so M is a quotient of $R^{\oplus n}$. $\square$

Chapter 30

Algebras

Definition 30.1 (Algebra)**.** Let R be a commutative ring. An R-*algebra* consists of a ring S and a ring homomorphism $\alpha : R \to S$ such that $\alpha(R)$ is included in the center of S. We write rs for $\alpha(r)s$.

Proposition 30.2. *Let R be a commutative ring and S a ring. Let $\cdot : R \times S \to S$. Then there exists $\alpha : R \to S$ that makes S into an R-algebra such that*

$$rs = \alpha(r)s \qquad (r \in R, s \in S)$$

iff S is an R-module under $\cdot$ and, for all $r_1, r_2 \in R$ and $s_1, s_2 \in S$,

$$(r_1 s_1)(r_2 s_2) = (r_1 r_2)(s_1 s_2) \ .$$

Proof: Immediate from definitions. □

Example 30.3. Let R be a commutative ring. Then R is an R-algebra under multiplication.

Example 30.4. Let R be a commutative ring and I an ideal in R. Then R/I is an R-algebra.

Example 30.5. Let R be a commutative ring and M an R-module. Then $\mathrm{End}_{R-\mathbf{Mod}}(M)$ is an R-algebra under composition.

Example 30.6. Let R be a commutative ring. Then $\mathfrak{gl}_n(R)$ is an R-algebra under matrix multiplication.

Definition 30.7 (Algebra Homomorphism)**.** Let R be a commutative ring. Let S and T be R-algebras. An *R-algebra homomorphism* $\phi : S \to T$ is a ring homomorphism such that, for all $r \in R$ and $s \in S$, we have $\phi(rs) = r\phi(s)$.

Let $R - \mathbf{Alg}$ be the category of R-algebras and R-algebra homomorphisms.

Example 30.8.

$$\mathbb{Z} - \mathbf{Alg} \cong \mathbf{Ring}$$

Example 30.9. Let R be a commutative ring. Then $R[x_1, \ldots, x_n]$, and any quotient ring of $R[x_1, \ldots, x_n]$, is a commutative R-algebra.

Example 30.10. R is the initial object in $R - \mathbf{Alg}$.

30.1 Rees Algebra

Definition 30.11 (Rees Algebra)**.** Let R be a commutative ring. Let I be an ideal in R. The *Rees algebra* is the direct sum

$$\mathrm{Rees}_R(I) = \bigoplus_{j \geq 0} I^j$$

under the multiplication

$$(r_0, r_1, r_2, r_3, \ldots)(s_0, s_1, s_2, \ldots) = (r_0 s_0, r_1 s_0 + r_0 s_1, r_0 s_2 + r_1 s_1 + r_2 s_0, \ldots)$$
$$r(r_0, r_1, r_2, \ldots) = (r r_0, r r_1, r r_2, \ldots)$$

Proposition 30.12. *Let R be a commutative ring. Let $a \in R$ be a non-zero-divisor. Then $R[x]$ is the Rees algebra of (a).*

Proof:
⟨1⟩1. Let: $\phi : R[x] \to \mathrm{Rees}_R((a))$ be the function $\phi(r_0 + r_1 x + r_2 x^2 + \cdots) = (r_0, r_1 a, r_2 a^2, \ldots)$.
⟨1⟩2. ϕ is an R-algebra homomorphism.
⟨1⟩3. ϕ is injective.
⟨2⟩1. Let: $\phi(r_0 + r_1 x + r_2 x^2 + \cdots) = \phi(s_0 + s_1 x + s_2 x^2 + \cdots)$
⟨2⟩2. For all n we have $r_n a^n = s_n a^n$
⟨2⟩3. $(r_n - s_n) a^n = 0$
⟨2⟩4. $r_n - s_n = 0$
Proof: Since a is not a zero-divisor.
⟨2⟩5. $r_n = s_n$
⟨1⟩4. ϕ is surjective.
□

Proposition 30.13. *Let R be a commutative ring. Let $a \in R$ be a non-zero-divisor. Let I be an ideal of R. Then $\mathrm{Rees}_R(I) \cong \mathrm{Rees}_R(aI)$.*

Proof:
⟨1⟩1. Let: $\phi : \mathrm{Rees}_R(I) \to \mathrm{Rees}_R(aI)$ be the function $\phi(r_0, r_1, r_2, \ldots) = (r_0, a r_1, a^2 r_2, \ldots)$.
⟨1⟩2. ϕ is an R-algebra homomorphism.
⟨1⟩3. ϕ is injective.
⟨1⟩4. ϕ is surjective.
□

30.2 Free Algebras

Proposition 30.14. *Let R be a ring. Then $R[x_1, \ldots, x_n]$ is the free commutative R-algebra on $\{1, \ldots, n\}$.*

Proof: Easy. □

Proposition 30.15. *Let R be a ring and A a set. Let A^* be the free monoid on A. Then the monoid ring $R[A^*]$ is the free R-algebra on A.*

PROOF: Easy. □

Proposition 30.16. *Let R be a commutative ring and S a commutative R-algebra. Then S is finitely generated as an R-algebra if and only if S is finitely generated as a commutative R-algebra.*

PROOF: Since a subalgebra of a commutative subalgebra is commutative, so the smallest algebra that contains $\{a_1, \dots, a_n\}$ is the smallest commutative subalgebra that contains $\{a_1, \dots, a_n\}$. □

Chapter 31

Algebras of Finite Type

Definition 31.1 (Algebra of Finite Type)**.** Let R be a ring. Let S be an R-algebra. Then R is of *finite type* iff S is a finitely generated R-algebra.

Proposition 31.2. *Let R be a Noetherian ring. Let S be a finite-type R-algebra. Then S is a Noetherian ring.*

Chapter 32

Finite Algebras

Definition 32.1 (Finite Algebra)**.** Let R be a ring. Let S be an R-algebra. Then S is a *finite* R-algebra iff it is a finitely generated left-R-module.

Proposition 32.2. *Let R be a ring. Every finite R-algebra is of finite type.*

PROOF: If S is generated by $a_1, \ldots, a_n$ as an R-module, then it is generated by $a_1, \ldots, a_n$ as an R-algebra. □

Example 32.3. The converse does not hold. $R[x]$ is of finite type but is not finite.

Chapter 33

Division Algebras

Definition 33.1 (Division Algebra)**.** Let R be a commutative ring. A *division R-algebra* is an R-algebra that is a division ring.

Example 33.2. Let R be a commutative ring. Let M be a simple R-algebra. Then $\mathrm{End}_{R-\mathbf{Mod}}(M)$ is a division algebra. For if $\phi \circ \psi = 0$ then ϕ and ψ cannot both be isomorphisms, hence $\phi = 0$ or $\psi = 0$ by Schur's Lemma.

Chapter 34

Chain Complexes

Definition 34.1 (Chain Complex)**.** Let R be a ring. A *chain complex of left-R-modules* $M_\bullet = (M_\bullet, d_\bullet)$ consists of a family of left-R-modules $\{M_i\}_{i\in\mathbb{Z}}$ and a family of left-R-module homomorphisms $\{d_i : M_i \to M_{i-1}\}_{i\in\mathbb{Z}}$ such that, for all i,

$$d_i \circ d_{i+1} = 0 \ .$$

We call each d_i a *differential* and the family $\{d_i\}_i$ the *boundary* of the chain complex.

Definition 34.2 (Exact)**.** A chain complex $M_\bullet$ is *exact* at M_i iff $\operatorname{im} d_{i+1} = \ker d_i$.

It is *exact* or an *exact sequence* iff it is exact at M_i for all i.

Proposition 34.3. *A complex*

$$\cdots \to 0 \to L \overset{\alpha}{\to} M \to \cdots$$

is exact at L iff α is a monomorphism.

Proof: Since both are equivalent to $\ker \alpha = 0$. □

Proposition 34.4. *A complex*

$$\cdots \to M \overset{\beta}{\to} N \to 0 \to \cdots$$

is exact at N iff β is a epimorphism.

Proof: Since both are equivalent to $\operatorname{im} \beta = N$. □

Definition 34.5 (Short Exact Sequence)**.** A *short exact sequence* is an exact complex of the form

$$0 \to L \overset{\alpha}{\to} M \overset{\beta}{\to} N \to 0 \ .$$

Proposition 34.6 (Four-Lemma)**.** *If*

$$\begin{array}{ccccccc} A_1 & \xrightarrow{f_1} & B_1 & \xrightarrow{g_1} & C_1 & \xrightarrow{h_1} & D_1 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\delta} \\ A_2 & \xrightarrow{f_2} & B_2 & \xrightarrow{g_2} & C_2 & \xrightarrow{h_2} & D_2 \end{array}$$

is a commutative diagram of left-R-modules with exact rows, α is an epimorphism, and β and δ are monomorphisms, then γ is an monomorphism.

Proof:
$\langle 1\rangle 1.$ Let: $x, y \in C_1$
$\langle 1\rangle 2.$ Assume: $\gamma(x) = \gamma(y)$
$\langle 1\rangle 3.$ $\delta(h_1(x)) = \delta(h_1(y))$
$\langle 1\rangle 4.$ $h_1(x) = h_1(y)$
  Proof: δ is injective.
$\langle 1\rangle 5.$ $x - y \in \ker h_1$
$\langle 1\rangle 6.$ $x - y \in \operatorname{im} g_1$
$\langle 1\rangle 7.$ Pick $b \in B_1$ such that $g_1(b) = x - y$.
$\langle 1\rangle 8.$ $g_2(\beta(b)) = 0$
  Proof: $g_2(\beta(b)) = \gamma(g_1(b)) = \gamma(x - y) = 0$
$\langle 1\rangle 9.$ $\beta(b) \in \ker g_2$
$\langle 1\rangle 10.$ $\beta(b) \in \operatorname{im} f_2$
$\langle 1\rangle 11.$ Pick $a' \in A_2$ such that $f_2(a') = \beta(b)$
$\langle 1\rangle 12.$ Pick $a \in A_1$ such that $\alpha(a) = a'$
  Proof: α is surjective.
$\langle 1\rangle 13.$ $\beta(f_1(a)) = \beta(b)$
$\langle 1\rangle 14.$ $f_1(a) = b$
  Proof: β is injective.
$\langle 1\rangle 15.$ $0 = g_1(b)$
  Proof: Since $g_1(b) = g_1(f_1(a)) = 0$.
$\langle 1\rangle 16.$ $x = y$
  Proof: $\langle 1\rangle 7$
□

Proposition 34.7 (Four-Lemma)**.** *If*

$$\begin{array}{ccccccc} A_1 & \xrightarrow{f_1} & B_1 & \xrightarrow{g_1} & C_1 & \xrightarrow{h_1} & D_1 \\ \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\delta} & & \downarrow{\scriptstyle\epsilon} \\ A_2 & \xrightarrow{f_2} & B_2 & \xrightarrow{g_2} & C_2 & \xrightarrow{h_2} & D_2 \end{array}$$

is a commutative diagram of left-R-modules with exact rows, β and δ are epimorphisms, and ϵ is a monomorphism, then γ is an epimorphism.

Proof:
$\langle 1\rangle 1.$ Let: $b_2 \in B_2$

$\langle 1\rangle 2.$ Pick $c_1 \in C_1$ such that $\delta(c_1) = g_2(b_2)$
Proof: δ is surjective.
$\langle 1\rangle 3.$ $\epsilon(h_1(c_1)) = 0$
$\langle 1\rangle 4.$ $h_1(c_1) = 0$
Proof: ϵ is injective.
$\langle 1\rangle 5.$ $c_1 \in \ker h_1$
$\langle 1\rangle 6.$ $c_1 \in \operatorname{im} g_1$
$\langle 1\rangle 7.$ Pick $b_1 \in B_1$ such that $g_1(b_1) = c_1$
$\langle 1\rangle 8.$ $g_2(\gamma(b_1)) = g_2(b_2)$
$\langle 1\rangle 9.$ $\gamma(b_1) - b_2 \in \ker g_2$
$\langle 1\rangle 10.$ $\gamma(b_1) - b_2 \in \operatorname{im} f_2$
$\langle 1\rangle 11.$ Pick $a_2 \in A_2$ such that $f_2(a_2) = \gamma(b_1) - b_2$.
$\langle 1\rangle 12.$ Pick $a_1 \in A_1$ such that $\beta(a_1) = a_2$.
Proof: β is surjective.
$\langle 1\rangle 13.$ $\gamma(f_1(a_1)) = \gamma(b_1) - b_2$
$\langle 1\rangle 14.$ $b_2 = \gamma(b_1 - f_1(a_1))$
□

Theorem 34.8 (Snake Lemma). *Suppose we have R-modules and homomorphisms*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L_1 & \xrightarrow{\alpha_1} & M_1 & \xrightarrow{\beta_1} & N_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\lambda} & & \downarrow{\scriptstyle\mu} & & \downarrow{\scriptstyle\nu} & & \\ 0 & \longrightarrow & L_0 & \xrightarrow{\alpha_0} & M_0 & \xrightarrow{\beta_0} & N_0 & \longrightarrow & 0 \end{array}$$

such that the diagram commutes and the two rows are short exact sequences. Then there exists a homomorphism $\delta : \ker \nu \to \operatorname{coker} \lambda$ *such that the following is an exact sequence.*

$$0 \to \ker \lambda \xrightarrow{\alpha_1} \ker \mu \xrightarrow{\beta_1} \ker \nu \xrightarrow{\delta} \operatorname{coker} \lambda \xrightarrow{\alpha_0} \operatorname{coker} \mu \xrightarrow{\beta_0} \operatorname{coker} \nu \to 0 \ .$$

Proof:
$\langle 1\rangle 1.$ Define $\delta : \ker \nu \to \operatorname{coker} \lambda$.
$\langle 2\rangle 1.$ Let: $a \in \ker \nu$
$\langle 2\rangle 2.$ Pick $c \in M_1$ such that $\beta_1(c) = a$.
Proof: Since β_1 is surjective.
$\langle 2\rangle 3.$ Let: $d = \mu(c)$
$\langle 2\rangle 4.$ $d \in \ker \beta_0 = \operatorname{im} \alpha_0$
Proof: Since $\beta_0(d) = \beta_0(\mu(c)) = \nu(a) = 0$.
$\langle 2\rangle 5.$ Let: $e \in L_0$ be the element such that $\alpha_0(e) = d$.
$\langle 2\rangle 6.$ Let: $\delta(a) = e + \operatorname{im} \lambda$
$\langle 1\rangle 2.$ δ is a left-R-module homomorphism.
$\langle 2\rangle 1.$ For $a, a' \in \ker \nu$ we have $\delta(a + a') = \delta(a) + \delta(a')$.
$\langle 3\rangle 1.$ Let: $a, a' \in \ker \nu$

⟨3⟩2. LET: $c, c', c'' \in M_1$ and $e, e', e'' \in L_0$ be the elements such that

$$\begin{aligned}
\beta_1(c) &= a \\
\beta_1(c') &= a' \\
\beta_1(c'') &= a + a' \\
\alpha_0(e) &= \mu(c) \\
\alpha_0(e') &= \mu(c') \\
\alpha_0(e'') &= \mu(c'') \\
\delta(a) &= e + \operatorname{im}\lambda \\
\delta(a') &= e' + \operatorname{im}\lambda \\
\delta(a + a') &= e'' + \operatorname{im}\lambda
\end{aligned}$$

⟨3⟩3. $c'' - c - c' \in \ker \beta_1 = \operatorname{im}\alpha_1$
⟨3⟩4. PICK $g \in L_1$ such that $\alpha_1(g) = c'' - c - c'$.
⟨3⟩5. $\alpha_0(\lambda(g)) = \alpha_0(e'' - e - e')$
⟨3⟩6. $\lambda(g) = e'' - e - e'$
⟨3⟩7. $e'' - e - e' \in \operatorname{im}\lambda$
⟨3⟩8. $e'' + \operatorname{im}\lambda = e + e' + \operatorname{im}\lambda$
⟨3⟩9. $\delta(a + a') = \delta(a) + \delta(a')$
⟨2⟩2. For $r \in R$ and $a \in \ker \nu$ we have $\delta(ra) = r\delta(a)$.
⟨3⟩1. LET: $r \in R$ and $a \in \ker \nu$
⟨3⟩2. LET: $c, c' \in M_1$ and $e, e' \in L_0$ be the elements such that

$$\begin{aligned}
\beta_1(c) &= a \\
\beta_1(c') &= ra \\
\alpha_0(e) &= \mu(c) \\
\alpha_0(e') &= \mu(c') \\
\delta(a) &= e + \operatorname{im}\lambda \\
\delta(ra) &= e' + \operatorname{im}\lambda
\end{aligned}$$

⟨3⟩3. $rc - c' \in \ker \beta_1 = \operatorname{im}\alpha_1$
⟨3⟩4. PICK $g \in L_1$ such that $\alpha_1(g) = rc - c'$.
⟨3⟩5. $\alpha_0(\lambda(g)) = \alpha_0(re - e')$
⟨3⟩6. $\lambda(g) = re - e'$
⟨3⟩7. $re - e' \in \operatorname{im}\lambda$
⟨3⟩8. $re + \operatorname{im}\lambda = e' + \operatorname{im}\lambda$
⟨3⟩9. $r\delta(a) = \delta(ra)$
⟨1⟩3. The sequence is exact at $\ker \lambda$.
PROOF: Since α_1 is injective.
⟨1⟩4. The sequence is exact at $\ker \mu$.
PROOF: Since $\operatorname{im}\alpha_1 = \ker \beta_1$.
⟨1⟩5. The sequence is exact at $\ker \nu$, i.e.
$beta_1(\ker \mu) = \ker \delta$.
⟨2⟩1. LET: $a \in \ker \nu$
⟨2⟩2. LET: $c \in M_1$ and $e \in L_0$ be the elements such that $\beta_1(c) = a$, $\alpha_0(e) = \mu(c)$, and $\delta(a) = e + \operatorname{im}\lambda$.

$\langle 2\rangle 3$. If $\delta(a) = \operatorname{im}\lambda$ then $a \in \beta_1(\ker\mu)$

$\langle 3\rangle 1$. Assume: $\delta(a) = \operatorname{im}\lambda$

$\langle 3\rangle 2$. $e \in \operatorname{im}\lambda$

$\langle 3\rangle 3$. Pick $g \in L_1$ such that $\lambda(g) = e$

$\langle 3\rangle 4$. $\mu(\alpha_1(g)) = \mu(c)$

$\langle 3\rangle 5$. $c - \alpha_1(g) \in \ker\mu$

$\langle 3\rangle 6$. $a = \beta_1(c - \alpha_1(g))$

$\langle 2\rangle 4$. If $a \in \beta_1(\ker\mu)$ then $\delta(a) = \operatorname{im}\lambda$

$\langle 3\rangle 1$. Assume: $c' \in \ker\mu$ and $a = \beta_1(c')$

$\langle 3\rangle 2$. $c - c' \in \ker\beta_1 = \operatorname{im}\alpha_1$

$\langle 3\rangle 3$. Pick $g \in L_1$ such that $\alpha_1(g) = c - c'$

$\langle 3\rangle 4$. $\alpha_0(\lambda(g)) = \mu(c) - \mu(c') = \alpha_0(e) - 0 = \alpha_0(e)$

$\langle 3\rangle 5$. $\lambda(g) = e$

$\langle 3\rangle 6$. $e \in \operatorname{im}\lambda$

$\langle 3\rangle 7$. $\delta(a) = \operatorname{im}\lambda$

$\langle 1\rangle 6$. THe sequence is exact at $\operatorname{coker}\lambda$.

$\langle 2\rangle 1$. Let: $e \in L_0$

Prove: $e + \operatorname{im}\lambda \in \operatorname{im}\delta$ iff $\alpha_0(e) \in \operatorname{im}\mu$.

$\langle 2\rangle 2$. For all $a \in \ker\nu$, if $\delta(a) = e + \operatorname{im}\lambda$ then $\alpha_0(e) \in \operatorname{im}\mu$

Proof: From $\langle 1\rangle 1$ and the fact that α_0 is injective hence e is unique given a.

$\langle 2\rangle 3$. For all $e \in L_0$, if $\alpha_0(e) \in \operatorname{im}\mu$ then $e + \operatorname{im}\lambda \in \operatorname{im}\delta$.

$\langle 3\rangle 1$. Let: $e \in L_0$

$\langle 3\rangle 2$. Assume: $\alpha_0(e) \in \operatorname{im}\mu$

$\langle 3\rangle 3$. Pick $c \in M_1$ such that $\mu(c) = \alpha_0(e)$.

Prove: $e + \operatorname{im}\lambda = \delta(\beta_1(c))$

$\langle 3\rangle 4$. Pick $c' \in M_1$ and $e' \in L_0$ such that $\beta_1(c') = \beta_1(c)$, $\alpha_0(e') = \mu(c')$ and $\delta(\beta_1(c)) = e' + \operatorname{im}\lambda$

$\langle 3\rangle 5$. $c - c' \in \ker\beta_1 = \operatorname{im}\alpha_1$

$\langle 3\rangle 6$. Pick $g \in L_1$ such that $\alpha_1(g) = c - c'$.

$\langle 3\rangle 7$. $\alpha_0(\lambda(g)) = \alpha_0(e - e')$

$\langle 3\rangle 8$. $\lambda(g) = e - e'$

$\langle 3\rangle 9$. $e + \operatorname{im}\lambda = e' + \operatorname{im}\lambda = \delta(\beta_1(c))$

$\langle 1\rangle 7$. The sequence is exact at $\operatorname{coker}\mu$.

Proof: Since $\operatorname{im}\alpha_0 = \ker\beta_0$.

$\langle 1\rangle 8$. The sequence is exact at $\operatorname{coker}\nu$.

Proof: Since β_0 is surjective.

□

Corollary 34.8.1. *Suppose we have R-modules and homomorphisms*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L_1 & \xrightarrow{\alpha_1} & M_1 & \xrightarrow{\beta_1} & N_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\lambda} & & \downarrow{\scriptstyle\mu} & & \downarrow{\scriptstyle\nu} & & \\ 0 & \longrightarrow & L_0 & \xrightarrow{\alpha_0} & M_0 & \xrightarrow{\beta_0} & N_0 & \longrightarrow & 0 \end{array}$$

such that the diagram commutes and the two rows are short exact sequences.

Suppose μ is surjective and ν is injective. Then λ is surjective and ν is an isomorphism.

Proof: We have $\ker \nu = \operatorname{coker} \mu = 0$ and so $0 \xrightarrow{\delta} \operatorname{coker} \lambda \xrightarrow{\alpha_0} 0$ is an exact sequence, hence $\operatorname{coker} \lambda = 0$ and so λ is surjective.
Since $\operatorname{coker} \mu = 0$ we have $0 \to \operatorname{coker} \nu \to 0$ is an exact sequence and so $\operatorname{coker} \nu = 0$, hence ν is surjective, hence ν is an isomorphism. ∎

Proposition 34.9 (Short Five-Lemma)**.** *Suppose we have R-modules and homomorphisms*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L_1 & \xrightarrow{\alpha_1} & M_1 & \xrightarrow{\beta_1} & N_1 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \nu} & & \\
0 & \longrightarrow & L_0 & \xrightarrow{\alpha_0} & M_0 & \xrightarrow{\beta_0} & N_0 & \longrightarrow & 0
\end{array}$$

such that the diagram commutes and the two rows are short exact sequences. If λ and ν are isomorphisms then μ is an isomorphism.

Proof:
⟨1⟩1. There exists a homomorphism $\delta : 0 \to L_0$ such that the following is an exact sequence.
$$0 \to 0 \to \ker \mu \to 0 \xrightarrow{\delta} L_0 \xrightarrow{\alpha_0} \operatorname{coker} \mu \xrightarrow{\beta_0} N_0 \to 0 \ .$$
Proof: Snake Lemma
⟨1⟩2. $\ker \mu = 0$
⟨1⟩3. $\operatorname{coker} \mu = M_0$
∎

Proposition 34.10. *If $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is an exact sequence and L and N are Noetherian then M is Noetherian.*

Proof:
⟨1⟩1. Let: P be a submodule of M.
⟨1⟩2. Pick $a_1, \ldots, a_m$ generate $\alpha^{-1}(P)$.
⟨1⟩3. Pick $c_1, \ldots, c_n$ that generate $\beta(P)$.
⟨1⟩4. For $i = 1, \ldots, n$, Pick b_i such that $\beta(b_i) = c_i$.
Prove: $\alpha(a_1), \ldots, \alpha(a_m), b_1, \ldots, b_n$ generate P.
⟨1⟩5. Let: $p \in P$
⟨1⟩6. Pick $r_1, \ldots, r_n \in R$ such that $r_1c_1 + \cdots + r_nc_n = \beta(p)$
⟨1⟩7. $r_1b_1 + \cdots + r_nb_n - p \in \ker \beta = \operatorname{im} \alpha$
⟨1⟩8. Pick $s_1, \ldots, s_m \in R$ such that $\alpha(s_1a_1 + \cdots + s_ma_m) = r_1b_1 + \cdots + r_nb_n - p$.
⟨1⟩9. $p = s_1\alpha(a_1) + \cdots + s_m\alpha(a_m) + r_1b_1 + \cdots + r_nb_n$
∎

Proposition 34.11. *Let R be a ring. Let*

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

be a short exact sequence of left-R-modules. Let L be an R-module. Then the following is an exact sequence:

$$0 \to R\text{–}\mathbf{Mod}[P, L] \stackrel{R-\mathbf{Mod}[\beta, \mathrm{id}_L]}{\longrightarrow} R\text{–}\mathbf{Mod}[N, L] \stackrel{R-\mathbf{Mod}[\alpha, \mathrm{id}_L]}{\longrightarrow} R\text{–}\mathbf{Mod}[M, L] \ .$$

PROOF:
⟨1⟩1. $R - \mathbf{Mod}[\beta, \mathrm{id}_L]$ is injective.
  PROOF: Since β is epi.
⟨1⟩2. $\mathrm{im}\, R - \mathbf{Mod}[\beta, \mathrm{id}_L] = \ker R - \mathbf{Mod}[\alpha, \mathrm{id}_L]$
  ⟨2⟩1. $\mathrm{im}\, R - \mathbf{Mod}[\beta, \mathrm{id}_L] \subseteq \ker R - \mathbf{Mod}[\alpha, \mathrm{id}_L]$
    PROOF: For any $\gamma \in R\text{–}\mathbf{Mod}[P, L]$ we have $\gamma \circ \beta \circ \alpha = 0$ because $\beta \circ \alpha = 0$.
  ⟨2⟩2. $\ker R - \mathbf{Mod}[\alpha, \mathrm{id}_L] \subseteq \mathrm{im}\, R - \mathbf{Mod}[\beta, \mathrm{id}_L]$
    ⟨3⟩1. LET: $\gamma \in \ker R - \mathbf{Mod}[\alpha, \mathrm{id}_L]$
    ⟨3⟩2. $\gamma \circ \alpha = 0$
    ⟨3⟩3. PICK $\delta : P \to L$ by: for all $p \in P$, we have $\delta(p) = \gamma(n)$ where $n \in N$ is an element such that $\beta(n) = p$.
      PROVE: $\delta \circ \beta = \gamma$
    ⟨3⟩4. LET: $n \in N$
      PROVE: $\delta(\beta(n)) = \gamma(n)$
    ⟨3⟩5. PICK $n' \in N$ such that $\delta(\beta(n)) = \gamma(n')$ and $\beta(n') = \beta(n)$
    ⟨3⟩6. $n - n' \in \ker \beta = \mathrm{im}\, \alpha$
    ⟨3⟩7. PICK $m \in M$ such that $\alpha(m) = n - n'$
    ⟨3⟩8. $0 = \gamma(\alpha(m)) = \gamma(n) - \gamma(n')$
    ⟨3⟩9. $\gamma(n) = \gamma(n') = \delta(\beta(n))$

□

Theorem 34.12 (Nine-Lemma)**.** *Let the following be a commuting diagram of left-R-modules.*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L_2 \arrow[r, "f_2"] \arrow[d, "\alpha_1"] & M_2 \arrow[r, "g_2"] \arrow[d, "\beta_1"] & N_2 \arrow[r] \arrow[d, "\gamma_1"] & 0 \\
0 \arrow[r] & L_1 \arrow[r, "f_1"] \arrow[d, "\alpha_0"] & M_1 \arrow[r, "g_1"] \arrow[d, "\beta_0"] & N_1 \arrow[r] \arrow[d, "\gamma_0"] & 0 \\
0 \arrow[r] & L_0 \arrow[r, "f_0"] \arrow[d] & M_0 \arrow[r, "g_0"] \arrow[d] & N_0 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

If the rows are exact and the two rightmost columns are exact then the left column is exact.

PROOF:
⟨1⟩1. (L_2, f_2) is the kernel of g_2, (L_1, f_1) is the kernel of g_1 and (L_0, f_0) is the kernel of g_0.

⟨1⟩2. 0 is the cokernel of g_2, g_1 and g_0.
⟨1⟩3. Pick a homomomorphism $\delta : L_0 \to 0$ such that the following is an exact sequence:

$$L_2 \overset{\beta_1 \restriction L_2}{\to} L_1 \overset{\beta_0 \restriction L_1}{\to} L_0 \overset{\delta}{\to} 0 \to 0 \to 0$$

Proof: Snake Lemma.
⟨1⟩4. $\beta_1 \restriction L_2 = \alpha_1$
⟨1⟩5. $\beta_0 \restriction L_1 = \alpha_0$
⟨1⟩6. The following is an exact sequence:

$$0 \to L_2 \overset{\alpha_1}{\to} L_1 \overset{\alpha_0}{\to} L_0 \to 0$$

□

Theorem 34.13. *Let the following be a commuting diagram of left-R-modules.*

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & L_{i+1} \arrow[r] \arrow[d, "\alpha_{i+1}"] & M_{i+1} \arrow[r] \arrow[d] & N_{i+1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L_i \arrow[r] \arrow[d, "\alpha_i"] & M_i \arrow[r] \arrow[d] & N_i \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L_{i-1} \arrow[r, "f_{i-1}"] \arrow[d] & M_{i-1} \arrow[r] \arrow[d] & N_{i-1} \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

Assume the central column is a complex and every row is an exact complex. Then the left and right columns are complexes. Further, if any two of the columns are exact, then so is the third.

Proof:
⟨1⟩1. The left column is a complex.
⟨2⟩1. Let: $x \in L_{i+1}$
⟨2⟩2. $f_{i-1}(\alpha_i(\alpha_{i+1}(x))) = 0$
⟨2⟩3. $\alpha_i(\alpha_{i+1}(x)) = 0$
Proof: f_{i-1} is injective.
⟨1⟩2. The right column is a complex.
⟨2⟩1. Let: $x \in N_{i+1}$
⟨2⟩2. Pick $y \in N_{i+1}$ such that $g_{i+1}(y) = x$
⟨2⟩3. $\gamma_i(\gamma_{i+1}(x)) = 0$
Proof:

$$\begin{aligned}
\gamma_i(\gamma_{i+1}(x)) &= \gamma_i(\gamma_{i+1}(g_{i+1}(y))) \\
&= g_{i-1}(\beta_i(\beta_{i+1}(y))) \\
&= g_{i-1}(0) \\
&= 0
\end{aligned}$$

$\langle 1\rangle 3$. If the left and center columns are exact then the right column is exact.
$\langle 2\rangle 1$. LET: $n_i \in \ker \gamma_{i-1}$
PROVE: $n_i \in \operatorname{im} \gamma_i$
$\langle 2\rangle 2$. PICK $m_i \in M_i$ such that $g_i(m_i) = n_i$
$\langle 2\rangle 3$. $g_{i-1}(\beta_i(m_i)) = 0$
$\langle 2\rangle 4$. $\beta_i(m_i) \in \ker g_{i-1} = \operatorname{im} f_{i-1}$
$\langle 2\rangle 5$. PICK $l_{i-1} \in L_{i-1}$ such that $f_{i-1}(l_{i-1}) = \beta_i(m_i)$
$\langle 2\rangle 6$. $\beta_{i-1}(f_{i-1}(l_{i-1})) = 0$
$\langle 2\rangle 7$. $f_{i-2}(\alpha_{i-1}(l_{i-1})) = 0$
$\langle 2\rangle 8$. $\alpha_{i-1}(l_{i-1}) = 0$
$\langle 2\rangle 9$. $l_{i-1} \in \ker \alpha_{i-1} = \operatorname{im} \alpha_i$
$\langle 2\rangle 10$. PICK $l_i \in L_i$ such that $\alpha_i(l_i) = l_{i-1}$
$\langle 2\rangle 11$. $\beta_i(f_i(l_i)) = \beta_i(m_i)$
$\langle 2\rangle 12$. $f_i(l_i) - m_i \in \ker \beta_i = \operatorname{im} \beta_{i+1}$
$\langle 2\rangle 13$. PICK $m_{i+1} \in M_{i+1}$ such that $\beta_{i+1}(m_{i+1}) = f_i(l_i) - m_i$
$\langle 2\rangle 14$. $\gamma_{i+1}(-g_{i+1}(m_{i+1})) = n_i$
$\langle 1\rangle 4$. If the left and right columns are exact then the center column is exact.
$\langle 2\rangle 1$. LET: $x \in \ker \beta_i$
PROVE: $x \in \operatorname{im} \beta_{i+1}$
$\langle 2\rangle 2$. $g_{i-1}(\beta_i(x)) = 0$
$\langle 2\rangle 3$. $\gamma_i(g_i(x)) = 0$
$\langle 2\rangle 4$. $g_i(x) \in \ker \gamma_i = \operatorname{im} \gamma_{i+1}$
$\langle 2\rangle 5$. PICK $n_{i+1} \in N_{i+1}$ such that $\gamma_{i+1}(n_{i+1}) = g_i(x)$
$\langle 2\rangle 6$. PICK $m_{i+1} \in M_{i+1}$ such that $g_{i+1}(m_{i+1}) = n_{i+1}$
$\langle 2\rangle 7$. $g_i(\beta_{i+1}(m_{i+1})) = g_i(x)$
$\langle 2\rangle 8$. $\beta_{i+1}(m_{i+1}) - x \in \ker g_i = \operatorname{im} f_i$
$\langle 2\rangle 9$. PICK $l_i \in L_i$ such that $f_i(l_i) = \beta_{i+1}(m_{i+1}) - x$
$\langle 2\rangle 10$. $\beta_i(f_i(l_i)) = 0$
$\langle 2\rangle 11$. $f_{i-1}(\alpha_i(l_i)) = 0$
$\langle 2\rangle 12$. $\alpha_i(l_i) = 0$
$\langle 2\rangle 13$. $l_i \in \ker \alpha_i = \operatorname{im} \alpha_{i+1}$
$\langle 2\rangle 14$. PICK $l_{i+1} \in L_{i+1}$ such that $\alpha_{i+1}(l_{i+1}) = l_i$
$\langle 2\rangle 15$. $\beta_{i+1}(f_{i+1}(l_{i+1})) = \beta_{i+1}(m_{i+1}) - x$
$\langle 2\rangle 16$. $x = \beta_{i+1}(m_{i+1} - f_{i+1}(l_{i+1}))$
$\langle 1\rangle 5$. If the center and right columns are exact then the left column is exact.
$\langle 2\rangle 1$. LET: $l_i \in \ker \alpha_i$
PROVE: $l_i \in \operatorname{im} \alpha_{i+1}$
$\langle 2\rangle 2$. $\beta_i(f_i(l_i)) = 0$
$\langle 2\rangle 3$. $f_i(l_i) \in \ker \beta_i = \operatorname{im} \beta_{i+1}$
$\langle 2\rangle 4$. PICK $m_{i+1} \in M_{i+1}$ such that $\beta_{i+1}(m_{i+1}) = f_i(l_i)$
$\langle 2\rangle 5$. $\gamma_{i+1}(g_{i+1}(m_{i+1})) = 0$
$\langle 2\rangle 6$. $g_{i+1}(m_{i+1}) \in \ker \gamma_{i+1} = \operatorname{im} \gamma_{i+2}$
$\langle 2\rangle 7$. PICK $n_{i+2} \in N_{i+2}$ such that $\gamma_{i+2}(n_{i+2}) = g_{i+1}(m_{i+1})$
$\langle 2\rangle 8$. PICK $m_{i+2} \in M_{i+2}$ such that $g_{i+2}(m_{i+2}) = n_{i+2}$
$\langle 2\rangle 9$. $g_{i+1}(\beta_{i+2}(n_{i+2})) = g_{i+1}(m_{i+1})$
$\langle 2\rangle 10$. $\beta_{i+2}(n_{i+2}) - m_{i+1} \in \ker g_{i+1} = \operatorname{im} f_{i+1}$

⟨2⟩11. Pick $l_{i+1} \in L_{i+1}$ such that $f_{i+1}(l_{i+1}) = \beta_{i+2}(n_{i+2}) - m_{i+1}$
⟨2⟩12. $f_i(\alpha_{i+1}(l_{i+1})) = -f_i(l_i)$
⟨2⟩13. $l_i = \alpha_{i+1}(-l_{i+1})$
□

Corollary 34.13.1 (Nine-Lemma)**.** *Let the following be a commuting diagram of left-R-modules.*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L_2 \arrow[r, "f_2"] \arrow[d, "\alpha_1"] & M_2 \arrow[r, "g_2"] \arrow[d, "\beta_1"] & N_2 \arrow[r] \arrow[d, "\gamma_1"] & 0 \\
0 \arrow[r] & L_1 \arrow[r, "f_1"] \arrow[d, "\alpha_0"] & M_1 \arrow[r, "g_1"] \arrow[d, "\beta_0"] & N_1 \arrow[r] \arrow[d, "\gamma_0"] & 0 \\
0 \arrow[r] & L_0 \arrow[r, "f_0"] \arrow[d] & M_0 \arrow[r, "g_0"] \arrow[d] & N_0 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

If the rows are exact and the two leftmost columns are exact then the right column is exact.

Proposition 34.14. *Let the following be a commuting diagram of left-R-modules.*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L_2 \arrow[r, "f_2"] \arrow[d, "\alpha_1"] & M_2 \arrow[r, "g_2"] \arrow[d, "\beta_1"] & N_2 \arrow[r] \arrow[d, "\gamma_1"] & 0 \\
0 \arrow[r] & L_1 \arrow[r, "f_1"] \arrow[d, "\alpha_0"] & M_1 \arrow[r, "g_1"] \arrow[d, "\beta_0"] & N_1 \arrow[r] \arrow[d, "\gamma_0"] & 0 \\
0 \arrow[r] & L_0 \arrow[r, "f_0"] \arrow[d] & M_0 \arrow[r, "g_0"] \arrow[d] & N_0 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

If the rows are exact and the left and right columns are exact then β_1 is monic.

Proof: By the Snake Lemma, the following is an exact sequence

$$0 \to \ker \alpha_1 \to \ker \beta_1 \to \ker \gamma_1$$

But $\ker \alpha_1 = \ker \gamma_1 = 0$ so $\ker \beta_1 = 0$. □

Proposition 34.15. *Let the following be a commuting diagram of left-R-modules.*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L_2 \arrow[r, "f_2"] \arrow[d, "\alpha_1"] & M_2 \arrow[r, "g_2"] \arrow[d, "\beta_1"] & N_2 \arrow[r] \arrow[d, "\gamma_1"] & 0 \\
0 \arrow[r] & L_1 \arrow[r, "f_1"] \arrow[d, "\alpha_0"] & M_1 \arrow[r, "g_1"] \arrow[d, "\beta_0"] & N_1 \arrow[r] \arrow[d, "\gamma_0"] & 0 \\
0 \arrow[r] & L_0 \arrow[r, "f_0"] \arrow[d] & M_0 \arrow[r, "g_0"] \arrow[d] & N_0 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

If the rows are exact and the left and right columns are exact then β_0 is epi.

Proof: Similar. □

Proposition 34.16. *Let the following be a commuting diagram of left-R-modules.*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L_2 \arrow[r, "f_2"] \arrow[d, "\alpha_1"] & M_2 \arrow[r, "g_2"] \arrow[d, "\beta_1"] & N_2 \arrow[r] \arrow[d, "\gamma_1"] & 0 \\
0 \arrow[r] & L_1 \arrow[r, "f_1"] \arrow[d, "\alpha_0"] & M_1 \arrow[r, "g_1"] \arrow[d, "\beta_0"] & N_1 \arrow[r] \arrow[d, "\gamma_0"] & 0 \\
0 \arrow[r] & L_0 \arrow[r, "f_0"] \arrow[d] & M_0 \arrow[r, "g_0"] \arrow[d] & N_0 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

If the rows are exact, the left and right columns are exact, and the central column is a complex, then the central column is exact.

Proof:
⟨1⟩1. Let: $x \in \ker \beta_0$
Prove: $x \in \operatorname{im} \beta_1$
⟨1⟩2. $\gamma_0(g_1(x)) = 0$
⟨1⟩3. $g_1(x) \in \ker \gamma_0 = \operatorname{im} \gamma_1$
⟨1⟩4. Pick $n_2 \in N_2$ such that $\gamma_1(n_2) = g_1(x)$
⟨1⟩5. Pick $m_2 \in M_2$ such that $g_2(m_2) = n_2$
⟨1⟩6. $g_1(\beta_1(m_2)) = g_1(x)$
⟨1⟩7. $\beta_1(m_2) - x \in \ker g_1 = \operatorname{im} f_1$
⟨1⟩8. Pick $l_1 \in L_1$ such that $f_1(l) = \beta_1(m_2) - x$.

⟨1⟩9. $f_0(\alpha_0(l_1)) = 0$
⟨1⟩10. $\alpha_0(l_1) = 0$
⟨1⟩11. $l_1 \in \ker \alpha_0 = \operatorname{im} \alpha_1$
⟨1⟩12. PICK $l_2 \in L_2$ such that $\alpha_1(l_2) = l_1$.
⟨1⟩13. $\beta_1(f_2(l_2)) = \beta_1(m_2) - x$
⟨1⟩14. $x = \beta_1(m_2 - f_2(l_2))$
$\square$

Example 34.17. We cannot remove the hypothesis that the central column is a complex. Consider the situation

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & 0 \arrow[r] \arrow[d] & \mathbb{Z} \arrow[r, equal] \arrow[d, "\Delta"] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "\kappa_1"] \arrow[d, equal] & \mathbb{Z} \oplus \mathbb{Z} \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r, equal] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

This diagram commutes, the rows are exact, the left and right columns are exact, but the central column is not a complex and $\operatorname{im} \Delta \neq \ker \pi_1$.

34.1 Split Exact Sequences

Definition 34.18 (Split Sequence)**.** Let $0 \to M_1 \xrightarrow{\alpha} N \xrightarrow{\beta} M_2 \to 0$ be a short exact sequence. Then this sequence *splits* iff there exists an isomorphism

$$\phi : N \cong M_1 \oplus M_2$$

such that $\phi \circ \alpha = \kappa_1 : M_1 \to M_1 \oplus M_2$ and $\beta \circ \phi^{-1} = \pi_2 : M_1 \oplus M_2 \to M_2$.

Proposition 34.19. *Let $\phi : M \to N$ be a left-R-module homomorphism. Then ϕ has a left-inverse if and only if the sequence*

$$0 \to M \xrightarrow{\phi} N \to \operatorname{coker} \phi \to 0$$

splits.

PROOF:
⟨1⟩1. If ϕ has a left-inverse then the sequence splits.
  ⟨2⟩1. ASSUME: ϕ has a left-inverse $\psi : N \to M$.
  ⟨2⟩2. Define $i : N \to M \oplus \operatorname{coker} \phi$ by $i(n) = (\psi(n), n + \operatorname{im} \phi)$.

⟨2⟩3. Define $i^{-1} : M \oplus \operatorname{coker}\phi$ by $i^{-1}(m, x + \operatorname{im}\phi) = \phi(m) + x - \phi(\psi(x))$.
⟨2⟩4. $i \circ i^{-1} = \mathrm{id}_{M \oplus \operatorname{coker}\phi}$
PROOF:

$$\begin{aligned} \psi(\phi(m) + x - \phi(\psi(x))) &= m + \psi(x) - \psi(x) \\ &= m \end{aligned}$$

⟨2⟩5. $i^{-1} \circ i = \mathrm{id}_N$
PROOF:

$$\begin{aligned} i^{-1}(\psi(n), n + \operatorname{im}\phi) &= \phi(\psi(n)) + n - \phi(\psi(n)) \\ &= n \end{aligned}$$

⟨2⟩6. $i \circ \phi = \kappa_1 : M \to M \oplus \operatorname{coker}\phi$
PROOF:

$$\begin{aligned} i(\phi(m)) &= (\psi(\phi(m)), \phi(m) + \operatorname{im}\phi) \\ &= (m, \operatorname{im}\phi) \end{aligned}$$

⟨2⟩7. $\pi \circ i^{-1} = \pi_2 : M \oplus \operatorname{coker}\phi \to \operatorname{coker}\phi$
PROOF:

$$\begin{aligned} i^{-1}(\psi(n), n + \operatorname{im}\phi) + \operatorname{im}\phi &= \phi(\psi(n)) + n - \phi(\psi(n)) + \operatorname{im}\phi \\ &= n + \operatorname{im}\phi \end{aligned}$$

⟨1⟩2. If the sequence splits then ϕ has a left-inverse.
PROOF: Since $\kappa_1 : M \to M \oplus \operatorname{coker}\phi$ has left inverse π_1.
□

Proposition 34.20. *Let $\phi : M \to N$ be a left-R-module homomorphism. Then ϕ has a right-inverse if and only if the sequence*

$$0 \to \ker\phi \to M \xrightarrow{\phi} N \to 0$$

splits.

PROOF:
⟨1⟩1. If ϕ has a right-inverse then the sequence splits.
⟨2⟩1. LET: $\psi : N \to M$ be a right inverse to ϕ.
⟨2⟩2. LET: $i : M \to \ker\phi \oplus N$ be the function $i(m) = (m - \psi(\phi(m)), \phi(m))$.
PROOF: $m - \psi(\phi(m)) \in \ker\phi$ since $\phi(m - \psi(\phi(m))) = \phi(m) - \phi(m) = 0$.
⟨2⟩3. LET: $i^{-1} : \ker\phi \oplus N \to M$ be the function $i^{-1}(x, n) = x + \psi(n)$.
⟨2⟩4. $i \circ i^{-1} = \mathrm{id}_{\ker\phi \oplus N}$
PROOF:

$$\begin{aligned} i(i^{-1}(x, n)) &= i(x + \psi(n)) \\ &= (x + \psi(n) - \psi(\phi(x)) - \psi(\phi(\psi(n))), \phi(x) + \phi(\psi(n))) \\ &= (x + \psi(n) - \psi(n), n) \\ &= (x, n) \end{aligned}$$

⟨2⟩5. $i^{-1} \circ i = \mathrm{id}_M$
PROOF:

$$\begin{aligned} i^{-1}(i(m)) &= m - \psi(\phi(m)) + \psi(\phi(m)) \\ &= m \end{aligned}$$

⟨2⟩6. $i \circ \iota = \kappa_1$

PROOF: For $m \in \ker \phi$ we have $i(m) = (m - \psi(\phi(m)), \phi(m)) = (m, 0)$.
⟨2⟩7. $\phi \circ i^{-1} = \pi_2$
PROOF:

$$\begin{aligned}\phi(i^{-1}(x,n)) &= \phi(x) + \phi(\psi(n)) \\ &= 0 + n \\ &= n\end{aligned}$$

⟨1⟩2. If the sequence splits then ϕ has a right-inverse.
PROOF: Since $\kappa_2 : N \to M \oplus N$ is a right-inverse to π_2.
□

Proposition 34.21. *Let*

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} F \to 0$$

be a short exact sequence where F is free. Then the sequence splits.

PROOF:
⟨1⟩1. LET: $F = R^{\oplus A}$
⟨1⟩2. PICK $\gamma : F \to N$ such that $\mathrm{id}_F = \beta \circ \gamma$
⟨1⟩3. LET: $i : M \oplus F \to N$ be the homomorphism $i(m, f) = \alpha(m) + \gamma(f)$
⟨1⟩4. i is injective.
⟨2⟩1. ASSUME: $i(m, f) = i(m', f')$
⟨2⟩2. $\alpha(m) + \gamma(f) = \alpha(m') + \gamma(f')$
⟨2⟩3. $\alpha(m - m') = \gamma(f - f')$
⟨2⟩4. $f - f' = 0$
PROOF: Applying β to both sides of ⟨2⟩3.
⟨2⟩5. $f = f'$
⟨2⟩6. $\alpha(m - m') = 0$
⟨2⟩7. $m = m'$
PROOF: Since α is injective.
⟨1⟩5. i is surjective.
⟨2⟩1. LET: $n \in N$
⟨2⟩2. $n - \gamma(\beta(n)) \in \ker \beta = \operatorname{im} \alpha$
⟨2⟩3. PICK $m \in M$ such that $\alpha(m) = n - \gamma(\beta(n))$
⟨2⟩4. $n = i(m, \beta(n))$
⟨1⟩6. $\alpha = i \circ \kappa_1$
⟨1⟩7. $\beta \circ i = \pi_2$
□

Chapter 35

Homology

Definition 35.1 (Homology)**.** Let $(M_\bullet, d_\bullet)$ be a chain complex. The *ith homology* of the complex is the R-module

$$H_i(M_\bullet) := \frac{\ker d_i}{\operatorname{im} d_{i+1}} \ .$$

Proposition 35.2. *Consider the complex*

$$0 \to M_1 \xrightarrow{\phi} M_0 \to 0 \ .$$

The 1st homology is $\ker \phi$*, and the 0th homology is* $\operatorname{coker} \phi$*.*

Part V

Field Theory

Chapter 36

Fields

Definition 36.1 (Field)**.** A *field* is a non-trivial commutative division ring.

Example 36.2. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

Proposition 36.3. *Every field is an integral domain.*

PROOF: By Propositions 12.8 and 12.9. □

Example 36.4. The converse does not hold: $\mathbb{Z}$ is an integral domain but not a field.

Proposition 36.5. *Every finite integral domain is a field.*

PROOF: In a finite integral domain, multiplication by any non-zero element is injective, hence surjective. □

Corollary 36.5.1. *For any positive integer n, the following are equivalent:*

- *n is prime.*
- *$\mathbb{Z}/n\mathbb{Z}$ is an integral domain.*
- *$\mathbb{Z}/n\mathbb{Z}$ is a field.*

Theorem 36.6 (Wedderburn's Little Theorem)**.** *Every finite division ring is a field.*

Proposition 36.7. *Every subring of a field is an integral domain.*

PROOF: Easy. □

Proposition 36.8. *The center of a division ring is a field.*

PROOF:
⟨1⟩1. LET: R be a division ring.
⟨1⟩2. LET: Z be the center of R.
⟨1⟩3. Z is non-trivial.

PROOF: Since $1 \in Z$.
$\langle 1 \rangle 4.$ Z is commutative.
$\langle 1 \rangle 5.$ Z is a division ring.
$\langle 2 \rangle 1.$ LET: $a \in Z$
$\langle 2 \rangle 2.$ $a^{-1} \in Z$
$\langle 3 \rangle 1.$ LET: $x \in R$
$\langle 3 \rangle 2.$ $ax = xa$
$\langle 3 \rangle 3.$ $xa^{-1} = a^{-1}x$
□

Definition 36.9. For any prime p and positive integer r, define a multiplication on $(\mathbb{Z}/p\mathbb{Z})^r$ that makes this group into a field by:

Proposition 36.10. *A commutative ring is a field if and only if it is simple.*

PROOF: Proposition 22.5. □

Corollary 36.10.1. *Every field has Krull dimension 0.*

Proposition 36.11. *Let K be a field. Then $K[x]$ is a PID, and every non-zero ideal in $K[x]$ is generated by a unique monic polynomial.*

PROOF:
$\langle 1 \rangle 1.$ LET: I be a non-zero ideal in $K[x]$
$\langle 1 \rangle 2.$ PICK a monic polynomial $f \in K[x]$ of minimal degree.
PROVE: $I = (f)$
$\langle 1 \rangle 3.$ LET: $g \in I$
$\langle 1 \rangle 4.$ PICK polynomials q, r with $\deg r < \deg f$ such that $g = qf + r$
$\langle 1 \rangle 5.$ $r \in I$
$\langle 1 \rangle 6.$ $r = 0$
$\langle 1 \rangle 7.$ $g \in (f)$
□

Proposition 36.12. *Let R be a commutative ring and I an ideal in R. Then I is maximal iff R/I is a field.*

PROOF: From Proposition 23.3. □

Example 36.13. Let R be a commutative ring and $a \in R$. Then $(x - a)$ is a maximal ideal in $R[x]$ iff R is a field, since $R[x]/(x - a) \cong R$.

Example 36.14. The ideal $(2, x)$ is a maximal ideal in $\mathbb{Z}[x]$, since $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$.

Proposition 36.15. *Every maximal ideal in a commutative ring is a prime ideal.*

PROOF: Since every field is an integral domain. □

Proposition 36.16. *Let R be a commutative ring and I an ideal in R. If I is a prime ideal and R/I is finite then I is a maximal ideal.*

Proof: Since every finite integral domain is a field. □

Proposition 36.17. *Let R be a commutative ring and I a proper ideal in R. Then I is maximal iff, whenever J is an ideal and $I \subseteq J$, then $I = J$ or $J = R$.*

Example 36.18. The inverse image of a maximal ideal under a homomorphism is not necessarily maximal.

Let $i : \mathbb{Z}[x] \to \mathbb{Q}[x]$ be the inclusion. Then (x) is maximal in $\mathbb{Q}[x]$ but its inverse image (x) is not maximal in $\mathbb{Z}[x]$.

Definition 36.19 (Maximal Spectrum)**.** Let R be a commutative ring. The *maximal spectrum* of R is the set of all maximal ideals in R.

Proposition 36.20. *Let K be a field. The Krull dimension of $K[x_1, \ldots, x_n]$ is n.*

Theorem 36.21 (Hilbert's Nullstellensatz)**.** *Let K be a field and L a subfield of K. If K is an L-algebra of finite type, then K is a finite L-algebra.*

Proposition 36.22. *Let K be a subfield of L. Then L is a K-algebra under multiplication.*

Proof: Easy. □

Chapter 37

Algebraically Closed Fields

Definition 37.1 (Algebraically Closed)**.** A field K is *algebraically closed* iff, for every $f \in K[x]$ that is not constant, there exists $r \in K$ such that $f(r) = 0$.

Theorem 37.2. *$\mathbb{C}$ is algebraically closed.*

Proposition 37.3. *Let K be an algebraically closed field. Let I be an ideal in $K[x]$. Then I is maximal if and only if $I = (x - c)$ for some $c \in K$.*

PROOF:
⟨1⟩1. If I is maximal then there exists $c \in K$ such that $I = (x - c)$.
  ⟨2⟩1. ASSUME: I is maximal.
  ⟨2⟩2. PICK f monic of minimal degree such that $f \in I$.
  ⟨2⟩3. f is not constant.
    PROOF: Otherwise $f = 1$ and $I = K[x]$.
  ⟨2⟩4. PICK $c \in K$ such that $f(c) = 0$
  ⟨2⟩5. $x - c \mid f$
  ⟨2⟩6. $I \subseteq (x - c)$
  ⟨2⟩7. $I = (x - c)$
⟨1⟩2. For all $c \in K$ we have $(x - c)$ is maximal.
  PROOF: Example 36.13.
□

Part VI

Linear Algebra

Chapter 38

Vector Spaces

Definition 38.1 (Vector Space)**.** Let K be a field. A *K-vector space* is a K-module. A *linear map* is a homomorphism of K-modules. We write $K - \mathbf{Vect}$ for $K - \mathbf{Mod}$.

Definition 38.2. Let $\mathrm{GL}_n(\mathbb{R})$ be the group of invertible $n \times n$ real matrices. $\mathrm{GL}_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by matrix multiplication.

Definition 38.3. Let $\mathrm{GL}_n(\mathbb{C})$ be the group of invertible $n \times n$ complex matrices. $\mathrm{GL}_n(\mathbb{C})$ acts on $\mathbb{C}^n$ by matrix multiplication.

Definition 38.4. Let $\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : \det M = 1\}$.

Proposition 38.5. $\mathrm{SL}_n(\mathbb{R})$ *is a normal subgroup of* $\mathrm{GL}_n(\mathbb{R})$.

Proof: If $\det M = 1$ then $\det(AMA^{-1}) = (\det A)(\det M)(\det A)^{-1} = 1$. □

Proposition 38.6.

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$$

Definition 38.7. Let $\mathrm{SL}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : \det M = 1\}$.

Definition 38.8. Let $\mathrm{O}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : MM^{\mathrm{T}} = M^{\mathrm{T}}M = I_n\}$.

Proposition 38.9. *The action of* $\mathrm{O}_n(\mathbb{R})$ *on* $\mathbb{R}^n$ *preserves lengths and angles.*

Definition 38.10. Let $\mathrm{SO}_n(\mathbb{R}) = \{M \in \mathrm{O}_n(\mathbb{R}) : \det M = 1\}$.

Definition 38.11. Let $\mathrm{U}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : MM^\dagger = M^\dagger M = I_n\}$.

Definition 38.12. Let $\mathrm{SU}_n(\mathbb{C}) = \{M \in U_n(\mathbb{C}) : \det M = 1\}$.

Proposition 38.13. *Every matrix in* $\mathrm{SU}_2(\mathbb{C})$ *can be written in the form*

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

for some $a, b, c, d \in \mathbb{R}$ *with* $a^2 + b^2 + c^2 + d^2 = 1$.

PROOF:
⟨1⟩1. LET: $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SU}_2(\mathbb{C})$
⟨1⟩2. $M^{-1} = M^\dagger$
⟨1⟩3. $\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} \overline{\alpha} & \overline{\gamma} \\ \overline{\beta} & \overline{\delta} \end{pmatrix}$
⟨1⟩4. LET: $\alpha = a + bi$ and $\beta = c + di$.
⟨1⟩5. $\delta = \overline{\alpha} = a - bi$
⟨1⟩6. $\gamma = -\overline{\beta} = -c + di$
⟨1⟩7. $\det M = a^2 + b^2 + c^2 + d^2 = 1$
□

Corollary 38.13.1. $\mathrm{SU}_2(\mathbb{C})$ *is simply connected.*

Corollary 38.13.2.

$$\mathrm{SO}_3(\mathbb{R}) \cong \mathrm{SU}_2(\mathbb{C})/\{I, -I\}$$

PROOF: The function that maps $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ to $\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(a \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(a \\ 2(bd-ac) & 2(ab+cd) & a^2-b \end{pmatrix}$

is a surjective homomorphism with kernel $\{I, -I\}$. □

Corollary 38.13.3. *The fundamental group of* $\mathrm{SO}_3(\mathbb{R})$ *is* C_2.

Part VII

Linear Algebra

Chapter 39

Vector Spaces

Definition 39.1 (Vector Space)**.** Let K be a field. A *vector space* over K is a module over K. A *linear transformation* is a K-module homomorphism.

Definition 39.2 (Bilinear Map)**.** Let K be a field. Let U, V and W be vector spaces over K. A function $f : U \times V \to W$ is *bilinear* iff, for all $u_1, u_2 \in U$ and $v_1, v_2 \in V$ and $\alpha \in K$,

$$f(u_1 + \alpha u_2, v_1) = f(u_1, v_1) + \alpha f(u_2, v_1)$$
$$f(u_1, v_1 + \alpha v_2) = f(u_1, v_1) + \alpha f(u_1, v_2)$$

Theorem 39.3. *Let K be a field. Let U and V be vector spaces. There exists a vector space $U \otimes V$ over K and bilinear map $- \otimes - : U \times V \to U \otimes V$, unique up to isomorphism, such that, for every vector space W over K and bilinear map $f : U \times V \to W$, there exists a unique linear map $\overline{f} : U \otimes V \to W$ such that the following diagram commutes.*

$$\begin{tikzcd} U \otimes V \arrow[r, "\overline{f}"] & W \\ U \times V \arrow[u, "-\otimes-"] \arrow[ur, "f"'] & \end{tikzcd}$$

Further, $- \otimes -$ is injective and its image spans $U \otimes V$.

Proof: We can construct $U \otimes V$ as follows. Let L be the free vector space generated by $U \times V$. Let R be the subspace generated by all vectors of the form

$$(u_1 + \alpha u_2, v) - (u_1, v) - \alpha(u_2, v)(u, v_1 + \alpha v_2) - (u, v_1) - \alpha(u, v_2)$$

Take $U \otimes V := L/R$. ∎

Proposition 39.4. *If $\sum_{i=1}^{n} u_i \otimes v_i = 0$ and $v_1, \ldots, v_n$ are linearly independent in V then $u_1 = \cdots = u_n = 0$.*

Proof:
⟨1⟩1. Let: $f : U \times V \to V^{U^*}$ be the function $f(u, v)(\Phi) = \Phi(u)v$

$\langle 1 \rangle 2.$ f is bilinear.
$\langle 1 \rangle 3.$ LET: $\overline{f} : U \otimes V \to V^{U^*}$ be the induced linear transformation.
$\langle 1 \rangle 4.$ $\overline{f}(\sum_{i=1}^{n} u_i \otimes v_i) = 0$
$\langle 1 \rangle 5.$ $\sum_{i=1}^{n} f(u_i, v_i) = 0$
$\langle 1 \rangle 6.$ For all $\Phi \in U^*$ we have $\sum_{i=1}^{n} \Phi(u_i) v_i = 0$
$\langle 1 \rangle 7.$ For all $\Phi \in U^*$ we have $\Phi(u_1) = \cdots = \Phi(u_n) = 0$
$\langle 1 \rangle 8.$ $u_1 = \cdots = u_n = 0$
□

Proposition 39.5. *Let U and V be vector spaces over K with bases $\mathcal{B}_1$ and $\mathcal{B}_2$. Then $\mathcal{B} = \{b_1 \otimes b_2 : b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2\}$ is a basis for $U \otimes V$.*

PROOF:
$\langle 1 \rangle 1.$ $\mathcal{B}$ is linearly independent.
$\langle 2 \rangle 1.$ ASSUME: $\sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} b_i \otimes b'_j = 0$
$\langle 2 \rangle 2.$ For all j we have $\sum_{i=1}^{m} \alpha_{ij} b_i = 0$
PROOF: Proposition 39.4.
$\langle 2 \rangle 3.$ Each α_{ij} is 0.
$\langle 1 \rangle 2.$ $\mathcal{B}$ spans $U \otimes V$.
PROOF: If $u = \alpha_1 b_1 + \cdots + \alpha_m b_m$ and $v = \beta_1 b'_1 + \cdots + \beta_n b'_n$ then

$$u \otimes v = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_i \beta_j (b_i \otimes b'_j)$$

The result follows since the vectors of the form $u \otimes v$ span $U \otimes V$.
□

Corollary 39.5.1. *If U and V are finite dimensional vector spaces over K then*

$$\dim(U \otimes V) = (\dim U)(\dim V) \ .$$

Proposition 39.6. $\mathbf{Vect}_K$ *is a symmetric monoidal category under $\otimes$.*

Part VIII

Measure Theory

Definition 39.7 (σ-algebra)**.** Let X be a set. A *σ-algebra* on X is a nonempty set $\Sigma \subseteq \mathcal{P}X$ that is closed under complement, countable union, and countable intersection.

A *measurable space* consists of a set with a σ-algebra.

Definition 39.8 (Measure)**.** Let (X, σ) be a measurable space. A *measure* on (X, σ) is a function $\mu : \Sigma \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$ such that:

- $\mu(\emptyset) = 0$
- For any countable set of pairwise disjoint sets $\{E_n : n \in \mathbb{N}\}$ in Σ,

$$\mu\left(\bigcup_{n=0}^{\infty} E_n\right) = \sum_{n=0}^{\infty} \mu(E_n) \ .$$