Notes on Abstract Algebra

Jonas T. Hartwig

Version 0.8 from Feb 8, 2022

Revision	**Date**	**Author(s)**	**Description**
0.6	Oct 25, 2022	JH	First version
0.7	Nov 11, 2022	JH	Added rings, algebras
0.75	Dec 7, 2022	JH	Added more ring theory sections
0.76	Dec 8, 2022	JH	Proof of Eisenstein's Criterion
0.8	Feb 8, 2022	JH	Added category theory section

Contents

0 Chapter Zero

0.1 Relations and Functions

Definition 0.1. Let X be a set.

- A *relation from A to B* is a subset R of $A \times B$. The statement $(a, b) \in R$ is denoted aRb. If $B = A$ we say R is a *relation on A*.

- A relation R on A is

  - *reflexive* if $\forall a \in A : aRa$

  - *symmetric* if $\forall a, b \in A : aRb \Rightarrow bRa$
  - *antisymmetric* if $\forall a, b \in A : aRb \wedge bRa \Rightarrow a = b$
  - *transitive* if $\forall a, b, c \in A : aRb \wedge bRc \Rightarrow aRc$.
  - an *equivalence relation* if R is reflexive, symmetric, and transitive;
  - a *partial order* if R is reflexive, antisymmetric, and transitive;
  - a *total order* if R is a partial order and $\forall a, b \in A : aRb \vee bRa$.

- A relation f from A to B is a *function* if for each $a \in A$ there is a unique element of B denoted $f(a)$ such that $\big(a, f(a)\big) \in f$.

Example 0.2.

(i) $\subset$ is a partial order on the power set $\mathscr{P}(X)$ of any set X.

(ii) The set of all equivalence relations on a set A is partially ordered by inclusion, and closed under intersections. There is a unique minimal equivalence relation, namely equality, and a unique maximal equivalence relation where all elements are equivalent.

(iii) Let R be any relation on a set A. The equivalence relation *generated by* R is the intersection of all equivalence relations contatining R.

Note that for any set A there is a unique function from $\emptyset$ to A, namely the function $\emptyset$.

Notation 0.3. $\mathbb{N} = \{0, 1, 2, \ldots\}$; $\underline{n} = \{1, 2, \ldots, n\}$; B^A is the set of all functions from A to B; and $A^n = A^{\underline{n}}$ for $n \in \mathbb{N}$; the power set $\mathscr{P}(A) \simeq \underline{2}^A$ is the set of all subsets of A. $\subset$ will always mean not-necessarily-strict subset: $A \subset B \Leftrightarrow \big(a \in A \Rightarrow a \in B\big)$.

Thus $A^0 = \{\emptyset\}$ and A^n for $n > 0$ is the set of n-tuples $(a_1, a_2, \ldots, a_n)$ of elements of A.

0.2 Equivalence Relations vs. Set Partitions; Surjections

Definition 0.4. A *(set) partition* P of a set X is a subset of $\mathscr{P}(X) \setminus \{\emptyset\}$ such that $X = \bigcup_{A \in P} A$ and $A \cap B = \emptyset$ for all $A, B \in P$, $A \neq B$.

Theorem 0.5. *Let X be a set.*

(a) *To each equivalence relation $\sim$ on X there is a partition $X/\sim$ of X given by*

$$X/\sim = \big\{[x]_\sim \mid x \in X\big\}, \qquad [x]_\sim = \{y \in X \mid y \sim x\}. \tag{0.1}$$

(b) *Conversely, to each partition P of X there is an equivalence relation $\sim_P$ on X defined by*

$$x \sim_P y \Leftrightarrow \exists A \in P : x \in A \wedge y \in A.$$

(c) *These two constructions establish a bijective correspondence between the set of all equivalence relations on X and the set of all partitions of X.*

Definition 0.6. The set $[x]_\sim$ from (0.1) is the *equivalence class containing x* (with respect to $\sim$).

Theorem 0.7. *Let X be a set.*

(a) *To each equivalence relation $\sim$ on X there is a surjective map $\pi : X \to X/\sim$, $x \mapsto [x]_\sim$.*

(b) *To each pair (B, f) where B is a set and $f : X \to B$ is a surjective map there is an equivalence relation on X given by $x \sim y \Leftrightarrow f(x) = f(y)$. The corresponding partition is $\{f^{-1}(\{b\}) \mid b \in B\}$.*

Definition 0.8. A *section* of a surjective map $f : X \to B$ is a map $s : B \to X$ such that $f \circ s = \mathrm{Id}_B$.

Definition 0.9. Let $\sim$ be an equivalence relation on X.

- The surjective map $\pi : X \to X/\sim$, $x \mapsto [x]_\sim$ is the *canonical (or natural) projection.*
- A *set of class representatives T* is the image of a section of the canonical projection.

In other words, a set of class representatives is a subset $T \subset X$ such that any $x \in X$ is equivalent to exactly one element in T.

Definition 0.10. For a surjective map $f : X \to B$ and $b \in B$, the set $f^{-1}(\{b\})$ is called the *fiber above b.*

0.3 Divisibility in $\mathbb{Z}$

Define a relation $\bigm|$ ("divides") on $\mathbb{Z}$ by $a \bigm| b \Leftrightarrow b = da$ for some $d \in \mathbb{Z}$. Then $\bigm|$ is a partial order on $\mathbb{Z}$. Note $\forall a \in \mathbb{Z} : 0 \bigm| a$ but $\forall a \in \mathbb{Z} : (a \bigm| 0 \Rightarrow a = 0)$.

0.3.1 Division Algorithm; gcd and lcm

Theorem 0.11 (Division Algorithm)**.** *If $a, b \in \mathbb{N}$ and $b \neq 0$ then there exist unique $r, q \in \mathbb{N}$ such that*

$$a = qb + r \quad \text{and} \quad 0 \leq r < b. \tag{0.2}$$

Proof. (Existence): The set $S = \mathbb{N} \cap \{a - qb \mid q \in \mathbb{N}\}$ is nonempty ($a \in S$) hence contains a least element r by the Well-Ordering Principle (Theorem A.1). Then $a = qb + r$, and $r < b$ otherwise $r - b \in S$ contradicting minimality. (Uniqueness): If $a = qb + r = q'b + r'$ then $b \bigm| (r' - r)$, so if $0 \leq r, r' < b$ then $|r' - r| < b$, forcing $r' - r = 0$. □

Definition 0.12. Let $a, b \in \mathbb{Z}$. A *greatest common divisor* is an integer $d \in \mathbb{Z}$ such that

(i) $d \mid a$ and $d \mid b$,

(ii) $\forall e \in \mathbb{Z} : e \mid a \wedge e \mid b \Rightarrow e \mid d$.

Theorem 0.13. *Let $a, b \in \mathbb{Z}$. Then there exists a greatest common divisor of a and b and it is unique up to sign.*

Proof. (Existence): If $a = b = 0$ then $d = 0$ is a gcd. Otherwise, we may without loss of generality assume $a > 0$ and $b > 0$. The set

$$S = \mathbb{Z}_{>0} \cap \{sa + tb \mid (s, t) \in \mathbb{Z}^2\}.$$

is non-empty ($a^2 + b^2 \in S$) and hence contains a least element d by the Well-Ordering Principle. Write

$$d = sa + tb, \tag{0.3}$$

where $(s, t) \in \mathbb{Z}^2$. We prove that d satisfies Properties (i) and (ii) of the theorem statement. (i): By the Division Algorithm, there exists $(q, r) \in \mathbb{N}^2$ such that

$$a = qd + r, \qquad 0 \le r < d. \tag{0.4}$$

Substituting (0.3) into (0.4) we obtain $a - q(sa + tb) = r$, or, after rearranging,

$$(1 - qs)a + tb = r.$$

If $r > 0$ this element belongs to S but that contradicts the minimality of d. Therefore $r = 0$ which shows that $d \mid a$. Interchanging the roles of a and b we conclude that $d \mid b$ too. (ii): Suppose $e \in \mathbb{Z}$ with $e \mid a$ and $e \mid b$. That is, $ec = a$ and $ec' = b$ for some integers c and c'. Substituting into (0.3) we get $d = sec + tec' = (sc + tc')e$ which shows that $e \mid d$.

(Uniqueness up to sign): If d and d' are both gcds of a and b, then by (ii) we have $d \mid d'$ and $d' \mid d$. This means $dc = d'$ and $d'c' = c$ for some integers c and c'. Hence $d = dcc'$ and $d' = d'cc'$, so either $d = d' = 0$, or $c \in \{1, -1\}$. Either way, $d' \in \{d, -d\}$. □

Definition 0.14. For integers a and b we let

$$\gcd(a, b)$$

be the unique non-negative greatest common divisor of a and b.

Analogously a *least common multiple* of two integers a and b is an integer $m \in \mathbb{Z}$ such that (i) $a \mid m$, $b \mid m$, and (ii) if $n \in \mathbb{Z}$ with $a \mid n$, $a \mid n$, then $m \mid n$. It exists and is unique up to sign. Let $\operatorname{lcm}(a, b)$ denote the unique non-negative least common multiple. We have

$$\gcd(a, b) \operatorname{lcm}(a, b) = ab. \tag{0.5}$$

The following abbreviated notation is sometimes convenient:

$$(a, b) = \gcd(a, b), \qquad [a, b] = \operatorname{lcm}(a, b).$$

Definition 0.15. Euler's ϕ-function is defined by

$$\phi(n) = |\{a \in \underline{n} \mid \gcd(a, n) = 1\}|. \tag{0.6}$$

We have the following properties:

$$\phi(mn) = \phi(m)\phi(n) \quad \text{if } \gcd(m, n) = 1, \tag{0.7}$$

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) \quad \text{if } p \text{ is prime and } k > 0. \tag{0.8}$$

and explicit formula:

$$\phi(n) = n \prod_{p|n} \big(1 - \frac{1}{p}\big) \tag{0.9}$$

where the product is taken over all prime numbers which divide n.

0.3.2 Congruence

Definition 0.16. For $n \in \mathbb{Z}$ define a relation $\equiv_n$ on $\mathbb{Z}$ called *congruence mod(ulo) n* by

$$a \equiv_n b \Leftrightarrow n \,\big|\, (a - b). \tag{0.10}$$

A strange but very common notation for $a \equiv_n b$ is $a \equiv b \pmod n$.

Lemma 0.17. *For any $n \in \mathbb{Z}$, the relation $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.*

Definition 0.18. The equivalence classes, denoted

$$[a]_n = [a]_{\equiv_n} = a + n\mathbb{Z} = \{a + nd \mid d \in \mathbb{Z}\}, \qquad a \in \mathbb{Z}, \tag{0.11}$$

are the *congruence classes mod n*. A set of class representatives with respect to $\equiv_n$ is called a set of *congruence class representatives mod n* (or a *system of residues mod n*)

Example 0.19. The most common set of congruence class representatives mod n is $\{0, 1, \dots, n-1\}$. Another choice is $\{-k, -k+1, \dots, -k+n-1\}$ where $k = \lfloor \frac{n-1}{2} \rfloor$. For $n = 4$ that gives $\{-1, 0, 1, 2\}$.

1 Monoids and Groups

1.1 Monoids

Definition 1.1. Let A be a set.

- A *binary operation on A* is a function $* : A \times A \to A$. We write $a * b$ instead of $*(a, b)$.
- A binary operation $*$ on A is *commutative* if $\forall (a, b) \in A^2 : a * b = b * a$; *associative* if $\forall (a, b, c) \in A^3 : a * (b * c) = (a * b) * c$.

Definition 1.2. A *monoid* M is a set together with an associative binary operation $*$ on M, and an *identity element* $e = e_M \in M$, such that $e * a = a = a * e$ for all $a \in A$. M is furthermore *commutative* if $*$ is commutative.

Proposition 1.3. *Let M be a monoid.*

(a) *Then for any $a_1, a_2, \ldots, a_n \in M$ the value of $a_1 * a_2 * \cdots * a_n$ is independent of how it is parenthesized. (Generalized Associativity Law.)*

(b) *If $e, \widetilde{e} \in M$ are two identity elements then $e = \widetilde{e}$.*

Example 1.4.

(i) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are monoids under both $+$ and $\cdot$. Neither is a monoid under $-$, subtraction being non-associative.

(ii) If $R = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ then the set $M_n(R)$ of $n \times n$-matrices with entries from R is a monoid under both matrix addition and under matrix multiplication.

(iii) Let X be a set. Then X^X is a monoid under function composition.

(iv) The *free monoid* on a set X is

$$F_{\text{mon}}(X) = \bigsqcup_{n=0}^{\infty} X^n.$$

Elements of X^n are here called *words*, written $x_1 x_2 \cdots x_n$, $x_i \in X$, with binary operation given by *concatenation*: for $w = x_1 \cdots x_m \in X^m$ and $w' = x'_1 \cdots x'_n \in X^n$ we define $ww' \in X^{m+n}$ by

$$(x_1 \cdots x_m)(x'_1 \cdots x'_n) = x_1 \cdots x_m x'_1 \cdots x'_n.$$

Then $F_{\text{mon}}(X)$ is a monoid with identity element $e = \emptyset \in X^0$. (Recall that $X^0 = \{\emptyset\}$ for any set X.)

(v) If V is a vector space then the set $\text{End}(V)$ of linear operators on V is a monoid under composition.

(vi) If $\{M_i\}_{i \in I}$ is a family of monoids, the *direct product* $\prod_{i \in I} M_i$ consisting of sequences $(x_i)_{i \in I}$, $x_i \in M_i$, is a monoid under pointwise operations: $(x_i)_{i \in I} * (y_i)_{i \in I} = (x_i * y_i)_{i \in I}$. In particular, if M and N are monoids then $M \times N = \{(x, y) \mid x \in M, y \in N\}$ is a monoid.

1.2 Groups

Definition 1.5. Let M be a monoid.

- $x \in M$ is *invertible* if there exists $x' \in M$, called an *inverse of* x, such that $x * x' = e_M = x' * x$.
- M is a *group* if every element is invertible.
- M is an *abelian group* if it is a commutative group.

Notation 1.6. If M is a monoid we let

$$M^\times = \{m \in M \mid m \text{ is invertible}\}.$$

Proposition 1.7. *If M is a monoid, then $M^\times$ is a group with the same operation as in M.*

Notation 1.8. Let G be a group with operation $*$, identity e_G.

Multiplicative notation: $gh = g * h$, $1 = e_G$, $g^{-1} = g'$, $g^n = \begin{cases} gg\cdots g, & n > 0, \\ 1, & n = 0, \\ g^{-1}g^{-1}\cdots g^{-1}, & n < 0. \end{cases}$

Additive notation: $g+h = g*h$, $0 = e_G$, $-g = g'$, $ng = \begin{cases} g+g+\cdots+g, & n > 0, \\ 0, & n = 0, \\ (-g)+(-g)+\cdots+(-g), & n < 0. \end{cases}$

We will usually use multiplicative notation. Additive notation is only used when G is known to be abelian.

Proposition 1.9. *Let G be a group and let $a, x, y \in G$.*

(a) *If a' and a'' are inverses of $a \in G$ then $a' = a''$. (Uniqueness of Inverse)*

(b) *$xy = a \Leftrightarrow y = x^{-1}a \Leftrightarrow x = ay^{-1}$. (Unique Solvability of Equations)*

(c) *If $xa = ya$ or $ax = ay$ then $x = y$. (Left and Right Cancellation Laws)*

Definition 1.10. Let G be a group. The *order* of G is the cardinality of the underlying set G. If G has finite order then G is *finite*. Otherwise G is *infinite*.

Example 1.11.

(i) Under addition, the monoids $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups, while $\mathbb{N}^\times = \{0\}$. Let M be $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ under multiplication. Then $M^\times = \{1\}, \{1, -1\}, \mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$, respectively.

(ii) For $R = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, the *general linear group* is $\mathrm{GL}_n(R) = \big(M_n(R)\big)^{\times}$.

(iii) Let X be a set. The group $S_X = (X^X)^{\times}$ of invertible functions from X to X is called the *symmetric group on* X.

(iv) Let X be a set. The *free group on* X, denoted $F(X)$, is constructed as follows. Let X^{-1} be a set with a bijection $X \to X^{-1}$ denoted $x \mapsto x^{-1}$. Let $\widetilde{F}$ be the free monoid on the set $X \sqcup X^{-1}$. Let $\sim$ be the equivalence on $\widetilde{F}$ generated by (Recall Example 0.2(iii)))

$$wxx^{-1}w' \sim ww' \sim wx^{-1}xw'$$

for all words $w, w' \in \widetilde{F}$. Define

$$F(X) = \widetilde{F}/\sim$$

with binary operation $[w_1]_{\sim}[w_2]_{\sim} = [w_1w_2]_{\sim}$. One checks this is well-defined ($w_1 \sim w_1', w_2 \sim w_2' \Rightarrow w_1w_2 \sim w_1'w_2'$) and makes $F(X)$ into a group.

(v) If $\{G_i\}_{i\in I}$ is a family of groups then $\prod_{i\in I} G_i$ is also a group.

1.3 Homomorphisms

Definition 1.12. Let M and N be monoids, and let $\varphi : M \to N$ be a map. We say that

- φ is a *homomorphism* if

$$\forall (a,b,c) \in M^3 : ab = c \implies \varphi(a)\varphi(b) = \varphi(c) \qquad \text{and} \qquad f(e_M) = e_N.$$

- φ is an *isomorphism* if it is a homomorphism and there exists a homomorphism $\psi : N \to M$ such that $\varphi \circ \psi = \mathrm{Id}_N$ and $\psi \circ \varphi = \mathrm{Id}_M$.
- M is *isomorphic* to N, written $M \cong N$, if there exists an isomorphism from M to N.
- N is a *homomorphic image* of M if there is a surjective homomorphism from M to N.

Note that $\cong$ is an equivalence relation on the class of all monoids.

Proposition 1.13.

(a) *Let M and N be monoids and $\varphi : M \to N$ be a map. Then φ is an isomorphism if and only if it is a bijective homomorphism.*

(b) *Let G and H be groups and $\varphi : G \to H$ be a map. Then φ is a homomorphism if and only if $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$.*

Proposition 1.14. *Let M, N be monoids and let $\varphi : M \to N$ be a homomorphism. Then $\varphi(M^{\times}) \subset N^{\times}$, hence φ restricts to a homomorphism of groups $M^{\times} \to N^{\times}$.*

1.4 Subgroups

1.4.1 Definition and Criterion

Definition 1.15. Let G be a group and H a subset of G. We say that H is a *subgroup* of G, written $H \leq G$, if H is a group and the inclusion map $i : H \to G$ is a homomorphism.

Proposition 1.16 (Subgroup Criterion)**.** *Let G be a group and H be a subset of G equipped with the same operation as G. The following are equivalent:*

(i) $h, h' \in H \Rightarrow hh' \in H, \;\; h \in H \Rightarrow h^{-1} \in H, \;\; 1_G \in H;$

(ii) $h, h' \in H \Rightarrow h^{-1}h' \in H;$

(iii) $H \leq G.$

1.4.2 Image and Kernel of a Homomorphism

Definition 1.17. Let $\varphi : G \to H$ be a homomorphism between groups. The *kernel* of φ

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = 1_H\}$$

and the *image* of φ is

$$\varphi(G) = \{\varphi(g) \mid g \in G\}.$$

Proposition 1.18. *Let $\varphi : G \to H$ be a homomorphism of groups. Then $\ker\varphi \leq G$ and $\varphi(G) \leq H$.*

Example 1.19.

(i) Let $U(1) = \{z \in \mathbb{C}^\times : |z| = 1\}$. Then $U(1)$ is a subgroup of $\mathbb{C}^\times$.

(ii) Let R be a commutative ring. Then $\det : M_n(R) \to R$ is a homomorphism of monoids, where $M_n(R)$ and R are considered monoids under multiplication. By Proposition 1.14, this gives a group homomorphism $\det : \mathrm{GL}_n(R) \to R^\times$. The kernel of this map is the *special linear group*:

$$\mathrm{SL}_n(R) = \ker(\det) = \{A \in \mathrm{GL}_n(R) \mid \det(A) = 1\}.$$

1.4.3 Intersections and Generation of Subgroups

Proposition 1.20. *If $\{H_i\}_{i\in I}$ is a family of subgroups of a group G, then $\bigcap_{i\in I} H_i$ is a subgroup of G.*

Definition 1.21. Let G be a group.

- Let $S \subset G$. The *subgroup of G generated by S*, denoted $\langle S \rangle$, is the intersection of all subgroups of G containing S. If $G = \langle S \rangle$ we say *G is generated by S*. We write $\langle g_1, g_2, \ldots, g_n \rangle = \langle \{g_1, g_2, \ldots, g_n\} \rangle$.
- G is *finitely generated* if $G = \langle S \rangle$ for some finite subset $S \subset G$.
- G is *cyclic* if $G = \langle g \rangle$ for some $g \in G$.
- The *join* of two subgroups $H, K \leq G$ is defined to be $H \vee K = \langle H \cup K \rangle$.

Here is a more concrete description of the subgroup $\langle S \rangle$:

Proposition 1.22. *Let G be a group and $S \subset G$. Then $\langle S \rangle$ consists of all finite products $s_1 s_2 \cdots s_k$ where $s_i \in S \cup S^{-1}$ where $S^{-1} = \{s^{-1} \mid s \in S\}$.*

1.4.4 Order of Elements and the Torsion Subgroup of an Abelian Group

Definition 1.23. The *order* of an element $g \in G$, written $|g|$ is defined to be $|\langle g \rangle|$, the order of the cyclic subgroup of G generated by g.

Proposition 1.24. *Let A be an abelian group. The set of elements of A of finite order is a subgroup of A.*

Definition 1.25. The subgroup of finite order elements in an an abelian group A is called the *torsion subgroup* of A, denoted $t(A)$.

Example 1.26. $t(\mathbb{C}^\times) \leq U(1)$.

1.5 Group-theoretic Properties

Consider a statement $S(G)$ about groups G, such as "G is abelian". We say that $S(G)$ is a *group-theoretic property* if $G \cong H$ implies that $S(G) \Leftrightarrow S(H)$.

Notation 1.27. For a cardinal k, let

$$\mathrm{E}_k(G) = \{g \in G : |g| = k\}$$

be the set of order k elements in G and

$$\mathrm{Sub}_k(G) = \{H \in \mathscr{P}(G) : H \leq G \text{ and } |H| = k\}$$

be the set of order k subgroups of G.

Proposition 1.28. *Let k, m be cardinal numbers. The following statements are group-theoretic properties:*

(a) *"G has order k"*

(b) *"G is abelian"*

(c) "$|\mathrm{E}_m(G)| = k$"

(d) "$|\operatorname{Sub}_m(G)| = k$"

Example 1.29. The group of quaternionic units, $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, is not isomorphic to the dihedral group D_8 of order 8. Indeed, although they are both non-abelian and have order 8, they have different number of order 2 elements:

$$\mathrm{E}_2(Q_8) = \{-1\}, \qquad \{s, r^2\} \subseteq \mathrm{E}_2(D_8).$$

We do not need to determine the exact number of order 2 elements in D_8, only that there are more than one.

2 Examples of Groups

2.1 Symmetric Groups

Definition 2.1. Let X be a set. The *symmetric group on* X, denoted S_X, is defined to be $(X^X)^\times$, the group of invertible functions from X to X under composition. We also put $S_n = S_{\underline{n}}$. In this context, elements of S_X are called *permutations* of X. A *permutation group* is a subgroup of S_X for some X. A *permutation representation* of a group G is a homomorphism from G to S_X for some X.

Definition 2.2. Let X be a set. A *cycle*

$$\sigma = (a_1\ a_2\ \cdots\ a_\ell)$$

where $a_1, a_2, \ldots, a_\ell$ are ℓ distinct elements of X, is the permutation of X defined by

$$\sigma(x) = \begin{cases} a_{i+1}, & x = a_i,\ 1 \le i \le \ell - 1, \\ a_1, & x = a_\ell, \\ x, & x \notin \{a_1, a_2, \ldots, a_\ell\}. \end{cases}$$

The positive number ℓ is the *length* of σ. An *ℓ-cycle* is a cycle of length ℓ. A *transposition* is a 2-cycle. Two cycles $(a_1\ a_2\ \cdots\ a_\ell)$ and $(b_1\ b_2\ \cdots\ b_k)$ are *disjoint* if $\{a_1, a_2, \ldots, a_\ell\} \cap \{b_1, b_2, \ldots, b_k\} = \emptyset$.

Remark 2.3. We have the following redundancies in the cycle notation: Any cycle of length one, (a_1), coincides with the identity element $1 = \mathrm{Id}_X$ in S_X. We call such cycles *trivial.* Also, a cycle σ of length ℓ can be written in exactly ℓ ways:

$$(a_1\ a_2\ \cdots\ a_{\ell-1}\ a_\ell) = (a_2\ a_3\ \cdots\ a_\ell\ a_1) = \cdots = (a_\ell\ a_1\ \cdots\ a_{\ell-2}\ a_{\ell-1}).$$

Theorem 2.4 (Cycle Decomposition)**.** *Let X be a finite set. Any nontrivial element π of S_X is a product of pairwise disjoint nontrivial cycles. Furthermore if $\pi = \sigma_1\sigma_2\cdots\sigma_r = \tau_1\tau_2\cdots\tau_s$ are two decompositions of π into products of disjoint nontrivial cycles, then $r = s$ and after reindexing if necessary, $\sigma_i = \tau_i$ for all i.*

Lemma 2.5 (Conjugation of Cycles)**.** *Let $\pi \in S_X$ and let $\sigma = (a_1\ a_2\ \cdots\ a_\ell)$ be a cycle in S_X. Then*

$$\pi\sigma\pi^{-1} = \big(\pi(a_1)\ \ \pi(a_2)\ \ \cdots\ \ \pi(a_\ell)\big). \tag{2.1}$$

Lemma 2.6. *An ℓ-cycle is a product of $\ell - 1$ transpositions:*

$$(a_1\ a_2\ \cdots\ a_\ell) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{\ell-2}\ a_{\ell-1})(a_{\ell-1}\ a_\ell)$$

Theorem 2.7. *The symmetric group S_n has the following presentation:*

$$S_n \cong \langle s_1, s_2, \ldots s_{n-1} \mid s_i^2 = 1\,\forall i;\ s_is_j = s_js_i \text{ if } |i-j| > 1;\ s_is_js_i = s_js_is_j \text{ if } |i-j| = 1\rangle \tag{2.2}$$

where s_i corresponds to the adjacent transposition $(i\ i+1)$.

2.2 Free Groups

The free group on a set X is denoted $F(X)$ can be thought of as the "most general group containing X". Thus, in $F(X)$ we can multiply and take inverses of elements of X, but there are no relations other than those required in order for $F(X)$ to be a group in the first place. There has to be an identity $1 \in F(X)$, $1x = x = x1$ and inverses $x^{-1} \in F(X)$, $xx^{-1} = 1 = x^{-1}x$ for all $x \in X$, and we have associativixty but that is all. Since we have no unnecessary relations, 1 will not be an element of X and neither will the inverse x^{-1} of any element $x \in X$.

In terms of presentations, one can say that $F(X) = \langle X \mid \text{no relations}\rangle$.

Example 2.8.

(i) If $X = \emptyset$ then $F(X) = 1$, the trivial group.

(ii) If $X = \{x\}$ then $F(X) \simeq \mathbb{Z}$. Indeed, $n \mapsto x^n$ provides an isomorphism $Z \to F(X)$.

(iii) If $X = \{x, y\}$ then $F(X)$ consists of all "words" in $\{1, x, y, x^{-1}, y^{-1}\}$ where the only simplifications are the obvious ones such as $xx^{-1} = 1$ and $1x = x$. Thus a typical element of $F(X)$ is

$$xy^{-5}x^2y^{-1}xyx^{-4}y^{-1}.$$

This word cannot be simplified any further. A general element can be written $x^{a_1}y^{b_1}\cdots x^{a_n}y^{b_n}$ where $n \in \mathbb{N}$ and $a_i, b_i \in \mathbb{N}$ for all $i \in \underline{n}$. Multiplication is just concatenation (write one word next to the other) followed by simplification. For example,

$$x^3yx^{-2} \cdot x^5y^{-7}xy = x^3yx^{-2}x^5y^{-7}xy = x^3yx^3y^{-7}xy$$

and that is as far as we can simplify. In particular $xy \neq yx$ so $F(X)$ is certainly not abelian.

The following theorem states that any function $j : X \to G$, where G is a group, extends to a group homomorphism $\widetilde{j} : F(X) \to G$.

Theorem 2.9 (Universal property of the free group $F(X)$)**.** *Let G be any group and $j : X \to G$ any function. Then there exists a homomorphism $\widetilde{j} : F(X) \to G$ such that $\widetilde{j}(x) = j(x)$ for all $x \in X$.*

Corollary 2.10. *Any group is isomorphic to a quotient of a free group.*

Proof. Take $X = G$ and define $j : G \to G$ by $j(g) = g$. By the universal property of free groups, j extends to a group homomorphism $\widetilde{j} : F(G) \to G$ where $F(G)$ is the free group on G. Since $\widetilde{j}(g) = j(g) = g$ for all $g \in G$, $\widetilde{j}$ is surjective so by the first isomorphism theorem $F(G)/\ker\widetilde{j} \simeq G$. □

2.3 Matrix Groups

2.3.1 Rings

Definition 2.11.

- A *ring* is a set R with two binary operations called addition, denoted $+$, and multiplication, denoted by juxtaposition, such that
  - (i) R is an abelian group under $+$,
  - (ii) $R \setminus \{0\}$ is a monoid under multiplication,
  - (iii) The following distributive laws hold: For all $x, y, z \in R$,

$$x(y+z) = xy + xz \qquad \text{and} \qquad (x+y)z = xz + yz. \tag{2.3}$$

- A *commutative ring* is a ring R such that $xy = yx$ for all $x, y \in R$.
- A *division ring* is a ring such that $R \setminus \{0\}$ is a group under multiplication.
- A *field* is a commutative division ring.

Notation 2.12. For a ring R, we denote by $R^\times$ the group of invertible elements of the multiplicative monoid $R \setminus \{0\}$. This is also called the *group of units* of R.

Example 2.13.

(i) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields under usual operations.

(ii) $\mathbb{Z}/n\mathbb{Z}$ (under addition and multiplication of congruence classes $\bar{a}+\bar{b}=\overline{a+b}$, $\bar{a}\cdot\bar{b}=\overline{a\cdot b}$) is a commutative ring for any $n\in\mathbb{Z}$. The group of units of $\mathbb{Z}/n\mathbb{Z}$ is

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a}\in\mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n)=1\}. \tag{2.4}$$

In particular $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$, where ϕ is Euler's ϕ-function. It also follows that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.

(iii) If R is a commutative ring, then $M_n(R)$ is a monoid under matrix multiplication and $\mathrm{GL}(n,R)=M_n(R)^\times$ is the *general linear group over R*. By Cramer's Rule for matrix inverse it follows that $\mathrm{GL}(n,R)=\{A\in M_n(R)\mid \det(A)\in R^\times\}$. Here $\det : M_n(R)\to R$ is a monoid homomorphism, which gives a group homomorphism $\det : \mathrm{GL}_n(R)\to R^\times$. The kernel of det is the *special linear group over R*: $\mathrm{SL}_n(R) = \{A\in \mathrm{GL}_n(R)\mid \det(A)=1\}$.

(iv) The ring of *real quaternions* $\mathbb{H}$ is a 4-dimensional real vector space with basis $\{1,i,j,k\}$:

$$\mathbb{H}=\{a1+bi+cj+dk \mid a,b,c,d\in\mathbb{R}\}$$

(hence an abelian group under vector addition) with multiplication determined by the rules

1) $(\lambda 1)x=\lambda x = x(\lambda 1)$ for all $\lambda\in\mathbb{R}, x\in\mathbb{H}$,

2) $(\lambda x+\mu y)z=\lambda(xz)+\mu(yz)$ and $z(\lambda x+\mu y)=\lambda(zx)+\mu(zy)$ for all $x,y,z\in\mathbb{H}$,

3) $i^2=j^2=k^2=ijk=-1$ (Hamilton 1843).

One checks that in $\mathbb{H}$ we have

$$ij=k,\ jk=i,\ ki=j,\quad ji=-k,\ ik=-j,\ kj=-i. \tag{2.5}$$

Theorem 2.14. *$\mathbb{H}$ is a noncommutative division ring.*

(v) The ring of *integer quaternions* is

$$\mathbb{H}_\mathbb{Z}=\{a1+bi+cj+dk \mid a,b,c,d\in\mathbb{Z}\}.$$

$\mathbb{H}_\mathbb{Z}$ is a noncommutative ring (a subring of $\mathbb{H}$). The *quaternion group* is $Q_8=(\mathbb{H}_\mathbb{Z})^\times$. It is an exercise to show that

$$Q_8=\{\pm1,\pm i,\pm j,\pm k\}.$$

Consequently, Q_8 is a nonabelian group of order 8.

2.3.2 The Orthogonal Groups

Equip $\mathbb{R}^n$ with the standard inner product (dot product):

$$\langle u, v\rangle = u_1v_1 + u_2v_2 + \cdots u_nv_n = u^T \cdot v$$

for any two column vectors $u = [u_1\ u_2\ \cdots\ u_n]^T$ and $v = [v_1\ v_2\ \cdots\ v_n]^T$ in $\mathbb{R}^n$.

Definition 2.15. The *orthogonal group* is the following subgroup of $\mathrm{GL}_n(\mathbb{R})$:

$$\begin{aligned} \mathrm{O}(n) &= \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \langle Au, Av\rangle = \langle u, v\rangle \text{ for all } u, v \in \mathbb{R}^n\} \\ &= \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^TA = I\}. \end{aligned}$$

(To see the last equality, note that $\langle Au, Av\rangle = \langle u, v\rangle$ if and only if $u^T(A^TA)v = u^Tv$ and then choose u and v to be arbitrary standard basis vectors for $\mathbb{R}^n$.)

Definition 2.16. An *isometry* of $\mathbb{R}^n$ is a bijective map $f : \mathbb{R}^n \to \mathbb{R}^n$ such that

$$d(f(x), f(y)) = d(x, y),$$

where the Euclidean metric (distance) is given by

$$d(x, y) = \|x - y\| = \sqrt{\langle x - y, x - y\rangle}. \tag{2.6}$$

Proposition 2.17. $\mathrm{O}(n)$ *is the group of all isometries of* $\mathbb{R}^n$*.*

Proof. If $A \in \mathrm{O}(n)$ then the formula (2.6) shows that the map $f(x) = Ax$ is a linear isometry. Conversely, if f is an isometry then the *polarization identity*

$$\langle x, y\rangle = \frac{1}{4}(\|x + y\|^2 - \|x - y\|^2) = \frac{1}{4}\big(d(x, -y)^2 - d(x, y)^2\big) \tag{2.7}$$

shows that $\langle f(x), f(y)\rangle = \langle x, y\rangle$ for all $x, y \in \mathbb{R}^n$. Now we have $\langle f(\lambda x + \mu y) - \lambda f(x) - \mu f(y), z\rangle = \langle f(\lambda x + \mu y), z\rangle - \lambda\langle f(x), z\rangle - \mu\langle f(y), z\rangle = \langle \lambda x + \mu y, f^{-1}(z)\rangle - \lambda\langle x, f^{-1}(z\rangle - \mu\langle y, f^{-1}(z)\rangle = 0$ for all $x, y, z \in \mathbb{R}^n$. Since f is surjective and $\langle\cdot,\cdot\rangle$ is non-degenerate, f is a linear map, hence given by a matrix $A \in \mathrm{O}(n)$. □

Definition 2.18. The *special orthogonal group* is defined as

$$\mathrm{SO}(n) = \mathrm{O}(n) \cap \mathrm{SL}_n(\mathbb{R}).$$

Geometrically $\mathrm{SO}(n)$ consists of the *orientation-preserving* linear isometries.

2.4 Dihedral groups

Let V_n be the set of vertices of the regular n-gon (n-sided polygon) in $\mathbb{R}^2$, with all vertices on the unit circle and one of vertex at $(1,0)$. Thus

$$V_n = \{P_0, P_1, \ldots, P_{n-1}\}, \qquad P_k = (\cos k\theta_n, \sin k\theta_n), \qquad \theta_n = 2\pi/n.$$

The *dihedral group of order* $2n$ is defined as the subgroup of $\mathrm{O}(2)$ consisting of all transformations that preserve the set V_n:

$$D_{2n} = \{A \in \mathrm{O}(2) \mid Ax \in V_n \text{ for all } x \in V_n\}.$$

D_{2n} also called the *group of symmetries* of the regular n-gon. Let

$$r = \begin{bmatrix} \cos 2\pi/n & -\sin 2\pi/n \\ \sin 2\pi/n & \cos 2\pi/n \end{bmatrix} \quad \text{and} \quad s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

The linear transformation r is rotation counter-clockwise by $2\pi/n$ radians, while s is the reflection in the x-axis.

Theorem 2.19. *$D_{2n} = \langle r, s\rangle$ and we have*

$$r^n = 1, \quad s^2 = 1, \quad sr = r^{-1}s.$$

Any element of D_{2n} can be uniquely written $r^i s^j$ where $i \in \{0,1,\ldots,n-1\}$ and $j \in \{0,1\}$. In particular D_{2n} has order $2n$.

3 Quotient Groups and Isomorphism Theorems

3.1 Normal Subgroups; Quotient Groups

Definition 3.1. A subgroup N of a group G is *normal (in G)* if $gNg^{-1} \subset N$ for all $g \in G$. We denote this property by $N \trianglelefteq G$.

Lemma 3.2. *Let N be a subgroup of a group G. The following are equivalent:*

(i) *$N \trianglelefteq G$,*

(ii) *$gNg^{-1} = N$ for all $g \in G$,*

(iii) *$gN = Ng$ for all $g \in G$.*

Remark 3.3. There is one subtlety here: It is not true that for every $g \in G$ the implication $gNg^{-1} \subset N \Rightarrow gNg^{-1} = N$ holds. However, if $gNg^{-1} \subset N$ *for all* $g \in G$, then $gNg^{-1} = N$ for all $g \in G$.

For a subgroup N of a group G, let

$$G/N = \{gN \mid g \in G\}. \tag{3.1}$$

The definition of multiplication in G/N is often done by choosing representatives. We follow an alternative route here.

Definition 3.4. For $X, Y \in G/N$ define $XY = \{xy \mid x \in X, y \in Y\}$.

The product XY is a subset of G and may or may not be anoter element of G/N.

Proposition 3.5. *Let G be a group and $N \le G$. The following are equivalent:*

(i) *For all $X, Y \in G/N$, $XY \in G/N$;*

(ii) *$N \trianglelefteq G$.*

If these conditions hold then G/N is a group under the operation defined.

Proof. (i)⇒(ii): Choose $X = gN$ and $Y = g^{-1}N$. By (i) there exists $g' \in G$ such that $gNg^{-1}N = g'N$. This implies that $gNg^{-1} \subset g'N$. In particular $1 = g1g^{-1} \in g'N$, hence $g' \in N$ so that $g'N = N$. Thus $gNg^{-1} \subset N$. Since g was arbitrary, N is normal in G.

(ii)⇒(i): Let $gN, g'N \in G/N$. By Lemma 3.2, $Ng' = g'N$ hence $gNg'N = gg'NN = gg'N \in G/N$.

Lasly, assuming the conditions (i) and (ii) hold, we show G/N is a group. Let $X, Y, Z \in G/N$. Then $(XY)Z = X(YZ)$ by associativity in G. For any $gN \in G/N$ we have $gN = gNN = NgN$ hence N is the identity element of G/N. Lastly, $gNg^{-1}N = Ngg^{-1}N = NN = N$ so $(gN)^{-1} = g^{-1}N$. This shows that G/N is a group. □

Definition 3.6. Let N be a normal subgroup of a group G. The group G/N just defined is the *quotient (or factor) group of G by N.*

3.2 Isomorphism Theorem

Proposition 3.7. *Let $\varphi : G \to H$ be a homomorphism of groups, and let N be a normal subgroup of G contained in $\ker\varphi$. Then there is a homomorphism $\bar\varphi : G/N \to H$ such that $\bar\varphi(gN) = \varphi(g)$ for all $g \in G$.*

Theorem 3.8 (First Isomorphism Theorem)**.** *Let $\varphi : G \to H$ be a group homomorphis with kernel K. Then there is an isomorphism $\bar\varphi : G/K \cong \varphi(G)$ satisfying $\bar\varphi(gK) = \varphi(g)$ for all $g \in G$.*

Theorem 3.9 (Second Isomorphism Theorem)**.** *Let G be a group and $H, N \le G$ such that $hNh^{-1} = N$ for all $h \in H$. Then $NH = HN \le G$ and $N \trianglelefteq NH$ and $H \cap N \trianglelefteq H$ and*

$$NH/N \cong H/(H \cap N). \tag{3.2}$$

In particular,

$$|NH| = \frac{|N||H|}{|H \cap N|}. \tag{3.3}$$

Theorem 3.10 (Subgroup Lattice Isomorphism Theorem)**.** *Let G be a group and $N \trianglelefteq G$, and put $\bar{G} = G/N$. Let $\mathrm{Sub}(G; N)$ be the set of subgroups of G containing N, and $\mathrm{Sub}(\bar{G})$ be the set of all subgroups of $\bar{G}$. For each $H \in \mathrm{Sub}(G; N)$, let $\bar{H} = H/N$. Then the assigment $H \mapsto \bar{H}$ is a bijection from $\mathrm{Sub}(G; N)$ to $\mathrm{Sub}(\bar{G})$. Furthermore, for any $H, K \in \mathrm{Sub}(G; N)$ the following statements hold:*

(a) $\overline{H \cap K} = \bar{H} \cap \bar{K}$*;*

(b) $\overline{H \vee K} = \bar{H} \vee \bar{K}$*;*

(c) $H \leq K$ *iff* $\bar{H} \leq \bar{K}$*, in which case* $|K : H| = |\bar{K} : \bar{H}|$*;*

(d) $H \trianglelefteq K$ *iff* $\bar{H} \trianglelefteq \bar{K}$*, in which case* $K/H \cong \bar{K}/\bar{H}$ *(Third Isomorphism Theorem).*

3.3 Presentations of Groups

Definition 3.11 (Group Presentation)**.** Let X be a set and R a subset $F(X)$. The group *presented by generators X and relations R*, denoted by

$$\langle X \mid r = 1 \; \forall r \in R \rangle$$

is defined to be the group

$$F(X)/N(R)$$

where $N(R)$ is normal subgroup of $F(X)$ generated by R. A group is said to be *finitely presented* if X and R can be chosen finite. In this case we write

$$\langle x_1, x_2, \ldots, x_m \mid r_1 = 1, r_2 = 1, \ldots, r_n = 1 \rangle.$$

Another way to define $N(R)$ is to say it is the intersection of all normal subgroups of $F(X)$ which contain R. It is thus the smallest normal subgroup of $F(X)$ containing R. Concretely, $N(R)$ consists of all products of $F(X)$-conjugates of elements of $R \cup R^{-1}$.

Example 3.12. (1) The following is a finitely presented group:

$$G = \langle x, y \mid xy^2x^{-1}y^{-1} = 1, \; x^3 = 1 \rangle$$

By definition, $G = F(\{x, y\})/N$ where N the normal subgroup generated by $\{xy^2x^{-1}y^{-1}, x^3\}$.

(2) We say that the relations $R \subseteq F(X)$ are *contradictory* if $N(R) = F(X)$. For example, if

$$G = \langle x, y \mid xy = 1,\ xyx = 1 \rangle$$

then using that $N(R)$ is a (normal) subgroup of $F(X)$ containing xy and xyx it is easy to see that $N(R)$ has to contain both x and y. Since those generate all of $F(X)$, we have $N(R) = F(X)$ which means that G is the trivial group.

Determining when a presented group is non-trivial is very difficult. Similarly, determining whether two groups with given presentations are isomorphic is also difficult. One can actually prove that there is no algorithm that always works.

Example 3.13. The dihedral group has a presentation

$$D_{2n} \cong \langle r, s \mid r^n = s^2 = srsr = 1 \rangle.$$

4 G-Sets

4.1 Definition and Examples

Definition 4.1. A *(left) G-set* is a set X together with a map $G \times X \to X$, $(g, x) \mapsto g.x$, called the *action of G on X* satisfying

(i) $g.(h.x) = (gh).x$ for all $g, h \in G, x \in X$;

(ii) $1_G.x = x$ for all $x \in X$.

Example 4.2.

(i) If X is a G-set, H is a group and $\varphi : H \to G$ is a group homomorphism, then X becomes an H-set by defining

$$h.x = \varphi(h).x, \qquad \forall h \in H, x \in X.$$

In particular if $H \leq G$ then the inclusion $H \to G$ turns any G-set into an H-set by restricting the action.

(ii) Let X be a set. Then the symmetric group S_X acts on X by $\sigma.x = \sigma(x)$.

(iii) If $\varphi : G \to S_X$ is any group homomorphism then the previous two examples show that G acts on X.

(iv) Conversely if G acts on a set X then we can define $\varphi : G \to S_X$ by $\varphi(g)(x) = g.x$. We say that φ is *afforded* by the action. (This gives a bijective correspondence between the set of actions of G on X and the set of group homomorphisms from G to S_X.)

(v) G acts on itself in three important ways:

$$\begin{aligned} g.x &= gx, && \textit{left regular action} \\ g.x &= xg^{-1}, && \textit{right regular action} \\ g.x &= gxg^{-1}, && \textit{conjugation action} \end{aligned}$$

Restricting these actions to a subgroup $H \leq G$ gives three actions (left/right regular and conjugation actions) of H on G.

(vi) If Y is a subset of a G-set X such that $g.y \in Y$ for all $y \in Y$, then Y becomes a G-set by restricing the action to $G \times Y$.

4.2 Decomposition into Orbits; Transitive and Free Actions

Lemma 4.3. *Let X be a G-set. The relation $\sim_G$ on X defined by by $x \sim_G y \Leftrightarrow \exists g \in G : y = g.x$ is an equivalence relation.*

Definition 4.4. The equivalence classes $[x]_{\sim_G}$ are called the *(G-)orbits in X* and are denoted $G.x$ or $\mathrm{Orb}_G(x)$:

$$\mathrm{Orb}_G(x) = G.x = \{g.x \mid g \in G\}. \tag{4.1}$$

The set $X/\sim_G$ of all G-orbits in X is denoted X/G.

By Theorem 0.5, and G-set X is partitioned into orbits:

Theorem 4.5 (Orbit Decomposition Theorem)**.** *Let X be a G-set. Then*

$$X = \bigsqcup_{\mathcal{O} \in X/G} \mathcal{O}. \tag{4.2}$$

In particular,

$$|X| = \sum_{\mathcal{O} \in X/G} |\mathcal{O}|. \tag{4.3}$$

Definition 4.6. Let X be a G-set and $x \in X$. The *(G-)stabilizer* of x is

$$\mathrm{Stab}_G(x) = G_x = \{g \in G \mid g.x = x\} \tag{4.4}$$

Proposition 4.7. *Let X be a G-set. Then* $\mathrm{Stab}_G(x) \leq G$ *for any $x \in X$.*

Definition 4.8. Let X be a G-set. We say that the action of G on X is

- *transitive* if $|X/G| = 1$,
- *free* if $\mathrm{Stab}_G(x) = 1$ for all $x \in X$.

Corollary 4.9. *Let G be a finite group and X be a finite G-set. If G is acting freely on X, then $|G|$ divides $|X|$.*

Proof. Since G is acting freely, the map $G \to \mathrm{Orb}_G(x)$, $g \mapsto g.x$ is bijective for every $x \in X$. Consequently all orbits have size $|G|$. The result now follows from the Orbit Decomposition Theorem. □

Proposition 4.10. *Let G be a group, $H \leq G$ and let X be a G-set. Regard X as an H-set via the restricted action.*

(a) *If the action of H on X is transitive, then the action of G on X is transitive.*

(b) *If the action of G on X is free, then the action of H on X is free.*

5 Structure Theory of Groups

5.1 Regular Action of $H \leq G$ on G; Lagrange's Theorem

If $H \leq G$ then the right and left regular actions of H on G are free. The orbits are, respectively

$$gH = \{gh \mid h \in H\} \qquad Hg = \{hg \mid h \in H\}$$

and are called *left* (respectively *right*) *cosets* of H in G. The set of left cosets of H in G is denoted G/H.

Theorem 5.1 (Langrange's Theorem)**.** *Let G be a finite group and $H \leq G$. Then $|H|$ divides $|G|$.*

Proof. Since the left regular action of H on G is free, the conclusion follows from Corollary 4.9. □

Definition 5.2. If G is a group and $H \leq G$, the *index of H in G*, denoted $|G : H|$ is the number of left cosets of H in G:

$$|G : H| = |G/H|. \tag{5.1}$$

When G is finite this number equals $|G|/|H|$.

Example 5.3. Let G be a group of order p, where p is a prime number. We show that G is cyclic. Let $g \in G$ be a nontrivial element. Then $|g| > 1$. By Lagrange's Theorem, $|g|$ divides p. Since p is prime, $|g| = p$. Thus $\langle g \rangle = G$.

5.2 Left Regular Action of G on G/H; Cayley's Theorem

G acts on G/H by $g.(g_1H) = (gg_1)H$. We refer to this as the left regular action as well.

Theorem 5.4. *The left regular action of G on G/H is transitive. The kernel K of the afforded permutation representation $\varphi : G \to S_{G/H}$ is $K = \bigcap_{x\in G} xHx^{-1}$. By the First Isomorphism Theorem, ϕ induces an injective group homomorphism*

$$\bar{\varphi} : G/K \to S_{G/H}. \tag{5.2}$$

In particular, G/K is isomorphic to a subgroup of $S_{G/H}$.

Taking $H = 1$ in this theorem we obtain Cayley's Theorem:

Corollary 5.5 (Cayley's Theorem)**.** *Any group is G isomorphic to a subgroup of the symmetric group S_n, where $n = |G|$.*

5.3 Orbit-Stabilizer Theorem

Definition 5.6. If X and Y are G-sets, a *map of G-sets* $\varphi : X \to Y$ is a function such that

$$\varphi(g.x) = g.\varphi(x), \qquad \text{for all } g \in G, x \in X.$$

Two G-sets X and Y are *isomorphic*, written $X \cong Y$, if there are maps of G-sets $\varphi : X \to Y$ and $\psi : Y \to X$ such that $\varphi \circ \psi = \mathrm{Id}_Y$ and $\psi \circ \varphi = \mathrm{Id}_X$.

Due to the decomposition (4.2), to describe all G-sets up to isomorphism it suffices to describe the transitive G-sets.

Lemma 5.7. *Let X be a G-set, $g \in G$ and $x \in X$. Then:*

$$g \operatorname{Stab}_G(x) g^{-1} = \operatorname{Stab}_G(g.x) \tag{5.3}$$

Theorem 5.8 (Orbit-Stabilizer Theorem)**.** *Let G be a group.*

(i) *Every transitive G-set X is isomorphic to G/H for some subgroup H. More precisely, for any $x \in X$ the map $G/G_x \to X$ given by $gG_x \mapsto g.x$ is a well-defined isomorphism of G-sets.*

(ii) *If $H, K \leq G$ then the G-sets G/H and G/K are isomorphic if and only if $H = gKg^{-1}$ for some $g \in G$.*

Corollary 5.9. *The cardinality of an orbit equals the index of the corresponding stabilizer. More precisely, if X is a G-set, then for any $x \in X$,*

$$|\operatorname{Orb}_G(x)| = |G : \operatorname{Stab}_G(x)|$$

Definition 5.10. A subset T of a G-set X is a *set of orbit representatives for X/G* if the map $T \to X/G$, $t \mapsto \mathrm{Orb}_G(t)$ is a bijection.

Combining Corollary 5.9 with the Orbit Decomposition Theorem we get:

Corollary 5.11. *For any G-set X we have*

$$|X| = \sum_{t\in T} |G : \mathrm{Stab}_G(t)|$$

where T is a set of orbit representatives for X/G.

It is useful to extract the singleton orbits from the sum. Each singleton orbit consists of a so called *fixed point*:

$$|\mathrm{Orb}_G(x)| = 1 \Leftrightarrow \mathrm{Orb}_G(x) = \{x\} \Leftrightarrow g.x = x \text{ for all } g \in G.$$

We denote the set of fixed points by X^G:

$$X^G = \{x \in X \mid g.x = x \text{ for all } g \in G\}.$$

By Corollary 5.11 we get:

Corollary 5.12. *For any G-set X we have*

$$|X| = |X^G| + \sum_{t\in T\setminus X^G} |G : \mathrm{Stab}_G(t)|$$

where T is a set of representatives for X/G.

5.4 Counting the Number of Orbits; Applications to Combinatorics

Theorem 5.13. *Let G be a group and X be a G-set. Then*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G} |X^g| \tag{5.4}$$

where $X^g = \{x \in X \mid g.x = x\}$.

Proof. Let

$$\widetilde{X} = \{(g,x) \in G \times X \mid g.x = x\}. \tag{5.5}$$

On the one hand,

$$|\widetilde{X}| = \sum_{g\in G} |X^g|. \tag{5.6}$$

On the other hand

$$|\widetilde{X}| = \sum_{x\in X} |\operatorname{Stab}_G(x)| \tag{5.7}$$

Since $\operatorname{Stab}_G(g.x) = g \operatorname{Stab}_G(x)g^{-1}$, and conjugate subgroups have the same order, it suffices to sum over a set of representatives T for the orbits. Thus (5.7) equals

$$|\widetilde{X}| = \sum_{x\in T} |\operatorname{Orb}_G(x)||\operatorname{Stab}_G(x)|$$

By the Orbit-Stablizer Theorem, $|\operatorname{Orb}_G(x)| = |G : \operatorname{Stab}_G(x)|$ hence we get

$$|\widetilde{X}| = \sum_{x\in T} |\operatorname{Orb}_G(x)||\operatorname{Stab}_G(x)| = \sum_{x\in T} |G| = |T||G| = |X/G||G|$$

Combining this with (5.6), the desired conclusion follows. □

5.5 Conjugation Action of G on itself; The Class Equation

When G act on itself by conjugation, we have:

$$\begin{aligned} \operatorname{Orb}_G(x) &= \{gxg^{-1} \mid g \in G\} = \mathrm{Cl_G(x)} && \text{the } G\text{-}\textit{conjugacy class containing } x, \\ \operatorname{Stab}_G(x) &= \{g \in G \mid gxg^{-1} = x\} = C_G(x) && \text{the } \textit{centralizer of } x \textit{ in } G, \\ X^G &= \{x \in G \mid gxg^{-1} = x \,\forall g \in G\} = Z(G) && \text{the } \textit{center of } G. \end{aligned}$$

Call a conjugacy class *singleton* if it has only one element. Corollary 5.12 and Corollary 5.9 imply

Corollary 5.14 (The Class Equation). *Let G be any group. Then:*

$$|G| = |Z(G)| + \sum_t |G : C_G(t)| \tag{5.8}$$

where we sum over all noncentral conjugacy class representatives t.

Example 5.15. Let G be a group of order p^n, where p is prime. We prove that $Z(G) \neq 1$. If $x \in G$, $x \notin Z(G)$, then $C_G(x)$ is a proper subgroup of G, hence p divides $|G : C_G(x)|$ by Lagrange's Theorem. The class equation implies that p divides $|Z(G)|$. Therefore $Z(G) \neq 1$.

5.5.1 Integer Partitions and Conjugacy Classes of Symmetric Groups

Let $n \in \mathbb{N}$. An *(integer) partition* of n is a weakly decreasing sequence $(\lambda_1, \lambda_2, \ldots)$ of natural numbers such that $\sum_{i=1}^{\infty} \lambda_i = n$. Let P_n denote the set of partitions of n. We omit the infinitely many trailing zeros from the notation. For example,

$$P_5 = \{(5), (4, 1), (3, 2), (3, 1, 1), (2, 2, 1), (2, 1, 1, 1), (1, 1, 1, 1, 1)\}.$$

The nonzero λ_i are the *parts* of λ and the number of parts is the *length* of λ. The number of times a positive integer k occurs as a part in λ is the *multiplicity* of k in λ and is denoted $m_k(\lambda) = |\{i \in \mathbb{Z}_{>0} \mid \lambda_i = k\}|$.

For a permutation $\sigma \in S_n$, we let $p(\sigma)$ be the partition of n whose parts are the cycle lengths in a cycle decomposition of σ, ordered in a weakly decreasing fashion. For example if $\sigma = (1\,2)(3\,4)(5\,6)(7)(8) \in S_8$ then $p(\sigma) = (2, 2, 2, 1, 1)$. Note that here we do include the 1-cycles.

Theorem 5.16. *The map $p : S_n \to P_n$ is surjective and the fibers $p^{-1}(\lambda)$ are the conjugacy classes of S_n. In other words, we have a bijection*

$$\bar{p} : \{\textit{conjugacy classes of } S_n\} \to P_n \qquad [\sigma] \mapsto p(\sigma). \tag{5.9}$$

Theorem 5.17. *Let $\sigma \in S_n$ and $\lambda = p(\sigma)$. Let $\sigma = \sigma_1\sigma_2 \cdots \sigma_\ell$ be a cycle decomposition of σ in which $|\sigma_i| = \lambda_i$. For each $k \in \mathbb{Z}_{>0}$ let S_{m_k} be the subgroup of S_n permuting the m_k factors of σ_i with $\lambda_i = k$. Then $|C_{S_n}(\sigma)| = |\langle\sigma_1, \sigma_2, \ldots, \sigma_\ell\rangle||S_{m_1} \times S_{m_2} \times \cdots|$.*

Proof. Let x_i be the smallest number appearing in σ_i and let $X = \{x_1, x_2, \ldots, x_\ell\}$. Define an action of $C_{S_n}(\sigma)$ on S_X as follows. For $\tau \in C_{S_n}(\sigma)$ and $x \in X$, let $\tau.x = x_i$ if $\tau(x)$ occurs in the cycle σ_i. The permutation representation afforded by this action is a group homomorphism $\psi : C_{S_n}(\sigma) \to S_X$. The image is $S_{X_1} \times \cdots \times S_{X_d}$ where X_j is the set of x_i occuring in a cycle of length λ_j and d is the number of distinct parts. The kernel is $\langle\sigma_1, \ldots, \sigma_\ell\rangle$. The conclusion now follows from the First Isomorphism Theorem. □

Corollary 5.18. *If $\sigma \in S_n$ then*

$$|\operatorname{Cl}_{S_n}(\sigma)| = \frac{n!}{\lambda_1^{m_1} \cdots \lambda_d^{m_d} m_1! m_2! \cdots m_d!} \tag{5.10}$$

where $\lambda_1, \ldots, \lambda_d$ are the distinct cycle lengths and m_i is the number of cycles of lengths λ_i in a cycle decomposition of σ.

5.6 Automorphism Groups

For each $g \in G$ there is an isomorphism $\varphi_g : G \to G$ given by $\varphi_g(h) = ghg^{-1}$.

Definition 5.19. An *automorphism* of a group G is a isomorphism from G to itself. The set of all automorphisms of G is denoted $\operatorname{Aut}(G)$. The subset of *inner automorphisms* is

$$\operatorname{Inn}(G) = \{\varphi_g \mid g \in G\}.$$

Theorem 5.20. *$G/Z(G) \simeq \operatorname{Inn}(G) \trianglelefteq \operatorname{Aut}(G) \leq S_G$.*

Theorem 5.21. *Let $H \leq G$. There is an injective group homomorphism*

$$N_G(H)/C_G(H) \to \operatorname{Aut}(H). \tag{5.11}$$

In particular, the order of $N_G(H)/C_G(H)$ divides the order of $\operatorname{Aut}(H)$.

5.7 Sylow's Theorem

Definition 5.22. Let p be a prime number.

- A *p-group* is a group whose order is a power of p.
- A *p-subgroup* of a group is a subgroup which is a p-group.
- A *Sylow p-subgroup* P of a finite group G is a p-subgroup such that $p \nmid |G : P|$.

The set of Sylow p-subgroups of a finite group G is denoted by $\operatorname{Syl}_p(G)$. Let $n_p = n_p(G) = |\operatorname{Syl}_p(G)|$.

Theorem 5.23. *Let G be a finite group and let p be any prime number.*

(i) $\operatorname{Syl}_p(G) \neq \emptyset$.

(ii) *Let P be a Sylow p-subgroup of G and Q be any p-subgroup of G. Then $Q \leq gPg^{-1}$ for some $g \in G$. In particular, any two Sylow p-subgroups of G are conjugate, so $n_P(G) = |G : N_G(P)|$ for any $P \in \operatorname{Syl}_p(G)$.*

(iii) *$n_p(G)$ is congruent to 1 modulo p and divides m, where $|G| = p^\alpha m$, $p \nmid m$.*

6 Finitely-Generated Abelian Groups

Definition 6.1. $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (r factors) is called *the free abelian group of rank r*. Any group isomorphic to $\mathbb{Z}^r$ is *a free abelian group (of rank r)*.

We allow $r = 0$, in which case $\mathbb{Z}^0$ is the trivial group.

Lemma 6.2 (Universal property of $\mathbb{Z}^r$)**.** *Let G be any abelian group and $\{x_1, x_2, \ldots, x_r\}$ a subset of G. Then there exists a homomorphism $\varphi : \mathbb{Z}^r \to G$ uniquely determined by $\varphi(e_i) = x_i$.*

Proof. (Uniqueness): Writing G additively, if such φ exists then necessarily

$$\varphi(a_1, a_2, \ldots, a_r) = \sum_{i=1}^{r} a_i \varphi(e_i) = \sum_{i=1}^{r} a_i x_i \tag{6.1}$$

for every $(a_1, a_2, \ldots, a_r) \in \mathbb{Z}^r$.
(Existence): Check that the formula (6.1) defines a homomorphism taking e_i to x_i. □

Lemma 6.3 (Smith's Normal Form)**.** *Let $m, n \in \mathbb{N}$. If A is an integer $m \times n$ matrix, then there exist an invertible $m \times m$ integer matrix P and an invertible $n \times n$ integer matrix Q such that the only nonzero entries of the $m \times n$-matrix PAQ are on the diagonal:*

$$PAQ = \begin{bmatrix} n_1 & & & \\ & n_2 & & \\ & & \ddots & \\ & & & \end{bmatrix} \tag{6.2}$$

and where furthermore n_i are non-negative integers with $n_1 \mid n_2 \mid \cdots$. In fact, if $n = \infty$ the same conclusion holds (PAQ will then have infinitely many zero columns to the right).

Proof. Using elementary integer row and column operations (permutations, multiplying by -1 (the only nontrivial invertible integer), and adding an integer multiple of one to another), which correspond to multiplication from the left and right by elementary matrices, one can transform A into a matrix having the gcd of all its entries in the upper left corner. Using more row and column operations one can clear out the elements to the right and below this entry and proceed by induction along the main diagonal. □

Proposition 6.4. *Let K be a subgroup of the free abelian group of rank k. Then there exists an automorphism σ of $\mathbb{Z}^k$ such that*

$$\sigma(K) = n_1\mathbb{Z} \times n_2\mathbb{Z} \times \cdots \times n_k\mathbb{Z} \tag{6.3}$$

for some non-negative integers n_j with $n_1 \mid n_2 \mid \cdots \mid n_k$. Moreover, $(n_1, n_2, \ldots, n_k)$ is uniquely determined by K. In particular, every subgroup of a free abelian group is a free abelian group.

Proof. Let $\{a_i\}_{i=1}^n$ be a generating set for K, where $n \in \mathbb{N} \cup \{\infty\}$. By adding zero vectors to the generating set if necessary, we may without loss of generality assume that $n \geq k$. Let A be the $k \times n$-matrix whose i:th column equals a_i. Multiplication by A gives a group homomorphism $\mathbb{Z}^n \to \mathbb{Z}^k$ and the image of A is equal to K. By Lemma 6.3, there are invertible integer matrices P and Q of appropriate sizes such that PAQ has the form (6.2). Define $\sigma : \mathbb{Z}^k \to \mathbb{Z}^k$ by $\sigma(x) = Px$. Then $\sigma(K) = \sigma(A\mathbb{Z}^n) = PAQ\mathbb{Z}^n = n_1\mathbb{Z} \times n_2\mathbb{Z} \times \cdots \times n_k\mathbb{Z}$. For the last part, note that $n\mathbb{Z} \cong \mathbb{Z}$ for any nonzero integer n. So $K \simeq \sigma(K) = n_1\mathbb{Z} \times n_2\mathbb{Z} \times \cdots \times n_k\mathbb{Z} \simeq \mathbb{Z}^r$ where r is the number of nonzero n_j. □

Remark 6.5. If $n_i = 1$ for some i then $n_1 = n_2 = \cdots = n_i = 1$, since $\big(n \mid 1 \wedge n \geq 0\big) \Rightarrow n = 1$. If $n_j = 0$ for some j then $n_j = n_{t+1} = \cdots = n_k = 0$, since $0 \mid n \Rightarrow n = 0$. Let t (respectively r) be the number of n_j that equal 1 (respectively 0). Then the RHS of (6.3) becomes

$$\mathbb{Z}^t \times (m_1\mathbb{Z} \times m_2\mathbb{Z} \times \cdots \times m_{k-(t+r)}\mathbb{Z}) \times \{0\}^r \tag{6.4}$$

where now m_j are integers ≥ 2 with $m_1 \mid m_2 \mid \cdots \mid m_{k-(t+r)}$.

Definition 6.6. The *torsion subgroup* $t(G)$ of an abelian group G is the set of finite order elements of G. It is a subgroup since G is abelian. The *exponent* of a group G is the smallest positive integer d such that $g^d = 1$ for all $g \in G$, or $d = \infty$ if no such integer exists.

Theorem 6.7 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Any finitely generated abelian group G is isomorphic to*

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s} \times \mathbb{Z}^r$$

for unique integers $r, s \geq 0$ and $n_j \geq 2$ with $n_1 \,\big|\, n_2 \,\big|\, \cdots \,\big|\, n_s$.

Proof. Let G be a finitely generated abelian group, say $G = \langle X \rangle$ where $X = \{x_1, x_2, \ldots, x_k\} \subseteq G$ and k is minimal. By Lemma 6.2 there exists a homomorphism $\varphi : \mathbb{Z}^k \to G$, $\varphi(e_i) = x_i$. Since $G = \langle X \rangle$, φ is surjective. Now apply Proposition 6.4 to $K = \ker \varphi$ to find an automorphism σ of $\mathbb{Z}^k$ such that $\sigma(K)$ is isomorphic to (6.4). By the First Isomorphism Theorem applied to $\varphi \circ \sigma^{-1}$, which has kernel $\sigma(K)$, we get

$$G \cong \mathbb{Z}^k/\sigma(K) \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_{k-(t+r)}} \times \mathbb{Z}^r.$$

For the uniqueness, note that $G/t(G) \cong \mathbb{Z}^r$ hence r is uniquely determined by G. Suppose $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$ where $n_i \,\big|\, n_{i+1}$ for all i. Then n_s is the exponent of G, n_{s-1} is the exponent of $G/(\{0\}^{s-1} \times \mathbb{Z}_{n_s})$ and so on. Thus the numbers n_i are uniquely determined by G. □

Definition 6.8. In Theorem 6.7, the number r is the *free rank* or *Betti number* of G, and the integers n_j are the *invariant factors* of G.

Definition 6.9. An *elementary p-group* is an abelian group of the form $\mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_k}}$, where we may assume a_i form a weakly monotone sequence of positive integers.

Using that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$, any finitely generated abelian group G is isomorphic to $\mathbb{Z}^r$ times a product of elementary p-groups for p ranging over a finite set of prime numbers. The numbers p^{a_i} appearing are the *elementary divisors* of G.

One can translate between invariant factors and elementary divisors.

7 Semidirect Products

Let K and H be any two groups. Then the set $G = K \times H = \{(k, h) \mid k \in K, h \in H\}$ becomes a group with pointwise operations:

$$(k, h)(k', h') = (kk', hh').$$

Notice that G contains two subgroups $\widetilde{K} = K \times 1$ and $\widetilde{H} = 1 \times H$. We wish to characterize the direct product $G = K \times H$ in terms of the two subgroups $\widetilde{G}$ and $\widetilde{H}$. We observe the following properties:

(i) $G = \widetilde{K}\widetilde{H}$ (since $(k,h) = (k,1)(1,h)$)

(ii) $\widetilde{K} \cap \widetilde{H} = 1$ (since if $g \in \widetilde{K} \cap \widetilde{H}$ then $g = (k,1) = (1,h)$ for some k, h, hence $g = (1,1) = 1_G$)

(iii) $\widetilde{K} \trianglelefteq G$ and $\widetilde{H} \trianglelefteq$ (indeed, $(h,k)(h',1)(h,k)^{-1} = (hh'h^{-1}, 1)$ and similarly for $\widetilde{K}$)

It turns out that these properties suffice to characterize G in terms of the two subgroups. More precisely, we have

Theorem 7.1. *Let G be a group and $K, H \leq G$ be two subgroups satisfying the following properties:*

(i) $G = KH$

(ii) $K \cap H = 1$

(iii) $K \trianglelefteq G$ *and* $H \trianglelefteq G$

Then the map $\phi : K \times H \to G$, $\phi(k,h) = kh$ is an isomorphism.

Proof. (i) evidently shows that ϕ is surjective. (ii) implies that ϕ is injective: Suppose $\phi(k,h) = \phi(k',h')$. That is, $kh = k'h'$. Then $(k')^{-1}k = h'h^{-1} \in K \cap H = 1$, hence $k' = k$ and $h' = h$. It remains to show that ϕ is a homomorphism. One checks that this is equivalent to that $kh = hk$ for all $k \in K, h \in H$. For any $k \in K, h \in H$ we have $khk^{-1}h^{-1} = k(hk^{-1}h^{-1}) = (khk^{-1})h^{-1} \in K \cap H$ since K and H are normal in G. By (ii), $H \cap K = 1$ hence $khk^{-1}h^{-1} = 1$, i.e. $kh = hk$. □

Definition 7.2. Let G be a group and $K, H \leq G$. We say that G is the *(internal) direct product* of K and H if conditions (i)–(iii) of Theorem 7.1 are satisfied.

To get the definition of internal *semi*direct product, we simply drop the condition of normality for one of the two subgroups:

Definition 7.3. Let G be a group and $N, H \leq G$. We say that G is the *(internal) semidirect product* of N by H if

(i) $G = NH$

(ii) $N \cap H = 1$

(iii) $N \trianglelefteq G$.

Since the first two conditions are unchanged, the map $\phi : N \times H \to G$, $\phi(x,h) = xh$, is still bijective. The question arises what the multiplication $*$ on the set $N \times H$ should be, in order for ϕ to be a homomorphism (hence an isomorphism). The answer is that we must have

$$(x,h) * (x',h') = \phi^{-1}\big(\phi(x,h)\phi(x',h')\big)$$

but we want to make this more explicit. For any $x, x' \in N, h, h' \in H$ we have:

$$\phi(x,h)\phi(x',h') = xhx'h' = (xhx'h^{-1})(hh')$$

In the right hand side x and $hx'h^{-1}$ are elements of N (since $N \trianglelefteq G$). Therefore ϕ^{-1} applied to $(xhx'h^{-1})(hh')$ equals $(xhx'h^{-1}, hh')$. To summarize, defining a binary operation $*$ on $N \times H$ by

$$(x,h) * (x',h') = (xhx'h^{-1}, hh'), \tag{7.1}$$

the map $\phi : N \times H \to G$ will be an isomorphism. What we learn from this is that in order to perform computations G, in addition to the structure of H and N, we need to know what $hx'h^{-1}$ is. That is, we need to know how to *conjugate an element of N by and element of H*. Define $\alpha : H \to \operatorname{Aut}(N)$ by $h \mapsto \alpha_h$, where $\alpha_h(x) = hxh^{-1}$ for all $x \in N, h \in H$. With this notation we can write the multiplication rule obtained in $N \times H$ as follows:

$$(x,h) * (x',h') = (x\alpha_h(x'), hh'). \tag{7.2}$$

This suggests the following definition.

Definition 7.4. Let N and H be any two groups, and let $\alpha : H \to \operatorname{Aut}(N), h \mapsto \alpha_h$, be a homomorphism. The *(external) semidirect product* of N by H (with respect to α), denoted $N \rtimes_\alpha H$, is the set $N \times H$ equipped with the multiplication $*_\alpha$ defined by

$$(x,h) *_\alpha (x',h') = (x\alpha_h(x'), hh'), \qquad \forall x \in N, h \in H. \tag{7.3}$$

Proposition 7.5. *For any two groups N, H and homomorphism $\alpha : H \to \operatorname{Aut}(N)$, the semidirect product $N \rtimes_\alpha H$ is a group.*

Proof. The element $(1_N, 1_H)$ will be an identity element of $N \rtimes_\alpha H$. The inverse of (x,h) is $(\alpha_{h^{-1}}(x^{-1}), h)$. Associativity consists in checking that the two expressions $\big((x,h) *_\alpha (x',h')\big) *_\alpha (x'',h'')$ and $(x,h) *_\alpha \big((x',h') *_\alpha (x'',h'')\big)$ equal

$$(x\alpha_h(x')\alpha_{hh'}(x''), hh'h'').$$

□

Example 7.6. *Construct two non-abelian groups of order* 42. Clearly $S_3 \times \mathbb{Z}_7$ is nonabelian of order 42. Consider $\operatorname{Aut}(\mathbb{Z}_7) \cong \mathbb{Z}_7^\times$. One checks that $\bar{3} = 3 + 7\mathbb{Z}$ has order 6 in $\mathbb{Z}_7^\times$, hence we have a homomorphism (in fact, isomorphism) $\alpha : \mathbb{Z}_6 \to \operatorname{Aut}(\mathbb{Z}_7)$, given by $\alpha_{\bar{n}}(\bar{a}) = \bar{3}^n\bar{a}$, $\bar{n} \in \mathbb{Z}_6$, $\bar{a} \in \mathbb{Z}_7$. Let $G = \mathbb{Z}_7 \rtimes_\alpha \mathbb{Z}_6$. Then G contains an element of order 6 (namely $(\bar{0}, \bar{1})$) while $S_3 \times \mathbb{Z}_7$ does not (using $|(g,h)| = \operatorname{lcm}(|g|, |h|)$). So G is not isomorphic to $S_3 \times \mathbb{Z}_7$.

The reason G in the above example is nonabelian is due to the following result, the proof of which is left as an exercise to the reader:

Proposition 7.7. *Let N, H be groups and $\alpha : H \to \operatorname{Aut}(N)$ be a homomorphism. Then $N \rtimes_\alpha H$ is abelian if and only if N and H are abelian and $\alpha_h = \operatorname{Id}_N$ for all $h \in H$.*

8 Ring Theory

8.1 Definition of Rings, Homomorphisms, and Subrings

8.1.1 Rings

Definition 8.1.

- A *ring* is a set R with two binary operations called addition, denoted $+$, and multiplication, denoted by juxtaposition, such that

  (i) R is an abelian group under $+$,

  (ii) $R \setminus \{0\}$ is a monoid under multiplication,

  (iii) The following distributive laws hold: For all $x, y, z \in R$,

$$x(y+z) = xy + xz \qquad \text{and} \qquad (x+y)z = xz + yz. \tag{8.1}$$

- A *ring homomorphism* $f : R \to S$ is a function such that f is a both a group homomorphism (with respect to $+$) and a monoid homomorphism (with respect to multiplication). That is, for all $r, r' \in R$:

$$f(r + r') = f(r) + f(r'), \qquad f(rr') = f(r)f(r'), \qquad f(1_R) = 1_S.$$

- A *subring* S of a ring R is a ring which is also a subset of R such that the inclusion map $S \to R$ is a ring homomorphism.

8.2 Examples

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}_\mathbb{Z}, \mathbb{H}_\mathbb{R}$ are rings.

2. If D is a square-free integer (i.e. D is not divisible by the square of any integer) the *ring of integers in $K = \mathbb{Q}(\sqrt{D})$* is defined by

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}, & D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] = \{a + b\frac{1+\sqrt{D}}{2} \mid a, b \in \mathbb{Z}\}, & D \equiv 1 \pmod 4 \end{cases} \tag{8.2}$$

   The slighly nontrivial fact one has to check here is that $\mathcal{O}_K$ is closed under multiplication in the case $D \equiv 1 \pmod 4$. Besides that it is straightforward to check $\mathcal{O}_K$ is a subring of $\mathbb{C}$. (If $D = k^2 D'$ then $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$.)

3. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is a ring and the canonical projection $\mathbb{Z} \to \mathbb{Z}_n$ is a ring homomorphism.

4. If R is a ring then so is $M_n(R)$ with usual operations.

5. If R is a ring then so is $R[x]$ with usual operations. Here x is a variable that is assumed to commute with every element of R. Iterating this we recursively define $R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$ for $n > 1$.

6. Let V be a vector space over a field $\mathbb{F}$. The set of linear maps from V to V is denoted $\mathrm{End}_{\mathbb{F}}(V)$ or $\mathrm{End}(V)$ when $\mathbb{F}$ is understood. It is a ring under composition and pointwise addition.

7. Let M be a monoid and R be a ring. We define a ring structure on the set RM of formal finite sums $\sum_{m \in M} r_m m$ where $r_m \in R$ (at most finitely many nonzero) by

$$\sum_{m \in M} r_m m + \sum_{m \in M} s_m m = \sum_{m \in M} (r_m + s_m) m$$

$$\left(\sum_{m \in M} r_m m \right) \left(\sum_{m \in M} s_m m \right) = \sum_{m \in M} \left(\sum_{x,y \in M : xy = m} r_x s_y \right) m.$$

For example, the monoid ring is $R\mathbb{N}$ which is isomorphic to $R[x]$ by identifying $\mathbb{N}$ with $\{x^n \mid n \in \mathbb{N}\}$.

8.3 Intersections and generation of subrings

Intersection of a family of subrings is a subring. This allows us to define the subring generated by a subset as the intersection of all subrings containing the subset.

8.4 Definition of Algebras

8.4.1 The Weyl Algebra

Definition 8.2. Let $\mathbb{F}$ be a field. An $\mathbb{F}$-*algebra* A is a ring with a ring homomorphism i_A from $\mathbb{F}$ to the center of A. A *homomorphism of* $\mathbb{F}$-*algebras* is a ring homomorphism $\varphi : A \to B$ such that $\varphi_\circ i_A = i_B$.

(In fact the same definition works, and is used, when $\mathbb{F}$ is just a commutative ring.)

Examples of $\mathbb{F}$-algebras include $M_n(\mathbb{F})$, $\mathrm{End}_{\mathbb{F}}(V)$ and $\mathbb{F}[x_1, x_2, \ldots, x_n]$ with natural ring homomorphisms from $\mathbb{F}$ in each case.

Note that any A algebra becomes a vector space over $\mathbb{F}$ if we define $\lambda a = i_A(\lambda) a$ for each $\lambda \in \mathbb{F}$ and $a \in A$.

Definition 8.3. The *Weyl algebra* over a field $\mathbb{F}$, denoted $A_1(\mathbb{F})$ is the subring of $\operatorname{End}_{\mathbb{F}}\big(\mathbb{F}[x])\big)$ generated by the set $\mathbb{F}\,\mathrm{Id} \cup \{D, X\}$ where

$$D\big(p(x)\big) = p'(x), \qquad X\big(p(x)\big) = xp(x), \qquad \forall p(x) \in \mathbb{F}[x].$$

Since the scalars commute with X and D, any element of $A_1(\mathbb{F})$ is a linear combination of products of X and D. By Leibniz' Rule, in the ring $A_1(\mathbb{F})$ we have

$$DX - XD = 1. \tag{8.3}$$

As a consequence of this, $A_1(\mathbb{F})$ is spanned by $\{X^i D^j \mid i, j \in \mathbb{N}\}$. In fact, that set is a basis for $A_1(\mathbb{F})$ (Exercise).

8.5 Ideals and Quotient Rings

8.5.1 Left, Right, and Two-Sided Ideals

8.5.2 Quotient Rings

8.5.3 The Isomorphism Theorems for Rings

8.5.4 Prime Ideals and Maximal Ideals

Definition 8.4. Let R be a ring and I be an ideal of R.

(i) I is *maximal* if for any ideal J of R with $I \subset J \subset R$ we have $I = J$ or $J = R$.

(ii) I is *prime* if for any ideals J, K of R with $I \supset JK$ we have $I \supset J$ or $I \supset K$.

In a commutative ring R, an ideal P is prime iff for any $a, b \in P$ with $ab \in P$ we have $a \in P$ or $b \in P$.

Example 8.5. An ideal $(p) = p\mathbb{Z}$ of $\mathbb{Z}$ is prime if and only if p is prime or zero.

Theorem 8.6. *Let R be a commutative ring and I be an ideal of R.*

(i) *I is a maximal ideal of R iff R/I is a field.*

(ii) *I is a prime ideal of R iff R/I is an integral domain.*

8.6 Integral Domains and Rings of Fractions

8.7 The Remainder Theorem

8.8 Every ED is a PID

Definition 8.7. A *Euclidean domain (ED) R* is an integral domain for which there is a function $N : R \to \mathbb{N}$ such that $N(0) = 0$ and for every $a \in R$ and $b \in R \setminus \{0\}$ there are $q, r \in R$ such that

$$a = qb + r, \qquad N(r) < N(b) \text{ or } r = 0.$$

Theorem 8.8. *Every ED is a PID.*

Theorem 8.9. *Every nonzero prime ideal of a PID is maximal.*

8.9 Every PID is a UFD

Definition 8.10. Let R be an integral domain.

(i) A nonzero nonunit $r \in R$ is *irreducible* if whenever $r = ab$ for some $a, b \in R$ then a or b is a unit.

(ii) A nonzero nonunit $r \in R$ is *prime* if (p) is a prime ideal.

Definition 8.11. A commutative ring R is *noetherian* if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq \cdots$$

eventually stabilizes: there exists an $n > 0$ such that $I_n = I_{n+1} = I_{n+2} = \cdots$.

Lemma 8.12. *Every PID is noetherian.*

Proof. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals. Then $I = \cup_i I_i$ is an ideal of R. Since R is a PID, $I = (a)$ for some $a \in R$. Since I is the union of the ideals I_j, there exists an $n > 0$ such that $a \in I_n$. Then for every $k \geq 0$ we have $I_{n+k} \subseteq I = (a) \subseteq I_n \subseteq I_{n+k}$ proving that $I_{n+k} = I_n$ for all $k \geq 0$. □

Theorem 8.13. *Every PID is a UFD.*

8.10 Irreducible Elements

8.11 Gauss' Lemma. R is a UFD iff $R[x]$ is a UFD

Theorem 8.14 (Gauss' Lemma)**.** *Let R be a UFD and $F = \mathrm{Frac}(R)$ and $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$.*

Theorem 8.15. *Let R be a ring. Then R is a UFD iff $R[x]$ is a UFD.*

8.12 Eisenstein's Irreducibility Criterion

Theorem 8.16. *Let R be an integral domain and $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ be a monic polynomial in $R[x]$ of degree $n \geq 1$. Suppose there exists a prime ideal P of R such that $a_0, a_1, \ldots, a_{n-1} \in P$, but $a_0 \notin P^2$. Then $f(x)$ is irreducible in $R[x]$.*

Proof. Suppose $f(x)$ is reducible in $R[x]$. Then

$$f(x) = g(x)h(x) \tag{8.4}$$

for some non-units $g(x)$, $h(x)$ in $R[x]$. Note that if $g(x)$ is constant then it divides the leading coefficient 1 of $f(x)$ hence is a unit in R, therefore a unit in $R[x]$, which is a contradiction. So both $g(x)$ and $h(x)$ have degree at least one. Write

$$g(x) = \sum_{i=0}^{k} b_i x^i, \qquad h(x) = \sum_{i=0}^{\ell} c_i x^i.$$

Then $k, \ell > 0$ and

$$b_k c_\ell = 1, \tag{8.5}$$

$$b_0 c_0 = a_0. \tag{8.6}$$

Reducing coefficients mod P in (8.4) we obtain the identity

$$x^n = \overline{g(x)} \cdot \overline{h(x)}$$

in the ring $(R/P)[x]$. Here $\overline{g(x)} = \sum_{i=0}^{k}(b_i + P)x^i$ is a nonconstant polynomial since $b_k \notin P$ by (8.5) and similarly $\overline{h(x)}$ is nonconstant. Since P is prime, R/P is an integral domain and we can consider its fraction field $F = \mathrm{Frac}(R/P)$. Since $F[x]$ is a UFD and x is irreducible hence prime, either x divides both $\overline{g(x)}$ and $\overline{h(x)}$ or one of the two is a unit in $F[x]$, contradicting that they are nonconstant. Therefore $x \,\big|\, \overline{g(x)}$ and $x \,\big|\, \overline{h}(x)$. That is, $b_0 \in P$ and $c_0 \in P$. Then, by (8.6), $a_0 = b_0 c_0 \in P^2$ which is a contradiction. □

9 Category Theory

9.1 Classes

A *class* is like a set but can be bigger. Every set is a class but not all classes are sets. A class which is not a set is a *proper class*. Just like with sets we can form the cartesian product of classes, consider functions between classes and so on.

The main reason that we need classes is so that we can talk about things like *the class of all sets* because there is no set that contains all sets. (Likewise there is no class that contains all classes, but usually we don't need to really worry about that.)

9.2 Partial binary operations

A *partial binary operation* $*$ on a class X is a function from some subclass of $X \times X$ to X. We write $* : X \times X \dashrightarrow X$ to indicate that the domain of $*$ may not be all of $X \times X$.

9.3 Definition of category

Definition 9.1. A *category* $\mathcal{C}$ is a quintuple $\mathcal{C} = (\mathcal{C}_0, \mathcal{C}_1, s, t, \circ)$ where

- $\mathcal{C}_0$ is a class whose elements are called the *objects* of $\mathcal{C}$,
- $\mathcal{C}_1$ is a class whose elements are called the *morphisms* of $\mathcal{C}$,
- $s : \mathcal{C}_1 \to \mathcal{C}_0$ is a map called the *source map*,
- $t : \mathcal{C}_1 \to \mathcal{C}_0$ is a map called the *target map*,
- $\circ : \mathcal{C}_1 \times \mathcal{C}_1 \dashrightarrow \mathcal{C}_1$ is a partial binary operation called *composition (of morphisms)* so that $\alpha \circ \beta$ is defined for any morphisms $\alpha, \beta \in \mathcal{C}_1$ with $t(\beta) = s(\alpha)$,

subject to the following two axioms:

(i) (identity) for every object $x \in \mathcal{C}_0$ there exists a morphism $1_x \in \mathcal{C}_1$ with

$$s(1_x) = t(1_x) = x$$

$$\begin{aligned} \alpha \circ 1_x = \alpha & \quad \text{for all morphisms } \alpha \in \mathcal{C}_1 \text{ with } s(\alpha) = x \\ 1_x \circ \beta = \beta & \quad \text{for all morphisms } \beta \in \mathcal{C}_1 \text{ with } t(\beta) = x \end{aligned}$$

(ii) (associativity) we have

$$(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$$

for any morphisms $\alpha, \beta, \gamma \in \mathcal{C}_1$ with $t(\gamma) = s(\beta)$ and $t(\beta) = s(\alpha)$.

Notation 9.2. $\mathcal{C}_0$ and $\mathcal{C}_1$ are sometimes denoted $\operatorname{Ob} \mathcal{C}$ and $\operatorname{Mor} \mathcal{C}$ respectively. You should think of the source and target maps as giving the domain and codomain of a morphism. In this spirit, if $\alpha \in \mathcal{C}_1$ is a morphism with $s(\alpha) = x$ and $t(\alpha) = y$ we write $\alpha : x \to y$.

9.4 Examples

To specify a category we have to say what the objects and morphisms are. If the objects are sets (with extra structure), the source, target and $\circ$ are almost always the domain, codomain and usual composition.

Example 9.3. 1) The category of sets and functions Set. This means that by definition Set_0 is the class of all sets, and Set_1 is the class of all functions between sets.

2) The category of abelian groups and group homomorphisms Ab.

3) For any ring R the category of left R-modules and R-module homomorphisms R-Mod.

4) If L and R are rings the category of (L, R)-bimodules and (L, R)-bimodule homomorphisms is denoted by L-Mod-R.

5) The category of topological spaces and continuous functions: Top.

6) The category of smooth manifolds and smooth maps: Mfd.

7) The *opposite* category, $\mathcal{C}^{\mathrm{op}}$, of a category $\mathcal{C} = (\mathcal{C}_0, \mathcal{C}_1, s, t, \circ)$ is defined as $\mathcal{C}^{\mathrm{op}} = (\mathcal{C}_0, \mathcal{C}_1, t, s, \circ^{\mathrm{op}})$ where $\alpha \circ^{\mathrm{op}} \beta = \beta \circ \alpha$. Simply put, in $\mathcal{C}^{\mathrm{op}}$ all the arrows are just *drawn* the opposite way, otherwise everything is the same as in $\mathcal{C}$.

10 Functors

10.1 Definition

Just like a group homomorphism is a structure preserving map between groups, a *functor* is a structure preserving map between categories. Since a category has two underlying classes, a functor actually needs to be a *pair* of functions.

Definition 10.1. Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A *(covariant) functor* F from $\mathcal{C}$ to $\mathcal{D}$ is a pair of maps $F = (F_0, F_1)$ where $F_i : \mathcal{C}_i \to \mathcal{D}_i$ for $i = 0, 1$ such that

(i) $F_1(1_x) = 1_{F_0(x)}$ for all $x \in \mathcal{C}_0$

(ii) if $\alpha : x \to y$ then $F_1(\alpha) : F_0(x) \to F_0(y)$

(iii) $F_1(\alpha \circ \beta) = F_1(\alpha) \circ F_1(\beta)$ for all morphisms $\alpha, \beta \in \mathcal{C}_1$ with $t(\beta) = s(\alpha)$.

A *contravariant functor* F from $\mathcal{C}$ to $\mathcal{D}$ is the same things as a covariant functor except it reverses the direction of morphisms in the sense that (ii) and (iii) are replaced by

(ii') if $\alpha : x \to y$ then $F_1(\alpha) : F_0(y) \to F_0(x)$

(iii') $F_1(\alpha \circ \beta) = F_1(\beta) \circ F_1(\alpha)$ for all morphisms $\alpha, \beta \in \mathcal{C}_1$ with $t(\beta) = s(\alpha)$.

A contravariant functor $\mathcal{C} \to \mathcal{D}$ is thus the same thing as a covariant functor from $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$.

Notation 10.2. Usually we write Fx for $F_0(x)$ and $F\alpha$ for $F_1(\alpha)$ if no confusion can arise.

10.2 Examples

Unless otherwise emphasized, all functors will be covariant. The following examples are related to the universal property of free R-modules (see next section).

Example 10.3. 1) The forgetful functor $\mathcal{O}_R : R\text{-}\mathsf{Mod} \to \mathsf{Set}$ (where $\mathcal{O}$ stands for oblivion) sends any left R-module M to the underlying set M, and any R-module homomorphism to itself (now regarded as just a function).

2) The free functor $\mathcal{F}_R : \mathsf{Set} \to R\text{-}\mathsf{Mod}$ sends any set X to the free left R-module on the set X, denoted $\mathcal{F}_R X$. And if $\alpha : X \to Y$ then $\mathcal{F}_R\alpha : \mathcal{F}_R X \to \mathcal{F}_R Y$ is the morphism induced by the composition $X \to Y \to \mathcal{F}_R Y$.

The next two examples are important in the context of tensor products (see next section on adjoint functors). Let L, S, R be rings with 1 and fix an (S, R)-bimodule B.

Example 10.4. 1)

$$- \otimes_S B : L\text{-}\mathsf{Mod}\text{-}S \to L\text{-}\mathsf{Mod}\text{-}R$$

is the functor that sends an (L, S)-bimodule A to the (L, R)-bimodule $A \otimes_S B$, and sends an (L, S)-bimodule morphism $\alpha : A \to A'$ to the (L, R)-bimodule morphism $\alpha \otimes 1_B : A \otimes_S B \to A' \otimes_S B$.

2) In the opposite direction we have the following functor:

$$\mathrm{Hom}_R(B, -) : L\text{-}\mathsf{Mod}\text{-}R \to L\text{-}\mathsf{Mod}\text{-}S$$

which sends an (L, R)-bimodule A to $\mathrm{Hom}_R(B, A)$, the set of right R-module maps $B \to A$. $\mathrm{Hom}_R(B, A)$ is an (L, S)-bimodule through

$$(\ell \cdot \varphi)(b) = \ell \cdot (\varphi(b)) \quad \ell \in L, b \in B, \varphi \in \mathrm{Hom}_R(B, A)$$

$$(\varphi \cdot s)(b) = \varphi(s \cdot b) \quad \forall s \in S, b \in B, \varphi \in \mathrm{Hom}_R(B, A)$$

On morphisms the functor $\mathrm{Hom}_R(B, -)$ takes $\alpha : A \to A'$ to the map $\widetilde{\alpha} : \mathrm{Hom}_R(B, A) \to \mathrm{Hom}_R(B, A')$ given by post-composition (push forward): $\widetilde{\alpha}(\varphi) = \alpha \circ \varphi$.

11 Pairs of adjoint functors

11.1 Definition

Definition 11.1. Given categories $\mathcal{C}$ and $\mathcal{D}$, and covariant functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ we say that F *is left adjoint to* G *and* G *is right adjoint to* F if there is a natural bijection

$$\mathrm{Hom}_{\mathcal{C}}(x, Gy) \xrightarrow{\eta_{x,y}} \mathrm{Hom}_{\mathcal{D}}(Fx, y)$$

for all $x \in \mathcal{C}_0$ and $y \in \mathcal{D}_0$. Here $\mathrm{Hom}_{\mathcal{C}}(a, b)$ denotes the class of morphisms in $\mathcal{C}$ from an object a to an object b. That the family $(\eta_{x,y})_{x\in\mathcal{C}_0, y\in\mathcal{D}_0}$ is "natural" means that whenever $\alpha : x \to x'$ and $\beta : y \to y'$ are morphisms in $\mathcal{C}_1$ and $\mathcal{D}_1$ respectively the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{C}}\big(x', Gy\big) \arrow[r, "\eta_{x',y}"] \arrow[d, "-\circ\alpha"] & \mathrm{Hom}_{\mathcal{D}}\big(Fx', y\big) \arrow[d, "-\circ F\alpha"] \\
\mathrm{Hom}_{\mathcal{C}}\big(x, Gy\big) \arrow[r, "\eta_{x,y}"] \arrow[d, "\mathcal{F}(\beta)\circ-"] & \mathrm{Hom}_{\mathcal{D}}\big(Fx, y\big) \arrow[d, "\beta\circ-"] \\
\mathrm{Hom}_{\mathcal{C}}\big(x, Gy'\big) \arrow[r, "\eta_{x,y'}"] & \mathrm{Hom}_{\mathcal{D}}\big(Fx, y'\big)
\end{tikzcd}$$

The commutativity of this diagram makes mathematically precise the vague statement that $\eta_{x,y}$ should be defined "the same way" regardless of the objects x and y. There is an analogous definition for contravariant functors.

11.2 Examples

Many universal properties can be expressed in terms of adjoint functors.

Example 11.2. 1) In example 10.3, the free functor $\mathcal{F}_R : \mathsf{Set} \to R\text{-}\mathsf{Mod}$ is left adjoint to the forgetful functor $\mathcal{O}_R : R\text{-}\mathsf{Mod} \to \mathsf{Set}$ because

$$\mathrm{Hom}_{\mathsf{Set}}(X, \mathcal{O}_R M) \cong \mathrm{Hom}_R(\mathcal{F}_R X, M)$$

for any set X and R-module M. In words, any set map $X \to M$ extends uniquely to an R-module morphism $\mathcal{F}_R X \to M$. The naturality is a tedious but straightforward exercise.

2) In Example 10.4, the functor $- \otimes_S B$ is left adjoint to $\mathrm{Hom}_R(B, -)$. Let ${}_L\mathrm{Hom}_R(X, Y)$ denote the set of (L, R)-bimodule homomorphisms between (L, R)-bimodules X and Y. Then what we are saying is that there is a natural bijection

$${}_L\mathrm{Hom}_S\big(A, \mathrm{Hom}_R(B, C)\big) \cong {}_L\mathrm{Hom}_R(A \otimes_S B, C).$$

Taking $L = R = \mathbb{Z}$ the left hand side can be identified with the set of S-balanced maps $A \times B \to C$, so this expresses precisely the universal property of the tensor product.

A Set Theory and Foundations

Most of mathematics can be formulated in *Zermelo-Fraenkel Set Theory with the Axiom of Choice (ZFC).* To briefly explain what that is, we need to visit the domain of formal logic.

A.1 First-Order Theories

In logic, a *formal system* consists of

- An alphabet, for ex.: $(,), \forall, \exists, \rightarrow, \ldots, P, Q, \ldots, x, y, \ldots, a, b, \ldots$
- Rules which determine which strings of symbols from the alphabet form *well-formed formulas (wffs)*. For ex., in Predicate Calculus $\forall x : P(x) \rightarrow Q(x)$ and $P(c) \vee Q(c)$ are wffs, while $) \rightarrow (P \wedge Q(\exists($ and $P(x) \vee Q(y)$ are not (x and y are meant to be variables, they need quantifiers, while $a, b, c, ...$ are constants which shouldn't have quantifiers).
- A list of wffs called *axioms*, declared as True.
- Deduction rules which tell you how to deduce new True wffs from one or more wffs already known to be True. For ex.: Modus Ponens (in Propositional Calculus): From $P \rightarrow Q$ and P we can conclude Q. Another is Specialization (in Predicate Calculus): From $\exists x : P(x)$ we can conclude $P(c)$ for some constant c.)

Examples of formal systems include

- Propositional Calculus (0th order logic) where a typical wff is $P \wedge Q \rightarrow P$.
- Predicate Calculus (1st order logic) where we have quantifiers and variables as in $\forall x \neg P(x)$.

A *first-order theory* is a formal system that "contains 1st order logic as a subsystem". Hilbert's axiomatization of Euclidean geometry is an example of a first-order theory. ZFC is another example of a first-order theory. Many theories, such as Hilbert's geometry, can be realized within ZFC Set Theory. In such a realization a *line* (which is an atomic concept in Hilbert's geometry) becomes an actual subset of the plane $\mathbb{R}^2$. It is for this reason that mathematicians like set theory so much; most things we want to do can be formulated using sets.

A.2 Zermelo-Fraenkel Set Theory and Induction

In ZF Set Theory (without the Axiom of Choice) there are approximately 8 axioms. We will not list them here, but one of them is the *Axiom of Infinity.* It implies that the natural numbers $\mathbb{N}$ with the usual total order $\leq$ exists and is well-ordered:

Theorem A.1 (Well-Ordering Principle)**.** *The natural numbers $\mathbb{N}$ (equipped with the usual total order $\leq$) is well-ordered. That is, every non-empty subset of $\mathbb{N}$ contains a least element.*

This in turn is equivalent to the Principle of Mathematical Induction. This means that even though ZF and ZFC are just first-order theories (rather than second-order theories in which one can quantify over predicates), we do have induction at our disposal. The reason is basically that a predicate $P(x)$ can be encoded as a set $X_P = \{x \mid P(x)\}$, and quantifying over sets is fine (everything is a set in ZF/ZFC).

A.3 Axiom of Choice

To reach ZFC from ZF one adds one axiom, the Axiom of Choice. This is a non-constructive axiom which asserts the existence of something without providing an algorithm for finding it. Most mathematicians accept and make use of this axiom, but some prefer to work without it and doing so can lead to a better understanding in some situations.

If $X = \{A_i\}_{i \in I}$ is a family of nonempty sets (I is some index set), we denote by $\cup X = \cup_{i \in I} A_i$ the union of all the sets in X.

Axiom A.2 (Axiom of Choice)**.** If X is any family of sets, then there exists a function $f : X \to \cup X$ such that $f(A) \in A$ for all sets $A \in X$.

Such a function f is called a *choice function.* We mention two immediate applications. First, the image of a choice function is a set B containing one element from each of the sets in X. Whenever we implicitly assume the existence of such a set B we are using the Axiom of Choice. Second, the Axiom of Choice implies that the product set $\prod X = \prod_{i \in I} A_i$, consisting of all sequences $(a_i)_{i \in I}$ with $a_i \in A_i$, is a non-empty set for any family of nonempty sets X.

Exercise A.1. Prove the converse to the previous sentence: If the product set $\prod X$ is non-empty for every family of nonempty sets X, then the Axiom of Choice holds.

Without the Axiom of Choice, the existence of a choice function is not guaranteed even for a countable family of sets. (For finite families X the existence of a choice function is ensured by the plain ZF axioms.)

A.4 Zorn's Lemma

The Axiom of Choice is equivalent to Zorn's Lemma, which we now state. Recall that a *partially ordered set (poset)* $(X, \leq)$ is a set with a partial order $\leq$ on X. A *chain* in $(X, \leq)$ is a totally ordered subset: $C \subset X, \forall c, c' \in C : c \leq c' \vee c' \leq c$. An *upper bound* for a subset $A \subseteq X$ is an element $x \in X$ such that $\forall a \in A : a \leq x$. An element $x_0 \in X$ is *maximal* if $\forall x \in X : (x_0 \leq x \Rightarrow x = x_0)$.

Theorem A.3 (Zorn's Lemma)**.** *If* $(X, \leq)$ *is a poset such that every chain has an upper bound, then* X *contains a maximal element.*

A common application of Zorn's Lemma is that every vector space has a basis: Let X be the family of all linearly independent sets in a vector space V, ordered by inclusion. The union of all sets in a totally ordered subset of X is also a linearly independent set, hence Zorn's Lemma applies to conclude that X contains a maximal element B. Then B must span V otherwise we could enlarge B by adjoining a linearly independent vector, contradicting maximality.

As another application, we show that every ring R with identity 1 contains a maximal ideal: Let X be the family of proper ideals of R, ordered by inclusion. If $\{J_i\}_{i\in I}$ is a totally ordered subset of X we show that $J = \cup_{i\in I} J_i$ is an upper bound in X. Clearly $J_i \subseteq J$ for all i so we must show that $J \in X$ i.e. that J is a proper ideal of R. That J is an ideal is easy to check using that $\{J_i\}_{i\in I}$ is totally ordered. It is a proper subset of R because none of the proper ideals J_i contains the identity 1, and consequently $1 \notin J$. Thus Zorn's Lemma applies and X contains a maximal element.

A.5 The Well-Ordering Theorem

A set X is *well-orderable* if there exists a total order $\leq$ on X such that every non-empty subset of X contains a least element (relative to $\leq$). A third statement equivalent to the Axiom of Choice is the following.

Theorem A.4 (Well-Ordering Theorem)**.** *Every set is well-orderable.*

A.6 Beyond ZFC

In category theory it is convenient to work in an extended theory, such as Grothendieck-Tarski Set Theory, in which one can talk about the *class of all sets*, for example. (The collection of all sets can not itself be a set; it leads to contradictions.)