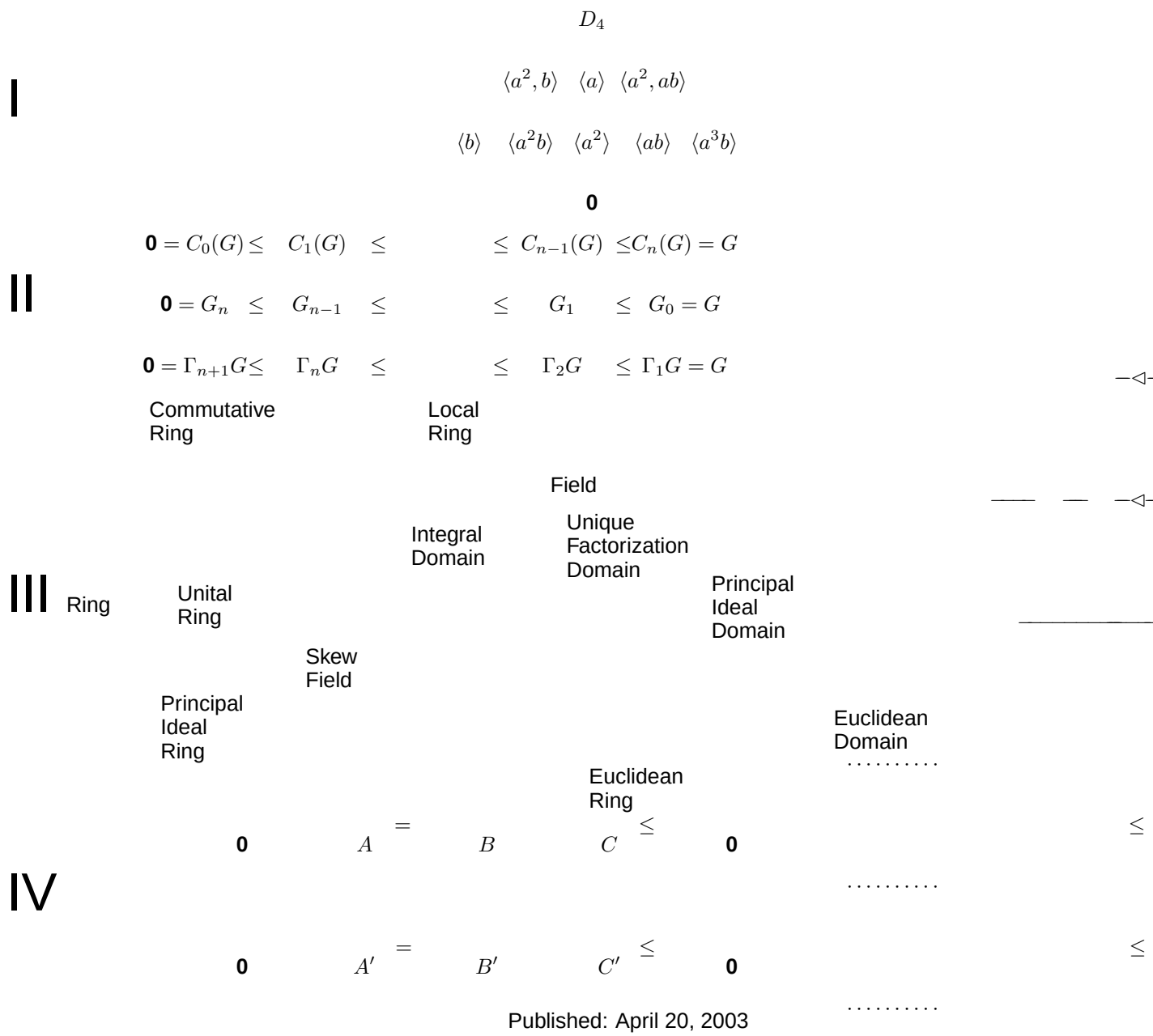
A *Hungerford's* **Algebra** Solutions Manual

Volume I: Introduction through Chapter IV

James Wilson



Published: April 20, 2003

©2002-2003. James Wilson
University of Oregon,
Portland State University.

3234 SE Spruce St.
Hillsboro OR 97123
James.Wilson@scatter.com

Written with LaTeX 2ε.
Please Recycle when finished.

Contents

Prerequisites and Preliminaries **11**

.7 The Axiom of Choice, Order and Zorn's Lemma . . . 11
- .7.1 Lattice. . . . 11
- .7.2 Complete. . . . 12
- .7.3 Well-ordering. . . . 13
- .7.4 Choice Function. . . . 14
- .7.5 Semi-Lexicographic Order. . . . 14
- .7.6 Projections. . . . 15
- .7.7 Successors. . . . 15

.8 Cardinal Numbers . . . 17
- .8.1 Pigeon-Hole Principle. . . . 17
- .8.2 Cardinality. . . . 18
- .8.3 Countable. . . . 19
- .8.4 Cardinal Arithmetic. . . . 19
- .8.5 Cardinal Arithmetic Properties. . . . 20
- .8.6 Finite Cardinal Arithmetic. . . . 21
- .8.7 Cardinal Order. . . . 22
- .8.8 Countable Subsets. . . . 22
- .8.9 Cantor's Diagonalization Method. . . . 23
- .8.10 Cardinal Exponents. . . . 23
- .8.11 Unions of Finite Sets. . . . 25
- .8.12 Fixed Cardinal Unions. . . . 26

I Groups **27**

I.1 Semigroups, Monoids, and Groups . . . 27
- I.1.1 Non-group Objects. . . . 27
- I.1.2 Groups of Functions. . . . 28
- I.1.3 Floops. . . . 28
- I.1.4 D_4 Table. . . . 28
- I.1.5 Order of S_n. . . . 29
- I.1.6 Klein Four Group. . . . 29
- I.1.7 $\mathbb{Z}_p^\times$. . . . 30
- I.1.8 $\mathbb{Q}/\mathbb{Z}$ – Rationals Modulo One. . . . 30
- I.1.9 Rational Subgroups. . . . 31
- I.1.10 PruferGroup. . . . 32
- I.1.11 Abelian Relations. . . . 32
- I.1.12 Cyclic Conjugates. . . . 33
- I.1.13 Groups of Involutions. . . . 33
- I.1.14 Involutions in Even Groups. . . . 33
- I.1.15 Cancellation in Finite Semigroups. . . . 34
- I.1.16 n-Product. . . . 35

I.2 Homomorphisms and Subgroups . . . 36
- I.2.1 Homomorphisms. . . . 36
- I.2.2 Abelian Automorphism. . . . 37
- I.2.3 Quaternions. . . . 37
- I.2.4 D_4 in $\mathbb{R}^{2\times 2}$. . . . 38

I.2.5 Subgroups. . . . 38
I.2.6 Finite subgroups. . . . 39
I.2.7 $n\mathbb{Z}$. . . . 39
I.2.8 Subgroups of S_n. . . . 39
I.2.9 Subgroups and Homomorphisms. . . . 40
I.2.10 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ lattice. . . . 40
I.2.11 Center. . . . 41
I.2.12 Generators. . . . 41
I.2.13 Cyclic Images. . . . 41
I.2.14 Cyclic Groups of Order 4. . . . 42
I.2.15 Automorphisms of $\mathbb{Z}_n$. . . . 42
I.2.16 Generators of PruferGroup. . . . 44
I.2.17 Join of Abelian Groups. . . . 44
I.2.18 Join of Groups. . . . 44
I.2.19 Subgroup Lattices. . . . 45
I.3 Cyclic Groups 47
I.3.1 Order of Elements. . . . 47
I.3.2 Orders in Abelian Groups. . . . 48
I.3.3 $\mathbb{Z}_{pq}$. . . . 48
I.3.4 Orders under Homomorphisms. . . . 48
I.3.5 Element Orders. . . . 48
I.3.6 Cyclic Elements. . . . 49
I.3.7 PruferGroup Structure. . . . 49
I.3.8 Finite Groups. . . . 51
I.3.9 Torsion Subgroup. . . . 52
I.3.10 Infinite Cyclic Groups. . . . 52
I.4 Cosets and Counting 53
I.4.1 Cosets. . . . 53
I.4.2 Non-normal Subgroups. . . . 53
I.4.3 p-groups. . . . 54
I.4.4 Little Theorem of Fermat. . . . 54
I.4.5 Groups of Order 4. . . . 55
I.4.6 Join. . . . 55
I.4.7 p-group Complex. . . . 56
I.4.8 HK-subgroup. . . . 56
I.4.9 Subgroups and the Complex. . . . 57
I.4.10 Identifying Subgroups. . . . 57
I.4.11 Groups of order $2n$. . . . 58
I.4.12 Join and Intersect. . . . 58
I.4.13 pq-groups. . . . 58
I.4.14 Quaternion Presentation. . . . 58
I.5 Normality, Quotient Groups, and Homomorphisms 60
I.5.1 Index 2 Subgroups. . . . 60
I.5.2 Normal Intersections. . . . 60
I.5.3 Normal and Congruence. . . . 61
I.5.4 Congruence. . . . 61
I.5.5 Normality in S_n. . . . 61
I.5.6 Conjugate Subgroups. . . . 62
I.5.7 Unique Subgroups Are Normal. . . . 62
I.5.8 Normality in Q_8. . . . 62
I.5.9 Center of S_n. . . . 62
I.5.10 Normality is Not Transitive. . . . 63
I.5.11 Normal Cyclic Subgroups. . . . 63
I.5.12 Finitely Generated. . . . 63
I.5.13 Normal Subgroup Lattice. . . . 64
I.5.14 Quotient Products. . . . 64
I.5.15 Normal Extension. . . . 65
I.5.16 Abelianization. . . . 65
I.5.17 Integer Quotients. . . . 65

I.5.18 Homomorphic Pre-image. . . . 66
I.5.19 Locating Finite Kernels. . . . 66
I.5.20 Locating Finite Subgroups. . . . 67
I.5.21 PruferQuotients. . . . 68
I.6 Symmetric, Alternating, and Dihedral Groups 69
I.6.1 Lattice of S_4. . . . 69
I.6.2 S_n generators. . . . 69
I.6.3 Permutation Conjugates. . . . 69
I.6.4 More S_n Generators. . . . 70
I.6.5 Permutation Conjugation. . . . 70
I.6.6 Index 2 subgroups of S_n. . . . 70
I.6.7 A_4 is not Simple. . . . 71
I.6.8 A_4 is not solvable. . . . 71
I.6.9 Matrix Form of D_n. . . . 72
I.6.10 D_n is Meta-cyclic. . . . 72
I.6.11 Normality in D_n. . . . 73
I.6.12 Center of D_n. . . . 73
I.6.13 D_n representation. . . . 73
I.7 Categories: Products, Coproducts, and Free Objects 76
I.7.1 Pointed Sets. . . . 76
I.7.2 Equivalence. . . . 76
I.7.3 Direct Product. . . . 77
I.7.4 Group Coproduct. . . . 77
I.7.5 Set Coproduct. . . . 78
I.7.6 Products of Pointed Sets. . . . 78
I.7.7 Free Inclusion. . . . 79
I.7.8 Free Basis. . . . 80
I.8 Direct Products and Direct Sums 81
I.8.1 Non-Product Groups. . . . 81
I.8.2 Product Decomposition. . . . 81
I.8.3 Split Extension. . . . 82
I.8.4 Weak Product. . . . 82
I.8.5 Cyclic Products. . . . 83
I.8.6 p-order Element Groups. . . . 83
I.8.7 84
I.8.8 Internal Product. . . . 84
I.8.9 Product Quotients. . . . 84
I.8.10 Weak Product. . . . 85
I.8.11 Counterexamples. . . . 85
I.9 Free Groups, Free Products, Generators & Realtions 86
I.9.1 Elements of Free Groups. . . . 86
I.9.2 Cyclic Free Group. . . . 86
I.9.3 87
I.9.4 Q_16. . . . 87

II The Structure of Groups **89**
II.1 Free Abelian Groups 89
II.1.1 mA groups.. . . . 89
II.1.2 Linear Indepedence. . . . 90
II.1.3 Commutators. . . . 91
II.1.4 Free-Abelian Groups and Torsion. . . . 92
II.1.5 Non-free, Torsion-free Groups. . . . 92
II.2 Finitely Generated Abelian Groups 93
II.3 The Krull-Schmidt Theorem 94
II.4 The Action of a Group on a Set 95
II.5 The Sylow Theorems 96
II.6 Classification of Finite Groups 97
II.7 Nilpotent and Solvable Groups 98
II.8 Normal and Subnormal Series 99

III Rings **101**
III.1 Rings and Homomorphisms . . . 101
III.1.1 Quaternion Group Ring vs. Division Ring. . . . 101
III.2 Ideals . . . 102
III.2.1 The Little Radical Ideal. . . . 102
III.2.2 Radical Ideal. . . . 102
III.2.3 The Annihilator Ideal. . . . 103
III.2.4 The "Idealizer". . . . 103
III.2.5 Division Rings have no Left Ideals. . . . 103
III.2.6 Nilpotent Factor Ring. . . . 104
III.2.7 Homomorphic Image of Ideals. . . . 104
III.2.8 Prime Ideal in Zero-Divisors. . . . 105
III.2.9 Maximal Ideals in Non-Unital Rings. . . . 105
III.2.10 Prime/Maximal Ideals in $\mathbb{Z}/m\mathbb{Z}$. . . . 105
III.2.11 Prime Decomposition of Integer Rings. . . . 105
III.2.12 Limitation of Chinese Remainder Theorem. . . . 106
III.3 Factorization in Commutative Rings . . . 107
III.3.1 Maximal and Prime Principal Ideals. . . . 107
III.3.2 Irreducible Non-Prime Elements. . . . 107
III.4 Rings of Quotients and Localization . . . 109
III.5 Rings of Polynomials and Formal Power Series . . . 110
III.6 Factorization in Polynomial Rings . . . 111

IV Modules **113**
IV.1 Modules, Homomorphisms, and Exact Sequences . . . 113
IV.1.1 $\mathbb{Z}/n\mathbb{Z}$ Modules. . . . 113
IV.1.2 Monic/Epic Morphisms of Modules. . . . 114
IV.1.3 R/I-Modules. . . . 115
IV.1.4 Unitary Cyclic Modules. . . . 115
IV.1.5 Schur's Lemma. . . . 116
IV.1.6 Finitely Generated Modules. . . . 116
IV.1.7 Hom and Endomorphisms. . . . 116
IV.1.8 Module Products and Sums. . . . 117
IV.1.9 Idempotent and Splitting Maps. . . . 119
IV.1.10 Split Decomposition. . . . 119
IV.1.11 5-Lemma. . . . 120
IV.1.12 Unitary Separation. . . . 121
IV.2 Free Modules and Vector Spaces . . . 123
IV.2.1 Quotient Modules. . . . 123
IV.2.2 Non-trivial Automorphisms of Groups. . . . 123
IV.3 Projective and Injective Modules . . . 125
IV.4 Hom and Duality . . . 126
IV.5 Tensor Products . . . 127
IV.6 Modules over a Prinicpal Ideal Domain . . . 128
IV.7 Algebras . . . 129

V Fields and Galois Theory **131**
V.1 Field Extensions . . . 131
V.1.1 Extension Degrees. . . . 131
V.1.2 Transcendental Dimension. . . . 132
V.2 The Fundamental Theorem . . . 133
V.3 Splitting Fields, Algebraic Closure and Normality . . . 134
V.4 The Galois Group of a Polynomial . . . 135
V.5 Finite Fields . . . 136
V.6 Separability . . . 137
V.7 Cyclic Extensions . . . 138
V.8 Cyclotomic Extensions . . . 139
V.9 Radical Extensions . . . 140

VI The Structure of Fields **141**

VII Linear Algebra **143**

VIIICommutative Rings and Modules **145**

IX The Structure of Rings **147**

X Categories **149**
X.1 Functors and Natural Transformations 149
X.1.1 Example Functors. 149
X.1.2 Functor Image. 151
X.2 Adjoint Functors 152
X.3 Morphisms 153

A Heuristics **155**
A.1 Needle in the Haystack 155
A.2 Principle of Refinement 155

B Syntax and Usage **159**
B.1 Lattices 159

> ...Hungerford's exposition is clear enough that an average graduate student can read the text on his own and understand most of it. ... and almost every section is followed by a long list of exercises of varying degrees of difficulty. ...
>
> –American Mathematical Monthly.

Anyone who has endured a 600 level Algebra course using Hungerford's Algebra is no doubt familiar with ability of one Hungerford problem to remain unsolved for most of the term only to one day surprise you with an elegant and obvious solution. While such episodes have their glorious endings, the process of waiting for "an answer from the sky" can be tedious and hinder exploration of new material. A student who dares lookup a reference to the problem is often surprised to find very few solutions to Hungerford exercises are available – at least they are not listed as solutions to these exercises and so are hard to find. The following material seeks to solve this problem.

This is largely the product of work done through out the terms of a 600 level Algebra course at Portland State University taught by Associate Professor F.R. Beyl. The style of the proofs and examples reflect his philosophy for exercises: while many of the exercises are bombastic and tangential to the main material, they are the types of proofs everyone does once in their lives as a reference for themselves since they will never be called out explicitly in the literature. To quote Professor Beyl "...I can't make you go back to Adam and Eve, but you should know how to do this when you have to..." To this end the proofs attempt to make use only of the material introduced by Hungerford, except with noted exceptions, and only the material presented to that point in the book – although many proofs are inspired by latter discovers that simplify the understanding. Some effort has been placed at referencing the theorems and previous exercises used in various proofs but many remain implicitly inferred.

The structural design of the exercises begins with the statement of the exercise, as found in Hungerford, enumerated identically. For the purpose of cross referencing and ease of use, a short descriptive title is added to each exercise. This title can be found in both the index and table of contents. Next a short paragraph lists some hints about the proofs employed by the authors. The problems are rated for difficulty on a scale of 1 to 5, with 1 the easiest and 5 the hardest. This scale is somewhat arbitrary but attempts to rate problems relative the the section material.

There are 825 exercises in Hungerford's Algebra; so there are mistaken solutions, and even the rare misprint and incorrect statements of the problem. If you find a mistake in the solutions or know of a better, appropriate, solution, please contact us with the relevant sources. Finally while many of the solutions reflect our own creativity, it is inevitable that many solutions borrow extensively from other authors. Where ever this is known we have cited the sources. For those we have missed, we here recognise their work and offer our apologies for miss appropriating it.

Chapter

Prerequisites and Preliminaries

.7 The Axiom of Choice, Order and Zorn's Lemma

1 Lattice 11
2 Complete 12
3 Well-ordering 13
4 Choice Function 14
5 Semi-Lexicographic Order 14
6 Projections 15
7 Successors 15

.7.1 Lattice.

Let $(A, \leq)$ be a partially ordered set and B a nonempty subset. A **lower bound** of B is an element $d \in A$ such that $d \leq b$ for *every* $b \in B$. A **greatest lower bound (g.l.b.)** of B is a lower bound d_0 of B such that $d \leq d_0$ for every other lower bound d of B. A **least upper bound (l.u.b.)** of B is an upper bound t_0 of B such that $t_0 \leq t$ for every other upper bound t of B. $(A, \leq)$ is a **lattice** if for all $a, b \in A$ the set $\{a, b\}$ has both a greatest lower bound and a least upper bound. [1]

(a) If $S \neq \varnothing$, then the power set $P(S)$ ordered by set-theoretic inclusion is a lattice, which has a unique maximal element.

(b) Give an example of a partially ordered set which is *not* a lattice.

(c) Give an example of a lattice with no maximal element and an example of a partially ordered set with two maximal elements.

Hint(2/5): (a) Use intersections and unions to define the greatest lower bound and least upper bound. (b) Construct a lattice with no *unique* candidate for greatest lower bound or least upper bound. (Refer to Appendix **??** for an explanation of a graphic approach to defining partial orderings.) (c) The integers are a simple example. Use pictures to illustrate two maximal elements.

(a) **Proof:** Consider the power set of a nonempty set S. Since S is nonempty so is its power set. Therefore let A, B be subset of S (that is, elements of $P(S)$). There intersection $A \cap B$ contains only elements of S and so it is included in $P(S)$. By construction, $A \cap B \subseteq A$ and $A \cap B \subseteq B$. Moreover

[1] Given two greatest lower bounds, d_0 and d_0', by their definitions $d_0 \leq d_0'$ and $d_0' \leq d_0$ forcing $d_0 = d_0'$. In the same way least upper bounds are unique.

given any subset C of S such that $C \subseteq A$ and $C \subseteq B$, it follows by the definition of the intersection that C is contained in the intersection. Thus $A \cap B$ is the greatest lower bound of A and B and is contained in $P(S)$.

Following suit, the set $A \cup B$ contains only elements of S and so it is a subset of S and even an element of $P(S)$. Again $A \cup B$ is an upper bound of A and B because it contains both sets by its definition. Once a subset C of S is an upper bound of both A and B it must contain all elements of A and B and so $A \cup B \subseteq C$. Therefore $A \cup B$ is the least upper bound of A and B and is contained in $P(S)$. Therefore $P(S)$ is a lattice under set inclusion.

The set S is a subset of S and so included in $P(S)$. Given any subset A, $A \cup S = S$, so in fact S is a maximal element of $P(S)$. Furthermore any subset, M, that is maximal still has the property that $M \cup S = S$. Therefore either S is greater than M contradicting the maximality of M, or M is simply S itself. Therefore $P(S)$ has a unique maximal element. By the analogous argument $\varnothing$ is the minimal element of $P(S)$. □

(b) **Example:** Define a relation on $\{-1, 0, 1\}$ as $0 < -1$ and $0 < 1$. Typically this example is drawn as follows:

$$-1 \qquad\qquad 1$$

$$0$$

Certainly $a \leq a$. Whenever $a \neq b$ either $a < b$ or $b < a$ exclusively; thus, the relation is antisymmetric by the contrapositive. Finally $a \leq b$ and $b \leq c$ implies either $a = b$ or $b = c$ hence $a \leq c$ thus verifying the relation is a partial ordering.

However the ordering does not produce a lattice since $\{-1, 1\}$ has no upper bounds and thus no least upper bound. □

(c) **Example:** The elements of $\mathbb{N}$ ordered in the traditional way form a lattice. This can be seen because given any two elements $m, n \in \mathbb{N}$, either $m \leq n$ or $n \leq m$ (which means min and max functions on pairs are well-defined) so the greatest lower bound is $min\{m, n\}$ and least upper bound is $max\{m, n\}$.

Suppose $\mathbb{N}$ has a maximal element M. By the Peano Axioms $M + 1 \in \mathbb{N}$ and furthermore $M + 1 \neq M$. Yet the ordering states $M < M + 1$ so we contradict the maximality of M. Therefore $\mathbb{N}$ has no maximal element.

Return the ordering in part (b). The size of the example makes it visible that -1 and 1 are maximal elements in the ordering, and they are certainly distinct. □

.7.2 Complete.

Hint$(5/5)$: Consider a chain $a \leq f(a) \leq f(f(a) \leq \cdots$ in A, for some $a \in A$.

A lattice $(A, \leq)$ (see Exercise-.7) is said to be **complete** if every nonempty subset of A has both a least upper bound and a greatest lower bound. A map of partially ordered sets $f : A \to B$ is said to preserve order if $a \leq a'$ in A implies $f(a) \leq f(a')$ in B. Prove that an order-preserving map f of a complete lattice A onto itself has at least one fixed element (that is, an $a \in A$ such that $f(a) = a$).

Proof: Given the entire set A as a subset we see A must have a greatest lower bound and least upper bound – that is unique top and bottom elements. The bottom element b has the property that $b \leq f(b)$. Thus we may construct a chain

$$b \leq f(b) \leq f(f(b)) \leq \cdots \leq f^n(b) \leq \cdots .$$

This chains is a nonempty subset of A so it has a least upper bound $f^\infty(b)$. Clearly $f^n(b) \leq f^\infty(b)$ for all $n \in \mathbb{N}$; therefore, $f^{n+1}(b) \leq f(f^\infty(b))$ for all $n \in \mathbb{N}$ (by applying the order preserving map f) – which is way of stating $f(f^\infty(b))$ is an upper bound of the chain as well. Since $f^\infty(b)$ was picked as the least upper bound it follows $f^\infty(b) \leq f(f^\infty(b))$.

We are now able establish the existence of a chain of chains:

$$\begin{array}{rcl} b & \leq & \cdots \leq f^n(b) \leq \cdots \\ & \leq & f^\infty(b) \leq \cdots \leq f^n(f^\infty(b)) \leq \cdots \\ & \leq & f^\infty(f^\infty(b)) \leq \cdots \leq f^n(f^\infty(f^\infty(b))) \leq \cdots \\ & \vdots & \end{array}$$

This chain must stop since A has a top element. Once the chain stops we have the result that the top element a in the chain has the property that $f(a) = a$. □

.7.3 Well-ordering.

Exhibit a well-ordering of the set $\mathbb{Q}$ of rational numbers.

Hint$(1/5)$: Take care in showing the ordering is well-defined; remember that fractions are equivalence classes. Consider a lexicographic ordering on reduced fractions.

Example: To avoid confusion let $\leq$ be the traditional order of $\mathbb{Z}$ and define a new ordering $\sqsubseteq$ as follows: $\frac{a}{b} \sqsubseteq \frac{c}{d}$ if $\frac{a}{(a,b)} < \frac{c}{(c,d)}$ or when $\frac{a}{(a,b)} = \frac{c}{(c,d)}$ and $\frac{b}{(a,b)} \leq \frac{d}{(c,d)}$. Since the greatest common divisor is unique given any two integers a, b or c, d; the elements $\frac{a}{(a,b)}$, $\frac{b}{(a,b)}$, $\frac{c}{(c,d)}$, and $\frac{d}{(c,d)}$ are defined, and by the properties of G.C.D. they are integers ordered according to the traditional ordering of $\mathbb{Z}$. Furthermore we now see $\frac{a}{b} = \frac{a}{(a,b)} / \frac{b}{(a,b)}$ which is the fraction expressed in lowest terms – notice also since $b \neq 0$ neither does (a, b) so division is defined. Therefore $\sqsubseteq$ is equivalent to testing the unique reduced fractions of the equivalence classes $\frac{a}{b}$ and $\frac{c}{d}$. Thus the order is nothing more than the lexicographic ordering of the reduced fractions. We will now show a lexicographic extension of a well-ordering is well-ordered.

Suppose S is a partially ordered set. Extend the ordering to $S \times S$ by $(a, b) \leq (c, d)$ if $a < c$ or when $a = c$, $b \leq c$.

- $a = a$ and $b \leq b$ in S so $(a, b) \leq (a, b)$.
- Suppose $(a, b) \leq (c, d)$ and $(c, d) \leq (a, b)$. Then: $a < c$ and $c < a$, which is a contradiction; or $a = c$ and $a < c$, again a contradiction; or lastly $a = c$ and $c = a$. Now that $a = c$ and $c = a$ it follows: $b \leq d$ and $d \leq b$, so by the antisymmetry of $\leq$ in S, $b = d$. Therefore $(a, b) = (c, d)$.
- Consider $(a, b) \leq (c, d)$ and $(c, d) \leq (e, f)$. Thus one of the following are true:

$$\begin{array}{llll|l|l} a < c & c < e & & & a < e & (a,b) \leq (e,f) \\ a < c & c = e & & & a < e & (a,b) \leq (e,f) \\ a = c & c < e & & & a < e & (a,b) \leq (e,f) \\ a = c & c = e & b \leq d & d \leq e & a = e, b \leq e & (a,b) \leq (e,f) \end{array}$$

  Therefore $\leq$ is transitive.

So $\leq_{S\times S}$ is a partial ordering whenever $\leq$ in S is a partial ordering.

Suppose S is linearly ordered. Given any two elements (a,b) and (c,d) in $S \times S$, it follows $a < c$, $a = c$, or $c < a$ by the linear ordering in S. Therefore $(a,b) < (c,d)$ in case one and $(c,d) < (a,b)$ in case three. In case two, again we know $b < d$, $b = d$, or $d < b$. Thus either $(a,b) < (c,d)$, $(a,b) = (c,d)$, or $(c,d) < (a,b)$. Therefore $S \times S$ is linearly ordered.

Finally suppose S is well-ordered. Take any nonempty subset A of $S \times S$. Index the elements of $A = \{(a_i, b_i) \mid i \in I\}$. The set $\{a_i \mid i \in I\}$ is a subset of S so it has a least element a, as does the set $\{b_i \mid i \in I\}$, call it b; therefore, $(a,b) \in A$; furthermore, $a \leq a_i$ for all $i \in I$ and $b \leq b_i$, so $(a,b) \leq (a_i, b_i)$ for all $i \in I$. So every nonempty subset of $S \times S$ has a least element; so $S \times S$ is well-ordered.

Returning to $\mathbb{Q}$, we now see the well-ordering of $\mathbb{Z}$ makes $\sqsubseteq$ a well-ordering of $\mathbb{Q}$. □

.7.4 Choice Function.

Hint$(3/5)$: Consider the product of all nonempty subsets of S. An element of this product is a choice function by Introduction, Definition-5.1.

Let S be a set. A **choice function** for S is a function f from the set of all nonempty subsets of S to S such that $f(A) \in A$ for all $A \neq \varnothing$, $A \subseteq S$. Show that the Axiom of Choice is equivalent to the statement that every set S has a choice function.

Proof: ($\Rightarrow$) Suppose the Axiom of Choice is true.

When $S = \varnothing$, the choice function has no definition since there are no nonempty subsets of S. Therefore the function exists vacuously. Suppose instead $S \neq \varnothing$.

The set of all nonempty subsets of S is nonempty since S is nonempty. Index these sets by $I = P(S) - \{\varnothing\}$ as follows: $\{A_i = i \mid i \in I\}$. So we have a family of nonempty sets indexed by a nonempty set so we may take its product to apply the Axiom of Choice: $\prod_{i\in I} A_i \neq \varnothing$. We may now assume there is an element, $f : I \to \bigcup_{i\in I} A_i$, in the product. Notice $S = \bigcup_{i\in I} A_i$. We know by Introduction, Definition-5.1, that $f(i) \in A_i$ for all $i \in I$. Now recall I is the set of all nonempty subsets of S, so in fact, given any nonempty subset A of S, $f(A) \in A$. Thus f is a choice function of S.

($\Leftarrow$) Suppose every set has a choice function. Given any family of nonempty sets $F = \{A_i \mid i \in I\}$ indexed by a nonempty set, define $S = \bigcup_{i\in I} A_i$. Since S is a set it has a choice function $f : P(S) - \{\varnothing\} \to S$ such that $f(A) \in A$ for all $A \subseteq S$, $A \neq \varnothing$. Now define the mapping $g : I \to S$ by $g(i) = f(A_i)$. Since every A_i is uniquely indexed and f is well-defined, we know g to be well-defined. Following Introduction, Definition-5.1, g is an element of the product $\prod_{i\in I} A_i$; so the product is nonempty. Therefore every product of nonempty sets, indexed by a nonempty set, is none empty; the Axiom of Choice is true. □

.7.5 Semi-Lexicographic Order.

Hint$(2/5)$: Use the linear ordering properties of the real line.

Let S be the set of all points (x,y) in the plane with $y \leq 0$. Define an ordering by $(x_1, y_1) \leq (x_2, y_2) \Leftrightarrow x_1 = x_2$ and $y_1 \leq y_2$. Show that this is a partial ordering of S, and that S has infinitely many maximal elements.

Proof: Given any order pairs $(a,b), (c,d)$ and (e,f) the ordering $(a,b) \leq (c,d)$ is well-defined since both the relations $a = c$ and $b \leq d$ are well-defined. Notably $a = a$ and $b \leq b$ so $(a,b) \leq (a,b)$ so the new relation is *reflexive*. Assuming $(a,b) \leq (c,d)$ and also $(c,d) \leq (a,b)$, then by the first we know $a = c$ and $b \leq d$, and by the second also $d \leq b$ so the antisymmetry of $\leq$ in $\mathbb{R}$ shows $b = d$. Thus $(a,b) = (c,d)$ so the new relation is antisymmetric. Finally when $(a,b) \leq (c,d)$ and $(c,d) \leq (e,f)$ the transitivity of equivalence shows $a = c$, $c = d$ implies

$a = d$. Likewise the transitivity of $\leq$ in $\mathbb{R}$ allows the assumed relations $b \leq d$ and $d \leq e$ to imply $b \leq e$. Therefore $(a, b) \leq (e, f)$ and so $\leq$ in S is transitive; so furthermore it is a partial ordering. □

Example: The elements $(n, 0)$ are comparable only to elements of the form (n, y), where $y \leq 0$ and $n \in \mathbb{Z}$. However S allows (a, b) only if $b \leq 0$ thus every comparable element of $(n, 0)$ is bounded above by $(n, 0)$. Since $(n, 0) \in S$ it follows $(n, 0)$ is a maximal element in S. As already presented, $(n, 0)$ is comparable with $(m, 0)$ only if $n = m$. Since the integers have infinitely many elements, there are correspondingly infinitely many maximal elements of the form $(n, 0)$. Therefore S has infinitely many maximal elements. □

.7.6 Projections.

Prove that if all the sets in the family $\{A_i \mid i \in I \neq \varnothing\}$ are nonempty, then each of the projections $\pi_k : \prod_{i \in I} A_i \to A_k$ is surjective.

Hint$(1/5)$: Using the axiom of choice, choose a function f in the product to define a new product element f_a, for each $a \in A_k$, with the property $f_a(k) = a$.

Proof: By Introduction, Definition-5.1, the product $\prod_{i \in I} A_i$ is the collection of all functions of the form $f : I \to \bigcup_{i \in I} A_i$ with the property that $f(i) \in A_i$ for all $i \in I$. By the Axiom of Choice – available since each A_i is nonempty and the product is indexed by a nonempty set I– it follows the product is nonempty. Therefore choose an element $f : I \to \bigcup_{i \in I} A_i$ in $\prod_{i \in I} A_i$. Given any $a \in A_k$, we can define a new mapping as follows:

$$f_a(i) = \begin{cases} f(i) & i \neq k, \\ a & i = k \end{cases} .$$

This function is well-defined as each image is still unique to the given domain element. Therefore f_a is in the product. The projection map π_k now takes f_a to $f_a(k) = a$; thus, the image of π_k is A_i, so each projection is surjective. □

.7.7 Successors.

Let $(A, \leq)$ be a linearly ordered set. The **immediate successor** of $a \in A$ (if it exists) is the least element in the set $\{x \in A \mid a < x\}$. Prove that if A is well-ordered by $\leq$, then at most one element of A has no immediate successor. Give an example of a linearly ordered set in which precisely two elements have no immediate successor.

Hint$(2/5)$: Use the properties of linear ordering to show uniqueness of a maximal element; such an element has no immediate successor.

Proof: Suppose A is well-ordered by $\leq$. Given any element $x \in A$, the set $A_x = \{x \in A \mid a < x\}$ is nonempty if even one element in A is greater than x; that is, x is not a maximal element. So x is not maximal so that A_x is a nonempty set. Since it is a subset of a well-ordered set it has a least element x^+ which lies in A. This least element is unique since well-ordered sets are linearly ordered. [2] Therefore x^+ is a well-defined immediate successor of x.

Now consider M to be a maximal element in A. The element M^+ is no longer defined since A_M is empty. Thus if A has a maximal element, then this element has no immediate successor. In the other direction, if $x \in A$ has no immediate successor, then A_x has no least element. But since A is well-ordered this occurs only when A_x is empty; thus x is maximal in A.

A is a linearly ordered set; so given any two maximal elements M and N, either $M < N$, $M = N$, or $N < M$. Either of the extreme cases violates the maximality of M or N; thus we conclude $M = N$. Therefore at most one element in A has no immediate successor. □

[2] Given $min\{a, b\}$ always exists, then either $a \leq b$ or $b \leq a$.

Example: Consider the set $A = \{0, \ldots, 1/n, \ldots, 1/2, 1\}$ with the standard ordering of $\mathbb{R}$. If a 0^+ existed it would be the least element of $(0,1] \cap A$, and so a lower bound of $(1/n)_{n\in\mathbb{Z}^+}$. However this sequence is bounded below only by 0, since it converges to 0. Thus $(0,1] \cap A$ does not have a least element; so 0 has no immediate successor.

The element 1 is maximal, so by the above argument is has no immediate successor.

Given any $x \in A$, $x \neq 0, 1$, then $x = 1/n$ for some $n > 1$. Therefore $1/(n-1)$ is defined and also included in A. The ordering of fractions makes it evident that $1/n < 1/(n-1)$ and in our set this is the immediate successor. Therefore A has exactly two elements with no immediate successor. □

.8 Cardinal Numbers

1 Pigeon-Hole Principle 17
2 Cardinality 18
3 Countable 18
4 Cardinal Arithmetic 19
5 Cardinal Arithmetic Properties 20
6 Finite Cardinal Arithmetic 21
7 Cardinal Order 22
8 Countable Subsets 22
9 Cantor's Diagonalization Method 22
10 Cardinal Exponents 23
11 Unions of Finite Sets 25
12 Fixed Cardinal Unions 25

.8.1 Pigeon-Hole Principle.

Hint$(5/5)$: Make sure not to assume what is to be proved.

Let $I_0 \neq \varnothing$ and for each $n \in \mathbb{Z}^+$ let $I_n = \{1, 2, 3, \ldots, n\}$.

(a) I_n is not equipollent to any of its proper subsets [*Hint:* induction.]

(b) I_m and I_n are equipollent if and only if $m = n$.

(c) I_m is equipollent to a subset of I_n but I_n is not equipollent to any subset of I_m if and only if $m < n$.

Proof:

(a) There are no proper subsets of I_0 so vacuously it is not equipollent to any proper subsets.

Now suppose every proper subset of I_n is not equipollent to I_n for some positive integer n. Given any subset J of I_{n+1}, the map $\iota : J \to I_{n+1}$ defined by $x \mapsto x$ is well-defined and injective. Therefore $J \preceq I_{n+1}$ by Introduction, Definition-8.4, and in particular $I_n \preceq I_{n+1}$. Consider now that J is a proper subset of I_{n+1} (that is, $J \neq I_{n+1}$) and that furthermore it is equipollent to I_{n+1}. Then there exists a bijection $f : I_{n+1} \to J$; $f|I_n$ remains injective; therefore, $I_n \preceq J$ by Introduction, Definition-8.4. Introduction, Theorem-8.7, describes how cardinal numbers are linearly ordered; therefore, $I_n \preceq J \preceq I_{n+1}$. But recall $J \neq I_{n+1}$ so $n \preceq J \prec n + 1$. Since elements of a set are counted as wholes it follows $|J| = n$. Therefore we need only consider if I_n is equipollent to I_{n+1}.

Suppose $g : I_{n+1} \to I_n$ is a bijection; again $g|I_n$ remains injective. Furthermore, $g|I_n$ is surjective onto $I_n - \{g(n+1)\}$. Since g is assumed to be well-defined $g(n+1)$ exists; therefore $I_n - \{g(n+1)\} \neq I_n$ and is in fact a proper subgroup. What we now have constructed is a bijection from I_n to a proper subset, which requires I_n be equipollent to a proper subset. However our induction hypothesis makes this impossible; therefore, g cannot exist so I_n is not equipollent to I_{n+1}.

Therefore by induction, I_n is not equipollent to a proper subset for any $n \in \mathbb{N}$.

(b) ($\Leftarrow$) Given $m = n$, the definitions of I_m and I_n are identical so $I_m = I_n$; therefore I_m and I_n are equipollent.

($\Rightarrow$) Suppose I_m and I_n are equipollent form some m and n in $\mathbb{N}$. By the well-ordering of the natural numbers we know m and n to be comparable so without loss of generality let $m \leq n$. This allows us to assert $I_m \subseteq I_n$. By part (a) we know I_n is not equipollent to any proper subset thus leaving only the case that $I_m = I_n$. However the definition of both is clear m is the greatest element of I_m and n that of I_n, so $m = n$ since the sets are no the same.

(c) ($\Leftarrow$) Suppose $m < n$ and consider the sets I_m and I_n. By construction $I_m \subseteq I_n$ and by part (b) it is a subset not equal to I_n. Therefore I_m is equipollent to a subset of I_n as it is a proper subset. However if I_n is equipollent to a subset of I_m, then it is equipollent to a proper subset of itself which violates the result of part (a). Therefore I_n is not equipollent to any subset of I_m.

($\Rightarrow$) Now suppose I_m is equipollent to a subset of I_n but I_n is not equipollent to any subset of I_m. Since I_m is a subset of itself, I_n is not equipollent to I_m which by part (b) ensures $m \neq n$ – that is $m < n$ or $m > n$. If $m > n$ then $I_n \subseteq I_m$ and so I_m is equipollent to a subset of a proper subset – something that cannot occur by part (a); therefore, $m < n$.

□

.8.2 Cardinality.

Hint$(2/5)$: Use Introduction, Theorem-8.8 for part (a). Part (b) follows from part (a) and Exercise-.8.

(a) Every infinite set is equipollent to one of its proper subsets.

(b) A set is finite if and only if it is not equipollent to one of its proper subsets [see Exercise-.8].

Proof:

(a) By Introduction, Theorem-8.8 we know every infinite set A has a denumerable subset D. A denumerable subset by its definition is equipollent to $\mathbb{N}$. The proper subset $\mathbb{Z}^+$ is equipollent to $\mathbb{N}$ by the map $n \mapsto n+1$ which is invertible through the inverse map $n \mapsto n-1$. Putting the pieces together we now have: a bijection $f : D \to \mathbb{N}$ and another $g : \mathbb{N} \to \mathbb{Z}^+$; a natural inclusion $\iota : \mathbb{Z}^+ \hookrightarrow \mathbb{N}$ of a proper subset; and therefore a proper subset $D' = f^{-1}(\iota(\mathbb{Z}^+))$ of D together with a bijection $f^{-1}gf : D \to D'$. Defining $A' = A \cap (D - D')$ we may construct a final function $h : A \to A'$ as follows:

$$h(a) = \begin{cases} f^{-1}gf(a), & a \in D \\ a. \end{cases}$$

The map is well-defined since it is composed of well-defined maps. Clearly $h(D) = D'$ and $h(A - D) = A - D$ so $h(A) = A'$ forcing h to be surjective. Also if $x, y \in D$ then $f^{-1}gf(x) = h(x) = h(y) = f^{-1}gf(y)$ so $x = y$; when $x, y \in A - D$ then $x = h(x) = h(y) = y$; and finally when $x \in A - D$ and $y \in D$, then $h(x) \in D'$ and $h(y) = A' - D'$ so $h(x) \neq h(y)$. In conclusion, h is injective, and so even bijective; therefore, A is equipollent to A' where A' is a proper subset of A.

(b) ($\Leftarrow$) This direction is simply the contrapositive of part (a).

($\Rightarrow$) A set A is finite only if it is equipollent (say by f) to the set I_n of Exercise-.8 for some $n \in \mathbb{N}$, by definition. In Exercise-.8 we settled that I_n could not be equipollent to a proper subset. If A is equipollent by g to a proper subset B, then the map fgf^{-1} is a bijection from I_n to a proper subset of I_n – this cannot occur; thus g cannot exist.

□

.8.3 Countable.

Hint$(2/5)$: Think of $\mathbb{N}$ as the disjoint union of even and odd numbers. For part (b) follow the given hint.

(a) $\mathbb{Z}$ is a denumerable set.

(b) The set $\mathbb{Q}$ of rational numbers is denumerable. [*Hint:* show that $|\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}|$.]

(a) **Proof:** We define a bijection between the integers and the natural numbers by using even numbers to index non-negative integers and odd to index negatives. [3]

$2n+1$	5	3	1	0	2	4	6	$2n$
$-(n+1)$	-3	-2	-1	0	1	2	3	n

So $\mathbb{N}$ and $\mathbb{Z}$ are equipollent making $\mathbb{Z}$ is denumerable. □

(b) **Proof:** The set of integers are typically identified with the fractions $n/1$ in $\mathbb{Q}$, so we have the natural injection $f : \mathbb{Z} \to \mathbb{Q}$ defined as $n \mapsto n/1$. Next define $g : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ as $a/b \mapsto (a/(a,b), b/(a,b))$. Since $b \neq 0$ neither does (a,b), and thus (a,b) divides both a and b – the function does map into $\mathbb{Z} \times \mathbb{Z}$. Also the definition of the G.C.D. demonstrates that the fraction $\frac{a/(a,b)}{b/(a,b)}$ is in lowest terms; thus, the function is well-defined as each equivalent fraction maps to the same image. Also $g(a/b) = g(c/d)$ implies $a/(a,b) = c/(c,d)$ and $b/(a,b) = d/(c,d)$ so

$$\frac{a}{b} = \frac{a/(a,b)}{b/(a,b)} = \frac{c/(c,d)}{d/(c,d)} = \frac{c}{d},$$

which again is valid since $b, d, (a,b)$, and (c,d) are all nonzero. Therefore g is injective. By Introduction, Theorem-8.12, $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}|$. Thus we have $|\mathbb{Z}| \leq |\mathbb{Q}|$ and $|\mathbb{Q}| \leq |\mathbb{Z}|$ so by the antisymmetry of cardinal ordering $|\mathbb{Z}| = |\mathbb{Q}|$. Therefore $\mathbb{Q}$ is denumerable. □

.8.4 Cardinal Arithmetic.

Hint$(1/5)$: Use the bijections of the components to construct bijections on the product and sum. Introduction, Theorem-5.2 may be helpful.

If A, A', B, B' are sets such that $|A| = |A'|$ and $|B| = |B'|$, then $|A \times B| = |A' \times B'|$. If in addition $A \cap B = \varnothing = A' \cap B'$, then $|A \cup B| = |A' \cup B'|$. Therefore multiplication and addition of cardinals is well-defined.

Proof: Given $|A| = |A'|$ and $|B| = |B'|$ we may assume the following bijections exist: $f : A \to A'$ and $g : B \to B'$. Using the universal property of products we

[3] Using the division algorithm we know every natural number to be of the form $2m + r$ for some unique m and r, with $r = 0, 1$. If $r = 0$ we say the number is even; otherwise, it is odd. For every even number m, $m + 1$ is odd; therefore, even and odd numbers are in a one-to-one correspondence; moreover, they partition the set of natural numbers and so they are both infinite sets.

obtain the following commutative diagram:

$$\begin{array}{ccccc} A & & A \times B & & B \\ & & & & \\ A' & & A' \times B' & & B'. \end{array}$$

But since $f\pi_A$ is a map into A' and $g\pi_B$ a map into B', Introduction, Theorem-5.2 states there is a unique map $h : A \times B \to A' \times B'$, as shown in the diagram, such that $f\pi_A = \pi_{A'}h$ and $g\pi_B = \pi_{B'}h$. Therefore if $h(a,b) = h(c,d)$ then $f(a) = f(c)$, which, since f is injective, implies $a = c$, and symmetrically $b = d$. Therefore h is injective. Given $(a', b') \in A' \times B'$ there exists elements $a \in A$ and $b \in B$ such that $f(a) = a'$ and $g(b) = b'$ since both functions are surjective. Therefore $h(a,b) = (f(a), g(b)) = (a', b')$ so h is surjective, and thus even bijective. Therefore $|A \times B| = |A' \times B'|$.

Now assume A and B are disjoint as well as A' and B'; maintain the same bijections of the sets. We define a new mapping $h : A \cup B \to A' \cup B'$

$$h(x) = \begin{cases} f(x) & x \in A, \\ g(x) & x \in B \end{cases} .$$

Since A and B are disjoint, this piecewise definition of h is well-defined. Therefore h is a function. Given any $x \in A' \cup B'$, the is union is disjoint so $x \in A'$ or in B' exclusively; thus, $x = f(a)$ for some element $a \in A$, or $x = g(b)$ for some element $b \in B$ and so $x = f(y)$ for some $y \in A \cup B$; h is surjective. Suppose $h(x) = h(y)$, then both are in A or B exclusively, and with out loss of generality suppose they are in A. $f(x) = h(x) = h(y) = f(y)$ so $x = y$, proving h is injective; therefore, h is bijective and $|A \cup B| = |A' \cup B'|$ □

.8.5 Cardinal Arithmetic Properties.

Hint$(2/5)$: Replace the cardinals with sets. Exercise-.8 demonstrates any selection is equivalent to showing for all sets of the given cardinality.

For all cardinal numbers α, β, γ:

(a) $\alpha + \beta = \beta + \alpha$ and $\alpha\beta = \beta\alpha$ (commutative laws).

(b) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ and $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ (associative laws).

(c) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ and $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ (distributive laws).

(d) $\alpha + 0 = \alpha$ and $\alpha 1 = \alpha$.

(e) If $\alpha \neq 0$, then there is no β such that $\alpha + \beta = 0$ and if $\alpha \neq 1$, then there is no β such that $\alpha\beta = 1$. Therefore subtraction and division of cardinal numbers cannot be defined.

Proof: Let A, B and C be a sets with $|A| = \alpha$, $|B| = \beta$ and $|C| = \gamma$. Exercise-.8 illustrates why this choice may be arbitrary. For simplicity assume the sets are all disjoint.

(a) By definition $|A \cup B| = \alpha + \beta$ – recall $A \cap B = \varnothing$. Since $A \cup B$ is the least upper bound of the unordered pair A and B, as is $B \cup A$, they must be equal as the least upper bound is unique. Therefore $\alpha + \beta = |A \cup B| = |B \cup A| = \beta + \alpha$. The product $A \times B$ maps to $B \times A$ by the simple bijection $(a, b) \mapsto (b, a)$ making them equipollent; therefore, $\alpha\beta = |A \times B| = |B \times A| = \beta\alpha$.

(b) The union $(A \cup B) \cup C = A \cup B \cup C = A \cup (B \cup C)$ thus $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$. Given $(A \times B) \times C$ we may use the map $((a,b),c) \mapsto (a,(b,c))$ as a bijection to $A \times (B \times C)$. Thus the two products are equipollent so $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

(c) Consider $A \times (B \cup C)$. Since the union here is disjoint, we may partition the elements as follows: $\{(a,x) \mid x \in B\} = A \times B$, $\{(a,x) \mid x \in C\} = A \times C$. These two sets are disjoint and partition the whole product; thus $A \times (B \cup C) = (A \times B) \cup (A \times C)$. Therefore $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$. In similar fashion (*mutatis mutandis*): $(\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma$.

(d) $A \cup \varnothing = A$ so $\alpha + 0 = \alpha$. A maps to A by the identity and to $\{0\}$ trivially, so applying Introduction, Theorem-5.2, there exists a map $f : A \to A \times \{0\}$. $f(a) = (a,0)$ so it is easily seen as injective and surjective, and so bijective. Therefore $\alpha 1 = \alpha$.

(e) Suppose $A \neq \varnothing$. Then for all B, $A \cup B$ contains A so it is not empty. Thus $\alpha + \beta \neq 0$ if $\alpha \neq 0$. If $A = \varnothing$ or $B = \varnothing$, then $A \times B = \varnothing$: [4] $\alpha 0 = 0\beta = 0 \neq 1$. Now suppose $\{a,b\} \subseteq A$ with $a \neq b$. Then $A \times B$, for any set B with an element c, has the elements (a,c) and (b,c) which are not equal since $a \neq b$. Therefore if $\alpha \neq 1$ then $\alpha\beta \neq 1$.

□

.8.6 Finite Cardinal Arithmetic.

Let I_n be as in Exercise-.8. If $A \sim I_m$ and $B \sim I_n$ and $A \cap B = \varnothing$, then $(A \cup B) \sim I_{m+n}$ and $A \times B \sim I_{mn}$. Thus if we identify $|A|$ with m and $|B|$ with n, then $|A| + |B| = m + n$ and $|A||B| = mn$.

Proof: Assume $A \sim I_m$ by a bijection $f : A \to I_m$ and $B \sim I_n$ by another $g : B \to I_n$. Without loss of generality let $m \leq n$. Now define the map $h : A \cup B \to I_{m+n}$ by

$$h(x) = \begin{cases} f(x), & x \in A \\ g(x) + m, & x \in B. \end{cases}$$

The map h is well-defined because the elements of the domain are partitioned into A or B exclusively by the assumption that $A \cap B = \varnothing$ – the rest comes from the assumption f and g are already well-defined.

Armed with this new map, we see when ever $1 \leq k \leq m$, $k = f(a) = h(a)$ for some $a \in A$ and likewise for every $m < k \leq m+n$, $k = g(b) + m = h(b)$ for some $b \in B$; therefore, h is surjective. Noticing the images of A and B are disjoint we need only test whether h is injective on the respective partitions. Clearly h is injective on A since it is equivalent to the bijective function f; on B, h is still injective since $g(x) + m = g(y) + m$ is the same as assuming $g(x) = g(y)$ whence $x = y$. Therefore h is injective and so even bijective. Thus $A \cup B \sim I_{m+n}$.

For convenience use the $J_n = \{0, \ldots, n-1\}$ in place of I_n and adjust the maps f and g accordingly. Define the map $u : A \times B \to J_{mn}$ by [5]

$$(a,b) \mapsto nf(a) + g(b).$$

Since $0 \leq f(a) \leq m-1$ and $0 \leq g(b) \leq n-1$ we bound u by: $0 \leq nf(a) < n(m-1)$, and so $1 \leq u(a,b) \leq mn$; therefore, the map is well-defined.

Next define a map $v : J_{mn} \to A \times B$ as [6]

$$j \mapsto (f^{-1}(\lfloor j/n \rfloor), g^{-1}(j \pmod n)).$$

Hint$(1/5)$: Notice $A \cup B$ is a disjoint union. For the second equivalence express the integers of $1, \ldots, mn$ in base n: this creates a bijection between I_{mn} and $I_m \times I_n$ by $digit2, digit1 \mapsto (n \cdot digit2 + 1, digit1 + 1)$.

[4] The elements in $A \times B$ are functions $f : 2 \to A \cup B$ with $f(0) \in A$, $f(1) \in B$. If A or B is empty then $f(0)$ or $f(1)$ is not defined; thus, no such functions exist so $A \times B = \varnothing$.

[5] Notice since $m \leq n$ that u expresses the element (a,b) as a 2 digit integer in base n.

[6] This assumes the congruence classes begin with 0 and end with $n-1$.

Every fraction has a unique least integer upper bound and also a unique congruence class modulo n; thus, v is well-defined.

Now together we see

$$\begin{aligned} vu(a,b) &= v(nf(a)+g(b)) \\ &= (f^{-1}(\lfloor (nf(a)+g(b))/n \rfloor), g^{-1}((nf(a)+g(b)) \pmod n)) \\ &= (f^{-1}(f(a)), g^{-1}(g(b))) = (a,b). \end{aligned}$$

Likewise

$$\begin{aligned} uv(j) &= u(f^{-1}(\lfloor j/n \rfloor), g^{-1}(j \pmod n)) \\ &= nf(f^{-1}(\lfloor j/n \rfloor)) + g(g^{-1}(j \pmod n)) \\ &= n\lfloor j/n \rfloor + j \pmod n = j. \end{aligned}$$

Therefore $uv = 1_{J_{mn}}$ and $vu = 1_{A\times B}$ so both are invertible and so they are bijections: $A \times B \sim J_{mn} \sim I_{mn}$. □

.8.7 Cardinal Order.

Hint$(1/5)$: Fill in the commutative square diagram.

If $A \sim A'$, $B \sim B'$ and $f : A \to B$ is in injective, then there is an injective map $A' \to B'$. Therefore the relation $\leq$ on cardinal numbers is well-defined.

Proof: Assume $A \sim A'$ by a bijective map $v : A \to A'$ and $B \sim B'$ by another $v : B \to B'$. From these pieces we may construct the following commutative diagram:

$$\begin{array}{ccc} A & & A' \\ & & \\ B & & B' \end{array}$$

The map vfu^{-1} is well-defined since each component in the composition is a well-defined map – recall inverses exist for both u and v. Furthermore each component is at least injective, and composition of injective functions is injective; thus we have constructed an injection from A' to B' as desired. □

.8.8 Countable Subsets.

Hint$(1/5)$: Use Introduction, Theorem-8.8.

An infinite subset of a denumerable set is denumerable.

Proof: A denumerable set is equipollent to the natural numbers so it shares the same cardinality $\aleph_0$. Given any infinite subset B of a denumerable set A, the inclusion map is an injection from B to A; thus, $B \preceq A$. However B is still and infinite set so it must have an infinite cardinal value. Employing Introduction, Theorem-8.8 it follows $\aleph_0 \leq |B| \leq A = \aleph_0$. Cardinal ordering is a partial ordering (Introduction, Theorem-8.7) so the law of antisymmetry forces $|B| = \aleph_0$. Therefore by definition B is denumerable. □

llow the hint as known as Can- zation Method.

.8.9 Cantor's Diagonalization Method.

The infinite set of real numbers $\mathbb{R}$ is not denumerable (that is $\aleph_0 < |\mathbb{R}|$). [*Hint:* It suffices to show that the open interval $(0,1)$ is not denumerable by Exercise-.8. You may assume each real number can be written as an infinite decimal. If $(0,1)$ is denumerable there is a bijection $f : \mathbb{Z}^+ \to (0,1)$. Construct an infinite decimal (real number) $.a_1a_2\cdots$ in $(0,1)$ such that a_n is not the nth digit in the decimal expansion of $f(n)$. This number cannot be in $Im\ f$.]

Proof: Given the set of real numbers, if any subset is not denumerable then the entire set is not denumerable by the contrapositive of Exercise-.8. Therefore consider the open interval $(0,1)$. We take the elements to be expressed in their unique decimal expansion, only base 2 instead of the traditional base 10. We can expresses precisely as the product $\prod_{\mathbb{N}} 2$ – where $2 = \{0,1\}$ in the traditional way.[7] We attempt an indirect proof.

Suppose $\prod_{\mathbb{N}} 2$ is denumerable and take any map $f : \mathbb{N} \to \prod_{\mathbb{N}} 2$ that is a bijection. We may now define a mapping $h_f : \mathbb{N} \to \{0,1\}$ by $h_f(n) = f(n) + 1 \pmod 2$. The definition makes h visibly well-defined and by its construction we see $h_f \in \prod \mathbb{N}2$. However $f(n) \neq h_f$ for any n since $f(n)(n) \neq h_f(n)$ for all $n \in \mathbb{N}$. Therefore f cannot be a surjection ever; therefore, f is not a bijection and so $\mathbb{N}$ is not equipollent to $\prod_{\mathbb{N}} 2 - \mathbb{R}$ is not denumerable. □

.8.10 Cardinal Exponents.

Hint$(5/5)$: Notice every map $f : B \to A$ has $f(b) \in A$ so in fact A^B and $\prod_B A$ have identical definitions: they are the same sets. This may help simplify notation and logic in some instances.

If α, β are cardinals, define α^β to be the cardinal number of the set of all functions $B \to A$, where A, B are sets such that $|A| = \alpha$, $|B| = \beta$.

(a) α^β is independent of the choice of A, B.

(b) $\alpha^{\beta+\gamma} = (\alpha^\beta)(\alpha^\gamma)$; $(\alpha\beta)^\gamma = (\alpha^\gamma)(\beta^\gamma)$; $\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma$.

(c) If $\alpha \leq \beta$, then $\alpha^\gamma \leq \beta^\gamma$.

(d) If α, β are finite with $\alpha > 1$,$\beta > 1$ and γ is infinite, then $\alpha^\gamma = \beta^\gamma$.

(e) For every finite cardinal n, $\alpha^n = \alpha\alpha\cdots\alpha$ (n factors). Hence $\alpha^n = \alpha$ if α is infinite.

(f) If $P(A)$ is the power set of a set A, then $|P(A)| = 2^{|A|}$.

Proof: A, B, and C be sets with cardinalities α, β, and γ respectively. For simplicity assume they are all pairwise disjoint.

(a) Let A and A' be equipollent sets with cardinality α and also let B be equipollent to B' both with cardinality β. Therefore there are bijections (invertible functions) $f : A \to A'$ and another $g : B \to B'$. Now given any function $h : B \to A$ and $h' : B' \to A'$ – that is, $h \in A^B$ and $h' \in A'^{B'}$ – the following diagrams commute:

$$\begin{array}{ccc} B & & A \\ & & \\ B' & & A' \end{array} \qquad \begin{array}{ccc} B & & A. \\ & & \\ B' & & A' \end{array}$$

[7] Here we may even replace $2^{\mathbb{N}}$ and write the cardinality as $2^{\aleph_0}$. This is sufficient, considering Exercise-.8, since $\mathbb{N} \prec P(\mathbb{N}) \sim 2^{\mathbb{N}}$.

The diagrams induce the mappings $i : A^B \to A'^{B'}$ defined as $h \mapsto fhg^{-1}$ and $i' : A'^{B'} \to A^B$ defined as $h' \mapsto f^{-1}h'g$. Applying composition we see: $ii'(h) = f(f^{-1}hg)g^{-1} = 1_A h 1_B = h$, and $i'i(h) = f^{-1}(fh'g^{-1})g = h'$; therefore $ii' = 1_{A'^{B'}}$ and $i'i = 1_{A^B}$. Since i is now seen as invertible it must be bijective, and so $|A|^{|B|} = |A'|^{|B'|}$; α^β is well-defined.

(b) Consider $A^{B\cup C}$ and $A^B \times A^C$. Every function $h : B \cup C \to A$ can be defined equivalently by the restrictions $h|B$ and $h|C$, since B and C are disjoint. Therefore define a map $i : A^{B\cup C} \to A^B \times A^C$ as $h \mapsto (h|B, h|C)$. Restricting functions is a well-defined process so i is well-defined.[8]

Define an inverse map $i^{-1} : A^B \times A^C \to A^{B\cup C}$ as $(f, g) \mapsto f \cup g$, where $f \cup g$ is:

$$(f \cup g)(x) = \begin{cases} f(x) & x \in B \\ g(x) & x \in C \end{cases} .$$

This is of course traditional piecewise definition of function and is well-defined since B and C are disjoint.

Now compose the two maps $ii^{-1}(f, g) = i(f \cup g) = ((f \cup g)|B, (f \cup g)|C) = (f, g)$. Likewise $i^{-1}i(h) = (h|B, h|C) = (h|B) \cup (h|C) = h$. Therefore they are inverse functions and so they are bijective and the two sets as a result are equipollent; $\alpha^{\beta+\gamma} = (\alpha^\beta)(\alpha^\gamma)$.

Now consider $(A \times B)^C$ compared with $A^C \times B^C$. Following the same strategy, define a map $i : (A \times B)^C \to A^C \times B^C$ by $h \mapsto (\pi_A h, \pi_B h)$, for all $h : C \to A \times B$; and another $i^{-1} : A^C \times B^C$ by $(f, g) \mapsto f \times g$, ($f : C \to A$, $g : C \to B$), where $f \times g : C \to A \times B$ is the unique map (with respect to f and g) with the property $\pi_A f \times g = f$ and $\pi_B f \times g = g$, as guaranteed by Introduction, Theorem-5.2. The first map, i, is defined by composition of functions which is well-defined, and the resulting maps are $C \to A$ and $C \to B$ as required. The latter map is well-defined by Introduction, Theorem-5.2. Now their compositions are:

$$\begin{aligned} ii^{-1}(f, g) &= i(\phi) = (\pi_A f \times g, \pi_B f \times g) = (f, g) \\ i^{-1}i(h) &= i^{-1}(\pi_A h, \pi_B h) = h. \end{aligned}$$

Since the maps are inverses the sets are equipollent. Therefore $(\alpha\beta)^\gamma = (\alpha^\gamma)(\beta^\gamma)$.

Finally consider the sets $A^{B\times C}$ and $(A^B)^C$. Given any $f : B \times C \to A$, defined $f_c : B \to A$ as $f_c(b) = f(b, c)$ for all $b \in B, c \in C$. The definition is well-defined since it is an evaluation of a well-defined function, and it determines a mapping $i : A^{B\times C} \to (A^B)^C$ as $i(f) = F : C \to A^B$ defined as $F(c) = f_c$.

An element of $(A^B)^C$ is a function $F : C \to A^B$, so that $F(c) : B \to A$ for all $c \in C$. Therefore define $i^{-1} : (A^B)^C \to A^{B\times C}$ as $i^{-1}(F) = f : B \times C \to A$ defined as: $f(b, c) = (F(c))(b)$.

Once again take the compositions of these two functions:

$$\begin{aligned} (ii^{-1}(F : C \to A^B))(c)(b) &= (i(f : B \times C \to A)) = (F'(c))(b) \\ &= f(b, c) = f_c(b) = (F(c))(b), \\ ii^{-1}(F) &= F; \\ (i^{-1}i(h : B \times C \to A))(b, c) &= (i^{-1}(H : C \to A^B))(b, c) = h'(b, c) \\ &= (H(c))(b) = h_c(b) = h(b, c), \\ i^{-1}i(f) &= f. \end{aligned}$$

[8] Restricting a function is defined even on empty sets.

Therefore i and i^{-1} are invertible and furthermore they are bijections, so $\alpha^{\beta\gamma} = (\alpha^{\beta})^{\gamma}$.

(c) Suppose there exists an injection $i : A \to B$. Given any maps $f : C \to A$ the map if maps $C \to B$ so $I : A^C \to B^C$ defined as $I(f) = if$ is well-defined. Furthermore $I(f) = I(g)$ implies $if = ig$. Introduction, Theorem-3.1, states injective functions are left cancelable (or that they have a left inverse i'); thus, $f = 1_A f = i'if = i'ig = 1_A g = g$. Therefore I is injective; thus, $\alpha \leq \beta$ implies $\alpha^{\gamma} \leq \beta^{\gamma}$.

(d) Let α and β be finite cardinals both greater than 1, and γ an infinite cardinal.

Notice in Exercise-.8 we used the construction of $\prod_{\mathbb{N}} 2$ to denote the unit interval in base 2. In base three the set would be equivalent to the infinite decimal expansions with three characters; thus $\prod_{\mathbb{N}} 3$, and in general $\prod_{\mathbb{N}} n$ for base n. However all these methods denote the same set $(0, 1) \subseteq \mathbb{R}$ and so they all have the same cardinality. Therefore $\alpha^{\aleph_0} = \beta^{\aleph_0}$. Thus

$$\alpha^{\gamma} = \alpha^{\aleph_0 \gamma} = (\alpha^{\aleph_0})^{\gamma} = (\beta^{\aleph_0})^{\gamma} = \beta^{\aleph_0 \gamma} = \beta^{\gamma}.$$

(e) The set of all function $f : n \to A$ has the property $f(n) \in A$, thus it is in the product $\prod_{i=1}^{n} A$. Also any function in the product maps $n \to A$; thus $A^n = \prod_{i=1}^{n} A$. Therefore $|A^n| = \alpha^n$. By Introduction, Theorem-8.12, whenever α is infinite then $|A^n| = |A|$ so, $\alpha^n = \alpha$.

(f) Given a function $f : A \to 2$ define a set $S_f = f^{-1}(1)$. Notice S_f is a subset of A. Whenever $f \neq g$ there exists an $x \in A$ such that $f(x) \neq g(x)$, and so $f(x) = 1$ while $g(x) = 0$, or $f(x) = 0$ while $g(x) = 1$ – since these are the only options in the image. Therefore $S_f = f^{-1}(1) \neq g^{-1}(1) = S_g$. Therefore S is an injective map from 2^A to $P(A)$.

For any subset S of A, define $f_S : A \to 2$ as $f(x) = 0$ if $x \notin S$ and $f(x) = 1$ if $x \in S$ – this a general piecewise function over disjoint sets so it is well-defined. When $S \neq T$ then $f_S(x) \neq f_T(x)$ for any element x in their symmetric difference $S + T$, which is not empty since $S \neq T$. Therefore $f_S \neq f_T$ so that f is an injective map from $P(A)$ to 2^A. Applying the Schroeder-Bernstein Theorem, $P(A)$ is equipollent to 2^A; that is, $|P(A)| = 2^{|}A|$.

□

.8.11 Unions of Finite Sets.

Hint$(3/5)$: Turn the problem on its head by swapping the A_i's with I.

If I is an infinite set, and for each $i \in I$ A_i is a finite set, then $|\bigcup_{i\in I} A_i| \leq |I|$.

Proof: Index the elements of A_i with $\mathbb{N}$ as they are each finite. So $A_i = \{a_{(i,0)}, \ldots, a_{(i,n)}\}$. Now we define $I(n) = \{i \in I \mid a_{(i,n)} \in A_i\}$ for all $n \in \mathbb{N}$. We identify the union through the indices to obtain:

$$\bigcup_{i\in I} A_i \sim \mathring{\bigcup}_{n\in\mathbb{N}} I(n) \subseteq \mathring{\bigcup}_{n\in\mathbb{N}} I.$$

Furthermore by part (e) of Exercise-.8, since I is infinite, $|I|^n = I$ and so

$$\mathring{\bigcup}_{n\in\mathbb{N}} I \sim \mathring{\bigcup}_{n\in\mathbb{N}} I^n.$$

Using Introduction, Theorem-8.12 part (ii), $|\bigcup i \in I A_i| \preceq |I|\aleph_0$. Since we assumed I was infinite, $|I|\aleph_0 = |I|$. □

Hint$(2/5)$: Identify all the elements of the sets A_i to a single set A with the same cardinality. Then show $\bigcup_{i\in I} A_i \sim A \times I$.

.8.12 Fixed Cardinal Unions.

Let α be a fixed cardinal number and suppose that for every $i \in I$, A_i is a set with $|A_i| = \alpha$. Then $|\bigcup_{i\in I} A_i| \leq |I|\alpha$.

Proof: We connect sums with products of cardinals to show: the size of the disjoint union of a set A with cardinality α indexed by a set B with cardinality β, is $\sum_\beta \alpha = \alpha\beta$.

We take the family $\{A_b \mid b \in B\}$ to be pairwise disjoint sets all equipollent to A; moreover we identify each element in A_b with those in a through the maps $i_b : A_b \to A$. Next we define a map $f : \bigcup_{b\in B} A_b \to A \times B$ by setting $f(a) = (i_b(a), b)$ where $a \in A_b$. Since each A_b is disjoint, the map is well-defined. Furthermore, if $f(a) = f(a')$ then $(i_b(a), b) = (i_{b'}(a'), b')$. However this requires $b = b'$ and so we have $i_b(a) = i_{b'}(a') = i_b(a')$, which results in $a = a'$ since i is bijective: f is injective. Given any $(a, b) \in A \times B$, $i_b^{-1}(a) \in A_b$; thus, $f(i_b^{-1}(a)) = (a, b)$ leaving f visibly surjective: f is bijective. We conclude saying $\bigcup_{b\in B} A_b \sim A \times B$ so in cardinals $\sum_\beta \alpha = \alpha\beta$. $\square$

Chapter I

Groups

I.1 Semigroups, Monoids, and Groups

1 Non-group Objects . . . 27
2 Groups of Functions . . . 27
3 Floops . . . 28
4 D_4 Table . . . 28
5 Order of S_n . . . 29
6 Klein Four Group . . . 29
7 $\mathbb{Z}_p^\times$ . . . 29
8 $\mathbb{Q}/\mathbb{Z}$ – Rationals Modulo One . . . 30
9 Rational Subgroups . . . 31
10 PruferGroup . . . 32
11 Abelian Relations . . . 32
12 Cyclic Conjugates . . . 33
13 Groups of Involutions . . . 33
14 Involutions in Even Groups . . . 33
15 Cancellation in Finite Semigroups . . . 34
16 n-Product . . . 34

I.1.1 Non-group Objects.

Give examples other than those in the text of semigroups and monoids that are not groups.

Example: Take G to be a linearly ordered group, such as: $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$, but not the trivial group. By definition we require the ordering respect the group product, which is to say: $a \leq b$ implies $ac \leq bc$.

Consider the subsets $G^+ = \{a \in G \mid e < a\}$ and $\overline{G}^+ = \{a \in G \mid e \leq a\}$. Given any two elements $a, b \in G^+$ (or $\overline{G}^+$) it follows $e < a$ and $e < b$ so $e < b = eb < ab$ thus $ab \in G^+$. Since the product in G is associative and there exist elements greater than e, it follows G^+ is a semigroup as it is closed to the associative operator. Furthermore $\overline{G}^+$ is a monoid. Finally the linear ordering requires $a < e$ or $e < a$ exclusively, for all non-trivial elements a. Thus multiplying by inverses we notice the following: if $a < e$ then $e < a^{-1}$, and if $e < a$ then $a^{-1} < e$. Therefore neither G^+ nor $\overline{G}^+$ contain inverses (except for e) so they cannot be groups. □

Hint$(1/5)$: Consider subsets of ordered groups. Other examples from the Computer Science field include: string concatenation; finite state machines, where the operation is following arrows; and in general any regular grammar. The proofs for these are successively more difficult but can be found in most compiler design books.

I.1.2 Groups of Functions.

Hint$(2/5)$: Think of $M(S,G)$ as the Cartesian product of G, S times; every function $f : S \to G$ can be thought of as a n-tuple where n is the size of S, and addition is simply done pointwise with each tuple pair. *Caution: do not assume S is finite.*

Let G be a group (written additively), S a nonempty set, and $M(S,G)$ the set of all functions $f : S \to G$. Define additions in $M(S,G)$ as follows: $(f+g) : S \to G$ is given by $s \mapsto f(s)+g(s) \in G$. Prove that $M(S,G)$ is a group, which is abelian if G is.

Proof: First knowing addition is well-defined in G it follows for any $s \in S$, and $f, g \in M(S,G)$, $f(s) + g(s)$ is well-defined as an element in G. Therefore $f + g : S \to G$ is a well-defined function and thus included in $M(S,G)$. So $M(S,G)$ has a well-defined binary operation in the given addition.

Furthermore the operation is associative since given any f, g and h in $M(S,G)$ and $s \in S$ it follows:

$$\begin{aligned}(f + (g + h))(s) &= f(s) + (g + h)(s) = f(s) + (g(s) + h(s)) \\ &= (f(s) + g(s)) + h(s) = (f + g)(s) + h(s) \\ &= ((f + g) + h)(s).\end{aligned}$$

This proves $f + (g + h) = (f + g) + h$ as required.

Now define $0 : S \to G$ by $0(s) = e$ for all $s \in S$. Clearly 0 is a well-defined map and so included in $M(S,G)$ (note this makes $M(S,G)$ a semigroup as it is now provably nonempty). Next $(0+f)(s) = 0(s)+f(s) = e+f(s) = f(s)$ for all $f \in M(S,G)$. Finally given $f : S \to G$, define $-f : S \to G$ as $s \mapsto -f(s)$. Since each image element $f(s)$ lies in the group G it has an inverse $-f(s)$ so $-f$ is well-defined. Again by construction $((-f) + f)(s) = -f(s) + f(s) = e = 0(s)$. Therefore we have 0 as a left identity together with $-f$ as the left inverses for any f so by Proposition-I.1.3 $M(S,G)$ is a group under the prescribed addition.

Suppose now G is abelian. Then $(f + g)(s) = f(s) + g(s) = g(s) + f(s) = (g + f)(s)$ by the commutativity in G. Therefore $f + g = g + f$ so $M(S,G)$ is abelian. □

I.1.3 Floops.

Hint$(2/5)$: The assertion is false; consider a set with 2 or more elements and define for it an operation of the form $xy = y$. These objects are sometimes called *floops*.

Is it true that a semigroup which has a *left* identity element and in which every element has a *right* inverse (see Proposition-I.1.3) is a group?

Example: Let S be a set with cardinality greater than 1. For any two elements x and y define their product as $xy = y$. Since y is already assumed to be in S the product is uniquely defined for the pair (x, y), and also contained in S so it is well-defined. Thus it is a valid binary operation. Take a, b and c as elements from S. Simply by definition $a(bc) = bc = (ab)c$, so our product is associative. Notice we may fix any element a in S to serve as a left identity since $ay = y$ for all elements y. For any y pick a to be a right inverse since $ya = a$. Thus all the properties of the hypothesis are met.

However S together with this operation is not a group. We see this because given S has at least two elements, we pick x to be any element and notice $e = xx^{-1} = x^{-1}$; thus, every inverse is the identity. But by Theorem-I.1.2.iv, if S where a group under this operation then $(x^{-1})^{-1} = x$ for all elements x. Thus $e = e^{-1} = (x^{-1})^{-1} = x$ which contradicts the assumption that S has two or more elements. Thus S is not a group. □

I.1.4 D_4 Table.

Hint$(1/5)$: Use the principles of a Latin Squares (each row and column contains one and exactly one instance of every element in the group) to reduce the computation nec-

Write out a multiplication table for D_4^*.

Example:

	I	R	R^2	R^3	T_x	$T_{2,4}$	T_y	$T_{1,3}$
I	I	R	R^2	R^3	T_x	$T_{2,4}$	T_y	$T_{1,3}$
R	R	R^2	R^3	I	$T_{2,4}$	T_y	$T_{1,3}$	T_x
R^2	R^2	R^3	I	R	T_y	$T_{1,3}$	T_x	$T_{2,4}$
R^3	R^3	I	R	R^2	$T_{1,3}$	T_x	$T_{2,4}$	T_y
T_x	T_x	$T_{2,4}$	T_y	$T_{1,3}$	I	R^3	R^2	R
$T_{2,4}$	$T_{2,4}$	T_x	$T_{1,3}$	T_y	R	I	R^3	R^2
T_y	T_y	$T_{1,3}$	T_x	$T_{2,4}$	R^2	R	I	R^3
$T_{1,3}$	$T_{1,3}$	T_y	$T_{2,4}$	T_x	R^3	R^2	R	I

□

I.1.5 Order of S_n.

Prove that the symmetric group on n letters, S_n, has order $n!$.

Proof: Take any permutation σ from S_n. $\sigma(1)$ can be any of the n characters in $X = \{1, \ldots, n\}$. Suppose $\sigma(i)$ can be any of the $n - i$ characters from $X - \sigma(\{1, \ldots, i-1\})$ for some $1 < i \leq n$. $\sigma(i+1) \neq \sigma(j)$, for any $j < i+1$ since σ is injective (it is in fact bijective). Thus $\sigma(i+1)$ can be any of the $n - (i+1)$ characters in $X - \sigma(\{1, \ldots, i\})$.

Hint$(2/5)$: Consider the problem combinatorially ignoring the group structure. After the first i characters are permuted how many characters are left to choose as the image of the $i+1$ character?

$\sigma(1)$ 1 n

$\sigma(2)$ 2 n 1 $n-1$

$\sigma(3)$ 3 n 2 $n-1$ 2 $n-1$ 1 $n-2$

$\sigma(n)$

Therefore by induction the total number of permutations are $n(n-1)\cdots 2 = n!$ so the order of S_n is $n!$. □

I.1.6 Klein Four Group.

Write out an addition table for $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is called the **Klein Four Group**.

Hint$(1/5)$: Compute the diagonal first: what is $(x, y) + (x, y)$? [1]

Example:

	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

□

I.1.7 $\mathbb{Z}_p^\times$.

If p is prime, then the nonzero elements of $\mathbb{Z}_p$ form a group of order $p-1$ under multiplication. [*Hint:* $\overline{a} \neq \overline{0} \Rightarrow (a,p) = 1$; use Introduction, Theorem 6.5.] Show that this statement is false if p is not prime.

Proof: Define $\mathbb{Z}_p^* = \{\overline{a} \in \mathbb{Z}_p \mid \overline{a} \neq \overline{0}\}$. The order of $\mathbb{Z}_p$ is p, so $\mathbb{Z}_p^*$ has order $p-1$ since it excludes only one element. The smallest prime is 2; thus each $\mathbb{Z}_p^*$ has at least one element so it is nonempty. By Introduction, Theorem-6.5, we know the greatest common divisor always exists. Furthermore this theorem states $(a,p) = 1$ or p, and p only when $p|a$. By assumption $\overline{a} \neq \overline{0}$; thus $p \nmid a$ so $(a,p) = 1$. Now take $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}_p^*$. Suppose their product $\overline{a}\overline{b} = \overline{ab} = \overline{0} = \overline{a \cdot 0}$. By Introduction, Theorem-6.8.iii, a and p are relatively prime; thus, $ab \equiv a \cdot 0 \pmod{p}$ implies $b \equiv 0 \pmod{p}$. This contradicts the assumption $\overline{b} \neq \overline{0}$ thus $\overline{ab} \neq \overline{0}$; therefore, $\overline{a}\overline{b} \in \mathbb{Z}_p^*$. Since multiplication module p is well-defined in $\mathbb{Z}_p$ and now seen as closed in $\mathbb{Z}_p^*$, it is well-defined as a binary operator in $\mathbb{Z}_p^*$. Furthermore it inherits the associativity so it is a semigroup.

Since $p \nmid 1$, $\overline{1} \neq \overline{0}$ for any p so $\overline{1} \in \mathbb{Z}_p^*$. Also $\overline{a}\overline{b} = \overline{ab} = \overline{ba} = \overline{b}\overline{a}$ – using the commutativity of multiplication in integers. From here the conclusion is simpler: $\overline{a}\overline{1} = \overline{a \cdot 1} = \overline{a}$, forcing $\overline{1}$ to be the identity of $\mathbb{Z}_p^*$.

Given any $a \in \mathbb{Z}_p^*$, $a^m \in \mathbb{Z}_p^*$, for all $m \in \mathbb{Z}^+$, since $\mathbb{Z}_p^*$ is closed to products. Since the set is finite, $a^m \equiv a^n \pmod{p}$ for some m and n, $m \neq n$, or otherwise there would be infinitely many elements. Without loss of generality let $m < n$. Then using Introduction, Theorem-6.8, part (iii), and the fact we know $(a,p) = 1$ so $(a^m,p) = 1$, we conclude $1 \equiv a^{n-m} \pmod{p}$. Now certainly this requires $a^k \equiv 1 \pmod{p}$ for some positive integer k, and we take the least such k. Therefore either $k = 1$ which implies $a = 1$ or $a^{k-1} \neq 1$ and $aa^{k-1} = a^{k-1}a = a^k \equiv 1 \pmod{p}$ and so $a^{k-1} = a^{-1}$. Since $\mathbb{Z}_p^*$ is closed to products, $a^{k-1} \in \mathbb{Z}_p^*$. So we may conclude our new set is closed to inverses and so it is a group under multiplication; $\mathbb{Z}_p^* = \mathbb{Z}_p^\times$ – the largest group inside the multiplication. [3] □

Example: Suppose m is a composite positive integer (not 1), which means it is a multiple of some k, $k \neq m$. Since m is positive we may take k to be positive and it is less than m since it does not equal m. Therefore $\overline{k} \neq \overline{0}$ and likewise $0 \neq m/k < m$ implies $\overline{m/k} \neq \overline{0}$ (recall m/k is an integer since $k|m$). Therefore both are elements of $\mathbb{Z}_m^*$. However their product $\overline{k}\overline{m/k} = \overline{k\frac{m}{k}} = \overline{m} = \overline{0}$ is *not* in $\mathbb{Z}_m^*$. So when m is not prime $\mathbb{Z}_m^* \neq \mathbb{Z}_m^\times$. □

I.1.8 $\mathbb{Q}/\mathbb{Z}$ – Rationals Modulo One.

Hint$(2/5)$: In part (a) verify all the properties. Theorem-I.1.5 will help in defining part (b). In part (b) consider how many equivalence classes are of the form $\frac{1}{n} + \mathbb{Z}$. [4]

(a) The relation given by $a \sim b \Leftrightarrow a - b \in \mathbb{Z}$ is a congruence relation on the additive group $\mathbb{Q}$ [see Theorem-I.1.5].

(b) The set $\mathbb{Q}/\mathbb{Z}$ of equivalence classes is an infinite abelian group.

Proof:

(a) Let a, b, and c be rational numbers.

- Certainly $a - a = 0$ is an integer so $a \sim a$; $\sim$ is *reflexive*.

[3] This proof uses the fact that $(a,p) = 1$; however, we can extend this proof to say $\mathbb{Z}_m^\times = \{n \in \mathbb{Z}_m \mid (m,n) = 1\}$ is a group under multiplication without problem, only the order of this group will now be smaller – in fact it will have the order of the Euler φ function, defined as the number of elements relatively prime to m, between 1 and m inclusively.

Hint$(4/5)$: M
nonempty and
hint to show
to multiplicati
tion, Theorem
be useful.
to assume th
orem of Fern
Theorem (a^p
$(a,p) = 1$; a
$\pmod{m}$, $(a,$
later Exercise-I
result to prove
orems. [Eyn] [2]

- Given $a \sim b$ implies $a - b$ is an integer, in which case certainly $-(a - b) = b - a$ is an integer since the integer have additive inverses. Thus $b \sim a$, so $\sim$ is *symmetric*.
- Finally $a \sim b$ and $b \sim c$ implies $c \sim b$ from above, and so $a-b$ and $c-b$ are integers. Therefore their difference $(a - b) - (c - b) = a - c$ is an integer; $a \sim b$ leaving $\sim$ *transitive*.

$\sim$ is an equivalence relation on $\mathbb{Q}$.

Now let $a_1, b_1, a_2,$ and b_2 be rational numbers such that $a_1 \sim a_2$ and $b_1 \sim b_2$. Then $a_1 - a_2$ and $b_1 - b_2$ are integers. The sum $(a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2)$ is an integer, leading to the conclusion $(a_1 + b_1) \sim (a_2 + b_2)$; proving $\sim$ is a congruence relation on $\mathbb{Q}$.

(b) By part (a) and Theorem-I.1.5 we know $\mathbb{Q}/\mathbb{Z}$ is defined and furthermore an abelian group since $\mathbb{Q}$ is one. Without loss of generality let m and n be integers such that $1 < m \leq n$ and furthermore assume the equivalence classes $\frac{1}{m} + \mathbb{Z}$ and $\frac{1}{n} + \mathbb{Z}$, are equal. Then $\frac{1}{n} \sim \frac{1}{m}$ by the definition of equivalence classes and thus $\frac{1}{m} - \frac{1}{n}$ is an integer. However $1 < m \leq n$ implies $0 < 1/n \leq 1/m < 1$ and so $0 \leq \frac{1}{m} - \frac{1}{n} < 1$. If this difference is to be an integer then it must therefore equal 0 and so $\frac{1}{m} = \frac{1}{n}$ or simply $m = n$. Therefore $\frac{1}{m} + \mathbb{Z}$ is distinct from $\frac{1}{n} + \mathbb{Z}$ for all $m \neq n$ of which there are infinitely many. Therefore $\mathbb{Q}/\mathbb{Z}$ contains an infinite subset and so it is infinite.

□

I.1.9 Rational Subgroups.

Let p be a fixed prime. Let R_p be the set of all those rational numbers whose denominator is relatively prime to p. Let R^p be the set of rationals whose denominator is a power of p ($p^i, i \geq 0$). Prove that both R_p and R^p are abelian groups under ordinary addition of rationals.

Hint$(1/5)$: Make sure to show the rules that define R_p and R^p are well-defined – remember rational numbers are equivalence classes.

Proof: Let a and $b \neq 0$ be integers such that $(b, p) = 1$. Suppose a/b is not in lowest terms so that there exists an a' and b' such that $a/b = a'/b'$ and a'/b' is in lowest terms. Then $(b, b') = b'$ and thus $(b', p) = (b, b', p) = 1$ so the selection of fractions with denominators relatively prime to p is well-defined. Therefore R_p is given by a well-defined rule and thus is defined.

Furthermore any integer k has denominator 1; $(1, p) = 1$, so $\mathbb{Z} \subset R_p$; thus 0 is in R_p. Since 0 is the additive identity of $\mathbb{Q}$ and we adopt the same addition in R_p it is clear 0 is the identity of R_p – if R_p is shown to have a well-defined addition.

Now let a/b, and c/d be elements of R_p; thus $(b, p) = (c, p) = 1$. So we add $a/b + c/d = \frac{ad+bc}{bd}$. But $p|bd$ if and only if $p|b$ or $p|d$ by Introduction, Theorem-6.6 (Euclid's Lemma). Neither of these is the case thus $p \nmid bd$ by the contrapositive; therefore, the sum is in R_p so addition is closed (well-defined) in R_p. Clearly addition remains associative since it is associative in all of $\mathbb{Q}$. For the same reason it is abelian. At last $-(a/b)$ can be seen as $a/(-b)$ which is the only interesting case. However $(-b, p) = (b, p) = 1$ so once again R_p contains all additive inverses. Therefore R_p is an additive abelian (sub)group.

Let a be an integer. Then a/p^i is a rational number in R^p by definition. Furthermore if a/p^i reduces to a'/b' then $b'|p^i$ so therefore $b' = p^j$ for some $j \leq i$: equivalent reduced forms of rationals in R^p are still in R^p so the rule for R^p is well-defined.

Taking $0/p^i = 0$ for any i shows that the additive identity is in R^p. Now take a/p^i and b/p^j in R^p. Their sum is $\frac{ap^j+bp^i}{p^i p^j}$ which can be seen as an

element of R^p since $p^i p^j = p^{ij}$. Thus R^p is closed under addition. Lastly $-(a/p^i) = (-a)/p^i$ which is in R^p by definition. Therefore R^p is a (sub)group. □

I.1.10 PruferGroup.

Hint$(2/5)$: Notice $\mathbb{Z}(p^\infty) = R^p/\mathbb{Z}$ from Exercise-I.1. For the infinity of the group consider the elements $\overline{1/p^i}$. How many are there? It may be useful to consider the visual interpretation as outlined in Exercise-I.1.

Let p be a prime and let $\mathbb{Z}(p^\infty)$ be the following subset of the group $\mathbb{Q}/\mathbb{Z}$ (see [Hun, 27]):

$$\mathbb{Z}(p^\infty) = \{\overline{a/b} \in \mathbb{Q}/\mathbb{Z} \mid a, b \in \mathbb{Z} \text{ and } b = p^i \text{ for some } i \geq 0\}.$$

Show that $\mathbb{Z}(p^\infty)$ is an infinite group under the addition operation of $\mathbb{Q}/\mathbb{Z}$.

Proof: Clearly $0 = 0/p$ so $0 \in \mathbb{Z}(p^\infty)$ thus the Prüfer Group is nonempty. Next given $\overline{a/p^i}$ and $\overline{b/p^j}$ in $\mathbb{Z}(p^\infty)$ their sum is defined as $\overline{\frac{ap^j+bp^i}{p^{ij}}}$ in $\mathbb{Q}/\mathbb{Z}$. But clearly such a fraction fits the rule for inclusion so $\mathbb{Z}(p^\infty)$ is closed under addition. Associativity is naturally inherited since the addition is associative in $\mathbb{Q}/\mathbb{Z}$. Finally inverses (negatives) have the property $-(a/p^i) = (-a)/p^i$ thus are also included, so $\mathbb{Z}(p^\infty)$ is a (sub)group of $\mathbb{Q}/\mathbb{Z}$.

Take the elements $\overline{1/p^i}$ and $\overline{1/p^j}$ to be equal for some i and j. Then $1/p^i \sim 1/p^j$ and thus $1/p^i - 1/p^j$ is and integer. But clearly $-1 < 1/p^i - 1/p^j < 1$ so the only integer between -1 and 1 is 0 forcing $1/p^i = 1/p^j$. Therefore $i = j$. Thus there are an infinite number of elements of the form $\overline{1/p^i}$ and so $\mathbb{Z}(p^\infty)$ has an infinite subset forcing it to be infinite. □

I.1.11 Abelian Relations.

Hint$(3/5)$: Use Theorems-I.1.2 and I.1.9 to show (i),(ii), and (iii) are equivalent;(i), (ii), and (iii) imply (iv); and (iv) implies and (v). Conclude the equivalence by showing (v) implies (i) by showing first the relations $ab^n = b^n a$ and $ab^{n+1} = b^{n+1}a$ are true. As a counter example of part (v) with only two consecutive integers, consider the two consecutive powers 0 and 1 in a non-abelian group.

The following conditions on a group G are equivalent: (i) G is abelian; (ii) $(ab)^2 = a^2b^2$ for all $a, b \in G$; (iii) $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$; (iv) $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$ and all $a, b \in G$; (v) $(ab)^n = a^n b^n$ for three consecutive integers n and all $a, b \in G$. Show (v)⇒(i) is false if "three" is replaced by "two."

Proof: Suppose (i) is true. Then $ab = ba$ for all $a, b \in G$; thus

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2,$$

so (i) implies (ii).

Now suppose (ii) is true. Then for all a and b, $abab = (ab)^2 = a^2b^2 = aabb$; thus, by cancellation, $ba = ab$, so G is abelian. Therefore (i) is equivalent to (ii).

By Theorem-I.1.2.v we know $(ab)^{-1} = b^{-1}a^{-1}$ and from here it is the simple step of commuting to say $(ab)^{-1} = a^{-1}b^{-1}$; thus (i) implies (iii) as well.

Suppose instead (iii) is true. Then for all a and b, using Theorem-I.1.2, it follows:

$$ba = (b^{-1})^{-1}(a^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1} = ab.$$

So $ba = ab$ and so G is abelian and (i) and (iii) are equivalent.

Again assume (i), and with it (ii), (iii) its equivalents. Suppose $(ab)^n = a^n b^n$ for some positive integer n. Then

$$(ab)^{n+1} = (ab)^n(ab) = (a^n b^n)(ab) = a^n(b^n a)b = a^{n+1}b^{n+1}.$$

So by induction $(ab)^n = a^n b^n$ for all positive integers n. When $n = 0$ by definition $(ab)^0 = e = ee = a^0 b^0$ so in fact $(ab)^n = a^n b^n$ for all non-negative integers. Finally given a negative integer n, $(ab)^n = (ab)^{-(-n)} = ((ab)^{-1})^{-n}$. But by (iii) this is simply $(a^{-1}b^{-1})^{-n}$ and since $-n$ is positive we now see this

as $(a^{-1})^{-n}(b^{-1})^{-n} = a^n b^n$ by Theorem-I.1.9 and the above. In conclusion $(ab)^n = a^n b^n$ for all integer n and elements a, b so (i) implies (iv). Clearly (v) is true if (iv) is true.

Now suppose (v) is true. Then every pair of elements a and b together with some integer n have the property that $(ab)^n = a^n b^n$, $(ab)^{n+1} = a^{n+1}b^{n+1}$ and $(ab)^{n+2} = a^{n+2}b^{n+2}$. This leads to the following two relations:

$$a^{n+1}b^{n+1} = (ab)^{n+1} = (ab)^n(ab) = a^n b^n ab,$$

which by cancellation reduces to $ab^n = b^n a$; next we swap the roles of a and b (recall the assumed relations work for all a and b) for convenience later:

$$bab^{n+1}a^{n+1} = (ba)(ba)^{n+1} = (ba)^{n+2} = b^{n+2}a^{n+2},$$

which thus infers the relation $ab^{n+1} = b^{n+1}a$. Together these imply:

$$bab^n = b(ab^n) = b(b^n a) = b^{n+1}a = ab^{n+1}$$

and thus once again canceling on the right we arrive at the final form $ba = ab$, so G is abelian. Therefore (i) implies (iv) which implies (v) which reciprocates by implying (i). Thus (i),(ii),(iii),(iv), and (v) are equivalent relations for abelian groups. □

Example: Consider the group S_3. Certainly given any two elements σ and τ, $(\sigma\tau)^0 = \varepsilon = \varepsilon\varepsilon = \sigma^0\tau^0$. Likewise $(\sigma\tau)^1 = \sigma\tau = \sigma^1\tau^1$ thus for two consecutive integers all elements have the property $(ab)^n = a^n b^n$. However clearly S_3 is non-abelian since $(12)(123) = (23)$ and $(123)(12) = (13)$. Of course any non-abelian group can serve in this counter example. □

I.1.12 Cyclic Conjugates.

If G is a group, $a, b \in G$ and $bab^{-1} = a^r$ for some $r \in \mathbb{N}$, then $b^i ab^{-i} = a^{r^i}$ for all $i \in \mathbb{N}$.

Proof: Let $i = 0$. By Definition-I.1.8 $b^0 ab^{-0} = eae = a^1 = a^{r^0}$. Now suppose $b^i ab^{-i} = a^{r^i}$ for some positive integer i. Then conjugating and using Theorem-I.1.9 we see $b^{i+1}ab^{-(i+1)} = b(b^i ab^{-i})b^{-1} = ba^{r^i}b^{-1}$. But here we employ the standard trick of multiplying by the identity:

$$ba^{r^i}b^{-1} = ba\cdots ab^{-1} = ba(b^{-1}b)a(b^{-1}b)\cdots(b^{-1}b)ab^{-1} = (bab^{-1})^{r^i} = (a^r)^{r^i} = a^{r^{i+1}}.$$

Therefore by induction $b^i ab^{-i} = a^{r^i}$. □

Hint$(1/5)$: Use the standard trick for conjugation: insert $b^{-1}b$ between powers of a to create conjugates of lower powers where information is given.

I.1.13 Groups of Involutions.

If $a^2 = e$ for all elements a of a group G, then G is abelian.

Proof: Let G be a group of involutions (i.e.: every non-trivial element has order 2.) Then $(ab)^2 = e = ee = a^2b^2$. This is relation (ii) of Exercise-I.1 and thus is equivalent to stating G is abelian. □

Hint$(1/5)$: Use Exercise-I.1 part (ii).

I.1.14 Involutions in Even Groups.

If G is a finite group of even order, then G contains an element $a \neq e$ such that $a^2 = e$.

Proof: Define the relation $a \sim b$ if and only if $a = b$ or $a = b^{-1}$. Let a, b, and c be elements of G:

Hint$(3/5)$: Partition the group into classes $[a] = \{a, a^{-1}\}$. Since $[e]$ has size 1, what else must exist?

- $a = a$ thus $a \sim a$ – reflexive.
- $a \sim b$ implies $a = b$ or $a = b^{-1}$. If $a = b$ then $b = a$ so $b \sim a$. Also if $a = b^{-1}$ then $a^{-1} = (b^{-1})^{-1} = b$ by Theorem-I.1.2.iv; so in general $b \sim a$ – symmetric.
- $a \sim b$ and $b \sim c$ implies $a = b$ or $a = b^{-1}$; and $b = c$ or $b = c^{-1}$. Naturally if $a = b$ and $b = c$ then $a = c$ so $a \sim c$. If $a = b$ and instead $b = c^{-1}$ then $a = c^{-1}$ so $a \sim c$. Next if $a = b^{-1}$ and $b = c$ clearly $b^{-1} = c^{-1}$ so $a \sim c$. Finally if $a = b^{-1}$ and $b = c^{-1}$ then $a = (c^{-1})^{-1} = c$ by Theorem-I.1.2.iv; therefore, $a \sim c$ – transitive.

So we have an equivalence relation on G and with it equivalence classes which partition the elements. By Theorem-I.1.2.iii we know inverses are unique and coupled with part iv of the theorem it is clear each equivalence class has at most 2 elements: $[a] = \{a, a^{-1}\}$.

However $e^{-1}e = e = ee$ so by cancellation $e^{-1} = e$; thus $[e]$ has only one element. Since the equivalence classes partition the even order group G it follows some equivalence class must have odd size so that together with the odd equivalence class $[e]$, the partition maintains the even order (note we know other equivalence classes exist because if not the order of G would be 1 which is not even). However as stated earlier each equivalence class has at most 2 elements; thus, there must exist an equivalence class that is not only of odd size but it must therefore be of size 1; call this class $[a]$. Therefore $\{a, a^{-1}\} = \{a\}$ so $a = a^{-1}$ which by multiplying by a shows $a^2 = e$, and $a \neq e$. □

I.1.15 Cancellation in Finite Semigroups.

Hint$(5/5)$: Consider a proof that every finite integral domain is a field. Show first a^n must be an identity (follows from the cancellation assumed) for some positive integer. Next decompose a^n to $a^{n-1}a = e$ to show inverses.

Let G be a nonempty finite set with an associative binary operation such that for all $a, b, c \in G$ $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$. Then G is a group. Show that this conclusion may be false if G is infinite.

Proof: Given any element $a \in G$ all powers of a must be in G – since G is closed under the binary operation. In fact the set $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}^+\}$ must be a subset of G. Furthermore $a^n a^m = a^{n+m}$ by Theorem-I.1.9 so it is a closed subset of G and we consider it in place of G.

Since G is finite so must $\langle a \rangle$ be finite; say $\langle a \rangle$ has order n. Clearly a^{n+1} is defined; however, it must also lie in $\langle a \rangle$ which has only n representatives; thus, there exists a $j \leq n$ such that $a^{n+1} = a^j$. If $j = 1$ then $a^{n+1} = a$. Suppose $j > 1$, then a^{j-1} is defined and still $n + 1 > j$, so $a^{n+1-j+1}$ is defined and so $a^{n+1-j+1}a^{j-1} = a^{n+1} = a^j = aa^{j-1}$. By cancellation we see $a^{n-j+2} = a$. Therefore for some power $2 \leq k \leq n$, $a^k = a$, $(k = n-j+2)$, and a^{k-1} is defined, and combined with the case $j = 1$ we see $a^k = a$ for some $1 < k \leq n + 1$ and a^{k-1} is also defined..

Now take any $b \in G$. First $ba^k = ba$; thus by cancellation on the right, $ba^{k-1} = b$. In similar fashion $a^k b = ab$ and so by cancellation on the left $a^{k-1}b = b$. Therefore a^{k-1} is the identity of G which we now call e – so G is a monoid.

Since e exists a^0 is now defined so a^{k-2} will always be defined. Therefore $a^{k-2}a = a^{k-1} = e$ so a^{k-2} is the left inverse of a. But in parallel $aa^{k-2} = a^{k-1} = e$ so it is in fact a two-sided inverse. Since the a was chosen arbitrarily such an inverse exists for all elements; so G is a group. □

Example: Consider the positive integers under addition. Certainly the addition is associative so they are in fact a semigroup. Also given integers m, n and k, $m+n = m+k$ implies $n = k$ and $n+m = k+m$ implies $n = k$ as we can prove since the equations must hold in the larger additive group of integers as well (refer to Proposition-I.1.4). Yet for instance, $1 + n \neq 1$ for any positive integer as is guaranteed by the ordering of the integers. Thus the positive integers do not form a group under addition. □

I.1.16 n-Product.

Let $a_1, a_2, \ldots$ be a sequence of elements in a semigroup G. Then there exists a unique function $\psi : \mathbb{Z}^+ \to G$ such that $\psi(1) = a_1$, $\psi(2) = a_1a_2$,$\psi(3) = (a_1a_2)a_3$ and for $n \geq 1$, $\psi(n+1) = (\psi(n))a_{n+1}$. Note that $\psi(n)$ is precisely the standard n product $\prod_{i=1}^{n} a_i$. [*Hint:* Applying the Recursion Theorem 6.2 of the Introduction with $a = a_1$, $S = G$ and $f_n : G \to G$ given by $x \mapsto xa_{n+2}$ yields a function $\varphi : \mathbb{N} \to G$. Let $\psi = \varphi\theta$, where $\theta : \mathbb{Z}^+ \to \mathbb{N}$ is given by $k \mapsto k - 1$.]

Hint$(3/5)$: Use the given hint directly. Prove each mapping is well-defined and apply the theorem appropriately.

Proof: The map $\theta : \mathbb{Z}^+ \to \mathbb{N}$ defined as $k \mapsto k - 1$ is well-defined and bijective since it is invertible. Therefore defining functions on $\mathbb{N}$ is equivalent to defining them on $\mathbb{Z}^+$ – note in our case this is akin to simply indexing our sequence beginning with 0 instead of 1.

The mappings $f_n : G \to G$ defined by right translation as $f_n(x) = xa_{n+2}$ relies on the well-defined definition of multiplication in G, since there always exists an $a_{n+2} \in G$, and so the image is well-defined leaving f_n well-defined for all n. By the Recursion Theorem there must therefore exist a function $\varphi : \mathbb{N} \to G$ such that $\varphi(n+1) = f_n(\varphi(n)) = (\varphi(n))a_{n+2}$ and $\varphi(0) = a_1$. Now define $\psi = \varphi\theta$ so that $\psi : \mathbb{Z}^+ \to G$. Clearly $\psi(1) = \varphi(\theta(1)) = \varphi(0) = a_1$; $\psi(2) = \varphi(\theta(2)) = \varphi(1) = (\varphi(0))a_2 = a_1a_2$; $\psi(3) = \varphi(\theta(3)) = \varphi(2) = (\varphi(1))a_3 = (a_1a_2)a_3$; and finally in general $\psi(n+1) = \varphi(\theta(n+1)) = \varphi(n) = (\varphi(n))a_{n+1} = (\psi(n))a_{n+1}$. So ψ defines the standard n-product for associative operators. $\square$

I.2 Homomorphisms and Subgroups

1 Homomorphisms . . . 36
2 Abelian Automorphism . . . 37
3 Quaternions . . . 37
4 D_4 in $\mathbb{R}^{2\times 2}$ . . . 37
5 Subgroups . . . 38
6 Finite subgroups . . . 38
7 $n\mathbb{Z}$ . . . 39
8 Subgroups of S_n . . . 39
9 Subgroups and Homomorphisms . . . 40
10 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ lattice . . . 40
11 Center . . . 40
12 Generators . . . 41
13 Cyclic Images . . . 41
14 Cyclic Groups of Order 4 . . . 42
15 Automorphisms of $\mathbb{Z}_n$ . . . 42
16 Generators of PruferGroup . . . 44
17 Join of Abelian Groups . . . 44
18 Join of Groups . . . 44
19 Subgroup Lattices . . . 45

I.2.1 Homomorphisms.

Hint$(2/5)$: For the counter example consider the a homomorphism between the multiplicative monoids of $\mathbb{Z}_3$ and $\mathbb{Z}_6$.

If $f : G \to H$ is a homomorphism of groups, then $f(e_G) = e_H$ and $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$. Show by example that the first conclusion may be false if G, H are monoids that are note groups.

Proof: Assuming $f : G \to H$ is a homomorphism of groups, then $f(a) = f(ae_G) = f(a)f(e_G)$ and likewise on the left, $f(a) = f(e_G a) = f(e_G)f(a)$. Therefore $f(e_G)$ acts like an identity in the image of $f(G)$ in H. By Theorem-I.2.5, $e_H = f(a)f(a)^{-1} \in f(G)$ and since identities are unique, by Theorem-I.1.2, it follows $f(e_G) = e_H$.

Let $a \in G$. Since both G and H are groups the elements a^{-1} and $f(a)^{-1}$ are defined. From here $e_H = f(e_G) = f(aa^{-1}) = f(a)f(a^{-1})$ and in similar fashion $e_H = f(a^{-1})f(a)$ – thus by Theorem-I.1.2 part iii (which states inverses are unique) it follows $f(a^{-1}) = f(a)^{-1}$. □

Example: Both $\mathbb{Z}_3$ and $\mathbb{Z}_6$ contain a $\overline{1}$ with the property that $n1 \equiv 1n \equiv n$ for all integers n. Since multiplication modulo k is associative it follows $\mathbb{Z}_3$ and $\mathbb{Z}_6$ are multiplicative monoids. Furthermore they are not multiplicative groups because $\overline{0}$ has no inverse: $0n \equiv 0$ for all n; thus $\overline{0}\overline{n} \neq \overline{1}$.

Now define the map $f : \mathbb{Z}_3 \to \mathbb{Z}_6$ by $f(\overline{0}) = \overline{0}$ and $f(\overline{1}) = \overline{4}$ and $f(\overline{2}) = \overline{2}$. Note the image $f(\mathbb{Z}_3) = \{\overline{0}, \overline{2}, \overline{4}\}$ is closed to multiplication and has multiplicative identity $\overline{4}$.

We may check this is a homomorphism under multiplication as follows: (first note both the domain and codomain are commutative so we need to check only one order of every pair) $f(\overline{0}\overline{n}) = f(\overline{0}) = \overline{0} = \overline{0}f(\overline{n}) = f(\overline{0})f(\overline{n})$ for all $n \in \mathbb{Z}_3$. $f(\overline{1}\overline{n}) = f(\overline{n})$, but furthermore, $f(\overline{n}) = \overline{4}f(\overline{n})$ since $\overline{4}$ is a multiplicative identity within the image. Thus $f(\overline{1}\overline{n}) = f(\overline{1})f(\overline{n})$. And finally $f(\overline{2} \cdot \overline{2}) = f(\overline{1}) = \overline{4} = \overline{2} \cdot \overline{2} = f(\overline{2})f(\overline{2})$. Therefore f is a multiplicative homomorphism; however, clearly $f(\overline{1}) \neq \overline{1}$.

In general the multiplicative homomorphisms $f : \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_m$ where p is prime and $m > 1$, defined as $n \mapsto (n, 0)$ have the property that $f(1) \neq (1, 1)$

and so they function as counter examples. □

I.2.2 Abelian Automorphism.

A group G is abelian if and only if the map $G \to G$ given by $x \mapsto x^{-1}$ is an automorphism.

Hint$(1/5)$: Use Exercise-I.1 part (ii) to show the map is a homomorphism.

Proof: Let G be an abelian group. Then by Exercise-I.1 part (ii) it is equivalent to say $(ab)^{-1} = a^{-1}b^{-1}$; thus, a map defined as $f(x) = x^{-1}$ is a homomorphism since $f(ab) = (ab)^{-1} = a^{-1}b^{-1} = f(a)f(b)$.

For the converse assume f is a homomorphism. Thus $(ab)^{-1} = f(ab) = f(a)f(b) = a^{-1}b^{-1}$ for all $a, b \in G$. But once again this is an equivalent definition for G being abelian so G is abelian. □

I.2.3 Quaternions.

Hint$(1/5)$: Use the normal form (A^iB^j) suggested. How many elements of order 4 are there?

Let Q_8 be the group (under ordinary matrix multiplication) generated by the complex matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, where $i^2 = -1$. Show that Q_8 is a non-abelian group of order 8. Q_8 is called the **quaternion group**. [*Hint:* Observe that $BA = A^3B$, whence every element of Q_8 is of the form A^iB^j. Note also that $A^4 = B^4 = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of Q_8.]

Proof: Using standard matrix multiplication observe that

$$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1I = -I.$$

Let $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and note it is a permutation matrix. Thus $B = iP$ and so $B^2 = (iP)^2 = i^2P^2 = -1I = -I$. So $A^2 = B^2$ and $-I^2 = (-1)^2II = 1I = I$; thus $A^4 = B^4 = I$ and moreover $A^3 = -IA = -A$ and $B^3 = -B = -IB = A^2B$.

Next

$$PA = P\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}P = A^3P;$$

therefore, $BA = iPA = iA^3P = A^3iP = A^3B$. Here we see Q_8 will not be abelian. Multiplication in Q_8 has a normal form: given any product of A's and B's we may express it in the form A^iB^j for some integers i and j; moreover, $B^3 = -B = -IB = A^2B$ so we in fact need only elements of the form A^i and A^iB. Since A has order 4 we have at least the following elements:

$$Q_8 = \{I, A, A^2, A^3, B, AB, A^2B, A^3B\}$$

and if we write these as matrices we see these are all distinct elements:

$$Q_8 = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\right\}.$$

Notice for all $X \in Q_8$, $X \neq I, -I$, $X^{-1} = -X$; thus the group is often described as

$$Q_8 = \{\hat{1}, -\hat{1}, \hat{i}, -\hat{i}, \hat{j}, -\hat{j}, \hat{k}, -\hat{k}\},$$

where $\hat{i} = A, \hat{j} = B, \hat{k} = AB$. Therefore Q_8 is a subgroup generated by A and B.

In reference to Exercise-I.2 notice $A^4 = B^4 = AB^4 = -I^2 = I$ so there are six elements of order 4: $\hat{i}$,$-\hat{i}$, $\hat{j}$, $-\hat{j}$, $\hat{k}$ and $-\hat{k}$. □

I.2.4 D_4 in $\mathbb{R}^{2\times 2}$.

Hint$(2/5)$: Consider the rotation matrix $R(\theta) = \begin{pmatrix} cos\ \theta & sin\ \theta \\ -cos\ \theta & sin\ \theta \end{pmatrix}$ for $\theta = 90°$, and notice the geometric action of D is $T_{1,3}$. How many elements of order 4 does D_4 have? How many in Q_8? The Principle of Refinement, Corollary-A.2.2 may be helpful. Refer to Exercise-I.1.

Let H be the group (under matrix multiplication) of real matrices generated by $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Show H is a non-abelian group of order 8 which is *not* isomorphic to the quaternion group of Exercise-I.2, but is isomorphic to the group D_4^*.

Proof: Notice that $R(90°) = C$ thus C is a linear transformation that rotates the plane (and thus a square contained in the plane) by $90°$. So identify C with R in D_4^*. $D\vec{e}_x = \vec{e}_y$ and $D\vec{e}_y = \vec{e}_x$ so D acts like the transform $T_{1,3}$ on the plane.

Therefore $C^4 = I$, since R has order 4, and $D^2 = I$ by $T_{1,3}$; furthermore, $DC = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = -CD$, $C^{-1} = C^3 = -C$ so once again we have a normal form for all the elements: C^iD^j – note from here we see it will not be abelian. Therefore our new set has the following elements: $H = \{I, C, C^2, C^3, D, CD, C^2D, C^3D\}$. If we construct these matrices we see each of these elements is distinct:

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

So define the function $f : D_4^* \to H$ as follows:

$$f = \begin{pmatrix} I & R & R^2 & R^3 & T_{1,3} & RT_{1,3} & R^2T_{1,3} & R^3T_{1,3} \\ I & C & C^2 & C^3 & D & CD & C^2D & C^3D \end{pmatrix}$$

Notice that $f(R^iT_{1,3}^j) = C^iD^j$ for all i and j, given $R^i, R^j \in D_4^*$,

$$\begin{aligned} f(R^iR^j) &= f(R^{i+j}) = C^{i+j} = C^iC^j = f(R^i)f(R^j); \\ f((R^iT_{1,3})(R^jT_{1,3})) &= f(R^{i-j}T_{1,3}) = C^{i-j}D = (C^iD)(C^jD) = f(R^iT_{1,3})f(R^jT_{1,3}); \end{aligned}$$

so f is a homomorphism which is in fact bijective. By Theorem-A.2.1 H is a group, and so f is an isomorphism.

D_4 has only two elements of order 4: C and C^3; yet Q_8 has six: A, $-A$, B, $-B$, AB and $-AB$; thus these groups are not isomorphic. □

I.2.5 Subgroups.

Hint$(3/5)$: For the forward direction show S is the equivalence class of the identity.

Let S be a nonempty subset of a group G and define a relation on G by $a \sim b$ if and only if $ab^{-1} \in S$. Show that $\sim$ is an equivalence relation if and only if S is a subgroup of G.

Proof: ($\Rightarrow$) Suppose $\sim$ is an equivalence relation on G. S is nonempty and thus it contains an element a. An element a is in S if and only if $a \sim e$, since $a = ae = ae^{-1}$. Therefore $S = \overline{e}$, and so for all $a, b \in S$, $a \sim e$ and $b \sim e$ so by the symmetry $e \sim b$ and by the transitivity of $\sim$, $a \sim b$; thus, $ab^{-1} \in S$ by the definition of $\sim$. Theorem-I.2.5 is satisfied thus S is a subgroup of G.

($\Leftarrow$) Let a, b and c be elements of G and suppose S is a subgroup of G. S being a subgroup implies it contains the identity e, so $aa^{-1} = e \in S$, thus implying $a \sim a$ so that $\sim$ is reflexive. Next, whenever $a \sim b$, $ab^{-1} \in S$. S is a subgroup so it must contain the inverse of ab^{-1} which by Theorem-I.1.2 is simply ba^{-1}; therefore, $b \sim a$ and $\sim$ is symmetric. Finally assuming $a \sim b$ and $b \sim c$, the definition of $\sim$ requires that ab^{-1}, bc^{-1} be in S. Furthermore S is a subgroup so it is closed to products, such as: $(ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = ac^{-1}$. So $a \sim c$ and in conclusion $\sim$ is transitive and so it is an equivalence relation. □

I.2.6 Finite subgroups.

Hint$(3/5)$: Use Exercise-I.1.

A nonempty finite subset of a group is a subgroup if and only if it is closed under the product in G.

Proof: Let S be a nonempty finite subset of G.

($\Rightarrow$) Suppose S is a subgroup of G. S must therefore be a group it self, so the product of two elements $a, b \in S$ must be a well-defined element in S. We assume G is a group so the product ab is well-defined in G and thus all that is required is that ab be in S. Therefore S is closed under the product in order to be a group, and thus a subgroup.

($\Leftarrow$) Suppose S is closed under products in G. Given the elements a, b, and c in S we have assumed ac and bc are in S. Furthermore whenever $ac = bc$, it must also be true in all of G where there exists a c^{-1}. Thus we can cancel to produce $a = b$ in S (also in G). On the left we take the elements ca and cb which are also in S since S is assumed closed. Once again whenever $ca = cb$ in S then it does so also in G thus $a = b$ in G and so also in S. Therefore S is a nonempty finite semigroup with left and right cancellation; therefore, it satisfies the hypothesis of Exercise-I.1 which results in the statement that S is a group. Since S is a group under the operation of G it is a subgroup of G. □

I.2.7 $n\mathbb{Z}$.

Hint$(1/5)$: Use the Principle of Refinement, Corollary-A.2.2.

If n is a fixed integer, then $\{kn \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$ is an additive subgroup of $\mathbb{Z}$, which is isomorphic to $\mathbb{Z}$.

Proof: Define $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. Since multiplication in $\mathbb{Z}$ is commutative this set is equivalent to that assumed in the hypothesis.

Define a function $f : \mathbb{Z} \to n\mathbb{Z}$ in the natural way so that $f(k) = nk$. Every element of $n\mathbb{Z}$ is of the form nk, so f is well-defined. Next $f(i+j) = n(i+j) = ni + nj = f(i) + f(j)$ so f is an additive homomorphism. Given $x \in n\mathbb{Z}$, there exists a k such that $x = nk = f(k)$; therefore, f is surjective. By Corollary-A.2.2 it follows $f(\mathbb{Z}) = n\mathbb{Z}$ is a group. Since $n\mathbb{Z}$ is a group under addition in $\mathbb{Z}$; it is a subgroup of $\mathbb{Z}$.

Now define the map $f^{-1} : n\mathbb{Z} \to \mathbb{Z}$ by $f(nk) = k$. The integers have the property $nk = nj$ if and only if $k = j$; thus every element of $n\mathbb{Z}$ is uniquely represented as an element nk. Therefore f^{-1} is well-defined. Finally $ff^{-1}(nk) = f(k) = nk$ so $ff^{-1} = 1_{n\mathbb{Z}}$ and $f^{-1}f(k) = f^{-1}(nk) = k$ so that $f^{-1}f = 1_{\mathbb{Z}}$. Therefore f is an isomorphism since it is a bijective homomorphism – proof of Theorem-I.2.3. □

I.2.8 Subgroups of S_n.

Hint$(1/5)$: Use the Principle of Refinement, A.2. The statement here proved actually allows any character to be fixed, not only the letter n.

The set $\{\sigma \in S_n \mid \sigma(n) = n\}$ is a subgroup of S_n, which is isomorphic to S_{n-1}.

Proof: Define $S_n^k = \{\sigma \in S_n \mid \sigma(k) = k\}$ for any $1 \leq k \leq n$. Define the mapping $f : S_{n-1} \to S_n$ as follows:

$$f(\sigma)(x) = \begin{cases} \sigma(x) & x < k \\ k & x = k \\ \sigma(x-1)+1 & x > k \end{cases}.$$

Each $f(\sigma)$ is a map of the form $\{1, \ldots, n\} \to \{1, \ldots, n\}$ and bijective on $\{1, \ldots, n\} - \{k\}$ since it is simply the bijective mapping σ in this case. Furthermore the added definition of $f(\sigma(k)) = k$ ensures it is bijective on all $\{1, \ldots, n\}$. Therefore it is a permutation of n elements so it is in S_n. Therefore f is well-defined. Furthermore $f(\sigma)$ is also in S_n^k as it fixes k.

Given $\sigma, \tau \in S_{n-1}$, consider $f(\sigma\tau)$: when $x < k$, $f(\sigma\tau)(x) = \sigma(\tau(x)) = f(\sigma)f(\tau)(x)$; when $x > k$ then

$$\begin{aligned} f(\sigma\tau)(x) &= \sigma\tau(x-1)+1 = \sigma(\tau(x-1))+1 \\ &= \sigma(\tau(x-1)+1-1)+1 \\ &= \sigma(f(\tau)(x)-1)+1 = f(\sigma)f(\tau)(x); \end{aligned}$$

finally when $x = k$, $f(\sigma\tau)(x) = k = f(\sigma)f(\tau)(x)$; therefore, $f(\sigma\tau) = f(\sigma)f(\tau)$, so f is a homomorphism. By the Principle of Refinement $f(S_{n-1}) = S_n^k$ is a group, and so a subgroup of S_n. □

I.2.9 Subgroups and Homomorphisms.

Hint$(1/5)$: For part (a) do $f^{-1}(B)$ which solves for the kernel since $\mathbf{0} = \{e\}$ is a subgroup of H. Use the Principle of Refinement, A.2, in part (b).

Let $f : G \to H$ be a homomorphism of groups, A a subgroup of G, and B a subgroup of H.

(a) Ker f and $f^{-1}(B)$ are subgroups of G.

(b) $f(A)$ is a subgroup of H.

Proof: The identity of H is in B, and $f(e) = e$, so $f^{-1}(B)$ contains e and is nonempty. Take any two elements $a, b \in f^{-1}(B)$ and using the definition let $x, y \in B$, be $x = f(a)$ and $y = f(b)$. Exercise-I.2 shows $f(b^{-1}) = f(b)^{-1}$ and so $f(ab^{-1}) = f(a)f(b)^{-1} = xy^{-1} \in B$, by Theorem-I.2.5 as applied to the subgroup B in H. Therefore $ab^{-1} \in f^{-1}(B)$ which means by Theorem-I.2.5, $f^{-1}(B)$ is a subgroup of G.

The nonempty subset $\mathbf{0} = \{e\}$ contains the identity and trivially all inverses. Therefore it is a group, and so even a subgroup of H. Thus $Ker\ f = f^{-1}(\mathbf{0})$ is a subgroup of G.

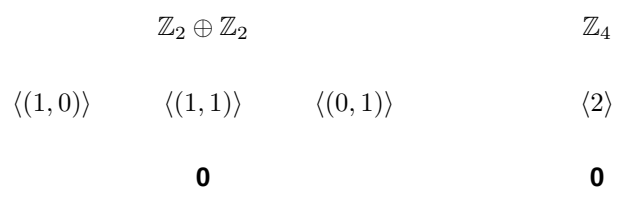
Certainly $f|A : A \to f(A)$ is a well-defined function (refer to Introduction, section 3). Now $f(ab) = f(a)f(b)$ for all elements in G so it must also for all element in A, which naturally come from G. Therefore $f|A$ is a homomorphism. By the Principle of Refinement (Corollary-A.2.2) $f(A)$ is a group and so it is a subgroup of H. □

I.2.10 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ lattice.

Hint$(1/5)$: Show any homomorphism $\mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ cannot be injective.

List all subgroups of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Is $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ isomorphic to $\mathbb{Z}_4$?

Example:



□

Proof: Suppose $f : \mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a homomorphism. Then $f(1) = (a, b)$. Yet Exercise-I.1 shows $(a, b) + (a, b) = (0, 0)$. Thus $f(2) = (0, 0) = f(0)$. Therefore f is not injective. Thus f has no inverse mapping so no homomorphism f^{-1} exists such that $f^{-1}f = 1_{\mathbb{Z}_4}$. Therefore the groups are not isomorphic. □

erify the defini-
oup.

I.2.11 Center.

If G is a group, then $C = \{a \in G \mid ax = xa \text{ for all } x \in G\}$ is an abelian subgroup of G. C is called the **center** of G.

Proof: The identity element has the property $ex = x = xe$ for any element $x \in G$; thus $e \in C$ so C is nonempty. Given any two elements $a, b \in C$, $xa = ax$ and $xb = bx$ for all $x \in G$, which allows

$$x(ab) = (xa)b = (ax)b = a(xb) = a(bx) = (ab)x.$$

So $ab \in C$. Finally $xa = ax$ implies

$$a^{-1}x = a^{-1}x(aa^{-1}) = a^{-1}(xa)a^{-1} = (a^{-1}a)xa^{-1} = xa^{-1}.$$

Therefore C is closed to inverses so it is a subgroup of G. □

I.2.12 Generators.

The group D_4^* is not cyclic, but can be generated by two elements. The same is true of S_n (nontrivial). What is the minimal number of generators of the additive group $\mathbb{Z} \oplus \mathbb{Z}$? [5]

Hint$(2/5)$: Refer to Exercise-I.2. How many generators are required in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$? How many might then be needed in $\mathbb{Z} \oplus \mathbb{Z}$?

Example: The group $\mathbb{Z} \oplus \mathbb{Z}$ needs no more than two generators as is seen with this example: given $(a, b) \in \mathbb{Z} \oplus \mathbb{Z}$ notice $(a, b) = (a, 0) + (0, b) = a(1, 0) + b(0, 1)$. Therefore any subgroup of $\mathbb{Z} \oplus \mathbb{Z}$ which contains the set $\{(1, 0), (0, 1)\}$ must contain all of $\mathbb{Z} \oplus \mathbb{Z}$, so by Definition-I.2.7 this set generates $\mathbb{Z} \oplus \mathbb{Z}$.

Additionally $\mathbb{Z} \oplus \mathbb{Z}$ cannot be generated by less than 2 elements. This is because given any lone element (a, b), Theorem-I.2.8 claims it generates only $\{n(a, b) \mid n \in \mathbb{Z}\}$. However $n(a, b) = (na, nb)$. Yet $(-a, b)$ is clearly also an element of $\mathbb{Z} \oplus \mathbb{Z}$. If it is not in $\langle(a, b)\rangle$ then by definition the $\mathbb{Z} \oplus \mathbb{Z}$ is not generated by one element. If however $(-a, b) \in \langle(a, b)\rangle$, then $(-a, b) = (na, nb)$ requires $b = nb$, or simply $n = 1$. Thus $-a = a$ so $a = 0$. Therefore the element $(1, 0)$ is excluded from $\langle(a, b)\rangle$. Therefore no lone element generates $\mathbb{Z} \oplus \mathbb{Z}$. □

I.2.13 Cyclic Images.

If $G = \langle a\rangle$ is a cyclic group and H is any group, then every homomorphism $f : G \to H$ is completely determined by the element $f(a) \in H$.

Hint$(1/5)$: Use induction to show $f(a^n) = f(a)^n$ for all integers n.

Proof: Consider any element $x \in f(G)$. By this assumption there exists an element in the domain b such that $x = f(b)$. However the domain is cyclic so by definition there exists an integer n such that $b = a^n$. Using the axiom of replacement, $x = f(a^n)$. Suppose $n = 0$, then $x = f(a^0) = f(e) = e = f(a)^0$ so the element is determined by $f(a)^0$. Assume for induction that $f(a^n) = f(a)^n$ for some non-negative integer n; thus,

$$f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = f(a)^n f(a) = f(a)^{n+1}.$$

Therefore $f(a^n) = f(a)^n$ for every non-negative integer n by induction.

Exercise-I.2 demonstrates that $f(a^{-1}) = f(a)^{-1}$ so now consider $f(a^n)$ when $n < 0$:

$$f(a^n) = f(a^{-(-n)}) = f((a^{-1}))^{-n}) = f(a^{-1})^{-n} = (f(a)^{-1})^{-n} = f(a)^n,$$

[5] The use of "*minimal* number of generators" is misleading. The set $\{(2, 0), (3, 0), (0, 2), (0, 3)\}$ is minimal in the sense that no proper subset generates all of $\mathbb{Z} \oplus \mathbb{Z}$, but as shown in the proof the small set $\{(1, 0), (0, 1)\}$ is also a minimal generating set. It is best to answer what is a *minimum* number of generators, which in fact will have to be a minimal number as well.

using of course the fact that $-n \geq 0$. Therefore $f(a^n) = f(a)^n$ for all integers.

In conclusion every image element of f is of the form $f(a)^n$ for some integer n and thus $f(a)$ determines the homomorphism. □

I.2.14 Cyclic Groups of Order 4.

Hint$(1/5)$: Identify a generator in each and use Exercise-I.2.

The following cyclic subgroups are all isomorphic: the multiplicative group $\langle i \rangle$ in $\mathbb{C}$, the additive group $\mathbb{Z}_4$ and the subgroup $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle$ of S_4.

Example: The group $\langle i \rangle$ contains by definition all integral powers of i; thus it includes $\{i, i^2 = -1, i^3 = -i, i^4 = 1\}$. Notice $i^5 = i$ so we need not pursue any more positive powers. Similarly $i(-i) = (-i)i = 1$ thus the inverse of i is already accounted for so no negative powers are required.

We abbreviate the permutation notation in the traditional way and write (1234) in place of $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. Now the set generated by this element contains $\{(1234), (13)(24), (1432), \varepsilon\}$. Again $(1234)^5 = (1234)$ and clearly this implies $(1234)^3 = (1234)^{-1}$ so these elements are in fact all the elements of our subgroup generated by (1234).

Define the mapping $f : \mathbb{Z}_4 \to \langle i \rangle$ by $f(1) = i$; the mapping $g : \mathbb{Z}_4 \to \langle (1234) \rangle$ by $f(1) = (1234)$. By Exercise-I.2 these functions determine a unique homomorphism. By the Principle of refinement $f(\mathbb{Z}_4)$ and $g(\mathbb{Z}_4)$ are subgroups and as we have shown both are surjective. We furthermore have a natural inverse mapping $f^{1-}(i) = 1$ and $g^{-1}((1234)) = 1$. These are again homomorphism from Exercise-I.2. Finally $ff^{-1}(i^n) = i^n$, so $ff^{-1} = 1_{\langle i \rangle}$; $f^{-1}f(n \cdot 1) = n \cdot 1$ so $f^{-1}f = 1_{\mathbb{Z}_4}$; $gg^{-1}((1234)^n) = (1234)^n$, so $gg^{-1} = 1_{\langle (1234) \rangle}$; $g^{-1}g(n \cdot 1) = n \cdot 1$ thus $g^{-1}g = 1_{\mathbb{Z}_4}$. Therefore the groups are all isomorphic. □

I.2.15 Automorphisms of $\mathbb{Z}_n$.

Hint$(5/5)$: (a) Notice each automorphism is a permutation and show $Aut\ G$ is simply a subgroup of S_G. (b) Consider Exercise-I.2. (c) Consider Exercise-I.3 and the Euler φ function.

Let G be a group and $Aut\ G$ the set of all automorphisms of G.

(a) $Aut\ G$ is a group with composition of functions as a binary operation. [*Hint:* $1_G \in Aut\ G$ is an identity; inverses exist by Theorem-I.2.3.]

(b) $Aut\ \mathbb{Z} \cong \mathbb{Z}_2$ and $Aut\ Z_6 \cong \mathbb{Z}_2$; $Aut\ \mathbb{Z}_8 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$; $Aut\ \mathbb{Z}_p \cong \mathbb{Z}_{p-1}$ (p prime).

(c) What is the $Aut\ \mathbb{Z}_n$ for arbitrary $n \in \mathbb{Z}^+$?

(a) **Proof:** Given any automorphism $\alpha : G \to G$ it is required that α be an isomorphism and therefore have an inverse map. However inverse maps exist if and only if a map is bijective; thus each automorphism is a bijection, and furthermore by mapping $G \to G$ they are in fact permutations. That is to say $Aut\ G$ is a subset of S_G. As desired the operation of $Aut\ G$ when considered as a group is composition as it is in S_G; so we need only show $Aut\ G$ is a subgroup of S_G.

The map $1_G(ab) = 1_G(a)1_G(b)$ and its inverse is 1_G; thus by Theorem-I.2.3 it is an isomorphism and so even an automorphism. Therefore $Aut\ G$ is nonempty.

Given an two automorphisms $\alpha : G \to G$ and $\beta : G \to G$ it follows from Theorem-I.2.3 that there exists an inverse isomorphism $\beta^{-1} : G \to G$ which is evidently an automorphism. Now $\alpha\beta^{-1}$ is a composition of permutations

and so it is again a permutation and thus invertible. Further more the composition remains a homomorphism since:

$$\alpha\beta(xy) = \alpha(\beta(xy)) = \alpha(\beta(x)\beta(y)) = \alpha(\beta(x))\alpha(\beta(y)) = \alpha\beta(x)\alpha\beta(y)$$

for any two elements $x, y \in G$. Therefore the composition is an invertible homomorphism. Take the inverse in S_G and note by Theorem-I.1.2 $(\alpha\beta^{-1})^{-1} = \beta\alpha^{-1}$. Notice the above argument was conducted on any automorphisms α and β so the results must also be true when α is β and when β is α; that is to say $\beta\alpha^{-1}$ is an invertible homomorphism. Furthermore by their definition in S_G, $(\alpha\beta^{-1})(\beta\alpha^{-1}) = 1_G = (\beta\alpha^{-1})(\alpha\beta^{-1})$ so by Theorem-I.2.3 $\alpha\beta^{-1}$ is an isomorphism and therefore an automorphism of G. Therefore $\alpha\beta^{-1}$ is in $Aut\ G$.

Finally by Theorem-I.2.5, $Aut\ G$ is a subgroup of S_G and so it is a group under composition. □

(b) **Example:** By Exercise-I.2 we know every abelian group has the automorphism $-1_G : x \mapsto -x$ (here expressed additively) so there may often be at least two automorphisms – notice sometimes $-1_G = 1_G$.

Given $\mathbb{Z}$ the automorphism $-1_G \neq 1_G$ since $-1_G(1) = -1 \neq 1 = 1_G(1)$. Therefore the automorphism group of $\mathbb{Z}$ has at least the elements $\{1_\mathbb{Z}, -1_\mathbb{Z}\}$. Notice this set is isomorphic to $\mathbb{Z}_2$ by the map $\overline{1} \mapsto -1_\mathbb{Z}$. Now consider any automorphism α of $\mathbb{Z}$. By Exercise-I.2 it follows α is uniquely defined by $\alpha(1)$ since 1 is a generator of $\mathbb{Z}$. We need α to be bijective and so $\alpha(1)$ must generate all of $\mathbb{Z}$. But in Exercise-I.2 we saw $m \in \mathbb{Z}$ generates a proper subgroup $m\mathbb{Z}$ whenever $m \neq 1, -1$; therefore, $Aut\ \mathbb{Z} \cong \mathbb{Z}_2$.

Again in $\mathbb{Z}_6$, the set maps $1_{\mathbb{Z}_6}$ and $-1_{\mathbb{Z}_6}$ are distinct automorphisms since $2 \neq -2$. Given any other automorphism α, using Exercise-I.2 we concentrate on the image of 1. $\alpha(1)$ must be a generator of $\mathbb{Z}_6$ of which me may empirically identify only 1, and 5=-1, work. Therefore there are no other automorphism and $Aut\ \mathbb{Z} \cong \mathbb{Z}_2$.

With $\mathbb{Z}_8$ again $-2 \neq 2$ so we have the two automorphism $1_{\mathbb{Z}_8}$ and $-1_{\mathbb{Z}_8}$ as usual. Now we once again look for all the generators of $\mathbb{Z}_8$, which we discover are 1,3,5,and 7=-1. Given any generator g, $\alpha(n) = gn$ is injective since $gi \equiv gj \pmod 8$ implies $i \equiv j \pmod 8$ as we know $(g, 8) = 1$; therefore, α is bijective by the Pigeon-Hole-Principle. Finally $\alpha(i+j) = g(i+j) = gi+gj = \alpha(i)+\alpha(j)$, so in fact the automorphisms of $\mathbb{Z}_8$ are $\alpha_k(i) = ki$ with $k = 1, 3, 5, 7$. To identify the group we consider $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$; thus we see it is the group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ as defined in Exercise-I.1.

For $\mathbb{Z}_p$ we locate all generators as $1, \ldots, p-1$, which leads to the automorphism group $\mathbb{Z}_p^*$ as defined in Exercise-I.1. When $p = 2$ trivially $\mathbb{Z}_p^* = \mathbf{0} = \mathbb{Z}_{p-1}$. Now let $p > 2$; therefore, $2 \in \mathbb{Z}_p^*$. Every prime has a primitive root, that is, an element a where $(a, p) = 1$ and $|a| = p - 1$ in $\mathbb{Z}_p^*$.[Eyn] □

(c) The automorphisms of $\mathbb{Z}_m$ are isomorphic to the group of generators of $\mathbb{Z}_m$ as a multiplicative group, that is, $\mathbb{Z}_m^\times$.

Proof: Suppose $\alpha : \mathbb{Z}_m \to \mathbb{Z}_m$ is an automorphism. We know $\mathbb{Z}_m$ is cyclic and generated by 1, so using Exercise-I.2, $\alpha(1)$ defines the homomorphism. Since we want α to be an automorphism, $\alpha(1)$ must be a generator of $\mathbb{Z}_m$; therefore,

$$\alpha(k) = \alpha(k \cdot 1) = k\alpha(k) = k(g \cdot 1) = gk,$$

where g is any generator of $\mathbb{Z}_m$. But we also require that α be invertible which provides there exist a g^{-1} such that $g^{-1}(gk) = k$. Therefore each

generator is an invertible element in $\mathbb{Z}_m$ under multiplication. In Exercise-I.3 we saw $\mathbb{Z}_m^\times = \{k \in \mathbb{Z}_m \mid (k,m) = 1\}$ is the largest group under multiplication. Therefore every generator is in $\mathbb{Z}_m^\times$ as $\mathbb{Z}_m^\times$ contains all invertible elements.

To check this we take any element g in $\mathbb{Z}_m^\times$. Then $(g,m) = 1$ so we know $gi \equiv gj \pmod m$ implies $i \equiv j$ by Introduction, Theorem-6.8; therefore, $\alpha(k) = gk$ is an injective function, and so by the Pigeon-Hole-Principle it is bijective. Finally, $\alpha(i+j) = g(i+j) = gi + gj = \alpha(i) + \alpha(j)$, so α is an automorphism. Therefore the automorphism group of $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_m^\times$. □

I.2.16 Generators of PruferGroup.

Hint$(1/5)$: Notice these generators are not independent: in fact, $\{\overline{1/p^n} \mid n \in \mathbb{Z}^+, n > k\}$ is also a generating set for any $k \in \mathbb{Z}^+$.

For each prime p the additive subgroup $Z(p^\infty)$ of $\mathbb{Q}/\mathbb{Z}$ (Exercise-I.1) is generated by the set $\{\overline{1/p^n} \mid n \in \mathbb{Z}^+\}$.

Proof: Given an element $\overline{a/b} \in \mathbb{Z}(p^\infty)$ we know $b = p^n$ for some $n \in \mathbb{N}$. Notice $a/p^n - a(1/p^n) = 0 \in \mathbb{Z}$, so $\overline{a/p^n} = a\overline{1/p^n}$; therefore, $\mathbb{Z}(p^\infty) = \langle \overline{1/p^n} \mid n \in \mathbb{Z}^+ \rangle$.

Notice that given any $m > n$, $p^{m-n}\overline{1/p^m} = \overline{1/p^n}$ so any set $\{\overline{1/p^n} \mid n \in \mathbb{Z}^+, n > k\}$ is also a generating set for any $k \in \mathbb{Z}^+$. □

I.2.17 Join of Abelian Groups.

Hint$(2/5)$: Use Theorem-I.2.8. In general $H_1 \vee \cdots \vee H_n = H_1 \cdots H_n$ in an abelian group.

Let G be an abelian group and let H,K be subgroups of G. Show that the join $H \vee K$ is the set $\{ab \mid a \in H, b \in K\}$. Extend this result to any finite number of subgroups of G.

Proof: Denote the set $\{ab \mid a \in H, b \in K\}$ by HK. Since $e \in H$ and $e \in K$, the elements $ae = a$ and $eb = b$ are in HK for all $a \in H$, $b \in K$. Thus HK contains H and K. Now given any element generated by $H \cup K$, we know by Theorem-I.2.8 that every element in the join is of the form $a_1^{n_1} \cdots a_t^{n_t}$, with $a_i \in H \cup K$, $n_i \in \mathbb{Z}$. But we know G to be abelian so we may commute all the elements so that we begin with all the elements in H and end with the elements in K. That is $(a_{i_1}^{n_{i_1}} \cdots a_{i_j}^{n_{i_j}})(a_{i_{j+1}}^{n_{i_{j+1}}} \cdots a_{i_t}^{n_{i_t}})$ where $a_{i_k} \in H$ for all $1 \le k \le j$ and in K otherwise. So every element in $H \vee K$ is of the form ab, where $a \in H$ and $b \in K$. Thus $H \vee K \subseteq HK$.

Finally every element $ab \in HK$ is a finite product of powers of the generators $H \cup K$, so $HK \subseteq H \vee K$ by the Theorem-I.2.8. Therefore $HK = H \vee K$.

Now suppose we have a finite collection of subgroups $H_1, \ldots, H_n$ of G. Since multiplication is associative, $H_1 \cdots H_n = (H_1 \cdots H_{n-1})H_n$, as the elements $a_1 \cdots a_n = (a_1 \cdots a_{n-1})a_n$. Suppose $H_1 \cdots H_n = H_1 \vee \cdots \vee H_n$ for some $n \in \mathbb{Z}^+$. Then $H_1 \cdots H_{n+1} = (H_1 \cdots H_n)H_{n+1} = (H_1 \vee \cdots \vee H_n)H_{n+1} = (H_1 \vee \cdots \vee H_n) \vee H_{n+1}$. Finally $\langle \bigcup_{i=1}^n H_i \rangle \vee H_{n+1}$ is defined as $\langle (\bigcup_{i=1}^n H_i) \cup H_{n+1} \rangle$ Which is simply $H_1 \vee \cdots \vee H_{n+1}$. Therefore by induction, $H_1 \vee \cdots \vee H_n = H_1 \cdots H_n$, for all $n \in \mathbb{Z}^+$. □

I.2.18 Join of Groups.

Hint$(2/5)$: Demonstrate the family of subgroups must contain its least upper bound with respect to set inclusion.

(a) Let G be a group and $\{H_i \mid i \in I\}$ a family of subgroups. State and prove a condition that will imply that $\bigcup_{i \in I} H_i$ is a subgroup, that is, that $\bigcup_{i \in I} H_i = \langle \bigcup_{i \in I} H_i \rangle$.

(b) Give an example of a group G and a family of subgroups $\{H_i \mid i \in I\}$ such that $\bigcup_{i\in I} H_i \neq \langle \bigcup_{i\in I} H_i \rangle$.

(a) **Proof:** Consider the family of subgroups $\{H_i \mid i \in I\}$ to contain its least upper bound, H, by set theoretic inclusion. Therefore $H = \bigcup_{i\in I} H_i$, since $H = H_i$ for some $i \in I$. Since H is in the family it was assumed to be a subgroup, and since it is the least upper bound it is the join; that is, $\bigcup_{i\in I} H_i = \langle \cup_{i\in I} H_i \rangle$. □

(b) **Example:** Take the subgroups $\langle 3 \rangle = \{0, 3\}$ and $\langle 2 \rangle = \{0, 2, 4\}$ of $\mathbb{Z}_6$. Their union is $\{0, 2, 3, 4\}$ which is not a subgroup of $\mathbb{Z}_6$ because of the sum $2 + 3 = 5$, which is not in the union; the union is not closed and so it does not have a well-defined binary operation in the sum. □

I.2.19 Subgroup Lattices.

Hint$(2/5)$: Show the completeness first. The lattice property will be an immediate consequence.

(a) The set of all subgroups of a group G, partially ordered by set theoretic inclusion, forms a complete lattice (Introduction, Exercise-.7 and Exercise-.7) in which the g.l.b. of $\{H_i \mid i \in I\}$ is $\bigcap_{i\in I} H_i$ and the l.u.b. is $\langle \bigcup_{i\in I} H_i \rangle$.

(b) Exhibit the lattice of subgroups of the groups S_3, D_4^*, $\mathbb{Z}_6$, $\mathbb{Z}_{27}$, and $\mathbb{Z}_{36}$.

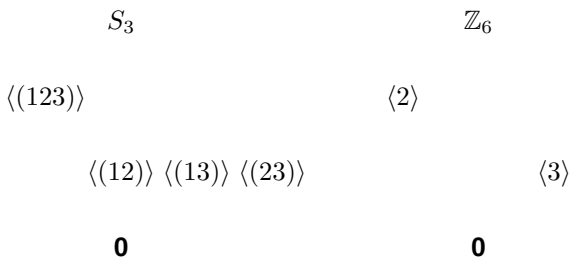
(a) **Proof:** Given any nonempty collection of subgroups $\{H_i \mid i \in I\}$, the sets $\langle \bigcup_{i\in I} H_i \rangle$ and $\bigcap_{i\in I} H_i$ are subgroups of G by Corollary-I.2.6 and Theorem-I.2.8.

Given any $S \in G$ such that $H_i \leq S$ for all $i \in I$ implies S contains the union $\bigcup_{i\in I} H_i$, and so it must contain the group generated by this union which is defined as the join. Therefore $\bigvee_{i\in I} H_i$ is the least upper bound of $\{H_i \mid i \in I\}$.

Whenever any subgroup S is contained in H_i for all $i \in I$, we know the elements of S are contained in the intersect of H_i by the set-theoretic definition of intersection. Therefore $\bigcap_{i\in I} H_i$ is the greatest lower bound of $\{H_i \mid i \in I\}$.

Therefore if we take any two subgroups H and K, $H \cap K$ is the greatest lower bound and $H \vee K$ is the least upper bound; so the collection of all subgroups forms a lattice under set-theoretic inclusion. Finally the above shows this lattice is in fact complete as every nonempty set of subgroups has both a greatest lower bound and least upper bound. □

(b) **Example:**



Let $a = R = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $b = T_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, for D_4; and $\hat{i} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $\hat{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\hat{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, and $-\hat{1} = -I$, in Q_8.

$\mathbb{Z}_8$	D_4	Q_8
$\langle 2 \rangle$	$\langle a^2, b \rangle$ $\langle a \rangle$ $\langle a^2, ab \rangle$	$\langle \hat{i} \rangle$ $\langle \hat{j} \rangle$ $\langle \hat{k} \rangle$
$\langle 4 \rangle$	$\langle b \rangle$ $\langle a^2 b \rangle$ $\langle a^2 \rangle$ $\langle ab \rangle$ $\langle a^3 b \rangle$	$\langle -\hat{1} \rangle$
0	**0**	**0**

$\mathbb{Z}_{36}$ —

$\mathbb{Z}_{27}$

$\langle 2 \rangle$ —

$\langle 3 \rangle$

$\langle 3 \rangle$ $\langle 4 \rangle$ —

$\langle 6 \rangle$

$\langle 9 \rangle$

$\langle 9 \rangle$ $\langle 12 \rangle$

$\langle 18 \rangle$

0 **0**

□

I.3 Cyclic Groups

1 Order of Elements 47
2 Orders in Abelian Groups 47
3 $\mathbb{Z}_{pq}$ 48
4 Orders under Homomorphisms 48
5 Element Orders 48
6 Cyclic Elements 49
7 PruferGroup Structure 49
8 Finite Groups 51
9 Torsion Subgroup 51
10 Infinite Cyclic Groups 52

I.3.1 Order of Elements.

Let a, b be elements of a group G. Show that $|a| = |a^{-1}|$; $|ab| = |ba|$, and $|a| = |cac^{-1}|$ for all $c \in G$.

Hint$(1/5)$: Use Theorem-I.3.4 for *both* infinite and finite order cases. Make sure a case is made that two elements of infinite order involve the same infinity (recall multiple infinite cardinals exist). Show $(cac^{-1})^n = ca^nc^{-1}$.

Proof: Consider the cyclic group generated by an element a. By Theorem-I.2.8 every element in the group is of the form a^n for some integer n; however, $a^n = (a^{-1})^{-n}$ by Theorem-I.1.9, and furthermore every integer is a negative for a unique other integer; thus $\langle a^{-1}\rangle = \langle a\rangle$ and so by Definition-I.3.3, $|a| = |a^{-1}|$.

Suppose the order, n, of ab is finite, so that $(ab)^n = e$. We re-associate the product as follows: $(ab)\cdots(ab) = a(ba)\cdots(ba)b = a(ba)^{n-1}b$. So $a(ba)^{n-1}b = e$ which implies $(ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1}$, and thus finally $(ba)^n = e$. Therefore the order of ba is less than or equal to the order of ab. However the argument is completely symmetric if we begin with the order of ba (notice this has implicitly guaranteed the order of ba is finite so we satisfy the hypothesis to begin); thus we have $|ba| \leq |ab|$ and $|ab| \leq |ba|$ so by the antisymmetry of integer ordering we know $|ab| = |ba|$.

The above proof actually states the stronger condition that if either the order of ab or ba is finite, then so is the other. Therefore if the order of one is infinite, then the other is as well. Definition-I.3.3 defines the order of an element as the order of the cyclic group generated by the element. Theorem-I.3.2 furthermore states that every infinite cyclic group is isomorphic (and thus equipollent) to the integers. Therefore $|ab| = \aleph_0 = |ba|$ even when infinite.

When $n = 0$, $(cac^{-1})^0 = e = cc^{-1} = cec^{-1} = ca^0c^{-1}$. Suppose $(cac^{-1})^n = ca^nc^{-1}$, then

$$(cac^{-1})^{n+1} = (cac^{-1})^n(cac^{-1}) = ca^nc^{-1}cac^{-1} = ca^{n+1}c^{-1};$$

therefore, $(cac^{-1})^n = ca^nc^{-1}$ for all $n \in \mathbb{N}$, by induction. Also, $(cac^{-1})^{-1} = (c^{-1})^{-1}a^{-1}c^{-1} = ca^{-1}c^{-1}$, which leads to

$$(cac^{-1})^n = (cac^{-1})^{-(-n)} = ((cac^{-1})^{-1})^n = (ca^{-1}c^{-1})^n = ca^{-(-n)}c^{-1} = ca^nc^{-1},$$

and so in general $(cac^{-1})^n = ca^nc^{-1}$ for all $n \in \mathbb{Z}$. If n is the finite order of a, then $a^n = e$ and so $(cac^{-1})^n = cec^{-1} = e$; so $|cac^{-1}| \leq |a|$. Equally important, when the order of cac^{-1} is m, $e = (cac^{-1})^m = ca^mc^{-1}$; thus $a^m = c^{-1}c = e$, so $|a| \leq |cac^{-1}|$. Once again the conditions implicitly imply that if one order is finite, then so is the other; therefore, $|a| = |cac^{-1}|$ when either has finite order. However as illustrated above, if one it infinite, then both are, and infinity here is always the first infinite cardinal $\aleph_0$; thus $|a| = |cac^{-1}|$ always. □

I.3.2 Orders in Abelian Groups.

Hint$(4/5)$: Consider $(m,n)a+b$. It may be useful to know $mn=(m,n)[m,n]$, where $[m,n]$ is the least common multiple of m and n. [6]

Let G be an abelian group containing elements a and b of orders m and n respectively. Show that G contains an element whose order is the least common multiple of m and n. [*Hint:* first try the case when $(m,n)=1$.]

Proof: Consider $(m,n)a+b$: using property (iv) of Exercise-I.1 for our abelian group,

$$[m,n]((m,n)a+b)=[m,n](m,n)a+[m,n]b=(mn)a+[m,n]b=0+0=0;$$

therefore, the order, k, of $(m,n)a+b$ divides $[m,n]$. We are assuming:

$$k((m,n)a+b)=k(m,n)a+kb=0.$$

This sets up the two cases: either $k(m,n)a=-kb$, or $k(m,n)a=kb=0$. In the first case we observe a is generated by b, and thus we know the order of a divides that of b, so the least common multiple is simply the order of b, and we take b as our required element. [7] In the second case we must conclude $n|k$ and $\frac{m}{(m,n)}|k$; therefore, $[n,\frac{m}{(m,n)}]|k$. But we notice any primes removed from m by (m,n) are replaced by their copy in n, that is, $[n,\frac{m}{(m,n)}]=[n,m]$; thus, $k=[m,n]$ and so we have $(m,n)a+b$ as our element of order $[m,n]$. □

I.3.3 $\mathbb{Z}_{pq}$.

Hint$(1/5)$: Use Exercise-I.3.

Let G be an abelian group of order pq, with $(p,q)=1$. Assume there exists $a,b\in G$ such that $|a|=p$, $|b|=q$ and show that G is cyclic.

Proof: G is abelian so from Exercise-I.3 there must exist an element of order $[p,q]$. As before we know $pq=[p,q](p,q)$ which is simply $pq=[p,q]$ in our case. Since there is an element $x\in G$, of order pq, using the Pigeon-Hole Principle, the order of the subset $\langle x\rangle$ is pq inside a group with of order pq, so $G=\langle x\rangle$. Thus G is cyclic. □

I.3.4 Orders under Homomorphisms.

Hint$(1/5)$: Use Theorem-I.3.4.

If $f:G\to H$ is a homomorphism, $a\in G$, and $f(a)$ has finite order in H, then $|a|$ is infinite or $|f(a)|$ divides $|a|$.

Proof: Suppose $|a|$ does not have infinite order. Assume n is the order of a. Therefore $a^n=e$ and as shown in the proof of Exercise-I.2, $f(e)=f(a^n)=f(a)^n$. Therefore the order of $f(a)$ divides n, by Theorem-I.3.4, part (iv). □

I.3.5 Element Orders.

Hint$(1/5)$: It is best simply to multiply and observe.

Let G be a multiplicative group of all nonsingular 2×2 matrices with rational entries. Show that $a=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ has order 4 and $b=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$ has order 3, but ab has infinite order. Conversely, show that the additive group $\mathbb{Z}_2\oplus\mathbb{Z}$ contains nonzero elements a,b of infinite order such that $a+b$ has finite order.

Example: $a^2=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=-I$, and $-I^2=(-1)^2I^2=I$. Therefore $a^4=I$ and a has order 4. Also $b^2=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}$ and from here $b^3=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, so b has order 3.

[7] Notice this is still the element $(m,n)a+b$ since in such a case $(m,n)=m$ so $(m,n)a=0$.

Now $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Suppose $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for some positive integer n. Then $(ab)^{n+1} = (ab)(ab)^n$ which is $\begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$. Therefore $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for all positive integers n. Certainly $(ab)^0 = I$ by definition, so we extend the rule for all non-negative integers. Finally $(ab)^n \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = I$ and $\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} (ab)^n = I$; therefore $(ab)^{-n} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$, for all $n > 0$. So we conclude $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for all integers n.

We take our matrices to lie in the rational 2×2 matrix space, therefore $(ab)^n = (ab)^m$ only if $m = n$. Therefore the order of ab is infinite. □

Example: Take the elements $(1,1)$ and $(0,-1)$ in $\mathbb{Z}_2 \oplus \mathbb{Z}$. Given any integer n, $n(1,1) = (n \cdot 1, n)$, so $n(1,1) = m(1,1)$ only if $m = n$, and likewise $n(0,-1) = m(0,-1)$ only when $-n = -m$, or simply $m = n$. Therefore both elements generate infinite cyclic groups, so they have infinite order by definition.

However $(1,1) + (0,-1) = (1,0)$ which clearly has order 2 since $2(1,0) = (0,0)$. □

I.3.6 Cyclic Elements.

If G is a cyclic group of order n and $k|n$, then G has exactly one subgroup of order k.

Proof: Let $G = \langle a \rangle$ be a cyclic group of order n, and let $k|n$.

Suppose an element $b \in G$ has order k. Since G is cyclic and finite, $b = a^r$ for some integer $0 \leq r < n$. From here we notice $e = b^k = (a^r)^k = a^{rk}$. By Theorem-I.3.4, part (iv), $n|rk$, that is, $nj = rk$ for some positive integer j. But we know also $k|n$ so $r = (n/k)j$.

Now we turn to the existence. Given $k|n$, clearly $s = n/k$ also divides n, so by Theorem-I.3.4, part (vii), we know $|a^s| = n/s = k$. Since a^s has order k it determines a cyclic subgroup of order k which we enumerate as follows:

$$\langle a^r \rangle = \{e, a^s, a^{2s}, \ldots, a^{(k-1)s}\}.$$

Recall above we showed any element of order k was of the form a^r where $r = (n/k)j$. Now we notice $\langle a^s \rangle$ contains all the elements of the form $a^{(n/k)j}$ so it contains each a^r; therefore, $\langle a^s \rangle$ is the unique subgroup of order k in G. □

Hint$(2/5)$: Use the Needle-in-the-Haystack Heuristic (A.1) to show all k order elements are in the same subgroup.

I.3.7 PruferGroup Structure.

Let p be prime and H a subgroup of $Z(p^\infty)$ (Exercise-I.1).

(a) Every element of $Z(p^\infty)$ has finite order p^n for some $n \geq 0$.

(b) If at least one element of H has order p^k and no element of H has order greater than p^k, then H is the cyclic subgroup generated by $\overline{1/p^k}$, whence $H \cong \mathbb{Z}_{p^k}$.

(c) If there is no upper bound on the orders of elements in H, then $H = Z(p^\infty)$; [see Exercise-I.2].

(d) The only proper subgroups of $Z(p^\infty)$ are the finite cyclic groups $C_n = \langle \overline{1/p^n} \rangle$ $(n = 1, 2, \ldots)$. Furthermore, $\langle 0 \rangle = C_0 \leq C_1 \leq C_2 \leq C_3 \leq \cdots$.

Hint$(2/5)$: Recall in Exercise-I.2 we proved $\overline{a/p^i} = a\overline{1/p^i}$. In part (e) notice G is defined in terms of equivalence classes so the case for well-defined must be explicit.

(e) Let $x_1, x_2, \ldots$ be elements of an abelian group G such that $|x_1| = p$, $px_2 = x_1$, $px_3 = x_2, \ldots, px_{n+1} = x_n, \ldots$. The subgroup generated by the $x_i (i \geq 1)$ is isomorphic to $Z(p^\infty)$. [*Hint:* Verify that the map induced by $x_i \mapsto \overline{1/p^i}$ is a well-defined isomorphism.]

Proof:

(a) Every element in $Z(p^\infty)$ is of the form $\overline{a/p^i}$ for some $i \in \mathbb{N}$. In taking the sum of a/p^i, p^i times we have $a/p^i + \cdots + a/p^i = p^i(a/p^i) = a \sim 0$; therefore, $(p^i)\overline{a/p^i} = \overline{0}$. By Theorem-I.3.4, part (iv), the order of $\overline{a/p^i}$ must therefore divide p^i, and so by Introduction, Theorem-6.6, (Euclid's Lemma) it must be p^n for some $n \geq 0$.

(b) Let H be a subgroup of G with an element $\overline{a/p^i}$ of highest order, p^k, in H. Note in $\mathbb{Q}$ that $a/p^i = \frac{a/(a,p^i)}{p^i/(a,p^i)}$ which is the reduced fraction ($(a_i, p^i) \neq 0$ since $p^i \neq 0$). So take the fraction to be in lowest terms so that $(a, p^i) = 1$. Then $(p^k)(a/p^i) \in \mathbb{Z}$ only when $i \leq k$ or $a = 0$, and the lowest power is clearly when $k = i$. Thus the order of the reduced fraction form $\overline{a/p^i}$ is p^i, so we know write $\overline{a/p^k}$.

Notice $\overline{a/p^k} = a\overline{1/p^k}$ and we also know $(a, p^k) = 1$, so by Theorem-I.3.6, $\overline{a/p^k}$ is a generator of $\langle\overline{1/p^k}\rangle$ and therefore H contains the subgroup $\langle\overline{1/p^k}\rangle$. Now given any element $\overline{b/p^i}$, it must by assumption have an order less than p^k, and so by part (a), one that divides p^k. So we may take b/p^i to be in lowest terms and then $i \leq k$. Therefore $\overline{b/p^i} = \overline{bp^{k-i}/p^k} = bp^{k-i}\overline{1/p^k}$. Therefore every element in H is generate by $\overline{1/p^k}$ so it is cyclic and furthermore of order p^k.

By Theorem-I.3.2 every proper subgroup is isomorphic to Z_{p^k}.

(c) Suppose there is no upper bound on the order of elements in H. We know from Exercise-I.2 that $Z(p^\infty)$ is generated by $\{\overline{1/p^k} \mid k \in \mathbb{N}\}$. Given any element (expressed in lowest terms) $\overline{a/p^i}$ in H, we know H contains $\overline{1/p^i}$. Since H has no upper bound on orders, and each element has finite order, then H must contain an infinite number of increasingly higher order elements. We make a chain of these elements by ordering them according to their order and take only the generator $\overline{1/p^i}$ of each order represented. However by part (b) we know a generator $\overline{1/p^i}$ generates all elements of an equal or lesser order. Thus our chain generates all lower order elements. And since our chain can have no top element, because no element has infinite order, it must eventually contain every generator of the form $\overline{1/p^i}$, for $i \in \mathbb{N}$. Thus $H = Z(p^\infty)$.

(d) In part (b) we see C_i contains all C_j, where $j \leq i$. Suppose $C_0 \leq C_1 \leq \cdots \leq C_n$ for some n. Then C_{n+1} contains this whole chain so $C_0 \leq C_1 \leq \cdots \leq C_n \leq C_{n+1}$. Therefore through induction $C_0 \leq C_1 \leq \cdots \leq C_n \leq \cdots$. By part (b) any subgroup that is finite must have a maximum order element, and so it is a C_n for some n. If a subgroup is infinite it must have an infinite number of distinct elements. Since each element has finite order, the number of these must be unbounded in our infinite subgroup; therefore, it is the entire group by part (c). Thus every proper subgroup is C_n for some $n \in \mathbb{N}$.

(e) Assume $G = \langle x_1, x_2, \ldots\rangle$ has the required properties and define the map $f : G \to Z(p^\infty)$ so that $x_i \mapsto \overline{1/p^i}$. First we notice x_i is equivalent to $p^n x_{i+n}$ so we must verify its image also equal:

$$\overline{1/p^i} = f(x_i) = f(p^n x_{i+n}) = p^n f(x_{i+n}) = p^n\overline{1/p^{(i+n)}} = \overline{p^n/p^{(i+n)}} = \overline{1/p^i};$$

therefore, f is well-defined on the generators. First we notice from Theorem-I.2.8, every element in G is a finite sum of multiples of x_i, that is,

$$x = \sum_{i=1}^{k} n_i x_i = \sum_{i=1}^{k} n_i \cdot p^{k-i} x_k = a x_k,$$

where a is some integer. So take the canonical generalization f to be

$$f(x) = f(a x_k) = a f(x_k) = a\overline{1/p^k} = \overline{a/p^k}.$$

Since f is well-defined on the generators and generalized accordingly it is well-defined.

Now evaluate a sum across the map:

$$\begin{aligned} f(ax_i) + f(bx_j) &= \overline{a/p^i} + \overline{b/p^j} = \overline{(ap^j + bp^i)/p^{i+j}} \\ &= f((ap^j + bp^i)x_{(i+j)}) = f(ap^j x_{(i+j)} + bp^i x_{(i+j)}) \\ &= f(ax_i + bx_j); \end{aligned}$$

therefore, f is a homomorphism.

Given any $\overline{a/p^i} \in Z(p^\infty)$, we know $\overline{a/p^i} = f(ax_i)$; therefore, $f(G) = Z(p^\infty)$ making f surjective.

Before continuing, we say ax_i is in reduced terms if $p^j \nmid a$ for any $j > 0$, in this way $ax_i \neq bx_j$ for any other b or j, and every element has such a reduced form. Finally, $f(x_i) = f(x_j)$ implies $1/p^i \sim 1/p^j$ and so $i = j$ which requires $x_i = x_j$. So in general, two reduced elements ax_i, and bx_j, with the property $f(ax_i) = f(bx_j)$, implies $a/p^i \sim b/p^j$, and each fraction is in lowest terms; therefore, $i = j$ and $a = b$, so $ax_i = bx_j$.

□

I.3.8 Finite Groups.

A group that has only a finite number of subgroups must be finite.

Hint$(2/5)$: Prove the statement in the contrapositive.

Proof: Suppose a group G is infinite. Therefore G has an infinite number of elements. Introduction, Theorem-8.8, ensures there are at least countably many elements in G which we enumerate $\{a_i \mid i \in \mathbb{N}\} \subseteq G$, where $a_i = a_j$ if and only if $i = j$.

Each element generates a subgroup $\langle a_i \rangle$ of G. For each subgroup $\langle a_i \rangle$ we have two options: it is infinite, or it is finite. If any such subgroup is infinite then it is isomorphic to $\mathbb{Z}$ which we saw in Exercise-I.2 has the infinite list of subgroups $m\mathbb{Z}$ for each $m \in \mathbb{Z}$; therefore no such case can exist.

Therefore we require G have no infinite cyclic subgroups, that is, that every element has finite order. Once again consider the subgroups $\langle a_i \rangle$. These subgroups are a subset of the lattice of subgroups of G (see Exercise-I.2) and therefore they are partially ordered. If they have either an infinite chain, or an infinite number of finite chains, there are infinitely many subgroups. Therefore suppose that there are only a finite number of chains and that each is finite.

This requires that an infinite number of elements be packaged in a finite number of subgroups all of which are finitely generated. A finite number of finite sets has only a finite number of elements; therefore, this last case cannot be. So G must have an infinite number of elements. □

I.3.9 Torsion Subgroup.

If G is an abelian group, then the set T of all elements of G with finite order is a subgroup of G. [Compare Exercise-I.3.]

Proof: Adopt an additive notation throughout the proof.

The zero element has order 1 trivially; thus T is never empty. Given two torsion elements $a, b \in T$, with $|a| = m$ and $|b| = n$, consider their sum. Since $mn(a+b) = (mn)a + (mn)b = n(ma) + m(nb) = 0$ (notice the implicit use of Exercise-I.1 part (iv) which is where abelian comes into play) we see that $a+b$ is a torsion element, $a+b \in T$, so T is closed. Finally by Exercise-I.3 we know $|a| = |-a|$, so T is closed to inverses. Therefore T is a subgroup of G by Theorem-I.2.5. □

Hint$(1/5)$: Co
vious exercises
and Exercise-I
subgroup of all
is called the To

I.3.10 Infinite Cyclic Groups.

Hint$(2/5)$: Use Exercise-I.2 and Theorem-I.3.2.

An infinite group is cyclic if and only if it is isomorphic to each of its proper subgroups.

Proof: ($\Rightarrow$) Suppose G is an infinite cyclic group then by Theorem-I.3.2 it is isomorphic to $\mathbb{Z}$. Exercise-I.2 shows the groups $m\mathbb{Z}$ are subgroups of $\mathbb{Z}$ which are furthermore isomorphic to $\mathbb{Z}$. Consider any subgroup $H \neq \mathbf{0}$ of $\mathbb{Z}$. By Theorem-I.3.1 we know $H = \langle m \rangle = \{mk \mid k \in \mathbb{Z}\} = m\mathbb{Z}$, where m is the least positive integer in H. Therefore every proper subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$, for $m \in \mathbb{Z}$, $m \neq 0, \pm 1$. Since every infinite cyclic group is isomorphic to $\mathbb{Z}$ they have, by Exercise-I.2 and Exercise-I.2, the same lattice of subgroups. Therefore every infinite cyclic subgroup is isomorphic to each of its proper subgroups.

($\Leftarrow$) Suppose G an infinite group isomorphic to each of its proper subgroups. In order to have a bijection, let alone an isomorphism, between G and a subgroup H of G, H must also be infinite. Given any element $a \in G$, we know the group $\langle a \rangle$ to be a subgroup of G. Assume $a \neq e$, then either $\langle a \rangle$ is a proper subgroup of G, or $G = \langle a \rangle$. This last case admits G is cyclic so it does not need to be pursued. Assume then that $\langle a \rangle$ is a proper subgroup of G. The assumption that G is isomorphic to each proper subgroup thus states $G \cong \langle a \rangle$. Take $f : \langle a \rangle \to G$ to be the isomorphism. In Exercise-I.2 we showed $f(a)$ determines the whole map and so since f is surjective (in fact bijective), $\langle f(a) \rangle = G$. Therefore G is cyclic. □

I.4 Cosets and Counting

1 Cosets . . . 53
2 Non-normal Subgroups . . . 53
3 p-groups . . . 54
4 Little Theorem of Fermat . . . 54
5 Groups of Order 4 . . . 55
6 Join . . . 55
7 p-group Complex . . . 56
8 HK-subgroup . . . 56
9 Subgroups and the Complex . . . 57
10 Identifying Subgroups . . . 57
11 Groups of order $2n$ . . . 57
12 Join and Intersect . . . 58
13 pq-groups . . . 58
14 Quaternion Presentation . . . 58

I.4.1 Cosets.

Let G be a group and $\{H_i \mid i \in I\}$ a family of subgroups. Then for any $a \in G$, $(\bigcap_i H_i)a = \bigcap_i H_i a$.

Proof: Given any element h of $\bigcap_{i\in I} H_i$, h is in each H_i by definition, therefore $ha \in (\bigcap_{i\in I} H_i)a$ is an element of $H_i a$ for each $i \in I$. Therefore $(\bigcap_{i\in I} H_i)a \subseteq \bigcap_{i\in I} H_i a$.

Take any element k from $\cap_{i\in I} H_i a$. Since k is in each $H_i a$, it follows for each $i \in I$, there exists an $h_i \in H_i$ such that $k = h_i a$. Therefore $h_i a = h_j a$ for all $i, j \in I$. But this requires $h_i = h_j$ by cancellation. Therefore there exists a unique $h \in \bigcap_{i\in I} H_i$ such that $k = ha$. Thus $(\bigcap_{i\in I} H_i)a \subseteq \bigcap_{i\in I} H_i a$.

Therefore $(\bigcap_{i\in I} H_i)a = \bigcap_{i\in I} H_i a$. □

Hint$(1/5)$: Make sure to prove every element in $\bigcap_{i\in I} H_i a$ has the form ha for some well-defined element h.

I.4.2 Non-normal Subgroups.

(a) Let H be the cyclic subgroup (of order 2) of S_3 generated by $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$. Then no left coset of H (except H itself) is also a right coset. There exists $a \in S_3$ such that $aH \cap Ha = \{a\}$.

(b) If K is the cyclic subgroup (of order 3) of S_3 generated by $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, then every left coset of K is also a right coset of K.

Example: The subgroup $H = \langle(12)\rangle$ in S_3 is not normal. The following are the left cosets of the subgroup:

$$\{\{\varepsilon, (12)\}, \{(13), (123)\}, \{(23), (132)\}\},$$

and these next are the right cosets:

$$\{\{\varepsilon, (12)\}, \{(13), (132)\}, \{(23), (123)\}\}.$$

Hint$(1/5)$: Refer to Exercise-I.2 for the subgroup lattice of S_3 which may be helpful.

Therefore since all nontrivial left cosets (although it is sufficient that only one fail) are not equal to their right cosets, H is not normal. Furthermore $(13)H \cap H(13) = \{(13)\}$ and also $(23)H \cap H(23) = \{(23)\}$.

However the subgroup $K = \langle(123)\rangle$ is normal in S_3 as seen with the cosets (left, then right):

$$\{\{\varepsilon, (123), (132)\}, \{(12), (23), (13)\}\},$$

$$\{\{\varepsilon, (123), (132)\}, \{(12), (13), (23)\}\}.$$

Since each left coset equals its right coset, $K \trianglelefteq S_3$. □

I.4.3 p-groups.

Hint$(2/5)$: Use the Theorem of Lagrange.

The following conditions on a finite group G are equivalent.

(i) $|G|$ is prime.

(ii) $G \neq \langle e\rangle$ and G has no proper subgroups.

(iii) $G \cong \mathbb{Z}_p$ for some prime p.

Proof: Suppose G has prime order p. Since we do not allow 1 to be prime (otherwise nothing would have unique factorization since $1 = 1 \cdot 1$) we know $G \neq$ **0**. Given any subgroup $H \leq G$, by the Theorem of Lagrange (Corollary-I.4.6) it follows $|G| = [G : H]|H|$, and thus the order of H divides the order of G. However $n|p$ if and only if $n = 1$ or p by the very definition of prime numbers. When $n = 1$ then H is forced to be the trivial subgroup **0**. When $n = p$, the order of H matches the finite order of G so by the Pigeon-Hole-Principle $H = G$. Therefore G has no proper subgroups. $(i) \Rightarrow (ii)$.

Suppose G is a finite nontrivial group with no proper subgroups. Given any element $a \in G$, the group generated by a is a subgroup of G and so $\langle a\rangle =$ **0** or G. If $a \neq e$ then $\langle a\rangle$ contains a and so it has an order greater than 1; thus $\langle a\rangle = G$. Since G is nontrivial there exists such an element $a \neq e$, so G is cyclic.

By Theorem-I.3.2, G is isomorphic to a group $\mathbb{Z}_m$ for some positive integer m. Since the order of $\mathbb{Z}_m$ is m, the order of G must be m. Given any composite number m, there exists a $k|m$, $k \neq m$, $k \neq 1$. Therefore by Theorem-I.3.4, a^k is an element of order $m/k \neq 1, m$. Thus the subgroup $\langle a^k\rangle$ is a proper subgroup of G, which is a contradiction. Therefore m may not be composite. Therefore $G \cong \mathbb{Z}_p$ for some prime p. $(ii) \Rightarrow (iii)$.

If $G \cong \mathbb{Z}_p$ for some prime p, then G has the same order of $\mathbb{Z}_p$ which is the prime p. Thus $(iii) \Rightarrow (i)$.

Therefore (i), (ii), and (iii) are equivalent. □

I.4.4 Little Theorem of Fermat.

Hint$(2/5)$: What must the order of every element of $\mathbb{Z}_p^\times$ divide?

Let a be an integer and p a prime such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod p$. [*Hint:* Consider $\overline{a} \in \mathbb{Z}_p$ and the multiplicative group of nonzero elements of $\mathbb{Z}_p$; see Exercise-I.1.] It follows that $a^p \equiv a \pmod p$ for any integer a.

Proof: For every integer $a \in \mathbb{Z}$ for which $p \nmid a$, it follows $a \neq 0 \pmod p$. Exercise-I.1 demonstrates all such nonzero integers form a multiplicative group, mod p, called $\mathbb{Z}_p^\times$, which furthermore has order $p - 1$. Therefore by the Theorem of Lagrange, every element in $\mathbb{Z}_p^\times$ must have an order dividing $p-1$. Recall the identity is now multiplicative and so it is the equivalence class of 1. Thus we have, for all a such that $p \nmid a$, then $\overline{a} \in \mathbb{Z}_p^\times$ and therefore $a^{|a|} \equiv 1 \pmod p$.

However since $|a|$ divides $p-1$, by Theorem-I.3.4, $a^{p-1} \equiv 1 \pmod{p}$.

Notice if we use the result of Exercise-I.2, part (c), we know the automorphisms of $\mathbb{Z}_m$ are isomorphic to the multiplicative group of all cyclic generators of $\mathbb{Z}_m$, denoted $\mathbb{Z}_m^\times$. Armed with Theorem-I.3.6 we now know an element $\bar{a}$ of $\mathbb{Z}_m$ is a cyclic generator if and only if $(a,m)=1$. Therefore the order of the $\mathbb{Z}_m^\times$ is equal to the number of integers between 1 and m that are relatively prime to m. This is defined as the *Euler-φ Function.* Thus as above, the order of each element in $\mathbb{Z}_m^\times$ must divide $\varphi(m)$. Therefore $a^{\varphi(m)} \equiv 1 \pmod{m}$ for all a and m such that $(a,m)=1$. □

I.4.5 Groups of Order 4.

Prove that there are only two distinct groups of order 4 (up to isomorphism), namely $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. [*Hint:* By Lagrange's Theorem-I.4.6 a group of order 4 that is not cyclic must consist of an identity and three elements of order 2.]

Hint$(2/5)$: Refer to Exercise-I.2 and use the given hint.

Example: In Exercise-I.2 we demonstrated that $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ are not isomorphic. Therefore there are at least to groups of order 4. Theorem-I.3.2 strictly states any cyclic group of order 4 must be isomorphic to $\mathbb{Z}_4$; thus only one group of this from exists. So let us assume G is a group of order 4 which is not cyclic.

By the Theorem of Lagrange, every element in G must have an order dividing 4. Since G is not to be cyclic, no element in G may have order 4, or else by the Pigeon-Hole-Principle it would generate all of G forcing G to be cyclic. Therefore each element must have order 1 or 2. Since an element of order 1 has the property $a = a^1 = e$, then only one element, the trivial element, may have order 1. So we resolve this by stating G has one element of order 1, e, and three elements of order 2: a, b, c. If we recall Exercise-I.1 we now know G is abelian, since all its elements are involutions; this simplifies our check for a homomorphism. We note $ab \neq a$ or b, as otherwise $a = e$ or $b = e$; nor does $ab = e$, or otherwise $a = b^{-1} = b$; thus $ab = c$ as it is all that is left.

Define a map $f : \mathbb{Z}_2 \oplus \mathbb{Z}_2 \to G$ as follows:

$$f(0,0) = e; f(1,0) = a; f(0,1) = b; f(0,0) = c.$$

The mapping is well-defined as each domain has a unique image, and it is also bijective as the inverse map is evident. Now we need only check for the homomorphism property:

$$\begin{aligned}
f((0,0)+(x,y)) &= f(x,y) = ef(x,y) = f(0,0)f(x,y)\\
f((1,0)+(0,1)) &= f(1,1) = c = ab = f(1,0)f(0,1)\\
f((0,1)+(1,1)) &= f(1,0) = a = cb^{-1} = bc = f(0,1)f(1,1)\\
f((1,0)+(1,1)) &= f(0,1) = b = ca^{-1} = ac = f(1,0)f(1,1)
\end{aligned}$$

and the rest of the sums are valid by the commutativity. Therefore f is a homomorphism which is bijective, so $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. □

I.4.6 Join.

Let H, K be subgroups of a group G. Then HK is a subgroup of G if and only if $HK = KH$.

Hint$(3/5)$: Consider how in Exercise-I.2, the abelian property of G was used. Does $HK = KH$ replace the need for this property?

Proof: ($\Rightarrow$) Let HK be a subgroup of G. It must therefore be closed to inverses. For every group we know for every element $g \in G$, g is the inverse of another element, in fact of the element g^{-1}, so $G = \{g^{-1} \mid g \in G\}$. Therefore:

$$\begin{aligned} HK &= \{hk \mid h \in H, k \in K\} = \{h^{-1}k^{-1} \mid h \in H, k \in K\} \\ &= \{(kh)^{-1} \mid h \in H, k \in K\} = \{kh \mid k \in K, h \in H\} \\ &= KH. \end{aligned}$$

($\Leftarrow$) Let $HK = KH$. Since $e \in H$ and $e \in K$, we know $e \in HK$, so HK is nonempty. Given any $hk, h'k' \in HK$, the product $(hk)(h'k') = h(kh')k'$. But since $HK = KH$, for every kh' there exists $h'' \in H$ and $k'' \in K$ such that $kh' = h''k''$, and substituting we see: $(hk)(h'k') = h(h''k'')k' = (hh'')(k''k')$. Since H and K are subgroups, they are closed to products; therefore, $hh'' = i \in H$, and $k''k' = j \in K$, so $(hk)(h'k') = ij \in HK$. Therefore HK is closed to products.

Finally given $hk \in HK$, $(hk)^{-1} = k^{-1}h^{-1}$ which is an element of KH. But $KH = HK$ so it is in fact an element of HK. Therefore HK is closed to inverses. So HK is a subgroup of G. □

I.4.7 p-group Complex.

Hint$(3/5)$: Follows from Theorem-I.4.7.

Let G be a group of order $p^k m$, with p prime and $(p, m) = 1$. Let H be a subgroup of order p^k and K a subgroup of order p^d, with $0 < d \leq k$ and $K \not\subseteq H$. Show that HK is not a subgroup of G.

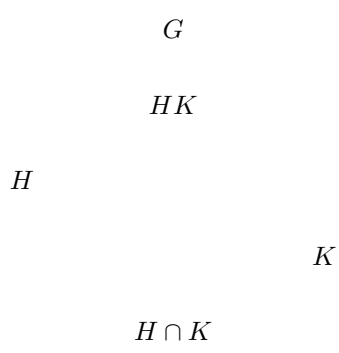
Proof: Given $|H| = p^k$ and $|K| = p^d$, it follows both are finite subgroups of G so Theorem-I.4.7 applies: $|HK| = |H||K|/|H \cap K|$. Since K is not completely contained in K it follows $H \cap K$ has an order less than p^d. The intersect is a subgroup of H and K so by the Theorem of Lagrange its order must divide that of H and K. Since the order order of K is $p^d \leq p^k$ we are concerned only that it divide p^d. Since it must be less than p^d, there exits a $0 \leq c < d$ such that $|H \cap K| = p^c$. Therefore we have $|HK| = (p^k p^d)/p^c = p^{k+d-c}$. Since $c < d$ it follows $k < k + d - c$. Therefore the order of HK, if it is a group, is a power of p greater than k. However k is the largest integer for which p^k divides the order of G. Therefore by the Theorem of Lagrange, HK cannot be a subgroup of G since its order would not divide G. □

I.4.8 HK-subgroup.

Hint$(5/5)$: Notice $[G : K][K : H \cap K] = [G : H][H : H \cap K]$.

If H and K are subgroups of finite index of a group G such that $[G : H]$ and $[G : K]$ are relatively prime, then $G = HK$.

Proof: We let $[G : K] = k$, $[G : H] = h$, $[H : H \cap K] = i$, and $[K : H \cap K] = j$. Then we have the following subset lattice (notice the labels on the lines indicate the index of the lesser in the greater):



$H \cap K$ is a subgroup in G. Furthermore both $[G : H]$ and $[G : K]$ are finite indices, so by the Lemma of Poincaré (Proposition-I.4.9) we know $[G : H \cap K] \leq [G : H][G : K]$ and is therefore finite. From the Theorem of Lagrange (Theorem-I.4.5) we know: $[G : H][H : H \cap K] = [G : H \cap K] = [G : K][K : H \cap K]$, which are all finite products.

We must resolve when $hi = kj$ knowing $(h, k) = 1$. Since h and k are relatively prime it follows $h|j$ and $k|i$, so $h \leq j$ and $k \leq i$. But by Proposition-I.4.8 we see $j = [K : H \cap K] \leq [G : H] = h$ and likewise $i \leq k$. Therefore $i = k$ and $j = h$. Finally Proposition-I.4.8 concludes since $[H : H \cap K] = [G : K]$ then $G = HK$. □

I.4.9 Subgroups and the Complex.

Hint$(2/5)$: Show $HN = N$.

If H, K and N are subgroups of G such that $H \leq N$, then $HK \cap N = H(K \cap N)$.

Proof: We begin by showing $H(K \cap N) = HK \cap HN$:

$$H(K \cap N) = \{hy \mid h \in H, y \in K \cap N\} = \{hx \mid h \in H, x \in K, y \in N, x = y\}$$

before continuing notice that $hx = hy$ if and only if $x = y$ by cancellation, therefore:

$$\begin{aligned} H(K \cap N) &= \{hx = hy \mid h \in H, x \in K, y \in N\} \\ &= \{hk \mid h \in H, k \in K\} \cap \{hn \mid h \in H, n \in N\} \\ &= HK \cap HN. \end{aligned}$$

Observe $e \in H$ so $N \subseteq HN$, but since $H \leq N$, $HN \subseteq N$, so again $N = HN$;

$$H(K \cap N) = HK \cap HN = HK \cap N.$$

□

I.4.10 Identifying Subgroups.

Hint$(4/5)$: Notice the proof of Proposition-I.4.8 constructs a map from all left cosets of $H \cap K$ into the left cosets of K in G. Show this map is always onto the left cosets of K in HK, even if HK is not a subgroup. Then the proposition actually states $[H : H \cap K] = [HK : K]$ where $[HK : K]$ is the number of left cosets of K in HK.

Let H, K, N be subgroups of a group G such that $H \leq K$, $H \cap N = K \cap N$, and $HN = KN$. Show $H = K$.

Proof: First expand the proof of Proposition-I.4.8. For convenience denote all left cosets of B in A as A/B. Use the same definition of $\varphi : H/H \cap K \to G/K$ as $h(H \cap K) \mapsto hK$. φ was previously shown to be well-defined. Suppose $\varphi(h(H \cap K)) = \varphi(h'(H \cap K))$ for some arbitrary elements $h, h' \in H$. Thus $hK = h'K$ and so $h'h^{-1}K = K$, or simply $h'h^{-1} \in K$. Since H is a subgroup it contains $h'h^{-1}$ and so $h'h^{-1} \in H \cap K$, which is equivalent to stating: $h(H \cap K) = h'(H \cap K)$. Therefore φ is injective. Now restrict the image to the set HK/K, and since we do not require HK/K to be a group we will not need HK to be a group either. Every left coset in HK/K is of the form $(hk)K = hK$, for some $h \in H$; therefore, $(hk)K = \varphi(h(H \cap K))$. So φ is surjective onto HK/K. Therefore if we define $[HK : K] = |HK/K|$ then we have in fact shown $[H : H \cap K] = [HK : K]$.

This facilitates our proof since $HN = KN$ and so:

$$[H : H \cap N] = [HN : N] = [KN : N] = [K : K \cap N].$$

But also $H \cap N = K \cap N$ we furthermore know (using the Theorem of Lagrange):

$$[K : H][H : H \cap N] = [K : H \cap N] = [K : K \cap N] = [H : H \cap N];$$

thus $[K : H] = 1$ (by Exercise-.8), so $K = H$. □

I.4.11 Groups of order $2n$.

Hint$(2/5)$: Use Exercise-I.1

Let G be a group of order $2n$; then G contains an element of order 2. If n is odd and G is abelian, there is only one element of order 2.

Proof: In Exercise-I.1 we proved G has an element of order 2. Now suppose n is odd and that G is abelian.

Suppose $a, b \in G$ are both elements of order 2. They both generate groups $\langle a \rangle$ and $\langle b \rangle$. Since G is abelian we may use Exercise-I.2 to show $H = \langle a, b \rangle = \{ma + nb \mid m, n \in \mathbb{Z}\}$. Since we have the order of the two elements fixed at 2, we in deed generate a group: $H = \{0, a, b, a + b\}$. By assumption $a \neq b$ and since both have order 2 neither equals 0. Suppose $a + b = e$, then $a = -b = b$; if $a + b = a$, then $b = 0$; and lastly when $a + b = b$, $a = 0$ – all of which are contradictions of our assumptions. Therefore $a + b$ is a distinct element and H has order 4. However since n is odd it follows $4 \nmid 2n$ so H cannot be a subgroup because it would violate the Theorem of Lagrange. Therefore G has a unique element of order 2. □

Example: S_3 has order $2 \cdot 3$ and in fact it has elements of order 2: (12), (13), and (23). However S_3 is not abelian so there is not a unique element of order 2. □

I.4.12 Join and Intersect.

Hint$(2/5)$: Use the product of the hint for Exercise-I.4.

If H and K are subgroups of a group G, then $[H \vee K : H] \geq [K : H \cap K]$.

Proof: Given any element $hk \in HK$, the element is in a finite product of the generators of $H \vee K$, so by Theorem-I.2.8 it must be included in $H \vee K$; so in fact $HK \subseteq H \vee K$. Now we know from Exercise-I.4 that $[K : H \cap K] = [HK : H]$, and the cosets of H in $H \vee K$ must contain all the cosets of H in HK since the complex is a subset of the join; therefore, $[HK : H] \leq [H \vee K : H]$; thus $[K : H \cap K] \leq [H \vee K : H]$. □

I.4.13 pq-groups.

Hint$(1/5)$: Use the hint provided.

If $p > q$ are primes, a group of order pq has at most one subgroup of order p. [*Hint:* Suppose H, K are distinct subgroups of order p. Show $H \cap K = \mathbf{0}$; use Exercise-I.4 to get a contradiction.]

Proof: Suppose that H and K are distinct subgroups G of order p. The intersection $H \cap K$ is a subgroup of both H and K and therefore by the Theorem of Lagrange its order must divide p. Since p is a prime this forces $H \cap K$ to have order 1 or order p. We assumed H and K were distinct therefore the order of $H \cap K$ cannot be p or else by the Pigeon-Hole-Principle we would have $H \cap K = H = K$. Therefore $H \cap K = \mathbf{0}$.

Now using Exercise-I.4, we see $[K : H \cap K] = |K| = p \leq [H \vee K : H]$ and therefore $|H \vee K|/p \geq p$, which implies $|H \vee K| \geq p^2$. However $pq < p^2$ since $p < q$, and thus $H \vee K$ is greater than the group that contains it, which is impossible. Therefore there cannot be two distinct groups of order p. □

I.4.14 Quaternion Presentation.

Hint$(2/5)$: Notice (iii) gives a normal form.

Let G be a group and $a, b \in G$ such that (i) $|a| = 4 = |b|$; (ii) $a^2 = b^2$; (iii) $ba = a^3b = a^{-1}b$; (iv) $a \neq b$; (v) $G = \langle a, b \rangle$. Show that $|G| = 8$ and $G \cong Q_8$. (See Exercise-I.2; observe that the generators A, B of Q_8 also satisfy (i)-(v).)

Proof: The presentation given for Q_8 always determines a group. What is required is that Q_8 have order 8, and that it be the only group with this presentation of that order.

To show this first we construct a maximal set of elements of which Q_8 must be a subset. Given $ba = a^{-1}b$ we may assume a normal form for all elements: for all $x \in Q_8$, $x = a^i b^j$ for some $i, j \geq 0$. Now define $c = a^2 = b^2$ and notice:

$$c(a^i b^j) = a^{2+i} b^j = a^i c b^j = a^i b^{j+2} = (a^i b^j) c;$$

therefore, c is central in Q_8. The order of a is at most 4, and thus the order of b divides 4. Using the property of c notice $a^i b^3 = a^i cb = a^{2+i} b$; therefore, all elements are of the form $a^i b^j$ with $j = 0, 1$. This produces the following maximal list of elements:

$$A = \{e, a, a^2, a^3, b, ab, a^2 b, a^3 b\}.$$

Since A visibly has 8 elements, by the Pigeon-Hole-Principle in fact we see $A = Q_8$. Therefore Q_8 exists and is unique. $\square$

I.5 Normality, Quotient Groups, and Homomorphisms

1 Index 2 Subgroups 60
2 Normal Intersections 60
3 Normal and Congruence 60
4 Congruence 61
5 Normality in S_n 61
6 Conjugate Subgroups 61
7 Unique Subgroups Are Normal 62
8 Normality in Q_8 62
9 Center of S_n 62
10 Normality is Not Transitive 63
11 Normal Cyclic Subgroups 63
12 Finitely Generated 63
13 Normal Subgroup Lattice 64
14 Quotient Products 64
15 Normal Extension 65
16 Abelianization 65
17 Integer Quotients 65
18 Homomorphic Pre-image 66
19 Locating Finite Kernels 66
20 Locating Finite Subgroups 67
21 PruferQuotients 68

I.5.1 Index 2 Subgroups.

Hint$(1/5)$: Check left and right cosets agree.

If N is a subgroup of index 2 in a group G, then N is normal in G.

Proof: Suppose $[G : N] = 2$. Therefore there are only two left/right cosets. Since $e \in G$, $eN = N$, one of the left cosets must always be N. Therefore the remaining left coset must be $G - N$. Again since $Ne = N$, N is always a right coset, so the remaining right coset must be $G - N$. Therefore every left coset equals its corresponding right coset; therefore $N \trianglelefteq G$. $\square$

I.5.2 Normal Intersections.

Hint$(1/5)$: Conjugate the intersection.

If $\{N_i \mid i \in I\}$ is a family of normal subgroups of a group G, then $\bigcap_{i\in I} N_i$ is a normal subgroup of G.

Proof: Suppose $\{N_i \mid i \in I\}$ is a family of normal subgroups of G. Therefore $aN_ia^{-1} = N$ for all $a \in G$. Given any element in $ana^{-1} \in a(\bigcap_{i\in I} N_i)a^{-1}$ it follows $n \in \bigcap_{i\in I} N_i$ and so from the definition of intersection, $n \in N_i$ for all $i \in I$. Therefore $ana^{-1} \in aN_ia^{-1}$ for all $i \in I$. Together this means:

$$a(\bigcap_{i\in I} N_i)a^{-1} = \bigcap_{i\in I} aN_ia^{-1} = \bigcap_{i\in I} N_i.$$

Therefore $\bigcap_{i\in I} N_i$ is normal in G. $\square$

I.5.3 Normal and Congruence.

Let N be a subgroup of G. N is normal in G if and only if (right) congruence modulo N is a congruence relation on G.

Proof: Suppose $N \trianglelefteq G$, then it is first a subgroup of G so by Exercise-I.2 we know left congruence is an equivalence relation. Suppose $a \equiv b \pmod N$ and $c \equiv d \pmod N$.[8] Therefore ab^{-1}, cd^{-1} are in N, and furthermore $ab^{-1}e, cd^{-1}e \in N$ so $ab^{-1} \equiv cd^{-1} \equiv e \pmod N$. By substituting we see:

$$e \equiv ab^{-1} \equiv aeb^{-1} \equiv a(cd^{-1})b^{-1} \equiv (ac)(bd)^{-1} \pmod N.$$

Therefore $ac \equiv bd \pmod N$; so N is a congruence relation.

Now suppose that left congruence modulo N is a congruence relation. Take $a \in G$ and any $n \in N$. Since $ne \in N$, $n \equiv_l e \pmod N$. We know $a \equiv_l a \pmod N$ and so $an \equiv_l a \pmod N$. Therefore $(an)a^{-1} \in N$; this then ensures $aNa^{-1} \subseteq N$, which satisfies Theorem-I.5.1, part (iv); therefore, N is normal in G. □

Hint$(2/5)$: Remember in Exercise-I.2 we showed that any subgroup determines an equivalence relation. All that remains is to show it respects products (see Definition-I.4.1).

I.5.4 Congruence.

Let $\sim$ be an equivalence relation on a group G and let $N = \{a \in G \mid a \sim e\}$. Then $\sim$ is a congruence relation on G if and only if N is a normal subgroup of G and $\sim$ is a congruence module N.

Proof: ($\Rightarrow$) Suppose $\sim$ is a congruence relation on G. Given $a \in G$ and $n \in N$, $a \sim a$ – since $\sim$ is reflexive – and $n \sim e$ – by the definition of N. Since this is a congruence we further know $an \sim ae = a$. Now multiplying by inverses on the left (again since $a^{-1} \sim a^{-1}$) we obtain $ana^{-1} \sim e$. Therefore $aNa^{-1} \subseteq N$ so by Theorem-I.5.1, part (iv), N is normal in G. Furthermore, $a \sim b$ if and only if $ab^{-1} \sim e$ which is to say if and only if $ab^{-1} \in N$. Therefore $\sim$ is a congruence module N.

($\Leftarrow$) Now suppose $\sim$ is a congruence module N, where N is a normal subgroup of G. In Theorem-I.5.1 we see N is normal forces left and right congruence to agree; therefore, N determines a congruence relation on G. Furthermore, given $n \in N$, $ne = ne^{-1} \in N$; therefore, $n \sim e$. And $a \sim e$ implies $ae^{-1} = ae = a \in N$; therefore, $N = \{a \in G \mid a \sim e\}$. □

Hint$(3/5)$: Use Theorem-I.5.1.

I.5.5 Normality in S_n.

Let $N \leq S_4$ consist of all those permutation σ such that $\sigma(4) = 4$. Is N normal in S_4?

Example: In Exercise-I.2 we proved the set S_n^k – all permutations with a fixed point at k – was a subgroup of S_n. Therefore we know S_4^4 is a perfectly fine subgroup of S_4 which is in fact isomorphic to S_3. Now consider the cosets $(13)(24)S_4^4$ and $S_4^4(13)(24)$.

$$\begin{aligned}(13)(24)S_4^4 &= (13)(24)\{\varepsilon, (123), (132), (12), (13), (23)\} \\ &= \{(13)(24), (142), (234), (1423), (24), (1342)\}. \\ S_4^4(13)(24) &= \{(13)(24), (243), (124), (1324), (24), (1243)\}\end{aligned}$$

Since not every left coset of S_4^4 agrees with the right coset; S_4^4 is not normal in S_4. □

Hint$(1/5)$: No. Use Exercise-I.2 to justify N is a subgroup. Then demonstrate some left coset is not its right coset.

[8] By Theorem-I.5.1, part (i), we know the left and right labels are interchangeable.

I.5.6 Conjugate Subgroups.

Hint$(3/5)$: Show $\lambda_g : G \to G$ defined as $x \mapsto gxg^{-1}$ is an automorphism. Then use Exercise-I.2 and/or Theorem-I.5.11.

Let $H \leq G$; then the set aHa^{-1} is a subgroup of G for each $a \in G$, and $H \cong aHa^{-1}$. [9]

Proof: Let g be an arbitrary element of G. Define the map $\lambda_g : G \to G$ as $x \mapsto gxg^{-1}$. Conjugation is a well-defined product in G; therefore, λ_g is well-defined. Given any $x, y \in G$ notice $\lambda_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \lambda_g(x)\lambda_g(y)$; therefore, λ_g is a homomorphism. Furthermore, $\lambda_g(x) = e$ only when $gxg^{-1} = e$ which implies $gx = g$ or simply $x = e$. Therefore since $Ker\ \lambda_g = \mathbf{0}$, by Theorem-I.2.3, λ_g is a monomorphism. Finally, given $x \in G$, $x = (gg^{-1})x(gg^{-1}) = g(g^{-1}xg)g^{-1} = \lambda_g(g^{-1}xg)$, therefore λ_g is surjective; thus it is bijective, and so even an isomorphism, or simply an automorphism.

This result, combined with Exercise-I.2, states whenever $H \leq G$, $\lambda_g(H) = gHg^{-1}$ is also a subgroup of G. Now consider restricting λ_g to H. The restriction is well-defined and leads to a mapping $f : H \to gHg^{-1}$ defined as $f(x) = \lambda_g(x)$. f retains the injectivity of λ_g and since we have chosen as a codomain the image of H under f, f is surjective as well. Finally $f(xy) = \lambda_g(xy) = \lambda_g(x)\lambda_g(y) = f(x)f(y)$, therefore f is a bijective homomorphism – an isomorphism. □

I.5.7 Unique Subgroups Are Normal.

Hint$(2/5)$: Use Exercise-I.5.

Let G be a finite group and H a subgroup of G of order n. If H is the only subgroup of G of order n, then H is normal in G.

Proof: In Exercise-I.5 we saw that gHg^{-1} is a subgroup, isomorphic to H, of G for every $g \in G$. Therefore H and gHg^{-1} have the same order, since there exists a bijection between them. Since H is the only subgroup of order n, it follows $gHg^{-1} = H$ for all $g \in G$. Therefore, by Theorem-I.5.1, H is normal in G. □

I.5.8 Normality in Q_8.

Hint$(1/5)$: Immediate result of Exercise-I.5 and Exercise-I.5 (see Exercise-I.2).

All subgroups of the quaternion group are normal (see Exercise-I.2 and Exercise-I.4).

Example: As seen in Exercise-I.2, the subgroups of Q_8 are: **0**,$\langle -\hat{1}\rangle$, $\langle \hat{i}\rangle$, $\langle \hat{j}\rangle$, $\langle \hat{k}\rangle$, and Q_8. Both **0** and Q_8 are normal trivially as they lead to trivial partitions. The subgroups generated by $\hat{i}, \hat{j}$ and $\hat{k}$ all have index 2; so by Exercise-I.5 they are normal in Q_8. Finally $\langle -\hat{1}\rangle$ is the intersection of normal subgroups of Q_8; so by Exercise-I.5 it also is normal in Q_8. Therefore every subgroup of Q_8 is normal.

Notice that Q_8 is non-abelian. □

I.5.9 Center of S_n.

Hint$(1/5)$: Apply the definitions.

(a) If G is a group, then the center of G is a normal subgroup of G (see Exercise-I.2);

(b) the center of S_n is the identity subgroup for all $n > 2$.

[9] Notice this says if any subgroup exists that is not isomorphic to any other subgroups, then it must be normal. The converse is generally not true: consider the integers.

(a) **Proof:** From Exercise-I.2 we know C is a subgroup of G. Now given any element $g \in G$, and any $x \in C$, it follows $gx = xg$; therefore, $gC = \{gx \mid x \in C\} = \{xg \mid x \in C\} = Cg$; so by Theorem-I.5.1, part (iii), $C \trianglelefteq G$. □

(b) **Example:** Let $n > 2$ and consider the center of S_n. Since cycles are independent of each other we may test for centrality on just the elements in the cycle. Given a central element σ, pick a cycle of the element $\kappa = (a_1, \ldots, a_i)$, with $2 < i \leq n$. Next choose τ to be $\tau = (a_1, a_2)$ Then $\kappa\tau = (a_1, a_3, a_4, \ldots, a_i)$ and $\tau\kappa = (a_2, a_3, \ldots, a_i)$. This means $\kappa\tau$ leaves a_2 fixed while $\tau\kappa$ fixes a_1; therefore, κ is not central and in fact the entire permuation σ is not central as none of the disjoint cycles are.

This leaves us only the case where σ is a product of disjoint transpositions. Now consider a cycle in such an element: it must be $\kappa = (a_1, a_3)$. But since $n > 2$ we know there exists a $\tau = (a_1, a_2, a_3)$, but once again $\kappa\tau$ fixes a_1 and $\tau\kappa$ fixes a_2 only in the cycle; therefore, no non-trivial element of S_n is central when $n > 2$. □

I.5.10 Normality is Not Transitive.

Find groups H and K of D_4^* such that $H \trianglelefteq K$ and $K \trianglelefteq D_4^*$, but H is not normal in D_4^*.

Example: Notice $\langle b \rangle$ is a subgroup of index 2 in $\langle a^2, b \rangle$, and therefore by Exercise-I.5 it is normal in $\langle b, a^2 \rangle$. Likewise $\langle a^2, b \rangle$ is of index 2 in D_4, so it is normal in D_4. However $\langle b \rangle$ is not normal in D_4 because $a\langle b \rangle = \{a, ab\}$ but $\langle b \rangle a = \{a, ba = a^3b\}$. □

Hint$(1/5)$: Refer to Exercise-I.2.

I.5.11 Normal Cyclic Subgroups.

If H is a cyclic subgroup of a group G and H is normal in G, then every subgroup of H is normal in G. [Compare Exercise-I.5.]

Example: Let $H = \langle a \rangle$ be a subgroup of G and assume $H \trianglelefteq G$. Consider a subgroup K of H. Every subgroup of H is cyclic by Theorem-I.3.5, and furthermore $K = \langle a^k \rangle$ for some $k \in \mathbb{Z}^+$. So we now take $g \in G$: $gag^{-1} = a^m$ for some $m \in \mathbb{Z}$, since H is normal. It follows then that $ga^kg^{-1} = (gag^{-1})^k = (a^m)^k = (a^k)^m$. So we see $gKg^{-1} \subseteq K$, for all $g \in G$; thus $K \trianglelefteq G$ by Theorem-I.5.1 part (iv). □

Hint$(1/5)$: It may help to use the proof of Exercise-I.3 where it was shown $(gag^{-1})^k = ga^kg^{-1}$.

I.5.12 Finitely Generated.

If H is a normal subgroup of a group G such that H and G/H are finitely generated, then so is G.

Proof: Since H is normal in G, G/H is a group. By assumption there exists a finite set $X \subseteq H$ that generates H and likewise a finite set $Y' \subseteq G/H$ that generates G/H. We take a transversal of G/H and elect Y to represent Y' in the transversal, that is: $Y \subseteq G$ such that $Y' = \{yH \mid y \in Y\}$ and $y_1H = y_2H$ implies $y_1 = y_2$. We know $|Y| = |Y'|$ so we index the elements of Y for convenience.

Now every element in G/H is by definition a finite product of Y' so it has the form:

$$y_{i_1}^{j_1}H \cdots y_{i_k}^{j_k}H = (y_{i_1}^{j_1} \cdots y_{i_k}^{j_k})H$$

Hint$(4/5)$: Notice H gives a normal form to the elements of G: every element is of the from

$$y_{i_1}^{j_1} \cdots y_{i_k}^{j_k} x_{s_1}^{t_1} \cdots x_{s_u}^{t_u}$$

where the $y's$ are generators in G/H and the x's are generators in H. Since H is normal, we may group the x's together.

where each $y_{i_m} \in Y$, for $m = 1, \ldots, k$. Likewise the elements in H can be described as $x_{s_1}^{t_1} \cdots x_{s_u}^{t_u}$ where $x_{s_v} \in X$ for $v = 1, \ldots, u$. We now combine these results.

G/H is a partition of G, so $G = \bigcup_{x \in G} xH$; therefore,

$$G = \bigcup_{Y} (y_{i_1}^{j_1} \cdots y_{i_k}^{j_k})H = \bigcup_{Y} \bigcup_{X} \{y_{i_1}^{j_1} \cdots y_{i_k}^{j_k} x_{s_1}^{t_1} \cdots x_{s_u}^{t_u}\}.$$

Therefore G is generated by $Y \cup X$ which is finite. [10] □

I.5.13 Normal Subgroup Lattice.

Hint$(1/5)$: As in Exercise-I.2, show that the partial ordering is complete and the lattice will follow directly.

(a) Let $H \trianglelefteq G$, $K \trianglelefteq G$. Show that $H \vee K$ is normal in G.

(b) Prove that the set of all normal subgroups of G forms a complete lattice under inclusion (Introduction, Exercise-.7).

Proof: First, the normal subgroup partial ordering is nonempty because **0** and G are normal in G always.

Let $\{N_i \mid i \in I\}$ be a collection of normal subgroups of G. Given any $g \in G$: an element of $g(\bigvee_{i \in I} N_i)g^{-1}$ is of the form:

$$gng = gn_1^{k_1} \cdots n_j^{k_j} g^{-1} = (gn_1^{k_1} g^{-1})(gn_2^{k_2} g^{-1}) \cdots (gn_j^{k_j} g^{-1}).$$

Since each N_i is normal, $gn_i^{k_i} g^{-1} \in N_i$ for all i and all g. Therfore $gng \in \bigvee_{i \in I} N_i$, and $g(\bigvee_{i \in I} N_i)g^{-1} \subseteq \bigvee_{i \in I} N_i$. So the general join is of normal groups is normal.[11]

By Exercise-I.5 we know the that intersection of normal subgroups are normal. Therefore the partial ordering of normal subgroups is complete. Therefore the partial ordering is in fact a lattice which can be verified by taking the greatest common divisor and least common multiple of $\{N_1, N_2\}$, as guaranteed by the completeness. □

I.5.14 Quotient Products.

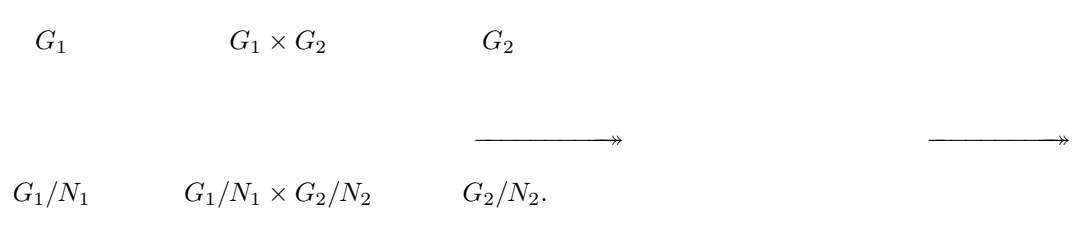
Hint$(2/5)$: Use the Fundamental Homomorphism Theorem.

If $N_1 \trianglelefteq G_1$, $N_2 \trianglelefteq G_2$ then $(N_1 \times N_2) \trianglelefteq (G_1 \times G_2)$ and $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.

Proof: Given the canonical epimorphisms $\mu_1 : G_1 \to G_1/N_1$ and $\mu_2 : G_2 \to G_2/N_2$. Using the projections of the product $G_1 \times G_2$ we obtain the functions $\mu_1\pi_1$ and $\mu_2\pi_2$ and so by the universal mapping property of product (Introduction, Theorem-5.2) there exists a map $\varphi : G_1 \times G_2 \to G_1/N_1 \times G_2/N_2$ such that $\pi_1'\varphi = \mu_1\pi_1$ and $\pi_2'\varphi = \mu_2\pi_2$. Since each is a homomorphisms, and composition of homomorphisms is a homomorphism, we know φ to be a homomorphism.

[10] Although $Y \cup X$ generates elements such as $x_1y_3x_4^7x_1y_1^{-1}$ which do not at first seem to be of the form $y \cdots yx \cdots x$, notice H is normal, so $xy = yx'$ for some $x' \in H$; thus we have a normal form theorem which allows us to group the elements of Y and X as we see in the proof.

[11] Alternately to prove just part (a), use Theorem-I.5.3, part (iii), to state $H \vee K = HK$. Thus for every element $g \in G$: $gH \vee Kg^{-1} = gHKg^{-1} = gHg^{-1}gKg^{-1} = HK$; therefore $H \vee K \trianglelefteq G$.



Now we identify the kernel of φ (recall the identity in $G_1/N_1 \times G_2/N_2$ is (N_1, N_2)): $\varphi(g,h) = (N_1, N_2)$ only if $gN_1 = N_1$ and $hN_2 = N_2$. Therefore $N_1 \times N_2$ is the kernel of φ, and so it is normal in $G_1 \times G_2$.

Also μ_1 and μ_2 are epimorphisms, as are π_1 and π_2, so their composition is an epimorphism. Since φ is defined by these two compositions, it too is an epimorphism. Therefore we now apply the Fundamental Homomorphism Theorem (Corollary-I.5.7): $G_1 \times G_2/N_1 \times N_2 \cong G_1/N_1 \times G_2/N_2$. □

I.5.15 Normal Extension.

Let $N \trianglelefteq G$ and $K \trianglelefteq G$. If $N \cap K = \mathbf{0}$ and $N \vee K = G$, then $G/N \cong K$.

Proof: Since N is normal, by Theorem-I.5.3, part (iii), $G = N \vee K = NK$. Furthermore from The Second Isomorphism Theorem (Theorem-I.5.9), we can assert

$$H \cong H/\mathbf{0} = H/N \cap K \cong NK/N = G/N.$$

□

Hint$(4/5)$: Use Theorem-I.5.9. G is said to be an extension of K by N.

I.5.16 Abelianization.

If $f : G \to H$ is a homomorphism, H is abelian and N is a subgroup of G containing $Ker\ f$, then N is normal in G.

Proof: Since H is abelian, $f(H)$ is an abelian subgroup. By the First Isomorphism Theorem $f(H) \cong G/Ker\ f$, and so it too is abelian. Thus for every $g \in G$, $n \in N$, $(gH)nH(g^{-1}H) = (gH)(g^{-1}H)nH = nH$. Therefore $(gH)(N/H)(g^{-1}H) = N/H$ and so N/H is normal in G/N. From here Corollary-I.5.12 concludes N must be normal in G since N/H is normal in $G/Ker\ f$. □

Hint$(3/5)$: Use Corollary-I.5.12.

I.5.17 Integer Quotients.

(a) Consider the subgroups $\langle 6\rangle$ and $\langle 30\rangle$ of $\mathbb{Z}$ and show $\langle 6\rangle/\langle 30\rangle \cong \mathbb{Z}_5$.

(b) For any $k, m > 0$, $\langle k\rangle/\langle km\rangle \cong \mathbb{Z}_m$; in particular, $\mathbb{Z}/\langle m\rangle = \langle 1\rangle/\langle m\rangle \cong \mathbb{Z}_m$.

Hint$(2/5)$: Use integer arithmetic.

(a) **Example:** Define a map $f : \langle 6\rangle/\langle 30\rangle \to \mathbb{Z}_5$ by $6m + 30\mathbb{Z} \mapsto m + 5\mathbb{Z}$. Whenever $6m \cong 6n \pmod{30}$ then $6(m-n) \cong 0 \pmod{30}$; therefore $5|m-n$, which implies $m \cong n \pmod 5$. Therefore f is well-defined. Moreover

$$\begin{aligned} f((6m+30\mathbb{Z}) + (6n+30\mathbb{Z})) &= f(6(m+n)+30\mathbb{Z}) = (m+n)+5\mathbb{Z} \\ &= (m+5\mathbb{Z}) + (n+5\mathbb{Z}) = f(6m+30\mathbb{Z}) + f(6n+30\mathbb{Z}); \end{aligned}$$

so f is a homomorphism.

Next suppose $f(6m+30\mathbb{Z}) \cong f(6n+30\mathbb{Z}) \pmod 5$; thus $m \cong n \pmod 5$. $5|m-n$ so in fact $30|6(m-n) = 6m-6n$; therefore $6m \cong 6n \pmod{30}$, so f is injective. Finally, given $m+5\mathbb{Z}$, there exists a $6m \in \mathbb{Z}$ and so $6m+30\mathbb{Z} \in \langle 6\rangle/\langle 30\rangle$; therefore $f(6m+30\mathbb{Z}) = m+5\mathbb{Z}$, and f is surjective; thus f is an isomorphism. □

(b) **Proof:** First note that every subgroup of an abelian group is normal. Since $\mathbb{Z}$ is cyclic it is abelian, and furthermore so are $\mathbb{Z}_m$ for any m as well as the subgroups $m\mathbb{Z}$.

Now define a map $f : \langle k\rangle/\langle km\rangle \to \mathbb{Z}_m$ by $ki + km\mathbb{Z} \mapsto i + m\mathbb{Z}$. Whenever $ki \cong kj \pmod{km}$ then $k(i-j) \cong 0 \pmod{km}$; therefore $m|i-j$, which implies $i \cong j \pmod m$. Therefore f is well-defined. Moreover

$$\begin{aligned} f((ki+km\mathbb{Z})+(kj+km\mathbb{Z})) &= f(k(i+j)+km\mathbb{Z}) = (i+j)+m\mathbb{Z} \\ &= (i+m\mathbb{Z})+(j+m\mathbb{Z}) = f(ki+km\mathbb{Z})+f(kj+km\mathbb{Z}); \end{aligned}$$

so f is a homomorphism.

Next suppose $f(ki+km\mathbb{Z})) \cong f(kj+km\mathbb{Z})) \pmod m$; thus $i \cong j \pmod m$. $m|i-j$, so in fact $km|k(i-j) = ki-kj$; therefore $ki \cong kj \pmod{km}$, so f is injective. Finally, given $i+m\mathbb{Z}$, there exists a $ki \in \mathbb{Z}$ and so $ki+km\mathbb{Z} \in \langle k\rangle/\langle km\rangle$; therefore $f(ki+km\mathbb{Z}) = i(m\mathbb{Z})$, and f is surjective; thus f is an isomorphism. □

I.5.18 Homomorphic Pre-image.

Hint$(3/5)$: Show any $NK \le S \le G$ with $K/N = S/N$ implies $KN = SN$.

If $f : G \to H$ is a homomorphism with kernel N and $K \le G$, then prove that $f^{-1}(f(K)) = KN$. Hence $f^{-1}(f(K)) = K$ if and only if $N \le K$.

Proof: Take $g : f(H) \to G/N$ to be the isomorphism guaranteed by the First Isomorphism Theorem (Corollary-I.5.7); thus $gf = \pi$, the canonical epimorphism.

We know $gf(K) = K/N$ by Corollary-I.5.12. Likewise $gf(KN) = KN/N$. Now given any $kn \in KN$, $knN = kN$. Therefore $KN/N = K/N$ in G/N. Therefore $f(K) = g^{-1}(K/N) = g^{-1}(NK/K) = f(KN)$; thus $f^{-1}(f(K)) = f^{-1}(f(KN)) \ge KN$.

Suppose $NK \le S \le G$, and $K/N = S/N$. Then we have for each kN a unique sN such that $kN = sN$; so $KN = SN$. Therefore $f^{-1}(f(KN)) \le KN$, and so $f^{-1}(f(KN)) = KN$; thus $f^{-1}(f(K)) = KN$. □

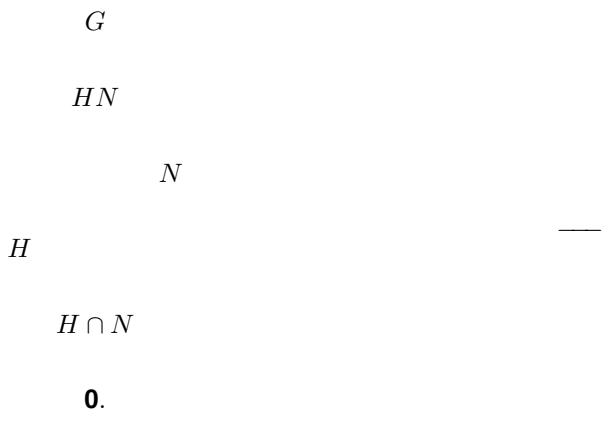
I.5.19 Locating Finite Kernels.

Hint$(3/5)$: Use the Parallelogram Law (Proposition-I.4.8).

If $N \trianglelefteq G$, $[G : N]$ finite, $N \le G$, $|H|$ finite, and $[G : N]$ and $|H|$ are relatively prime, then $H \le N$.

Proof: Since N is normal, HN is a subgroup of G by Theorem-I.5.3. This pro-

duces that standard subgroup diagram labeled with the relevant finite indices:



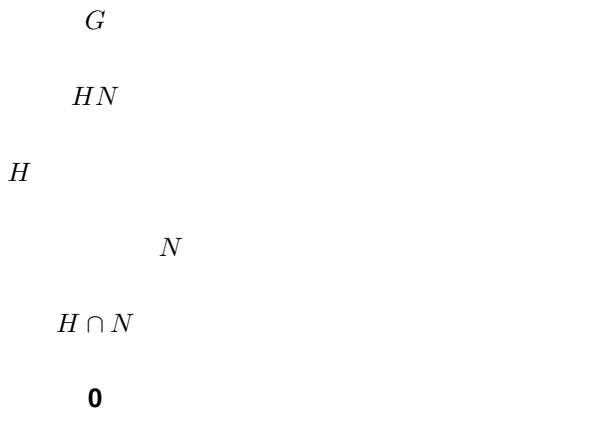
Now using Proposition-I.4.8, we see $b = c$, and both are finite since they are less than $|H|$ and $[G : N]$ respectively. Since we assume $(ab, cd) = 1$ and now know $b = c$, it follows $b = c = 1$. Therefore $[H : H \cap N] = 1$ so $H = H \cap N$ which implies $H \leq N$. □

I.5.20 Locating Finite Subgroups.

Hint$(4/5)$: Use the Parallelogram Law (opposite sides are congruent), Theorem-I.4.8, to show a $N/H \cap N \cong \mathbf{0}$.

If $N \trianglelefteq G$, $|N|$ finite, $H \leq G$, $[G : H]$ finite, and $[G : H]$ and $|N|$ are relatively prime, then $N \leq H$.

Proof: Since N is normal it follows from Theorem I.5.3 that HN is a subgroup of G containing N and H as subgroups. We also know $H \cap N$ to be a subgroup of H and N. Therefore we know the following subgroup lattice to exists and we conveniently label each edge in the lattice by the index of the groups it connects.



We may now apply Theorem I.4.8 to state $[N : H \cap N] = j = [HN : N]$. Now N is finite and $H \cap N \leq N$ so $H \cap N$ is finite. Therefore by the Theorem of Lagrange (Corollary I.4.6) we know $[N : H \cap N]|H \cap N| = |N|$ and two components are finite, therefore so is the third, that is, $[N : H \cap N]$ is finite. We also know $H \leq HN \leq G$ so by Lagrange (Theorem I.4.5) we find $[G : H] = [G : HN][HN : H]$.

We now recall that $[N : H \cap N] = [HN : H]$ and both are finite. Clearly we notice $[HN : H]$ divides $[G : HN][HN : H] = [G : H]$ and $[N : H \cap N]$ also divides $[N : H \cap N]|H \cap N| = |N|$. However we assume $[G : H]$ and $|N|$ to be relatively prime. We now have a positive integer $m = [HN : H] = [N : H \cap N]$

which divides both; therefore, m divides their greatest common factor which is simply 1; therefore, $m = 1$ and so we see that $[N : H \cap N] = 1$.

There is therefore only one coset in $N/H \cap N$. Given $e \in N$ we know $eH \cap N = H \cap N$ is a coset. Therefore for all $x \in N$, $xH \cap N = H \cap N$ and so it follows $N \leq H \cap N$ which requires that $N \leq H$. □

I.5.21 PruferQuotients.

Hint$(2/5)$: Use Exercise-I.3 part (d) and follow the given hint.

If H is a subgroup of $Z(p^\infty)$ and $H \neq Z(p^\infty)$, then $Z(p^\infty)/H \cong Z(p^\infty)$. [*Hint:* if $H = \langle \overline{1/p^n} \rangle$, let $x_i = \overline{1/p^{n+i}} + H$ and apply Exercise-I.3(e).]

Proof: Given H is a proper subgroup of $Z(p^\infty)$, by Exercise-I.3 part (d), $H = \langle \overline{1/p^i} \rangle = C_i$. Now we have the canonical projection homomorphisms $\pi_i : Z(p^\infty) \to Z(p^\infty)/C_i$. Notice the image contains the elements $x_n = \overline{1/p^{n+i}} + C_i = f(\overline{1/p^{n+i}})$; therefore,

$$px_{n+1} = pf(\overline{1/p^{(n+1)+i}}) = f(\overline{p/p^{(n+1)+i}}) = f(\overline{1/p^{n+i}}) = x_n.$$

Also, i is finite, so x_n exists for any $n \in \mathbb{Z}^+$. The element $x_1 \neq C_i$, and $px_1 = \overline{p/p^{i+1}} + C_i = C_i$, so $|x_i| = p$. Finally, $Z(p^\infty)/C_i = \langle f(\overline{1/p^i}) \mid i \in \mathbb{N} \rangle = \langle x_i \mid i \in \mathbb{Z}^+ \rangle$. We have satisfied the hypothesis of Exercise-I.3 part (e), so $Z(p^\infty)/C_i \cong Z(p^\infty)$ for all $i \in \mathbb{N}$. □

I.6 Symmetric, Alternating, and Dihedral Groups

1 Lattice of S_4 . . . 69
2 S_n generators . . . 69
3 Permutation Conjugates . . . 69
4 More S_n Generators . . . 70
5 Permutation Conjugation . . . 70
6 Index 2 subgroups of S_n . . . 70
7 A_4 is not Simple . . . 71
8 A_4 is not solvable . . . 71
9 Matrix Form of D_n . . . 72
10 D_n is Meta-cyclic . . . 72
11 Normality in D_n . . . 72
12 Center of D_n . . . 73
13 D_n representation . . . 73

I.6.1 Lattice of S_4.

Find four different subgroups of S_4 that are isomorphic to S_3 and nine isomorphic to S_2.

Example: The subgroups S_4^1, S_4^2, S_4^3, and S_4^4, as defined in Exercise-I.2, are distinct subgroups of S_4 all isomorphic to S_3. The involutions of S_4 are simply: (12),(13),(14),(23),(24),(34), and their products, (12)(34),(13)(24), and (14)(23). These all generate distinct subgroups isomorphic to S_2. Notice we can show this by considering (12) as $S_4^{3,4}$, etc. □

Hint$(1/5)$: Exercise-I.2 may be helpful.

I.6.2 S_n generators.

(a) S_n is generated by the $n-1$ transpositions $(12), (13), (14), \ldots, (1n)$. [*Hint:* $(1i)(1j) = (ij)$.]

(b) S_n is generated by the $n-1$ transpositions $(12), (23), (34), \ldots, (n-1\ n)$. [*Hint:* $(1j) = (1\ j-1)(j-1\ j)(1\ j-1)$; use (a).]

Proof: As suggested we note $(ij) = (1i)(1j)$ for any two characters i, j where $i \neq j$. In Corollary-I.6.5 we see every permutation in S_n can be written as a product of transpositions. Since the set $A = \{(12), \ldots, (1n)\}$ generates every transposition (ij), we know in fact that the set will generate every permutation in S_n.

Likewise given the set $B = \{(12), \ldots, (n-1\ n)\}$, we may produce any transposition in A by taking the product $(1\ j-1)(j-1\ j)(1\ j-1) = (1j)$. Thus since we generate a set of generators, A, form the set B, it follows B is a set of generators for S_n as well as A. □

Hint$(1/5)$: Reference Corollary-I.6.5.

I.6.3 Permutation Conjugates.

If $\sigma = (i_1 i_2 \cdots i_r) \in S_n$ and $\tau \in S_n$, then $\tau\sigma\tau^{-1}$ is the r-cycle $(\tau(i_1)\tau(i_2)\cdots\tau(i_r))$.

Hint$(3/5)$: Show $\tau(i_s i_t)\tau^{-1} = (\tau(i_s)\tau(i_t))$ then use Corollary-I.6.5.

Proof: Notice $(i_1 \cdots i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_2)$; therefore

$$\tau\sigma\tau^{-1} = \tau(i_1 i_r)\tau^{-1}\tau(i_1 i_{r-1})\tau^{-1} \cdots \tau(i_1 i_2)\tau^{-1}.$$

Now let $\tau(i_s i_t)\tau^{-1} = \upsilon$. Next $\tau(i_s i_t) = \upsilon\tau$, so $\tau(i_s i_t)(i_s) = \upsilon\tau(i_s)$ and therefore $\tau(i_t) = \upsilon(\tau(i_s))$; likewise $\tau(i_s) = \upsilon(\tau(i_t))$; and finally i_k, $k \neq s, t$, implies $\tau(i_k) = i_k = \upsilon(\tau(i_k))$. Whence $\upsilon = (\tau(i_s)\tau(i_t))$. Applying this to the whole we notice:

$$\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_r))(\tau(i_1)\tau(i_{r-1})) \cdots (\tau(i_1)\tau(i_2)) = (\tau(i_1)\tau(i_2) \cdots \tau(i_r)).$$

□

I.6.4 More S_n Generators.

Hint$(1/5)$: It may help to write $\sigma_i = \tau^{i-1}\sigma_1\tau^{-i+1}$. [See Also:Exercise-I.2]

(a) S_n is generated by $\sigma_1 = (12)$ and $\tau = (123 \cdots n)$. [*Hint:* Apply Exercise-I.6 to σ_1, $\sigma_2 = \tau\sigma_1\tau^{-1}, \ldots, \sigma_{n-1} = \tau\sigma_{n-1}\tau^{-1}$ and use Exercise-I.6(b).]

(b) S_n is generated by (12) and $(23 \cdots n)$.

Proof: Notice $\tau^{-1} = (n \cdots 21)$. Define $\sigma_i = \tau^{i-1}\sigma_1\tau^{-i+1}$ for $i = 1, \ldots, n-1$.

Notice by Exercise-I.6 that $\sigma_i = (\tau^{i-1}(1)\tau^{i-1}(2)) = (i\ i+1)$. Therefore $G = \langle\tau, \sigma\rangle$ contains the set $\{(12), \ldots, (n-1\ n)\}$ and so by Exercise-I.6, $G = S_n$.

Likewise when $\tau = (23 \cdots n)$ we have $\sigma_i = (\tau^{i-1}(1)\tau^{i-1}(2)) = (1\tau^{i-1}(2)) = (1\ i+1)$. Therefore the generators produce the elements (12),(13),...,$(1\ n)$, so again by Exercise-I.6 they generate S_n. □

I.6.5 Permutation Conjugation.

Hint$(1/5)$: Use the rules of parity: even+even=even; odd+even=odd; odd+odd=even.

Let $\sigma, \tau \in S_n$. If σ is even (odd), then so is $\tau\sigma\tau^{-1}$.

Proof: Suppose σ is even; then by definition it decomposes into an even number, $2n$, of transpositions. Let m be the number of transpositions in some decomposition of τ into transpositions; that is $\tau = (a_1 a_2) \cdots (a_{2m-1} a_{2m})$; thus $\tau^{-1} = (a_{2m-1} a_{2m}) \cdots (a_1 a_2)$ – so it has the same parity as τ.

It follows $\tau\sigma\tau^{-1}$ decomposes into $m + 2n + m$ transpositions by simply substituting, and thus we see that one possible decomposition into transpositions is of length $2(m+n)$ which is always even. Therefore $\tau\sigma\tau^{-1}$ is even, which is guaranteed to be well-defined by Theorem-I.6.7.

If σ is instead odd, then it has a decomposition into transposes of length $2n+1$ for some n. Again $\tau\sigma\tau^{-1}$ has a transposition decomposition of length $2(m+n)+1$ which is always odd; therefore, $\tau\sigma\tau^{-1}$ is odd. □

I.6.6 Index 2 subgroups of S_n.

Hint$(3/5)$: Show that a subgroup of index 2 must contain all 3-cycles of S_n and apply Lemma-I.6.11.

A_n is the only subgroup of S_N of index 2.

Remark I.6.1 *In fact, S_n does not have subgroups of index k, where $2 < k < n$, $n > 4$. (The proof follows from the simplicity of A_n and the induced group action of on the left cosets.)*

Proof: If $n = 2$ then S_n is isomorphic to $\mathbb{Z}_2$ and so it has only one subgroup of index 2 which is **0**, and only one element is even, which is ε. Therefore A_2 is the only subgroup of index 2 in S_2.

Now let $n > 2$; thus S_n contains some 3-cycle, α; and consider $T \leq S_n$ so that $[S_n : T] = 2$. Suppose $\alpha \notin T$. As it is a three cycle it has order 3. If $\alpha^{-1} \in T$ then all powers of it are in T which means $\alpha \in T$ – a contradiction so we know $\alpha^{-1} \notin T$. Since T is of index 2 this leaves both α and α^{-1} in the nontrivial coset αT. However $T = \alpha T \alpha T = \alpha^2 T = \alpha^{-1} T = \alpha T$; so we once again reach a contradiction; therefore in fact $\alpha \in T$ for any 3-cycle $\alpha \in S_n$.

Finally apply Lemma-I.6.11, T contains all 3-cycles so it must generate A_n. But since we assumed T to have index 2, and A_n has index 2, so by the theorem of Lagrange $|T| = |A_n|$ and hence $T = A_n$ by the Pigeon-Hole-Principle. □

I.6.7 A_4 is not Simple.

Hint$(2/5)$: Notice N is the kernel of the group action of conjugation on the three copies of D_4 in S_4.

Show that $N = \{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is a normal subgroup of S_4 contained in A_4 such that $S_4/N \cong S_3$ and $A_4/N \cong \mathbb{Z}_3$.

Example: Three copies of D_4 are embedded in S_4 as $\langle (k\ 4), (k\ 4\ a\ b)\rangle$, where $k = 1, 2, 3$, and $a < b, a, b \notin \{k, 4\}$ (from the presentation alone we determine there are only 3 possible, and it is a simple check to verify they are all distinct.) As they contain the same composition of elements, they are all conjugate as each combination of disjoint cycles is conjugate to all others of the same combination. Therefore, S_4 acts on D_4^k by conjugation and so there is a non-trivial homomorphism $f : S_4 \to S_3$, the kernel of which must be the intersection of the normalizers of each D_4^k. Notice $D_4^1 \cap D_4^2 \cap D_4^3 = N$ so clearly N is contained in each normalizer and subsequently in the kernel of f. Notice $D_4^k \leq N_{S_4}(D_4^k)$ as usual, and so if the kernel is to be any larger than N, we require that each normalizer of order greater than 8 – that is order 12 or 24, or simply A_4 and S_4 respectively. Neither will serve as each leads to quotient group too small to act transitively on three elements. Therefore, $Ker\ f = N$, and hence N is normal, $S_4/N \cong S_3$, and $A_4/N \cong \mathbb{Z}/3$.[12] □

I.6.8 A_4 is not solvable.

Hint$(3/5)$: Refer to Exercise-I.6. Notice S_4^x all have odd elements and so are not in A_4, and S_4 has no elements of order 6.

The group A_4 has has no subgroup of order 6.

Example: As in the proof of Corollary-I.6.5, we knowing that $(ab\cdots z) = (az)\cdots(ab)$, thus $\sigma \in S_4$ is even only if it is of the form $\varepsilon, (abc)$, or $(ab)(cd)$ – even when these last two transpositions are not disjoint.

$$A_4 = \{\varepsilon, (123), (321), (124), (421), (134), (431), (234), (432), (12)(34), (13)(24), (14)(23)\}.$$

Let S be a subgroup of A_4 of order 6. Since a group of order 6 has even order, by Exercise-I.4 it must have an element of order 2; thus S contains (12)(34), (13)(24), or (14)(23). Furthermore any two of these generates the Klein Four Group N described in Exercise-I.6; so S contains only one element of order 2 as $4 \nmid 6$. Therefore S contains four elements of order 3, since no element in A_4 is of order 6. So far we know S contains the following:

$$S = \{\varepsilon, \alpha, \beta, \alpha^{-1}, \beta^{-1}, \chi\},$$

where α, β are elements of order 3 in A_4 and χ is an element of order 2 in A_4. Therefore $\alpha\beta = \beta\alpha = \chi$; however, for no two distinct (also distinct with respect

[12] This proof is not the most simple, but it illustrates an important proof technique.

to inverses) α, β in A_4 is $\alpha\beta = \beta\alpha$, as we see in the following checks:

$$\begin{aligned}
(123)(124) &= (13)(24) \neq (14)(23) = (124)(123);\\
(123)(134) &= (234) \notin S\\
(123)(234) &= (12)(34) \neq (13)(24) = (234)(123);\\
(124)(134) &= (13)(24) \neq (12)(34) = (134)(124);\\
(124)(234) &= (123) \notin S\\
(134)(234) &= (13)(24) \neq (12)(34) = (134)(234);
\end{aligned}$$

therefore A_4 does not contain a subgroup of order 6. [13] □

I.6.9 Matrix Form of D_n.

Hint$(3/5)$: Use Theorem-I.6.13. In particular notice that $e^{2\pi i/n}$ is a primitive n^{th} root of unity.

For $n \geq 3$, let G_n be the multiplicative group of complex matrices generated by $x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{pmatrix}$, where $i^2 = -1$. Show that $G_n \cong D_n$. [*Hint:* recall that $e^{2\pi i} = 1$ and $e^{k2\pi i} \neq 1$, where k is real, unless $k \in \mathbb{Z}$.]

Example: The matrix x is a transposition so it has order 2. In the case of y, suppose $y^k = \begin{pmatrix} e^{k\frac{2\pi i}{n}} & 0 \\ 0 & e^{-k\frac{2\pi i}{n}} \end{pmatrix}$, for some positive integer k; then

$$y^{k+1} = y^k y = \begin{pmatrix} e^{k\frac{2\pi i}{n}} & 0 \\ 0 & e^{-k\frac{2\pi i}{n}} \end{pmatrix} \begin{pmatrix} e^{\frac{2\pi i}{n}} & 0 \\ 0 & e^{-\frac{2\pi i}{n}} \end{pmatrix} = \begin{pmatrix} e^{(k+1)\frac{2\pi i}{n}} & 0 \\ 0 & e^{-(k+1)\frac{2\pi i}{n}} \end{pmatrix};$$

so by induction $y^k = \begin{pmatrix} e^{k\frac{2\pi i}{n}} & 0 \\ 0 & e^{-k\frac{2\pi i}{n}} \end{pmatrix}$, for all positive integers k. Therefore $y^n = \begin{pmatrix} e^{2\pi i} & 0 \\ 0 & e^{-2\pi i} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Thus y has order at most n. Furthermore $1 = e^{k\frac{2\pi i}{n}} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ only if $n|k$, and likewise for $e^{-k\frac{2\pi i}{n}}$; therefore y has order n; so $y^{-1} = y^{n-1}$.

Now take the products xy and $y^{-1}x$:

$$\begin{aligned}
y^{-1}x &= \begin{pmatrix} 0 & e^{(n-1)2\pi i/n} \\ e^{-(n-1)2\pi i/n} & 0 \end{pmatrix} = x \begin{pmatrix} e^{-(n-1)2\pi i/n} & 0 \\ 0 & e^{(n-1)2\pi i/n} \end{pmatrix}\\
&= x \begin{pmatrix} e^{-2\pi i} e^{2\pi i/n} & 0 \\ 0 & e^{2\pi i} e^{-2\pi i/n} \end{pmatrix} = xy;
\end{aligned}$$

thus $xy = y^{-1}x$. Therefore letting $a = y$ and $b = x$, Theorem-I.6.13 confirms $G_n \cong D_n$. □

I.6.10 D_n is Meta-cyclic.

Hint$(1/5)$: Exercise-I.5 trivializes the question.

Let a be the generator of order n in D_n. Show that $\langle a\rangle \trianglelefteq D_n$ and $D_n/\langle a\rangle \cong \mathbb{Z}_2$.

Proof: Since a has order n, so does its subgroup $\langle a\rangle$. By Theorem-I.6.13 we know D_n has order 2n therefore the index $[D_n : \langle a\rangle] = 2$. Using the result of Exercise-I.5 it is clear $\langle a\rangle \trianglelefteq D_n$. □

[13] Alternatively, it can be shown the only subgroups of order 6 are $\mathbb{Z}_6$ and S_3. No element of S_4 is of order 6, and every S_4^x contains odd permutations; therefore A_4 contains no subgroups of order 6.

I.6.11 Normality in D_n.

[14] Find all normal subgroups of D_n.

Example: Let $\langle a, b\rangle = D_n$ where $|a| = n$ and $|b| = 2$ as allowable by Theorem-I.6.13.

From Exercise-I.6 we see $\langle a\rangle$ is normal in D_n and so using Exercise-I.5 all subgroups of $\langle a\rangle$ are also normal in D_n. We now break up into two cases.

For all j it follows $a(a^j b)a^{-1} = a^{j+2}b$, so that $a^j b$ is conjugate to $a^{j+2}b$. Indeed this tells us of two possible cases: either there is one conjugacy class for all flips when n is odd, or there are precisely 2 conjugacy classes:

$$[b] = \{b, a^2b, a^4b, \dots\}, \qquad [ab] = \{ab, a^3b, a^5b, \dots\},$$

when n is even. Thus when n is odd, any normal subgroup which contains one flip must contain them all, and thus must be the entire group as with the inclusion of the identity element we have more than half the elements of the group.

When n is even, given any a normal subgroup containing any flip, it must contain the entire conjugacy class; thus, it contains $[b]$ or $[ab]$. If it contains both then it is the entire group, so without loss of generality suppose it contains only $[b]$. Certainly then it also contains $\langle a^2\rangle$ and so it is precisely the group $\langle a^2, b\rangle$. As this has index 2 it is in fact normal. In the case where it contains $[ab]$ we simply get the subgroup $\langle a^2, ab\rangle$ which is again normal.

Thus we conclude: if n is odd the only proper normal subgroups are of the from $\langle a^i\rangle$. If n is even we also include the subgroups $\langle a^2, b\rangle$ and $\langle a^2, ab\rangle$. □

Hint$(2/5)$: It may be useful to observe every subgroup of D_n is isomorphic $D_{n/i}$, where $i|n$ or is cyclic, then consider Exercise-I.5.

I.6.12 Center of D_n.

The center (Exercise-I.2) of the group D_n is $\langle e\rangle$ if n is odd and isomorphic to $\mathbb{Z}_2$ if n is even, $n > 2$.

Proof: Suppose a^i is central form some i. Then certainly

$$a^i b = ba^i = a^{-i}b;$$

thus, $a^i = a^{-i}$ and so $i = n/2$ and we require that $2|n$, or else the center does not contain any rotations.

Now suppose it contains any flip $a^i b$. Again,

$$a^{i-1}b = (a^i b)a = a(a^i b) = a^{i+1}b$$

so here $a^{i-1} = a^{i+1}$ or rather $n = 2$, at which point $D_n \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and the center is the entire group.

Thus the center of D_n when $n > 2$ is trivial if $2 \nmid n$ and $\langle a^{n/2}\rangle \cong \mathbb{Z}_2$ when $2|n$. □

Hint$(1/5)$: Test the elements a^i and $a^i b$ for centrality.

I.6.13 D_n representation.

For each $n \geq 3$ let P_n be a regular polygon of n sides. A symmetry of P_n is a bijection $P_n \to P_n$ that preserves distances and maps adjacent vertices onto adjacent vertices.

[14] A geometric proof is best: any subgroup must be a group of symmetries for an inscribed regular polygon. Every inscribed polygon must have a vertex count dividing n. If all the symmetries of the inscribed polygon are counted, it must be a subgroup of the form $D_{n/i}$. If not, then it can have no reflections, as any reflection together with a rotation will generate a dihedral group. Therefore all non-cyclic subgroups are dihedral. (Notice the group of a single reflection is always a cyclic C_2 group, but can equally be classified as D_1 group.)

(a) The set D_n^* of all symmetries of P_n is a group under the binary operation of composition of functions.

(b) Every $f \in D_n^*$ is completely determined by its action on the vertices of P_n. Number the vertices consecutively $1, 2, \ldots, n$; then each $f \in D_n^*$ determines a unique permutation σ_f of $\{1, 2, \ldots, n\}$. The assignment $f \mapsto \sigma_f$ defines a monomorphism of groups $\varphi : D_n^* \to S_n$.

(c) D_n^* is generated by f and g, where f is a rotation of $2\pi/n$ degrees about the center of P_n and g is a reflection about the "diameter" through the center and vertex 1.

(d) $\sigma_f = (1\ 2\ 3\ \cdots n)$ and $\sigma_g = (2\ n)(3\ n-1)(4\ n-2)\cdots$, whence $Im\ \varphi = D_n$ and $D_n^* \cong D_n$.

Proof:

(a) Given that the identity map is a clear isometry it is included in D_n^* so that D_n^* is non-empty. Function composition is well-defined and associative so we have a semigroup. Composition with the identity is transparent so we have a monoid. Finally given any symmetry f of D_n^*, f is bijective so its inverse exists. Since f is an isometry it follows for all A, B, $d(A, B) = d(f(A), f(B))$ and so in fact

$$d(f^{-1}(C), f^{-1}(D)) = d(f^{-1}(f(A)), f^{-1}(f(B)) = d(f(A), f(B)) = d(C, D)$$

so f^{-1} is an isometry. Finally, as f takes adjacent vertices to adjacent vertices, so does f^{-1}. Therefore $f^{-1} \in D_n^*$ proving D_n^* is a group under composition.

(b) We require that adjacent vertices go to adjacent vertices. So suppose f is a symmetry, and A and B two adjacent vertices of the regular n-gon embedded in the plane. To every point P on the edge between A and B, there corresponds a unique $t \in [0, 1]$ such that $P = tA + (1-t)B$. The distance of P to A is t and the distance of P to B is $(1-t)$. As this distance must be preserved it follows the distance of $f(P)$ to $f(A)$ is t and the likewise the distance of $f(P)$ to B is $(1-t)$. Thus in fact $f(tA+(1-t)B) = tf(A)+(1-t)f(B)$ for all $t \in [0, 1]$. Therefore the action on each edge is uniquely determined by the action on the edge's vertices. Moreover, adjacent vertices go to adjacent vertices so the action on the regular n-gon is determined entirely by the action on the vertices.[15]

Enumerate the vertices of P_n A_1 to A_n counter clockwise. To each symmetry f, assign $\sigma_f \in S_n$ to be

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \#f(A_1) & \#f(A_2) & \cdots & \#f(A_n) \end{pmatrix},$$

where $\#$ returns the number of the index of each vertex. Since f is bijective, σ_f is as well, and thus, it is a permutation in S_n. Thus the map $\varphi : f \mapsto \sigma_f$ is well-defined. Given any $f, g \in D_n^*$, it follows $\sigma_{fg} = \sigma_f\sigma_g$ and so we have a homomorphism. Finally, if $\sigma_f = \varepsilon$ then $f(A_i) = A_i$ for all i, and so $f = id$; thus, we have a monomorphism φ.

(c) Given a rotation of $2\pi/n$ radians it follows the vertex A_1 is carried to A_2, and in general A_i moves to A_{i+1}. Thus this determines a unique symmetry ρ. Likewise, we may flip along the diagonal by a symmetry ζ.

Clearly every rotational symmetry is simply a power of ρ, and thus any flip along a diagonal through a vertex is a rotation followed by ζ. All That remains to explain are the possible flips along diagonals which do not pass

[15] Notice in fact the regularity of the n-gon was never used so the concept can be extended to other shapes.

through a vertex.[16] Such a symmetry can only occur when n is even, and thus $\rho^{n/2}$ is defined, and moreover we notice all such symmetries are accommodate by taking $\rho^{n/2}$ followed by ζ followed by some rotation.

(d) Clearly the order of ρ is n and the order of ζ is 2. More importantly we can easily see $\sigma_\rho = (1\ 2\ \cdots n)$ and $\sigma_\zeta = (2\ n)(3\ n-1)(4\ n-2)\cdots$, as it leaves 1 fixed and flips all other vertices to the vertex directly opposite from the diagonal. This means in fact $Im\ \varphi = D_n$ and $D_n^* \cong D_n$ as φ is monic.

□

[16] Here the use of diagonal is perhaps unfortunate. This does not describe a line segment connecting two vertices, but any axis of symmetry.

I.7 Categories: Products, Coproducts, and Free Objects

1 Pointed Sets 76
2 Equivalence 76
3 Direct Product 76
4 Group Coproduct 77
5 Set Coproduct 77
6 Products of Pointed Sets 78
7 Free Inclusion 79
8 Free Basis 80

I.7.1 Pointed Sets.

Hint$(1/5)$: Use the categorical properties of the category of sets.

A *pointed set* is a pair (S, x) with S a set and $x \in S$. A morphism of pointed sets $(S, x) \to (S', x')$ is a triple (f, x, x'), where $f : S \to S'$ is a function such that $f(x) = x'$. Show that pointed sets form a category.

Proof: Note there is an implicit requirement that the set S, of a pointed set (S, x), be non-empty as it must contain the point x.

Given three pointed set $(S, x), (T, y)$ and (U, z) and two morphisms $(f, x, y) : (S, x) \to (T, y)$ and $(g, y, z) : (T, y) \to (U, z)$ we define their composition as composition of functions: $(gf, x, z) : (S, x) \to (U, z)$ is defined by $gf : S \to U$. Since $f(x) = y$ and $g(y) = z$ we see in fact $gf(x) = z$ so composition induces a proper morphism of pointed sets and so the composition is well-defined.

Given three morphisms $(f, x, y), (g, y, z)$ and (h, z, w) we test for associativity. Since $h(gf) = (hg)f$ in the category of sets so it applies here;

$$\begin{aligned}(h, z, w)((g, y, z)(f, x, y)) &= (h, z, w)(gf, x, z) = (h(gf), z, w) = ((hg)f, z, w)\\ &= (hg, y, w)(f, x, y) = ((h, z, w)(g, y, z))(f, x, y).\end{aligned}$$

Finally the identity map, 1_S, for S in the category has the property $1_S(x) = x$; thus it is a morphism $(1_S, x, x) : (S, x) \to (S, x)$ which furthermore has the property that $(1_S, y, y)(f, x, y) = (1_S f, x, y) = (f, x, y)$ and $(f, x, y)(1_S, x, x) = (f1_S, x, y) = (f, x, y)$; therefore we have identity maps for each pointed set, so pointed sets form a category. □

I.7.2 Equivalence.

Hint$(2/5)$: Make sure not to assume $\mathscr{C}$ is concrete; that is, do not assume f or g are functions.

If $f : A \to B$ is an equivalence in a category $\mathscr{C}$ and $g : B \to A$ is the morphism such that $g \circ f = 1_A$, $f \circ g = 1_B$, show that g is unique.

Proof: Suppose $g : B \to A$ and $g' : B \to A$ have the property that $g \circ f = 1_A = g' \circ f$ and $f \circ g = 1_B = f \circ g'$. Therefore $g \circ f = g' \circ f$ and we compose on the right with g:

$$g = 1_A \circ g = (g \circ f) \circ g = (g' \circ f) \circ g = g' \circ (f \circ g) = g' \circ 1_B = g'.$$

Therefore g is unique. □

se Introduction
and verify the
is a homomor-

I.7.3 Direct Product.

In the category $\mathscr{G}$ of groups, show that the group $G_1 \times G_2$ together with the homomorphisms $\pi_1 : G_1 \times G_2 \to G_1$ and $\pi_2 : G_1 \times G_2 \to G_2$ (as in the Example preceding Definition-I.2.2) is a product for $\{G_1, G_2\}$.

Proof: Given that $\mathscr{G}$ is a concrete category, we may treat every homomorphism as a function between sets.

Let $\{G_i \mid i \in I\}$ be a family of groups. Given any group T together with a family of homomorphisms $\{\varphi_i : T \to G_i \mid i \in I\}$, define $\varphi : T \to \prod_{i\in I} G_i$ as the unique map guaranteed by Introduction Theorem-5.2 in the category of sets.

We know π_i is a well-defined map of sets and need to confirm it is included in the morphism of $\mathscr{G}$. Take $f, g \in \prod_{i\in I} G_i$, so that $f, g : I \to \bigcup_{i\in I} G_i$ and $f(i), g(i) \in G_i$. Recall products in $\prod_{i\in i} G_i$ are defined pointwise so that $fg : I \to \bigcup_{i\in I} G_i$ is defined as $fg(i) = f(i)g(i) \in G_i$. Now $\pi_i(fg) = fg(i) = f(i)g(i) = \pi_i(f)\pi_i(g)$; therefore each projection map is a homomorphism.

Finally, we know from Introduction Theorem-5.2 that $\pi_i\varphi = \varphi_i$ for all $i \in I$, and is the unique map to do this. If we can show φ is a homomorphism – so in the category $\mathscr{G}$ – then the direct product is a product in the category of groups.

At this point recall the proof of Introduction Theorem-5.2 which defines $\varphi(x) = f_x$ where $f_x(i) = \varphi_i(x)$. Thus in fact $\varphi(xy) = f_{xy}$ where

$$f_{xy}(i) = \varphi_i(xy) = \varphi_i(x)\varphi_i(y) = f_x(i)f_y(i),$$

and so $\varphi(xy) = f_{xy} = f_x f_y = \varphi(x)\varphi(y)$. Thus φ is a homomorphism.

Thus $\prod_{i\in I} G_i$ is a product in the category of groups. □

I.7.4 Group Coproduct.

In the category $\mathscr{A}$ of abelian groups, show that the group $A_1 \times A_2$ together with the homomorphisms $\iota_1 : A_1 \to A_1 \times A_2$ and $\iota_2 : A_2 \to A_1 \times A_2$ (as in the Example preceding Definition-I.2.2) is a coproduct for $\{A_1, A_2\}$.

Hint$(3/5)$: Use the Needle-in-the-Haystack heuristic. The universal map will have to take the form $(a, b) \mapsto \psi_1(a)\psi_2(b)$ for any two maps $\psi_i : A_i \to T$, $i = 1, 2$.

Proof: Define the map $\iota_1 : A_1 \to A_1 \times A_2$ as $a \mapsto (a, 0)$ and similarly for $\iota_2(b) = (0, b)$. $\iota_1(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \iota_1(a) + \iota_1(b)$, therefore with out loss of generality the injections are homomorphisms.

Given any abelian group T and any two morphisms $\psi_1 : A_1 \to T$ and $\psi_2 : A_2 \to T$, suppose $\psi : A_1 \times A_2 \to T$ is a map where $\psi\iota_i = \psi_i$. Then given $a \in A_1$ and $b \in A_2$, we know $\psi_1(a) = \psi\iota(a) = \psi(a, 0)$ and likewise $\psi_2(b) = \psi(0, b)$. Thus

$$\psi(a, b) = \psi((a, 0) + (0, b)) = \psi(a, 0) + \psi(0, b) = \psi_1(a) + \psi_2(b).$$

Therefore the form of the map is unique.

Thus define the map $\psi : A_1 \times A_2 \to T$ as $(a, b) \mapsto \psi_1(a)\psi_2(b)$. If ψ is a homomorphism then we have shown this to be a coproduct in the category of abelian groups.

Since ψ_i are well-defined and into T, the definition of ψ is well-defined. Now given $(a, b), (c, d) \in A_1 \times A_2$ we notice

$$\begin{aligned}\psi((a, b) + (c, d)) &= \psi(a + c, b + d) = \psi_1(a + c) + \psi_2(b + d)\\ &= \psi_1(a) + \psi_1(c) + \psi_2(b) + \psi_2(d) = \psi_1(a) + \psi_2(b) + \psi_1(c) + \psi_2(d)\\ &= \psi(a, b) + \psi(c, d).\end{aligned}$$

Therefore ψ is a homomorphism and so included in the category of abelian groups.

Therefore $A_1 \times A_2$ is a coproduct in the category of abelian groups for the elements A_1, A_2. □

I.7.5 Set Coproduct.

Hint$(1/5)$: Use the Needle-in-the-Haystack heuristic.

Every family $\{A_i \mid i \in I\}$ in the category of sets has a coproduct. [*Hint:* consider $\mathring{\bigcup}_{i\in I} A_i = \{(a,i) \in (\bigcup_{i\in I} A_i) \times I \mid a \in A_i\}$ with $A_i \to \mathring{\bigcup}_{i\in I}$ given by $a \mapsto (a,i)$. $\mathring{\bigcup}_{i\in I} A_i$ is called the **disjoint union** of the sets A_i.]

Proof: Let $\{A_i \mid i \in I\}$ be a family of sets. Both unions and products are well-defined therefore the disjoint union of sets is a well-define set: $\bigcup_{i\in I} A_i \times \{i\}$.

Now define $\iota_i : A_i \to \mathring{\bigcup}_{i\in I} A_i$ as $a \mapsto (a,i)$. The image of ι is contained in the disjoint union and each element of the domain has a unique image so the function is well-defined.

Now let T be a set and $\{\psi_i : A_i \to T \mid i \in I\}$ a family of functions. Suppose $\psi : \mathring{\bigcup}_{i\in I} A_i \to T$ satisfies the properties of a coproduct. Then $\psi\iota_i = \psi_i$ for all $i \in I$, and ψ is the unique map that does this. Notice therefore $\psi_i(a) = \psi(\iota_i(a)) = \psi(a,i)$. Therefore define $\psi : \mathring{\bigcup}_{i\in I} A_i \to T$ as $(a,i) \mapsto \psi_i(a)$. Since $(a,i) \in \mathring{\bigcup}_{i\in I} A_i$ implies $a \in A_i$, it follows $\psi_i(a)$ is well-defined, and therefore ψ is well-defined and so it is a function.

Therefore the disjoint union defines a coproduct in the category of sets. □

I.7.6 Products of Pointed Sets.

Hint$(3/5)$: Build a (co)product that uses the (co)product of regular sets. Remember while many constructions may exist, they must all be equivalent, which in S_* means the sets are equipollent. Make sure to include the special cases when the family of objects is empty; notice $\varnothing$ cannot be made into a pointed set, but $(\{\varnothing\}, \varnothing)$ is a *zero* (initial and terminal) object.

(a) Show that the category S_* of pointed sets (see Exercise-I.7) products always exist; describe them.

(b) Show that in S_* every family of objects has a coproduct (often called a "wedge product"); describe this coproduct.

Proof: Let $\{(A_i, a_i) \mid i \in I\}$ be a family of pointed sets and (T,t) some pointed set.

Empirically we see $(\{a\}, a)$ is a pointed set. Furthermore any function $f : T \to \{a\}$ is a function if and only if $f(t) = a$ for each $t \in T$. Therefore (f,t,a) is the unique morphism from (T,t) to $(\{a\},a)$ and so $(\{a\},a)$ is terminal. Suppose $(f,a,t) : (\{a\},a) \to (T,t)$ is a morphism; then $f(a) = t$ and so in fact f is unique. Therefore $(\{a\},a)$ is initial as well, and thus it is in fact a zero object. Therefore when $I = \varnothing$ define the product and coproduct as $(\{\varnothing\}, \varnothing)$. Now suppose $I \neq \varnothing$.

Suppose $\{(\varphi_i, t, a_i) : (T,t) \to (A_i, a_i) \mid i \in I\}$ is a family of mappings in the category of pointed sets. Consider the existence of a product in S_*. This requires $\prod_{i\in I}(A_i, a_i)$ be a pointed set, (P,p), together with the property that there exists a $(\varphi, t, p) : (T,t) \to (P,p)$ such that $(\pi_i, p, a_i)(\varphi, t, p) = (\varphi_i, t, a_i)$, for all $i \in I$. However using the rules of composition we see: $(\pi\varphi, t, a_i) = (\varphi_i, t, a_i)$ which implies $\pi\varphi = \varphi_i$ in the category of sets. This property is unique, up to equivalence, in the category of sets; therefore, it will also be unique up to equivalence, in the category of pointed sets and furthermore we now see $P = \prod_{i\in I} A_i$.

Therefore define $\prod_{i\in I}(A_i, a_i) = (\prod_{i\in I} A_i, p)$, with $p : I \to \bigcup_{i\in I} A_i$ defined as $p(i) = a_i$ as a well-defined function contained in this set product, since each $p(i) = a_i$ is in A_i, for all $i \in I$. Therefore $(\prod_{i\in I} A_i, p)$ is a pointed set and so contained in our category. As anticipated, $\pi_i : \prod_{i\in I} A_i \to A_i$ sends p to $p(i) = a_i$; thus $(\pi_i, p, a_i) : (\prod_{i\in I} A_i, p) \to (A_i, a_i)$, defined as π_i, is a well-defined morphism (canonical projection) of pointed sets.

By design $\prod_{i\in I} A_i$ is a product in the category of sets; therefore, there exists a $\varphi : T \to \prod_{i\in I} A_i$ such that $\pi_i\varphi = \varphi_i$, for all $i \in I$. So define (φ, t, p) :

$(T,t) \to (\prod_{i\in I} A_i, p)$ as $x \mapsto \varphi(x)$. To prove (φ,t,p) is a well-defined point set morphism, recall the definition of the set product: $\varphi(x) = f_x : I \to \bigcup_{i\in I} A_i$, where $f_x(i) = \varphi_i(x)$. Thus in our context, $\varphi(t) = f_t$ and $f_t(i) = \varphi_i(t) = a_i$. However this is our definition of p so in fact $\varphi(t) = f_t = p$. Therefore (φ,t,p) is a well-defined pointed set morphism.

Finally $(\pi_i,p,a_i)(\varphi,t,p) = (\pi_i\varphi,t,a_i) = (\varphi_i,t,a_i)$ so the category of pointed sets has a product.

For the coproduct presume $\{(\psi_i,a_i,t) : (A_i) \to (T,t) \mid i \in I\}$ is a family of pointed set morphisms. Once again the existence of a coproduct demands that $\coprod_{i\in I}(A_i,a_i)$ be a pointed set (C,c). As such it must have the property $(\psi_i,a_i,t) = (\psi,c,t)(\iota_i,a_i,c) = (\psi\iota_i,a_i,t)$, for some ψ and all $i \in I$. This matches the requirement for the unique (up to equivalence) coproduct of sets, and therefore imposes its structure.

Since $I \neq \varnothing$ we may pick an element $0 \in I$. Define $\coprod_{i\in I}(A_i,a_i) = (\overset{\circ}{\bigcup}_{i\in I} A_i, a_0)$. All that is required is to show (ψ,a_0,t) is a well-defined pointed set morphism. This requires we show $\psi(a_0) = t$, which is simple since $t = \psi_i(a_i) = \psi\iota_i(a_i) = \psi(a_0)$. Therefore we have a coproduct in the category of pointed sets. □

I.7.7 Free Inclusion.

Let F be a free object on a set X ($i : X \to F$) in a concrete category $\mathscr{C}$. If $\mathscr{C}$ contains an object whose underlying set has at least two elements in it, then i is an injective map of sets.

Proof: By assumption $\mathscr{C}$ is a concrete category; therefore each object has an underlying set. Let σ be the forgetful functor associated with the category, and rewrite $i : X \to \sigma F$.

If $X = \varnothing$ then i is unique since the empty-set is initial. Vacuously $i : \varnothing \to F$ is injective. Similarly if $X = \{x\}$, given any $i : X \to F$, $x \neq y$ does not exist so in fact i is still injective. Now consider only $X \succeq 2$.

Assuming the hypothesis, let A be an object in $\mathscr{C}$ with $\sigma A \succeq 2$. Assuming the Axiom of Choice we may well-order X by J so that $X = \{x_j \mid j \in J\}$. Since both X and σA have cardinalities greater than or equal to 2, we may choose arbitrary subsets $\{j,k\} \subset J$ and $\{a,b\}$ where $x_j \neq y_k$, and $a \neq b$. Furthermore we may now define a map $f_{j,k} : X \to \sigma A$ by

$$f_{j,k}(x_m) = \begin{cases} a & m = j \\ b & m \neq j \end{cases} .$$

Recalling F is free, there must now exist a unique map $\varphi_{j,k} : F \to A$, in $\mathscr{C}$, such that

$$\begin{array}{ccc} & & X \\ & & \\ \sigma F & & \sigma A \end{array}$$

commutes; thus $\varphi' i|\{x_j,x_k\} = f_{j,k}|\{j,k\}$. Clearly $f_{j,k}|\{j,k\}$ is injective since $f_{j,k}(x_j) = a \neq b = f_{j,k}(x_k)$; thus $i|\{x_j,x_k\}$ is injective (refer to property (10) in Introduction, Section 3.)

However the choice of j and k was completely arbitrary. If we take all $j,k \in J$ such that $j \neq k$, the associated $f_{j,k}$ is always well-defined and induces a $\varphi_{j,k}$; yet the i does not vary for any j,k. Thus $i|\{x_j,x_k\}$ is injective for any distinct pair of elements $x_j,x_k \in X$, which are all elements. Therefore

Hint$(3/5)$: Use the fact that freeness must work for all objects A and associated mappings $f : X \to A$. So if an f can be made that shows i is injective on some pair of elements, together with all functions, i must be injective on the entire set X.

$x \neq y$ in X, implies $i(x) \neq i(y)$, so i is injective. □

Hint$(4/5)$: Use the freeness of F to show $F \to G \hookrightarrow F$ is 1_F.

I.7.8 Free Basis.

Suppose X is a set and F is a free object on X (with $i : X \to F$) in the category of groups (the existence of F is proved in Section I.9). Prove that $i(X)$ is a set of generators for the group F. [*Hint:* If G is the subgroup of F generated by $i(X)$, then there is a homomorphism $\varphi : F \to G$ such that $\varphi i = i$. Show that $F \to G \hookrightarrow F$ is the identity map.]

Proof: Let $G = \langle i(X) \rangle$ and define $i' : X \to G$ by $i'(x) = i(x)$. Since $i(X) \subseteq F$, $G \leq F$ so we may define the canonical inclusion homomorphism $\mu : G \hookrightarrow F$ as $g \mapsto g$. Clearly $\mu(gh) = gh = \mu(g)\mu(h)$; so μ is in our category of groups. Additionally, $\mu(i'(x)) = \mu(i(x)) = i(x)$, so $\mu i' = i$. Since F is furthermore assumed to be free there exists a unique homomorphism $\varphi : F \to G$ such that the following diagram commutes:

$$\begin{array}{ccc} & X & \\ & & \\ F & & G \end{array}$$

Notice the identity map 1_F satisfies the property $1_F i = i$ and so by the uniqueness guaranteed by the free property of F, it is the unique map that does so. However notice $\mu\varphi i = \mu i' = i$; thus $\mu\varphi = 1_F$.

Since $\mu\varphi = 1_F$ it follows μ is surjective; thus $G = F$. □

I.8 Direct Products and Direct Sums

1 Non-Product Groups 81
2 Product Decomposition 81
3 Split Extension 81
4 Weak Product 82
5 Cyclic Products 83
6 p-order Element Groups 83
7 83
8 Internal Product 84
9 Product Quotients 84
10 Weak Product 84
14 Counterexamples 85

I.8.1 Non-Product Groups.

S_3 is *not* the direct product of any family of its proper subgroups. The same is true of $\mathbb{Z}_p^n$ (p prime, $n \geq 1$) and $\mathbb{Z}$.

Example: Suppose A and B are abelian groups. Then given $(a,b),(c,d) \in A \times B$, it follows $(a,b)(c,d) = (ac,bd) = (ca,db) = (c,d)(a,b)$; thus $A \times B$ is abelian.

Now the proper subgroups of S_3 are of order 2 or 3 by the Theorem of Lagrange. Being of prime order they are all cyclic and furthermore abelian. Therefore their products must be abelian. S_3 is not abelian, since $(12)(13) = (132) \neq (123) = (13)(12)$; therefore, S_3 is not direct product of any of its proper subgroups.

Every proper subgroup of $\mathbb{Z}_p^n$ is of the form $\langle p^k \rangle$, where $k = 1, \ldots, n-1$, by Theorem-I.3.5. Now consider any product of these subgroups $\langle p^i \rangle \times \langle p^j \rangle$.

Notice $G = \mathbb{Z}_p^{i_1} \times \cdots \times \mathbb{Z}_p^{i_n}$ contains the subgroups $\langle (p^{i-1}, 0, \ldots, 0) \rangle$ and $\langle (0, \ldots, 0, p^{j-1}) \rangle$ which are both of order p. Thus G cannot be cyclic, since every $\mathbb{Z}_p^n$ cyclic group contains a unique subgroup of order p (refer to Exercise-I.3). Therefore $\mathbb{Z}_p^n$ is not the internal direct product of any of its proper subgroups.

The group of integers is again cyclic. However any product of subgroups (even infinite products) contains as a subgroup $m\mathbb{Z} \times n\mathbb{Z}$ for some $m, n > 1$. Such a subgroup is not cyclic since $i(x,0) = j(0,y)$ for any $i,j,x,y \in \mathbb{Z}$, $i,j,x,y \neq 0$. Therefore $\mathbb{Z}$ is not the internal direct product of some of its proper subgroups. □

Hint$(1/5)$: Notice products of abelian groups are abelian. However products of cyclic groups are cyclic only if all groups are finite and their order are all relatively prime.

I.8.2 Product Decomposition.

Give and example of groups H_i, K_i such that $H_1 \times H_2 \cong K_1 \times K_2$ and no H_i is isomorphic to any K_i.

Example: Compare the groups $\mathbb{Z}_2 \times \mathbb{Z}_6$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3$. The element $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ generates all of the group, therefore $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Therefore the map defined on the generators: $(1,0) \mapsto ((1,0),0)$ and $(0,1) \mapsto ((0,1),1)$ is an isomorphism; that is: $\mathbb{Z}_2 \times \mathbb{Z}_6 \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3$. However the components $\mathbb{Z}_2$, $\mathbb{Z}_6$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, and $\mathbb{Z}_3$ are not pairwise isomorphic, as they all have different finite orders. □

Hint$(1/5)$: Use abelian groups. Notice this says decomposition into products is not unique.

I.8.3 Split Extension.

Hint$(3/5)$:

Let G be an (additive) abelian group with subgroups H and K. Show that $G \cong H \oplus K$ if and only if there are homomorphisms $H \rightleftarrows G \rightleftarrows K$ such that $\pi_1\iota_1 = 1_H$, $\pi_2\iota_2 = 1_K$, $\pi_1\iota_2 = 0$ and $\pi_2\iota_1 = 0$, where 0 is the map sending every element onto the zero (identity) element, and $\iota_1\pi_1(x) + \iota_2\pi_2(x) = x$ for all $x \in G$.

Proof: ($\Rightarrow$) Suppose $G \cong H \oplus K$. Since this is a finite product, the external direct product is the same object as external weak product; [17] therefore π_i and ι_i are defined by Theorem-I.8.1 and Theorem-I.8.5 – which applies since we consider only abelian groups – and $H \oplus K$ is both a product and a coproduct.

Every element $g \in G$ is of the form $g = (h, k)$, and for all $h \in H$, we have $h = (h, 0)$. Now $\pi_1\iota_1(h) = \pi_1(h, 0) = h$; so in fact $\pi_1\iota_1 = 1_H$ and $\pi_2\iota_2 = 1_K$. Moreover $\pi_1\iota_2(k) = \pi_1(0, k) = (0, 0)$ so $\pi_1\iota_2 = 0$ and $\pi_2\iota_1 = 0$. Finally

$$\iota_1\pi_1(h, k) + \iota_2\pi_2(h, k) = \iota_1(h) + \iota_2(k) = (h, 0) + (0, k) = (h, k).$$

($\Leftarrow$) Assume $H \rightleftarrows G \rightleftarrows K$ and $\pi_1\iota_1 = 1_H$, $\pi_2\iota_2 = 1_K$, $\pi_1\iota_2 = 0$ and $\pi_2\iota_1 = 0$, where 0 is the map sending every element onto the zero (identity) element, and $\iota_1\pi_1(x) + \iota_2\pi_2(x) = x$ for all $x \in G$.

First note $\pi_1\iota_1 = 1_H$ is bijective which implies ι_1 is injective and π_1 surjective. Thus H is embedded in G; that is: $H' = \iota(H) \leq G$, and given any $h' \in H'$, there exists a unique $h \in H$ such that $\iota(h) = h'$ and since $\pi_1\iota_1(h) = h$ it follows $\pi_1(h') = h$. Therefore $H \cong H'$ by the invertible homomorphisms π_1 and ι_1. Likewise $K \cong K' \leq G$.

Now every $g \in G$ is of the from $\iota_1\pi_1(g)+\iota_2\pi_2(g) = g$ implies $g = \iota_1(h)+\iota_2(k)$ for some $h \in H$, $k \in K$, particularly $h = \pi_1(g)$ and $k = \pi_2(g)$. Therefore G has the normal form $h'+k'$, and so $G = H'+K'$. Therefore define $f : G \to H \oplus K$ by $h' + k' \mapsto (h, k)$. Clearly this map is bijective. Furthermore since G is abelian, $(h'+k')+(h''+k'') = (h'+h'')+(k'+k'')$ and $(h'+h'', k'+k'') = (h', k')+(h'', k'')$; so f is a homomorphism. Therefore $G \cong H \oplus K$. $\square$

I.8.4 Weak Product.

Hint$(2/5)$: Consider non-abelian groups.

Give an example to show that the weak direct product is not a coproduct in the category of all groups. [*Hint:* it suffices to consider the case of two factors $G \times H$.]

Example: Consider $S_3 \times^w \mathbb{Z}_4$. Given S_4, we may construct a map $f : S_3 \to S_4$ by replacing 1 with 4, so that

$$(123) \mapsto (234); (132) \mapsto (243); (12) \mapsto (24); (13) \mapsto (34); (23) \mapsto (23).$$

Likewise $g : \mathbb{Z}_4 \to S_4$ by mapping the generator $1 \mapsto (1234)$.

If $S_3 \times^w \mathbb{Z}_4$ is in deed a coproduct, then there exists a unique map $F : S_3 \times^w \mathbb{Z}_4 \to S_4$ such that $F\iota_{S_3} = f$ and $F\iota_{\mathbb{Z}_4} = g$. Moreover we now observe the definition of F: $F(x, e) = f(x)$, $F(e, y) = g(y)$, and since F is presumed to be a homomorphism it follows $F(x, y) = F(x, e)F(e, y) = f(x)g(y)$.

Now consider $F(((12), 1)((123), 1))$, and evaluate the function in two ways: first with the homomorphism property, next straight forward – the evaluations

[17] Later it is shown that all products and coproducts are equivalent in the category of abelian groups.

should agree.

$$\begin{aligned} F((12),1)((123),1)) &= F((12),1)F((123),1) = f(12)g(1)f(123)g(1) \\ &= (24)(1234)(234)(1234) = (12); \\ F(((12),1)((123),1)) &= F((23)(123),1+1) = F((23),2) = f(23)g(2) \\ &= (23)(13)(24) = (1243). \end{aligned}$$

Since $(12) \neq (1243)$ it is clear F is not in fact a homomorphism. Therefore $S_3 \times^w \mathbb{Z}_4$ is not a coproduct; the weak direct product is not a coproduct in the category of all groups. □

I.8.5 Cyclic Products.

Hint$(1/5)$: Consider the results of Exercise-I.3 and Exercise-I.3.

Let G and H be finite cyclic groups. Then $G \times H$ is cyclic if and only if $(|G|, |H|) = 1$.

Proof: Let $|G| = m$ and $|H| = n$ and assume $G = \langle a \rangle$, $H = \langle b \rangle$.

($\Rightarrow$) Suppose $G \times H$ is cyclic. If $(m,n) = k$ then it follows $a^{m/k}$ and $b^{n/k}$ are elements of G and H respectively, and both have order k. Thus $\langle (a^{m/k}, 0) \rangle$ and $\langle (0, b^{n/k}) \rangle$ are two distinct subgroups of order k. By Exercise-I.3, every finite cyclic group must have a unique subgroup for every order dividing its own; thus this situation is impossible unless $a^{m/k} = 0 = b^{n/k}$ – that is only when $k = 1$. Therefore $(m,n) = 1$.

($\Leftarrow$) Suppose $(m,n) = 1$. Using Exercise-I.3 notice $G \times H$ is an abelian group with elements a and b of order m and n respectively; thus $G \times H$ must contain an element of order $[m,n]$. Since $mn = (m,n)[m,n] = [m,n]$, it follows $G \times H$ is cyclic by the Pigeon-Hole Principle – recall $|G \times H| = |G| \times |H| = mn$. □

I.8.6 p-order Element Groups.

Hint$(2/5)$: Use the properties of an internal direct product.

Every finitely generated abelian group $G \neq \langle e \rangle$ in which every element (except e) has order p (p prime) is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (n summands) for some $n \geq 1$. [*Hint:* Let $A = \{a_1, \ldots, a_n\}$ be the set of generators such that no proper subset of A generates G. Show that $\langle a_i \rangle \cong \mathbb{Z}_p$ and $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle$.]

Proof: Let A be a subset of G such that $G = \langle A \rangle$ but $\langle A - \{a\} \rangle \neq G$ for any $a \in A$. Since $G \neq \mathbf{0}$, $A \neq \varnothing$. Since G is assumed to be finitely generated, $|A| = n$ for some $n \in \mathbb{Z}^+$. Therefore enumerate the elements of A: $A = \{a_1, \ldots, a_n\}$.

If any element $a \in A$ is equal to e, then $G = \langle A - \{a\} \rangle$, therefore by our assumptions on A, $e \notin A$. Thus assuming the hypothesis on G, every element of A has order p. This means $N_i = \langle a_i \rangle \cong \mathbb{Z}_p$ for all $i = 1, \ldots, n$, by Theorem-I.3.2.

First note since G is abelian all subgroups are normal; in particular $N_i \trianglelefteq G$ for all $i = 1, \ldots, n$. Since A generates G, and $A \subseteq \bigcup_{i=1, i\neq k}^{n} N_i$, it follows $G = \langle \bigcup_{i=1, i\neq k}^{n} N_i \rangle$.

Since each $|N_k| = p$ it follows by the Theorem of Lagrange the subgroup $N_k \cap H$ of N_k must have order 1 or p; thus it equals $\mathbf{0}$ or N_k – for any $H \leq G$. Therefore $N_k \cap \langle \bigcup_{i=1, i\neq k}^{n} N_i \rangle = \mathbf{0}$ or N_k. If it is N_k then $A - \{a_i\}$ generates a_i, which violates our assumptions. Therefore $N_k \cap \langle \bigcup_{i=1, i\neq k}^{n} N_i \rangle = \mathbf{0}$.

Thus by Theorem-I.8.6 we know $G = \prod_{i=1}^{n} N_i$. Since each $N_i \cong \mathbb{Z}_p$ we further may state $G \cong \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ with n summands. □

I.8.7 .

Hint(4/5):

Let H, K, N be a nontrivial normal subgroups of a group G and suppose $G = H \times K$. Prove that N is in the center of G or N intersects one of H, K non-trivially. Give examples to show that both possibilities can actually occur when G is non-abelian.

Example: $D_2 = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ [18] has a normal subgroup $\langle ab \rangle$ which does not intersect either product. However since the group is abelian every thing is contained in the center.

In D_6 the center is no longer the entire group but simply $\langle a^3 \rangle$ (see Exercise-I.6). $\langle a^3 \rangle, \langle a^2, b \rangle \trianglelefteq D_6$ and nontrivial. $\langle a^3 \rangle \cap \langle a^2, b \rangle = \mathbf{0}$ and finally $\langle \langle a^3 \rangle \cup \langle a^2, b \rangle \rangle = \langle a^2, a^3, b \rangle = D_6$. Therefore $D_6 = \langle a^3 \rangle \times \langle a^2, b \rangle \cong \mathbb{Z}_2 \times D_3$. [19]

The list of nontrivial normal subgroups of D_6 is (Exercise-I.6):

$$\langle a^3 \rangle, \langle a^2 \rangle, \langle a \rangle, \langle a^2, b \rangle, \langle a^2, ab \rangle.$$

Clearly the first non-trivially intersects $\langle a^3 \rangle$ – and it is contained in the center (it is the center); the next four non-trivially intersect $\langle a^2, b \rangle$ – they all contain $\langle a^2 \rangle$. □

Thanks to David Hill.

Proof: Suppose $H \cap N = K \cap N = \mathbf{1}$. Take a commutator from each: let $h \in H$, $k \in K$ and $n \in N$; then $[h, n] \in N$ as N is normal, and also $[h, n] \in H$ as H is normal, so $[h, n] = 1$ as their intersection is trivial. The same goes for $[k, n]$. Therefore N is central to all elements of H and to all elements of K, so since $HK = G$ it follows N is central to all elements in G, so $N \leq Z(G)$. □

I.8.8 Internal Product.

Hint(1/5): Use the result of Exercise-I.8.

Corollary-I.8.7 is false if one of the N_i is not normal.

Example: In S_3 the subgroups $\langle (123) \rangle$ and $\langle (12) \rangle$ have the properties $\langle (123) \rangle \cap \langle (12) \rangle = \mathbf{0}$, and

$$\langle (123) \rangle \langle (12) \rangle = \{\epsilon, (123), (132), (12), (13), (23)\} = S_3.$$

However in Exercise-I.8 we saw S_3 is not the internal direct product of any of its subgroups. Therefore $S_3 \neq \langle (123) \rangle \times \langle (12) \rangle$. As has previously been shown, $\langle (12) \rangle$ is not normal in S_3; thus this does not violate Corollary-I.8.7 but illustrates its limitation. □

I.8.9 Product Quotients.

Hint(1/5): Use the projection maps together with the First Isomorphism Theorem.

If a group G is the (internal) direct product of its subgroups H, K, then $H \cong G/K$ and $G/H \cong K$.

Proof: Let $G = H \times K$. The group $H \times K$ comes equipped with the canonical projection maps $\pi_H : H \times K \to H$ and $\pi_K : H \times K \to K$, without loss of generality we will treat only one.

By definition $\pi_K(h, k) = k$; thus $\pi_k(x, y) = e$ if and only if $y = e$ – that is to say $Ker\ \pi_K = H \times \mathbf{0} = H$.[20] Furthermore π_K is surjective since $\pi_K(\mathbf{0} \times K) = K$. From the First Isomorphism Theorem we know $K \cong H \times K/Ker\ \pi_K = G/H$.

Analogously $H \cong G/K$. □

[18] D_2 is the symmetries of a rectangle.

[19] D_6 is the symmetries of a hexagon, which contains two disjoint regular triangles whose symmetries are D_3 – hence D_6 is structurally equivalent to a product of D_3.

[20] Recall this is an internal direct product so $H \times \mathbf{0} = H\mathbf{0} = H$.

I.8.10 Weak Product.

If $\{G_i \mid i \in I\}$ is a family of groups, then $\prod_{i\in I}^{w} G_i$ is the internal weak direct product its subgroups $\{\iota_i(G_i) \mid i \in I\}$.

Hint$(3/5)$: Use Theorem-I.8.4 and I.8.9.

Proof: By Theorem-I.8.4 part iii, we already know $\iota_i(G_i)$ is normal in $\prod_{i\in I}^{w} G_i$ for all $i \in I$.

By construction every element in $\prod_{i\in I}^{w} G_i$ is of the from $f : I \to \bigcup_{i\in I} G_i$, $f(i) = e_i$ for all but finitely many $i \in I$ – denumerate them as $i_1, \ldots i_n$. Thus we can decompose each nontrivial f as follows:

$$f = \iota_{i_1}(f(i_1)) + \cdots + \iota_{i_n}(f(i_n)).$$

This decomposition is unique because it must agree with f for each i. Clearly each $\iota_{i_j}(f(i_j)) \in \iota_{i_j}(G_j)$, thus $\prod_{i\in I}^{w} G_i$ is the internal direct product of $\{\iota_i(G_i) \mid i \in I\}$ by Theorem-I.8.9. □

I.8.11 Counterexamples.

For $i = 1, 2$ let $H_i \trianglelefteq G_i$ and give example to show that each of the following statements may be false: (a) $G_1 \cong G_2$ and $H_1 \cong H_2 \Rightarrow G_1/H_1 \cong G_2/H_2$. (b) $G_1 \cong G_2$ and $G_1/H_1 \cong G_2/H_2 \Rightarrow H_1 \cong H_2$. (c) $H_1 \cong H_2$ and $G_1/H_1 \cong G_2/H_2 \Rightarrow G_1 \cong G_2$.

Hint$(3/5)$: C

onsider $\mathbb{Z}$, D_4, and $\mathbb{Z}_4$ together with $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. **Example:**

(a) $\mathbb{Z} \cong \mathbb{Z}$ and $2\mathbb{Z} \cong \mathbb{Z} \cong 3\mathbb{Z}$ but certainly $\mathbb{Z}/2\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/3\mathbb{Z}$ as they do not even have the same order.

(b) $D_4 \cong D_4$ and $D_4/\langle a\rangle \cong \mathbb{Z}_2 \cong D_4/\langle a^2, b\rangle$ but $\langle a\rangle$ is cyclic and $\langle a^2, b\rangle$ is not, so they are not isomorphic (see Exercise-I.6).

(c) $\langle 2\rangle \trianglelefteq \mathbb{Z}_4$ and $\langle (1, 0)\rangle \trianglelefteq \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Notice $\langle 2\rangle \cong \mathbb{Z}_2 \cong \langle (1, 0)\rangle$, and $\mathbb{Z}_4/\langle 2\rangle \cong \mathbb{Z}_2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2/\langle (1, 0)\rangle$; however, $\mathbb{Z}_4$ is cylic while $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not, so they are not isomorphic.

□

I.9 Free Groups, Free Products, Generators & Realtions

1 Elements of Free Groups 86
2 Cyclic Free Group 86
3 86
5 $Q_1 6$ 87

I.9.1 Elements of Free Groups.

Hint$(2/5)$: Use the freeness to construct a homomorphism $F \to \mathbb{Z}$ where every generator of F maps to 1; then reach a contradiction with a nontrivial element of finite order.

Every nonidentity element in a free group F has infinite order.

Proof: Let F be free on a set X (by the map $\iota : X \to F$).

If $X = \varnothing$ then there is a unique homomorphism from F to any other group G; therefore, F is an initial object.[21] However the group **0** is a zero object – that is both initial and terminal – and therefore all initial groups are isomorphic to **0**.[22] Notice the group **0** has no nontrivial elements so it vacuously satisfies the proposition.

Now let $X \neq \varnothing$. Suppose there exists an element $a \in F$ of finite order $n > 1$ – so as to be nontrivial. Define the map $f : X \to \mathbb{Z}$ by $x \mapsto 1$. Then since F is free there exists a unique homomorphism $\varphi : F \to \mathbb{Z}$ such that $\varphi\iota = f$. We saw in Exercise-I.7, that $\iota(X)$ is a set of generators for F; therefore, $a = \iota(x_{i_1})^{n_{i_1}} \cdots \iota(x_{i_j})^{n_{i_j}}$ and using the homomorphism property of φ:

$$\begin{aligned} \varphi(a) &= \varphi(\iota(x_{i_1})^{n_{i_1}} \cdots \iota(x_{i_j})^{n_{i_j}}) = \varphi\iota(x_{i_1})^{n_{i_1}} \cdots \varphi\iota(x_{i_j})^{n_{i_j}} \\ &= (n_{i_1})f(x_{i_1}) + \cdots + (n_{i_j})f(x_{i_j}) = \sum_{k=1}^{j} n_{i_k} = m. \end{aligned}$$

This means the element $m \in \mathbb{Z}$ has a finite order dividing that of $a \in F$. The only element of finite order in $\mathbb{Z}$ is 0; therefore, $m = 0$. This means $a \in Ker\ \varphi$. **PENDING:** figure me out. Of course, this cannot be sense 1 has infinite order in $\mathbb{Z}$; therefore, no such element, a, may exist in F. □

I.9.2 Cyclic Free Group.

Hint$(1/5)$: Use Exercise-I.9.

Show that the free group on the set $\{a\}$ is an infinite cyclic group, and hence isomorphic to $\mathbb{Z}$.

Proof: Since the set $X = \{a\}$ is nonempty, $F(X)$ is not the trivial group; in fact F contains the nontrivial element a. By Exercise-I.9, a has infinite order; therefore, $\langle a \rangle \cong \mathbb{Z}$ by Theorem-I.3.2. Furthermore by Exercise-I.7, if F is free on X, as is here assumed, then X generates F. Therefore $F = \langle a \rangle \cong \mathbb{Z}$. □

[21] $\varnothing$ is initial in the category of sets so there exists a unique map $\varnothing \to G$ forcing the freeness to imply there exists a unique homomorphism $F \to G$.

[22] Given a category with a zero object O and an initial object I, there is a unique morphism into I form any object T by way of O: $T \to O \to I$, where each of these morphisms are unique by the definition of O; thus, I also terminal, and therefore a zero object, and so equivalent to O – Theorem-I.7.10.

I.9.3 .

Let F be a free group and let N be the subgroup generated by the set $\{x^n \mid x \in F, n$ a fixed integer $\}$. Show that $N \trianglelefteq F$.

Hint$(2/5)$: Use the freeness to construct a homomorphism whose kernel is N.

Proof: Let F be free on X by a map $\iota : X \to F$.

Define the map $f : X \to \mathbb{Z}_n$ by $x \mapsto 1$. Using the free property of F, there exists a unique homomorphism $\varphi : F \to \mathbb{Z}_n$ with the property $\varphi\iota = f$. By Exercise-I.7, $\iota(X)$ generates F so we see every generator of F is mapped to 1. Since every element in $\mathbb{Z}_n$ has order n or less, then for every $x \in F$, $\varphi(x^n) = \varphi(x)^n = 0 = \varphi(e)$, so $x^n \in Ker\ \varphi$. Thus $N \leq Ker\ \varphi$. **PENDING:** This isn't the map, kernel is too big. □

I.9.4 $Q_1 6$.

The group defined by generators a, b and relations $a^8 = b^2a^4 = ab^{-1}ab = e$ has order at most 16. [23]

Hint$(3/5)$:

Proof:

□

[23] This group is isomorphic to the general quaternion group of order 16.

Chapter II

The Structure of Groups

II.1 Free Abelian Groups

1	mA groups.	89
2	Linear Indepedence	89
3	Commutators	91
9	Free-Abelian Groups and Torsion	91
10	Non-free, Torsion-free Groups	92

II.1.1 mA groups..

(a) If A is an abelian group and $m \in \mathbb{Z}$, then $mA = \{ma \mid a \in A\}$ is a subgroup of A.

(b) If $A \cong \sum_{i\in I} G_i$, then $mA \cong \sum_{i\in I} mG_i$ and $A/mA \cong \sum_{i\in I} A_i/mA_i$.[1]

Hint$(2/5)$: Reference Exercise-I.1 and use the Fundamental Homomorphism Theorem.

Proof: Given $a, b \in A$, ma, mb are in mA and by Exercise-I.1 we know $ma + mb = m(a + b)$, and since $a + b \in A$ we see $ma + mb \in mA$ making it closed to sums. Next $0 \in A$ and $m0 = 0$ so $0 \in mA$. Finally, $-ma = m(-a)$ and since $-a \in A$, it follows $-ma \in mA$; notice $ma + -ma = ma + m(-a) = m(a - a) = m0 = 0$; thus mA is closed to inverses, the last requirement to make it a subgroup.

Suppose $G \cong \sum_{i\in I} G_i$, that is, that G is the internal direct sum of G_i's, associate $N_i \leq G$ with G_i. Each G_i is isomorphic to the subgroup N_i of G, so they too must be abelian. Therefore mG_i is a subgroup of each G_i and since all are abelian each is normal and so G_i/mG_i are defined. Furthermore, form Theorem-I.8.9 we see every element in G is a unique sum of $n_{i_1} + \cdots + n_{i_k}$ where $i_j \in I$ and each is distinct. Therefore elements of mG are of the form :

$$m(n_{i_1} + \cdots + n_{i_k}) = mn_{i_1} + \cdots + mn_{i_k},$$

and clearly each $mn_{i_j} \in mN_{i_j}$; thus, mG is all finite sums of elements from mN_i, and so we now know $mG \cong \sum_{i\in I} mG_i$. Now we have

$$G/mG = \sum_{i\in I} N_i / \sum_{i\in I} mN_i \cong \sum_{i\in I} G_i / \sum_{i\in I} mG_i,$$

so by Corollary-I.8.9, it follows $G/mG \cong \sum_{i\in I} G_i/mG_i$. □

[1] Since the spaces are abelian, normality is automatic.

II.1.2 Linear Indepedence.

Hint$(3/5)$: In part (d) notice $\{2, 3\}$ generates $\mathbb{Z}$.

A subset X of an abelian group F is said to be **linearly independent** if $n_1x_1 + \cdots + n_kx_k = 0$ always implies $n_i = 0$ for all i (where $n_i \in \mathbb{Z}$ and $x_1, \ldots, x_k$ are distinct elements of X).

(a) X is linearly independent if and only if every nonzero element of the subgroup $\langle X\rangle$ may be written uniquely in the form $n_1x_1 + \cdots + n_kx_k$ ($n_i \in \mathbb{Z}$, $n_i \neq 0$, $x_1, \ldots, x_k$ distinct elements of X).

(b) If F is free-abelian of finite rank n, it is *not* true that every linearly independent subset of n elements is a basis. [*Hint:* consider $F = \mathbb{Z}$.]

(c) If F is free-abelian, it is *not* true that every linearly independent subset of F may be extended to a basis of F.

(d) If F is free-abelian, it is *not* true that every generating set of F contains a basis of F. However, if F is also finitely generated by n elements, F has rank $m \leq n$.

(a) **Proof:** Since F is abelian we know $\langle X\rangle$ is as well. Using this we first enumerate the elements of X by a set I. Thus every element of $\langle X\rangle$ is of the from $\sum_{i\in I} n_ix_i$ because we may use the commutativity to group all elements x_i together – recall also the sum must be finite so this is valid. Given $\sum_{i\in I} n_ix_i = \sum_{i\in I} m_ix_i$ it follows:

$$\sum_{i\in I} n_ix_i - \sum_{i\in I} m_ix_i = 0; \qquad \sum_{i\in I} n_ix_i + \sum_{i\in I} -m_ix_i = 0;$$

$$\sum_{i\in I} n_ix_i - m_ix_i = 0; \qquad \sum_{i\in I} (n_i - m_i)x_i = 0.$$

($\Rightarrow$) Now if X is linearly independent we are able to conclude $n_i - m_i = 0$ for all $i \in I$, which we reduce to say $n_i = m_i$; therefore, every element is a unique linearly combination of elements of X.

($\Leftarrow$) If every element of $\langle X\rangle$ is the unique linearly combination of elements from X, then to begin with we know $n_i = m_i$ for each $i \in I$. Since $0 = \sum_{i\in I} 0x_i$ it follows any linear combination $\sum_{i\in I} n_ix_i = 0$ forces $n_i = 0$ for all $i \in I$; therefore, X is linearly independent. □

(b) **Example:** Consider $\mathbb{Z}$. The subset $\{2\}$ is linearly independent sense $m2 = 0$ requires $m = 0$. By Theorem-II.1.1 we can claim $\mathbb{Z}$ has rank 1 – consider the basis $\{1\}$. Therefore our subset satisfies the hypothesis. Yet $\langle 2\rangle = 2\mathbb{Z}$ and does not include 1 – in part because 1 is not even – so $2\mathbb{Z} \neq \mathbb{Z}$; therefore, $\{2\}$ is not a basis of $\mathbb{Z}$. □

(c) **Example:** Staying with the example of part (b), if we extend $\{2\}$ to a set X that we wish to be a basis, there is no way to add any elements without changing the rank of $\mathbb{Z}$; however, this violates Theorem-II.1.2.

As a further example, the set $\{(2, 0)\}$ is linearly independent in $\mathbb{Z} \oplus \mathbb{Z}$ since $m(2, 0) = (0, 0)$ only when $2m = 0$, that is when $m = 0$. We know $\mathbb{Z} \oplus \mathbb{Z}$ can be generated by the basis $\{(1, 0), (0, 1)\}$, so it has rank 2. By Theorem-II.1.2, in $\mathbb{Z} \oplus \mathbb{Z}$ every basis will have rank 2. So we need to add one element to our set to hopefully construct a basis; so consider now $X = \{(2, 0), (x, y)\}$. If $y = 0$ then $\langle X\rangle$ does not contain $(0, 1)$, so in the contrapositive $y \neq 0$. Now suppose $(1, 0) = m(2, 0) + n(x, y)$ which implies

$1 = 2m + nx$ and $0 = ny$. But as we know, $y \neq 0$ so $n = 0$ and this requires $1 = 2m$ which cannot be; therefore, X cannot generate $\mathbb{Z} \oplus \mathbb{Z}$ and so $\{(2, 0)\}$ cannot be extended to a basis. □

(d) **Example:** Finally notice for every integer n, $n = n1 = n(2 + -3) = n2 + (-n)3$ so in fact the set $\{2, 3\}$ generates $\mathbb{Z}$. However we saw in part (b) that because $1 \neq 2m$ (and likewise $1 \neq 3m$) the set $\{2\}$ (and so also $\{3\}$) was not a basis of $\mathbb{Z}$. Therefore this generating set does not contain a basis of $\mathbb{Z}$.

Suppose every element of F can be expressed in the form $\sum_{i=1}^{n} n_i x_i$ for a fixed set $X = \{x_1, \ldots, x_n\}$. If X is linearly independent then we have satisfied the requirements for a basis and we say F has rank n. If not, then it must be the case that $\sum_{i=1}^{n} n_i x_i = 0$ where at least one $n_i \neq 0$ (recall we already assumed X generates F so there is no problem assuming X generates 0 at some point).

Suppose F has a rank $m > n$, so that it has a basis $Y = \{y_1, \ldots, y_m\}$. The trick now is to replace each y_i with its corresponding linear combination of X. So for every element we have a linear combination of linear combinations:

$$\sum_{i=1}^{m} m_i y_i = \sum_{i=1}^{m} m_i \sum_{j=1}^{n} n_j x_j = \sum_{i=1}^{m} \sum_{j=1}^{n} (m_i n_j) x_j = \sum_{j=1} k_j x_j.$$

Therefore $\sum_{i=1}^{m} m_i y_i = 0$ does not require each $m_i = 0$ as there is some $k_j = \sum_{i=1}^{m} m_i n_j \neq 0$ where $\sum_{j=1}^{n} k_j x_j = 0$; therefore, Y is not linearly independent. Thus we conclude any basis of F has rank less than or equal to n. □

II.1.3 Commutators.

Let $X = \{a_i \mid i \in I\}$ be a set. Then the free-abelian group on X is (isomorphic to) the group defined by the generators X and the relations (in multiplicative notation) $\{a_i a_j a_i^{-1} a_j^{-1} = e \mid i, j \in I\}$.[2]

Hint$(2/5)$: Notice these relators yield the relations $ab = ba$ for all generators a and b in X.

Proof: Let F be the free group on X, through the map $\iota : X \to F$, as outlined in Theorem-I.9.1, and let A be the free-abelian group on X as defined for Theorem-II.1.1, with the map $\alpha : X \to A$ from part (iv). Therefore by the freeness of F we have a unique homomorphism $\varphi : F \to A$ such that $\varphi\iota = \alpha$. Furthermore, X is a set of generators of both F and A so the map φ is surjective.

We know A is abelian and also generated by X, so for every $i, j \in I$, $\alpha(a_i)\alpha(a_j) = \alpha(a_j)\alpha(a_i)$ which equates to $\alpha(a_i)\alpha(a_j)\alpha(a_i)^{-1}\alpha(a_j)^{-1} = e$, so

$$\begin{aligned} \varphi(e) &= e = \alpha(a_i)\alpha(a_j)\alpha(a_i)^{-1}\alpha(a_j)^{-1} \\ &= \varphi\iota(a_i)\varphi\iota(a_j)\varphi\iota(a_i)^{-1}\varphi\iota(a_j)^{-1} \\ &= \varphi(\iota(a_i)\iota(a_j)\iota(a_i)^{-1}\iota(a_j)^{-1}). \end{aligned}$$

So we see each commutator $\iota(a_i)\iota(a_j)\iota(a_i)^{-1}\iota(a_j)^{-1}$ is in the kernel of φ.

Now suppose $[F, F] = \langle \iota(a_i)\iota(a_j)\iota(a_i)^{-1}\iota(a_j)^{-1} \mid i, j \in I \rangle$. **PENDING:** finish. □

[2] These relators are called the commutators of a group.

II.1.4 Free-Abelian Groups and Torsion.

Let G be a finitely generated abelian group in which no non-trivial element has finite order.[3] Then G is a free-abelian group.

Hint$(2/5)$: Use Theorem-II.1.6

Proof:

□

II.1.5 Non-free, Torsion-free Groups.

(a) Show that the additive group of rationals $\mathbb{Q}$ is not finitely generated.

(b) Show $\mathbb{Q}$ is not a free nor free-abelian group. [4]

(c) Conclude that Exercise-II.1 fails if "finitely generated" is removed.

Hint$(3/5)$: In part (a) notice a finite set of rationals always leaves $1/(b_1 \cdots b_n + 1)$ out of the generating set. For (b) notice no two fractions are linearly independent.

Example: Take a any finite set $\{a_1/b_1, \ldots, a_n/b_n\}$ of rationals. The space they generate is equivalent to

$$A = \left\{ k_1 \frac{a_1}{b_1} + \cdots + k_n \frac{a_n}{b_n} \ : \ k_i \in \mathbb{Z} \right\}$$

as $\mathbb{Q}$ is abelian. However,

$$k_1 \frac{a_1}{b_1} + \cdots + k_n \frac{a_n}{b_n} = \frac{k_1 a_1 b_2 \cdots b_n + \cdots + k_n a_n b_1 \cdots b_{n-1}}{b_1 \cdots b_n};$$

whence, A never contains $\frac{1}{b_1 \ldots b_n + 1}$ but $\mathbb{Q}$ does. So we must conclude that no finite subset of $\mathbb{Q}$ generates $\mathbb{Q}$; so $\mathbb{Q}$ is not finitely generated.

To show $\mathbb{Q}$ is not a free group consider a homomorphism f of $\mathbb{Q}$ to S_3. Recall $f(n \cdot q) = f(q)^n$ for all $q \in \mathbb{Q}$ and $n \in \mathbb{Z}$. Notice $f(q)^6 = \varepsilon$ as every element in S_3 has order dividing 6. Thus $f(6q) = \varepsilon$ for all $q \in \mathbb{Q}$. But certainly every $q = 6p$, for some $p \in \mathbb{Q}$; hence, $f(q) = f(6p) = \varepsilon$ so f is trivial.

Now consider the abelian case. Take any two rational numbers $a/b, c/d$. Notice that

$$cb\frac{a}{b} + (-ad)\frac{c}{d} = ca - ac = 0,$$

so a/b and c/d are linearly dependent over $\mathbb{Z}$, so there can be no basis for $\mathbb{Q}$. Therefore by Theorem-1.1 $\mathbb{Q}$ cannot be a free-abelian group. □

[3] Such a group is called torsion-free.

[4] Later this can be adapted to say: Given an integral domain I and its field of fractions $Q(I)$, $Q(I)$ is a free I-module if and only if $I = Q(I)$. The proof follows from replacing $\mathbb{Z}$ with I and $\mathbb{Q}$ with $Q(I)$.

II.2 Finitely Generated Abelian Groups

II.3 The Krull-Schmidt Theorem

II.4 The Action of a Group on a Set

II.5 The Sylow Theorems

II.6 Classification of Finite Groups

II.7 Nilpotent and Solvable Groups

II.8 Normal and Subnormal Series

Chapter III

Rings

III.1 Rings and Homomorphisms

9 Quaternion Group Ring vs. Division Ring 101

III.1.1 Quaternion Group Ring vs. Division Ring.

Show the algebra of quaternions(Hamiltonions) $\mathbb{H}$ determined by:

$$\hat{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \hat{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \hat{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ and } \hat{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

over the reals is not isomorphic to $\mathbb{R}Q_8$. *Refer to Appendix-?? for a detailed treatment of group algebras and Theorem-?? for the general proof employed here.*

Proof: Take the element $i \in Q_8$. Using the geometric series notice

$$\begin{aligned}(\hat{1} - \hat{i})(\hat{1} + \hat{i} + \widehat{-1} + \widehat{-i}) &= \hat{1} + \hat{i} + \widehat{-1} + \widehat{-i} \\ &\quad -\hat{i} - \widehat{-1} - \widehat{-i} - \hat{1} = 0.\end{aligned}$$

Yet clearly $\hat{1} - \hat{i} \neq 0$ and neither does $\hat{1} + \hat{i} + \widehat{-1} + \widehat{-i}$ so they are in fact zero-divisors in $\mathbb{R}Q_8$. Thus $\mathbb{R}Q_8$ is not a field and so cannot be isomorphic to $\mathbb{H}$. □

However the mapping $f : \mathbb{R}Q_8 \to \mathbb{H}$ by $f(\widehat{-1}) = 1$ – so that $f(\widehat{-i}) = i, f(\widehat{-j}) = j$ and $f(\widehat{-k}) = k$ – determines a surjective linear homomorphism that also preserves products; that is: $\mathbb{H}$ is a factor ring of $\mathbb{R}Q_8$.

III.2 Ideals

1 The Little Radical Ideal 102
2 Radical Ideal 102
4 The Annihilator Ideal 103
5 The "Idealizer" 103
7 Division Rings have no Left Ideals 103
11 Nilpotent Factor Ring 104
13 Homomorphic Image of Ideals 104
15 Prime Ideal in Zero-Divisors 104
19 Maximal Ideals in Non-Unital Rings 105
21 Prime/Maximal Ideals in $\mathbb{Z}/m\mathbb{Z}$ 105
25 Prime Decomposition of Integer Rings 105
26 Limitation of Chinese Remainder Theorem 105

III.2.1 The Little Radical Ideal.

The set of all nilpotent elements in a commuative ring forms an ideal.

Proof: Given R is a commutative ring, let $S \subseteq R$ such that S consists of all nilpotent elements of R. Clearly $0^1 = 0$ so $0 \in S$ so S is non-empty. Given $a, b \in S$, by the definition of S, $a^m = 0$ and $b^n = 0$ for some positive integers m and n. Given $ab = ba$ the binomial theorem applies:

$$(a+b)^{mn} = a^{mn} + \sum_{k=1}^{mn-1} \binom{mn}{k} a^k b^{mn-k} + b^{mn}.$$

If $m = n = 1$ then $a = 0$ and $b = 0$ so $a + b = 0$. Without loss of generality suppose $m > 1$. Whenever $k < m$, $nk < mn$ so $(n-1)k < mn - k$. With $k > 1$, $(n-1)k \geq n$ and when $k = 1$, $mn - k \geq n$, so in general $n \leq mn - k$. So $b^{mn-k} = b^n b^{mn-k-n} = 0b^{mn-k-n} = 0$ and whenever $k \geq m$, $a^k = a^m a^{k-m} = 0a^{k-m} = 0$. Cancelling appropriately the binomial expansion reduces to:

$$(a+b)^{mn} = (a^m)^n + \sum_{k=1}^{m-1} a^k 0 + \sum_{k=m}^{mn-1} 0b^{mn-k} + (b^n)^m = 0 + 0 + 0 + 0 = 0$$

leaving S closed to sums.

Again using the commutative multiplication observe $0 = 0 \cdot 0 = (a^m)^n (b^n)^m = (ab)^{mn}$ so $ab \in S$. To close S to negatives notice, when n is even $(-a)^n = (a^n) = 0$, and when n is odd $(-a)^n = -(a^n) = 0$, leaving $-a \in S$. Therefore S is a subring of R.

Finally given any $x, y \in R$, R is commutative so $(xay)^n = x^n a^n y^n = x^n 0 y^n = 0$ so $xay \in S$, proving S is an ideal of R. □

III.2.2 Radical Ideal.

Let I be and ideal in a commutative ring R and let $Rad\ I = \{r \in R \mid r^n \in I\}$ for some n. $Rad\ I \trianglelefteq R$.

Proof: Since I is an ideal of R take $f : R \to R/I$ to be the canonical homomorphism. If $(r+I)^n = r^n + I = I$ then $r^n \in I$ so $r \in Rad\ I$, and for all $r \in Rad\ I$, $f(r)^n = r^n + I = I$. Therefore $Rad\ I$ is simply the pre-image of the nilpotent

elements of R/I. Exercise III.2.1 ensures the nilpotent elements of a ring form an ideal. Applying Theorem III.2.13 it follows the pre-image of an ideal is an ideal, therefore $Rad\ I$ is and ideal of R. □

III.2.3 The Annihilator Ideal.

If I is and ideal of R, then $A(I) = \{r \in R \mid rI = 0\}$ is an ideal in R.

Proof: Note that $\alpha_r : I \to I$ defined as $\alpha_r(x) = rx$ is a group endomorphism of R since $r(x + y) = rx + ry$. Additionally α_r is well-defined for all r in R because I is an ideal and thus $rx \in I$. Also note that the endomorphisms of R form a ring with pointwise addition and composition as multiplication. Now define the map $f : R \to End(I)$ by $r \mapsto \alpha_r$. A unique image element exists for each domain element so f is well-defined. Also $f(r + s) = \alpha_{r+s}$ but evaluating $\alpha_{r+s}(x) = (r + s)x = rx + sx = \alpha_r(x) + \alpha_s(x)$ so $\alpha_{r+s} = \alpha_r + \alpha_s$ and so $f(r + s) = f(r) + f(s)$. Finally $f(rs) = \alpha_{rs}$ and once again $\alpha_{rs}(x) = (rs)x = r(sx) = \alpha_r(\alpha_s(x))$ leaving $\alpha_{rs} = \alpha_r\alpha_s$ so $f(rs) = f(r)f(s)$.

Since f is now seen as a ring homomorphism its kernel is an ideal of R. Furthermore $f(r) = 0 = \alpha_0$ only when $rx = 0$ for all $x \in R$. Therefore $r \in Ker\phi$ only if it is also in $A(I)$. Lastly given $r \in A(I)$ it follows $\alpha_r(x) = rx = 0$ so $r \in Ker\ f$ sandwhiching $A(I)$ between $Ker\ f$ thus $A(I) = Ker\ f \trianglelefteq R$. □

III.2.4 The "Idealizer".

Let $I \trianglelefteq R$ and define $[R : I] = \{r \in R \mid Rr \leq I\}$. Prove $I \trianglelefteq [R : I] \trianglelefteq R$.

Proof: First note given $i \in I$ it follows $ri \in I$ for all r in R so in deed I is contained in $[R : I]$. With r, s taken from $[R : I]$ it is assumed xr and xs are contained in I for all $x \in R$. Therefore $x(r - s) = xr - xs$ is contained in I since I is a subgroup of R, acknowledging that $r - s \in [R : I]$.

Next with $a \in R$ notice $Rr \leq I$ and thus $a(Rr) \leq aI \leq I$ and $(Rr)a \leq Ia \leq I$ so $a[R : I] \leq [R : I]$ and $[R : I]a \leq [R : I]$. Thus $[R : I] \trianglelefteq R$. □

III.2.5 Division Rings have no Left Ideals.

A ring with identity ($1 \neq 0$) is a division ring if and only if it has no proper left (right) ideals. Furthermore If S is a ring with no proper left (right) ideals, then either $S^2 = 0$ or S is a division ring.

Proof: Consider R, a unital ring. When R is a division ring and I a left (right) ideal of R, I must absorb product. But for all $r \in I$, if $r \neq 0$ then there exists a left inververse r' (correspondingly $'r$ for a right inverse) such that $r'r = 1$. Therefore when I is nonzero it is the entire ring. So R has no proper left(right) ideals.

Consider R to be a unital ring with no left (right) proper ideals. Given any nonzero element a in R, which must exists since $1 \neq 0$, then Ra is a left ideal (correspondingly aR is a right ideal). Left (right) ideals may not be proper so Ra (aR) is **0** or R. The unity of R allows $a \in Ra$ ($a \in aR$) where $a \neq 0$ so $Ra = R$ ($aR = R$). Thus $1 \in Ra$ ($1 \in aR$) so there exists an a' (correspondingly $'a$) such that $1 = a'a$, so a is left (right) invertible.

Having shown $Ra = R$ for all nonzero a in R take a and b to be non-zero elements in R and suppose they are zero-divisors so that $ab = 0$. Thus it would follow that $0 = R0 = Rab = (Ra)b = Rb = R$ but $1 \neq 0$, forcing $R \neq 0$ so a and b are not zero-divisors. Therefore $R - \{0\}$ is closed under multiplication and so it is a semigroup with left identity and left inverses so it has a multipliative group

structure. Therefore R is a division ring.

Let R be any ring with no proper left (right) ideals. Let $T = \{a \in R \mid Ra = 0\}$. Given that $0a = 0$, T is nonempty and furthermore given $s, t \in T$ and $r \in R$, $(s+t)a = sa + ta = 0 - 0 = 0$ so $r + s \in T$, and finally $(rs)a = r(sa) = r0 = 0$ so $rs \in T$. Therefore T is a left (right) ideal of R and so it must be **0** or R. If $T = R$ then $R^2 = 0$. Suppose instead $T =$ **0**.

Since $T \neq$ **0** there exists a $d \in R$ such that $d \neq 0$ and $cd \neq 0$ for some c in R. Now define the map $f : R \to Rd$ as $f(r) = rd$. This map is R-linear so the kernel is a left submodule of R, and thus a left ideal of R. Therefore $Ker\ f$ is **0** or R: if it is R then $cd = 0$ which is a contradiction, so it is **0**, that is to say $Rd = R$. Therefore there exists an $e \in R$ such that $ed = d$. [PENDING: show left cancellation. From cancellation note $rd = red$ implies $r = re$ and next use the following argument to show e is two-sided so that the first part may be used. This part provided by David Oury:] Suppose there exists two left identities e and e'; then $0 = a - a = ea - e'a = (e - e')a$ and using left cancelation $0 = e - e'$ thus $e = e$. □

III.2.6 Nilpotent Factor Ring.

If N is the ideal of all nilpotent element of R as demonstrated in Exercise-III.2, then R/N is a ring with no nonzero nilpotent elments.

Proof: Given a nilpotent element $x + N$ in R/N, $N = (x + N)^m = x^m + N$ by definition. However this implies $x^m \in N$ and since N is the set of all nilpotent elements it follows x^m is nilpotent. That is there exists an n such that $0 = (x^m)^n = x^{mn}$. However this implies x is nilpotent so $x \in N$ thus $x + N = N$ so all nilpotent elements are trivial. □

III.2.7 Homomorphic Image of Ideals.

Let $f : R \to S$ be a homomorphism of rings, I and ideal of R, and J an ideal of S.

(a) $f^{-1}(J)$ is an ideal in R that contains the kernel of f.

(b) If f is an epimorphism then $f(I)$ is an ideal in S. If f is not surjective, $f(I)$ need not be an ideal in S.

Proof:

(a) Let a, b be elements of R. Clearly $f(a)Jf(b) \subseteq J$ since J is an ideal of S. Thus $af^{-1}(J)b \subseteq f^{-1}(J)$ so $f^{-1}(J)$ is an ideal in R. Since $0 \in J$ it follows $Ker\ f = f^{-1}(0) \leq f^{-1}(J)$.

(b) Suppose f is an epimorphism. Then given an ideal $I \in R$, and $a, b \in R$, $f(aIb) = f(a)f(I)f(b) \subseteq f(I)$ and therefore $f(I) \trianglelefteq f(R) = S$. As a counterexample for when f is not an epimorphism take the mapping: $f : \mathbb{Z} \to \mathbb{R}$ where $f(x) = x$. Clearly $2\mathbb{Z} \trianglelefteq \mathbb{Z}$ because $m(2i)n = 2(imn)$ is always even. However $2\mathbb{Z}$ is not an ideal of $\mathbb{R}$ as seen for example with π: $\pi 2 = 2\pi$ which is not an integer thus not included in $2\mathbb{Z}$.

□

III.2.8 Prime Ideal in Zero-Divisors.

In a commutative unital ring R, the set $Z = \{a \in R \mid ab = 0, \text{for some } b \in R, b \neq 0\}$ contains a prime ideal.

Proof: Define $S = R - Z$. Every element of S is not a zero-divisor nor is it zero. Therefore the product of elements $a, b \in S$ is not equal to zero. Suppose ab where a zero divisor, that is that ab is in Z not S. Then there exists a $c \in R$, $c \neq 0$ such that $(ab)c = 0$. Therefore $a(bc) = 0$ and using the commutativity $b(ac) = 0$ forcing either a or b to be zero-divisors. This is a contradiction of the definition of S so it follows ab is not a zero-divisor. Therefore S is multiplacative.

Applying Theorem VIII, 2.2 it follows there exists a prime ideal in $R - S = Z$. □

III.2.9 Maximal Ideals in Non-Unital Rings.

The ring of even integers contains a maximal ideal whose factor ring is not a field.

Proof: Notice in general $2\mathbb{Z}/(2m)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$. Thus to choose and m where $2m\mathbb{Z}$ is maximal requires only that $(2, m) = 1$. And since furthermore we want the factor ring to not be a ring choose such and m that is a composite number so the factor ring will have zero-divisors; $m = 15$ works: $2\mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$ which is not a field since $3 \cdot 5 = 0$. □

III.2.10 Prime/Maximal Ideals in $\mathbb{Z}/m\mathbb{Z}$.

Determine all prime and maximal ideals of $\mathbb{Z}/m\mathbb{Z}$.

Proof: By Theorem-III.2.19 we know every maximal ideal in these commutative unital rings is a prime ideal. Therefore it sufficies to find all prime ideals. The factor ring of a prime ideal must have no zero-divisors. If a factor ring is to have no zero-divisors and yet be a cyclic unitary commutative ring isomorphic to some $k\mathbb{Z}$, then k must be prime. Thus the general prime ideals are of the form $p\mathbb{Z}/m\mathbb{Z}$. Notice that in fact all these prime ideals are also maximal because they have prime index, meaning their factor rings are $\mathbb{Z}/p\mathbb{Z}$. □

III.2.11 Prime Decomposition of Integer Rings.

If m is an integer with (unique) prime decomposition $p_1^{k_1} \cdots p_t^{k_t}$, with each p_i distinct, then $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{k_t}\mathbb{Z}$.

Proof: Clearly $p_i^{k_i}\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for all i. Also $\mathbb{Z}^2 + p_i^{k_i}\mathbb{Z} = \mathbb{Z} + p_i^{k_i}\mathbb{Z} = \mathbb{Z}$ and given $i \neq j$, $(p_i^{k_i}, p_j^{k_j}) = 1$ implies $p_i^{k_i}\mathbb{Z} + p_j^{k_j}\mathbb{Z} = \mathbb{Z}$ so the map described by Corollary-III.2.27 is an isomorphism; that is:

$$\mathbb{Z}/(p_1^{k_1}\mathbb{Z} \cap \cdots \cap p_t^{k_t}\mathbb{Z}) \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{k_t}\mathbb{Z}.$$

However $(p_1^{k_1}\mathbb{Z} \cap \cdots \cap p_t^{k_t}\mathbb{Z}) = (p_1^{k_1} \cdots p_t^{k_t})\mathbb{Z} = m\mathbb{Z}$ so in fact:

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{k_t}\mathbb{Z}.$$

□

III.2.12 Limitation of Chinese Remainder Theorem.

The map $f : \mathbb{Z}/6\mathbb{Z} \cap 4\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ as described in Corollary-III.2.27 is not surjective.

Proof: Note that $[6, 4] = 12$ thus $6\mathbb{Z} \cap 4\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} = 12\mathbb{Z}$. But clearly then the order of the domain is 12 while the order of the image remains 24, thus no surjection exists between the sets, let alone one that is a ring homomorphism such as f. Therefore f is not surjective. $\square$

III.3 Factorization in Commutative Rings

1 Maximal and Prime Principal Ideals 107
3 Irreducible Non-Prime Elements 107

III.3.1 Maximal and Prime Principal Ideals.

A nonzero ideal in a principal ideal domain is maximal if and only if it is prime.

Proof: Theorem 3.4 part *iv* demonstrates an element p in a principal ideal domain D is prime if and only if p is irreducible in D. By part *i* of the same theorem p is prime if and only if (p) is a prime ideal, and part *ii* states p is irreducible if and only if (p) is maximal in P. Therefore (p) is prime if and only if (p) is irreducible in P. Since P is a principal ideal domain, for every ideal I there exists an element x such that $(x) = I$. Thus in a principal ideal domain every ideal is prime if and only if it is irreducible. □

III.3.2 Irreducible Non-Prime Elements.

Let $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ be a subring of $\mathbb{R}$.

(a) The map $N : R \to \mathbb{Z}$ defined by $N(x) = x\overline{x}$ (if $x = a + b\sqrt{10}$ then $\overline{x} = a - b\sqrt{10}$) has the properties $N(xy) = N(x)N(y)$ and $N(x) = 0$ if and only if $x = 0$.

(b) u is a unit in R if and only if $N(u) = \pm 1$.

(c) 2,3, $4 + \sqrt{10}$, and $4 - \sqrt{10}$ are irreducible in R.

(d) 2,3, $4 + \sqrt{10}$, and $4 - \sqrt{10}$ are *not* prime in R.

Therefore there are irreducible elements that are not prime.

Proof:

(a) Since a and b are integers it follows $a^2 - 10b^2$ is also an integer. Given $x = a + b\sqrt{10}$ an element in R it follows $b \in \mathbb{Z}$ and so $-b \in \mathbb{Z}$ thus $\overline{x} = a - b\sqrt{10}$ is in R. Multiplication in R is defined by multiplication in the reals therefore $x\overline{x}$ is well-defined and in fact $x\overline{x} = a^2 - 10b^2 \in \mathbb{Z}$. Therefore N is well-defined.

Let $x = a + b\sqrt{10}$ and $y = c + d\sqrt{10}$ be arbitrary elements of R.

$$\begin{aligned} N(xy) &= N((ac + 10bd) + (ad + bc)\sqrt{10}) = (ac + 10bd)^2 - 10(ad + bc)^2 \\ &= a^2c^2 + 100b^2d^2 - 10a^2d^2 - 10b^2c^2 = (a^2 - 10b^2)(c^2 - 10d^2) \\ &= N(x)N(y). \end{aligned}$$

When $x = 0$ it is clear $N(x) = 0$. Given $N(x) = 0$ it follows $a^2 - 10b^2 = 0$ therefore $a^2 = 10b^2$ and so $|a| = |b|\sqrt{10}$, so either a is not an integer or b is not, unless both are zero. Therefore $x = 0$.

(b) Suppose $uv = 1$ for two elements u, v in R. Applying the norm function it is clear $N(u)N(v) = N(uv) = N(1) = 1$. Since N maps only into the integers and only 1 and -1 have multiplicative inverses in $\mathbb{Z}$ it follows $N(u) = \pm 1$.

(c) Suppose $2 = uv$ for two non-units u and v in R. Then $N(u)N(v) = N(2) = 4$ and with u and v being non-units it is forced that $N(u) = \pm 2$. Let $u = a + b\sqrt{10}$ and consider the equation $a^2 - 10b^2 = N(u) = \pm 2$. Since the equation is true in the integers it must be true in its factor rings therefore $a^2 - 10b^2 \equiv 2 \pmod 5$. However no element exists in $\mathbb{Z}/5\mathbb{Z}$ such that $a^2 = 2$ (proved by testing all five elemtns.) So no u exists in R with the property $N(u) = \pm 2$ concluding by contradiction that 2 is irreducible in R.

Again suppose $3 = uv$ with u and v again non-unit elements. Picking up the pace suppose $a^2 - 10b^2 = N(u) = \pm 3$. Then $a^2 - 10b^2 \equiv 3 \pmod 5$ but once again $a^2 \neq 3$ mod 5 for any elements a. Therefore 3 is irreducible in R.

Finally $N(4 \pm \sqrt{10}) = 16 - 10 = 6$. Suppose $4 \pm \sqrt{10} = uv$ for non-units u and v. Then clearly $N(u)N(v) = 6$ and thus $N(u) = \pm 2$ or ± 3 however from the above argument it is clear no such element exists therefore $4 \pm \sqrt{10}$ is irreducible.

(d) Notice $2 \cdot 3 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$. If 2 is prime then since 2 divides 6 it should follow 2 divides $4 + \sqrt{10}$ or $4 - \sqrt{10}$ which it cannot since both are irreducible and 2 is not a unit. Therefore 2 is not prime. The same argument implies 3 and $4 \pm \sqrt{10}$ are not prime either.

□

III.4 Rings of Quotients and Localization

III.5 Rings of Polynomials and Formal Power Series

III.6 Factorization in Polynomial Rings

Chapter IV

Modules

IV.1 Modules, Homomorphisms, and Exact Sequences

1 $\mathbb{Z}/n\mathbb{Z}$ Modules 113
2 Monic/Epic Morphisms of Modules 113
3 R/I-Modules 114
4 Unitary Cyclic Modules 115
5 Schur's Lemma 115
6 Finitely Generated Modules 116
7 Hom and Endomorphisms 116
8 Module Products and Sums 117
9 Idempotent and Splitting Maps 119
15 Split Decomposition 119
12 5-Lemma 119
17 Unitary Separation 121

IV.1.1 $\mathbb{Z}/n\mathbb{Z}$ Modules.

Hint$(1/5)$: Verify the axioms directly.

If A is abelian where for some integer $n > 0$, $na = 0$ for all $a \in A$ then A is a unitary $\mathbb{Z}/nZ$-module where $k \equiv \overline{k} \pmod{n}$ implies $ka = \overline{k}a$.

Proof: Clearly A remains an abelian group thus only the scalar properties need be verified for the ring action of $\mathbb{Z}/n\mathbb{Z}$. Suppose $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ then by definition $m \equiv \overline{m} \pmod{n}$ and thus $\overline{m}a = ma \in A$ for all elements a of A, so that A is closed to scalar multiplication by $\mathbb{Z}/n\mathbb{Z}$.

Let a, b be elements of A and $\overline{k}, \overline{m}$ elements of $\mathbb{Z}/n\mathbb{Z}$. It follows $\overline{m}(a + b) = m(a + b)$ by definition thus $\overline{m}(a + b) = ma + mb = \overline{m}a + \overline{m}b$. Likewise $(\overline{k}+\overline{m})a = \overline{k + m}a = (k+m)a = ka+ma = \overline{k}a+\overline{m}a$ therefore scalars distribute over A and A distributes over scalars.

Finally $\overline{k}(\overline{m}a) = \overline{k}(ma) = k(ma) = (km)a = \overline{km}a = (\overline{k}\overline{m})a$. Notice $n+1 \equiv 1 \pmod{n}$ and therefore $1a = \overline{(n + 1)}a = (n+1)a = na+a = 0+a = a$. Therefore A is a unitary $\mathbb{Z}/n\mathbb{Z}$ module. $\square$

IV.1.2 Monic/Epic Morphisms of Modules.

A homomorphism $f : A \to B$ of modules is:

- Injective if and only if it is a monomorphism (left/forward cancelable,) that is: $fg = fh$ implies $g = h$.
- Surjective if and only if it is an epimorphism (right/rear cancelable,) that is: $gf = hf$ forces $g = h$.
- Bijective if and only if it is an isomorphism. Together this means every map that is both a monomorphism and an epimorphism is an isomorphism.

Show where the presumption of modules is used in the proof for epimorphisms.

Proof:

- Let g and h be mappings such that the following diagram commutes:

$$D \qquad A \qquad B.$$

Thus the diagram requires $f(g(x)) = f(h(x))$ for all $x \in D$. When f is injective clearly $g(x) = h(x)$ for all $x \in D$ leaving $g = h$. *Therefore in any concrete category an injective morphism is a monomorphism.*

Now suppose f is a monomophism and take $D = Ker\ f$ with $g : x \mapsto x$ and $h : x \mapsto 0$. Each map follows canonical definition so they are accepted as well-defined. Since f has the left cancelation property for all morphisms any requirements on its structure infered from these two morphisms must apply to f always. Notice $f(g(x)) = 0$ and $f(h(x)) = f(0) = 0$ for all $x \in Ker\ f$ thus $fg = fh$. By assumption (f a monomorphism) it follows $g = h$. Thus $Ker\ f = g(Ker\ f) = h(Ker\ f) =$ **0** so f is injective.

Notice this property assumes only the group structure of modules.

- Let g and h be mappings such that the following diagram commutes:

$$A \qquad B \qquad D,$$

so that $gf = hf$. Suppose f is surjective so that given $y \in B$ there exists $x \in A$ such that $f(x) = y$. With no use of modules it follows $g(y) = g(f(x)) = h(f(x)) = h(y)$ so $g = h$. *So once again any surjection in a concrete category is an epimorphism.*

Towards the converse however the properties of modules will be used. Take f to be an epimorphism and let $D = B/Im\ f$. In modules $Im\ f$ can function as a kernel, as all submodules can (refer to Theorem 1.6 and Definition 1.3), so D is a well-defined module. Now take $g : x \mapsto x + Im\ f$ and $h : x \mapsto Im\ f$. Both maps are canonical maps so they are easily seen as well-defined.

To conclude $g(f(x)) = f(x) + Im\ f = Im\ f = h(f(x))$ thus $gf = hf$ and by the assumption that f is an epimorphism it follows $g = h$. Therefore $y + Im\ f = g(y) = h(y) = Im\ f$ for all $y \in B$. Therefore $B \leq Im\ f$ and clearly $Im\ f \leq B$ so $B = Im\ f$ forcing f to be surjective.

- An isomorphism is a bijective homomorphism of modules. Additionally a map is bijective if and only if it is both injective and surjective and thus if and only if it is a monomorphism and epimorphism of modules.

□

Hint$(2/5)$: T
rections of th
follow in all
gories and th
best treated wi
methods.

IV.1.3 R/I-Modules.

Let I be a left ideal of a ring R and A an R-module.

Hint$(2/5)$: Take care not to assume S is in IS, or that S is a submodule of A itself. Direct verification is required.

(a) If S is a nonempty subset of A, then

$$IS = \left\{ \sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{Z}^+, r_i \in I, a_i \in S \right\}$$

is a submodule of A. Note that if $S = \{a\}$, then $IS = Ia = \{ra \ : \ r \in I\}$.

(b) If I is a two-sided ideal, then A/IA is an R/I-module with the action of R/I given by $(r + I)(a + IA) = ra + IA$.

Proof: Since S is non-empty there exists and $a \in S$ and as such $0 = 0a \in IS$, so IS is non-empty. Now take any $r = \sum_{i=1}^{n} r_i a_i, s = \sum_{j=1}^{m} s_j a_j \in IS$. Without loss of generality we may take $n = m$ and $i = j$ by setting $r_i = 0$ or $s_j = 0$ whenever there is no term in some position. Thus we have:

$$r + s = \sum_{i=1}^{n} r_i a_i + \sum_{i=1}^{n} s_i a_i = \sum_{i=1}^{n} (r_i + s_i) a_i$$

and as I is a left ideal it is closed the sums $r_i + s_i$ allowing us to conclude $r + s \in IS$.

Finally, given any $t \in R$, as I is a left-ideal, $tI \subseteq I$ and so: $tr = t \sum_{i=1}^{n} r_i a_i = \sum_{i=1}^{n} (tr_i) a_i$ which lies again in IS. Hence IS is a submodule of A.

Suppose that I is a two-sided ideal of R. Then R/I is a well-defined quotient ring and from our previous work IA is a submodule of A allowing us to take the quoteint A/IA certainly as abelian groups. Moreover we need to verify that A/IA is an R/I-module when equiped with the proper action.

Take $a + IA, b + IA$ and $r + I, s + I \in R/I$.

$$\begin{aligned}
(r + I)((a + IA) + (b + IA)) &= (r + I)((a + b) + IA) = r(a + b) + IA \\
&= (ra + rb) + IA = (ra + IA) + (rb + IA); \\
((r + I) + (s + I))(a + IA) &= ((r + s) + I)(a + IA) = (r + s)a + IA \\
&= (ra + sa) + IA = (ra + IA) + (rs + IA); \\
(r + I)((s + I)(a + IA)) &= (r + I)(sa + IA) = r(sa) + IA = (rs)a + IA \\
&= (rs + I)(a + IA).
\end{aligned}$$

Furthermore, if R is a unital ring, and A a unital R-module, then

$$(1 + I)(a + IA) = (1a) + IA = a + IA$$

so A/IA is a unital R/I-module. □

IV.1.4 Unitary Cyclic Modules.

Let R be a unital ring. Every unitary cyclic R-module is isomorphic to an R-module of the form R/J for some left ideal J in R.

Hint$(1/5)$: As such a module by definition is of the form Ra, construct an R-linear map onto $R \to Ra$.

Proof: Every unitary cyclic R-module is of the form Ra for some a in the module by its definition. Define $f : R \to Ra$ by $f(r) = ra$. f is well-defined since Ra is an R-module and thus has well-defined scalar multiplication. Take r, s from R; $f(r+s) = (r+s)a = ra + sa = f(r) + f(s)$, and $f(rs) = (rs)a = r(sa) = rf(s)$.

Therefore f is a linear mapping so $R/Ker\ f \cong Ra$ as modules. Clearly $Ker\ f$ is a normal subgroup of R. Notice also given $r \in R$ and $s \in Ker\ f$ it follows $f(rs) = rf(s) = r0 = 0$ thus $rs \in Ker\ f$ so $Ker\ f$ is a left ideal of R. □

IV.1.5 Schur's Lemma.

Hint$(2/5)$: For the first part proceed by contradiction. In the second consider what are the possible kernels of any endomorphism.

A non-zero unitary R-module A is *simple* if its only submodules are 0 and A.

(a) Every simple module is cyclic.

(b) If A is simple each endomorphism is either the zero map or an automorphism. [Schur's Lemma.]

Refer to Exercise-IV.1.

Proof:

- Suppose A is not cyclic so that is has a set X which generates A. A is non-zero so X is non-empty. Choose a from X and not Ra is clearly a submodule of A since A is a unitary module. Also $Ra \neq A$ or otherwise A would be cyclic. Since A is assumed simple it follows therefore $Ra = 0$ for all generators $a \in X$. Therefore X generates no more than 0 and thus A is zero which is a contradiction. Therefore A is cyclic.
- Take A to be simple and let $f : A \to A$ be an arbitrary endomorphism of A. Clearly $f(A)$ is a submodule of A and so $f(A) = \mathbf{0}$ or $f(A) = A$. If $f(A) = \mathbf{0}$ then f is the zero map so the hypothesis is verified. Suppose then that f is not the zero map and thus $f(A) = A$. Thus f is an epimorphism. But also note that the kernel of f is also a submodule of A and therefore $Ker\ f = \mathbf{0}$ or A. Thus $Im\ f \cong A/\mathbf{0} \cong A$ or $Im\ f \cong A/A \cong \mathbf{0}$. The last case was assumed to be false thus $Im\ f \cong A/\mathbf{0}$ and so $Ker\ f = \mathbf{0}$ so f is also a monomorphism. In the category of modules a mapping that is monic and epic is an isomorphism, refer to Exercise-IV.1.

□

IV.1.6 Finitely Generated Modules.

Hint$(3/5)$: Consider the rational numbers as a left regular module (module over itself).

A finitely generated R-module need not be finitely generated as an abelian group. Refer to Exercise-II.1.

Example: As $\mathbb{Q}$ is a ring we consider it as a module over itself, denoted as ${}_{\mathbb{Q}}\mathbb{Q}$. This left regular module is unital as $\mathbb{Q}$ contains a 1 which clearly is respected in the left regular action. Thus ${}_{\mathbb{Q}}\mathbb{Q} = \mathbb{Q} \cdot 1$ so it is a cyclic module and thus finitely generated. However $\mathbb{Q}$ is not finitely generated as a $\mathbb{Z}$-modules, that is as an abelian group. □

IV.1.7 Hom and Endomorphisms.

Hint$(1/5)$: Take advantage of Exercise-I.1 in part (a). The rest requires axiomatic verification.

Take A and B to be R-modules and the set $Hom_R(A, B)$ the collection of all R-linear maps from A to B.

(a) $Hom_R(A, B)$ is an abelian group with $f + g$ given on $a \in A$ by $(f + g)(a) = f(a) + g(a) \in B$. The identity element is the zero map.

(b) $Hom_R(A, A)$ is a ring with identity, where multiplication is composition of functions. $Hom_R(A, A)$ is called the **endomorphism ring** of A.

(c) A is a unital left $Hom_R(A,A)$-module with fa defined as $fa = f(a)$ where $a \in A$, and $f \in Hom_R(A,A)$.

Proof: From Exercise-I.1 we know $M(A,B)$, the set of all maps from A to B is an abelian group under pointwise addition since B is an abelian group. Thus we need only show $Hom_R(A,B)$ is a subgroup. Given two R-linear maps $f, g \in Hom_R(A,B)$ and $s,t \in A$ $r \in R$, it follows:

$$(f-g)(rs+t) = f(rs+t)-g(rs+t) = rf(s)+f(t)-rg(s)-g(t) = r(f-g)(s)+(f-g)(t).$$

Thus $f-g$ is R-linear so $Hom_R(A,B)$ is closed to sums and inverse. Moreover, the trivial map $x \mapsto 0$ is in $Hom_R(A,B)$ so $Hom_R(A,B)$ is non-empty and so it is a subgroup of $M(A,B)$, and thus an abelian group.

Now consider multiplication: take $f, g \in Hom_R(A,A)$. As $f, g : A \to A$, their composition is always defined on either the right or left. Moreover,

$$(f\circ g)(rs+t) = f(g(rs+t)) = f(rg(s)+g(t)) = rf(g(s))+f(g(t)) = r(f\circ g)(s)+(f\circ g)(t),$$

proving multiplication is well-defined as $f \circ g$ is R-linear. Since composition of functions is associative, so is our multiplication. In general the multiplication is non-commutative; however, we do have an identity, simply the identity map which is trivially R-linear and unital.

Finally, define $f \cdot s = f(s)$. The following results follow:

$$\begin{aligned} f\cdot(s+t) &= f(s+t) = f(s)+f(t) = f\cdot s + f\cdot t; \\ (f+g)\cdot s &= (f+g)(s) = f(s)+g(s) = f\cdot s + g\cdot s; \\ (f\circ g)\cdot s &= (f\circ g)(s) = f(g(s)) = f\cdot(g\cdot s); \\ 1_A \cdot s &= 1_A(s) = s. \end{aligned}$$

Thus, A is a unital $Hom_R(A,A)$-module. □

IV.1.8 Module Products and Sums.

Let $\{f_i : V_i \to W_i \mid i \in I\}$ be a family of R-linear maps between R-modules V_i and W_i. Define

$$f = \prod_{i\in I} f_i : \prod_{i\in I} V_i \to \prod_{i\in I} W_i$$

so that $f(\{a_i \,:\, i \in I\}) = \{f_i(a_i) \,:\, i \in I\}$.

Prove f is a homomorphism of groups where:

$$f\left(\bigoplus_{i\in I} V_i\right) \le \bigoplus_{i\in I} W_i, Ker\ f = \prod_{i\in I} Ker\ f_i, \text{ and } Im\ f = \prod_{i\in I} Im\ f_i.$$

Conclude that f is monic if and only if each f_i is monic, and f is epic if and only if each f_i is epic.[1]

Suppose $\{Y_i \,:\, i \in I\}$ is a family of submodules, $Y_i \le G_i$ for each $i \in I$. Show:

- $\prod_{i\in I} Y_i$ is a submodule of $\prod_{i\in I} V_i$ and

$$\prod_{i\in I} V_i / \prod_{i\in I} Y_i \cong \prod_{i\in I} V_i/Y_i.$$

Hint$(3/5)$: Observe a principle advantage of modules is that every submodule is already a normal subgroup and so the quotients are all well-defined. Make use of this and the first isomorphism theorem for modules. Make sure not to assume the pre-image of $\bigoplus_{i\in I} W_i$ is $\bigoplus_{i\in I} V_i$ for the final part.

[1] Notice the first conclussion allows us to say f can be restricted to a map of direct sums.

- $\bigoplus_{i\in I} Y_i$ is a submodule of $\bigoplus_{i\in I} V_i$ with

$$\bigoplus_{i\in I} V_i/\bigoplus_{i\in I} Y_i \cong \bigoplus_{i\in I} V_i/Y_i.$$

Proof: To begin with the map f is well-defined as it is simply the set-thoeretic map induced by the universal property for cartesian products of sets (Introduction, Theorem-5.2.) We must no verify f is R-linear.

Take $r \in R$, and $\{a_i \ : \ i \in I\}, \{b_i \ : \ i \in I\}$ in $\prod_{i\in I} V_i$.

$$\begin{aligned} f(r\{a_i \ : \ i \in I\} + \{b_i \ : \ i \in I\}) &= f(\{ra_i + b_i \ : \ i \in I\}) \\ &= \{f_i(ra_i + b_i) \ : \ i \in I\} \\ &= \{rf_i(a_i) + f_i(b_i) \ : \ i \in I\} \\ &= r\{f_i(a_i) \ : \ i \in I\} + \{f_i(b_i) \ : \ i \in I\} \\ &= rf(\{a_i \ : \ i \in I\}) + f(\{b_i \ : \ i \in I\}). \end{aligned}$$

Thus f is R-linear.

Given any $\{c_i \ : \ i \in I\} \in \bigoplus_{i\in I} V_i$, it follows all most all c_i's are trivial. Let $I' = \{i \in I \ : \ c_i \neq 0\}$, which accordingly must be finite. As f is R-linear, 0 must go to 0, so $\{f_i(a_i) \ : \ i \in I'\}$ is the largest subfamily of $f(\{a_i \ : \ i \in I\})$ which can have non-zero entries. As I' is finite, this set is also finite, and so the image of $\{a_i \ : \ i \in I\}$ is contained in $\bigoplus_{i\in I} W_i$.

Given $f(\{a_i \ : \ i \in I\}) = \{0 \ : \ i \in I\}$ it follows from the definition that $f_i(a_i) = 0$ for each $i \in I$, and visa-versa. Thus if and only if $a_i \in Ker \ f_i$ for each $i \in I$. Hence $Ker \ f = \prod_{i\in I} Ker \ f_i$. Once again,

$$\{b_i \ : \ i \in I\} = f(\{a_i \ : \ i \in I\}) = \{f_i(a_i) \ : \ i \in I\}$$

so $b_i = f_i(a_i)$ for each $i \in I$. Hence, $Im \ f \leq \prod_{i\in I} Im \ f_i$. Moreover, for each $\{b_i \ : \ i \in I\} \in \prod_{i\in I} Im \ f_i$, we have the existance of some $a_i \in V_i$ for each f_i such that $f(a_i) = b_i$ and so indeed $f(\{a_i \ : \ i \in I\}) = \{b_i \ : \ i \in I\}$ proving $Im \ f \geq \prod_{i\in I} Im \ f_i$, and so in fact they are equal.

Also notice if f is restricted to $\bigoplus_{i\in I} V_i$, then

$$Ker \ f|_{\bigoplus_{i\in I} V_i} = Ker \ f \cap \bigoplus_{i\in I} V_i = \prod_{i\in I} Ker \ f_i \cap \bigoplus_{i\in I} V_i = \bigoplus_{i\in I} Ker \ f_i.$$

It is clear that $Im \ f|_{\bigoplus_{i\in I} V_i} \leq \bigoplus_{i\in I} Im \ f_i$; however, it is incorrect to assume the entire pre-image of $\bigoplus_{i\in I} Im \ f_i$ lies in $\bigoplus_{i\in I} V_i$. So instead, take any $\{b_i \ : \ i \in I\}$ in $\bigoplus_{i\in I} Im \ f_i$. As this sequence has finite carrier, say $\{b_i \ : \ i \in I'\}$ is the set of all non-zero elements (finiteness guaranteed), then there exist $a_i \in V_i$ for each $i \in I'$ such that $f_i(a_i) = b_i$ as each f_i is surjective on its image. Thus the elements $\{a_i \ : \ i \in I'\} \cup \{0 \ : \ i \in I \backslash I'\}$ is an element in $\bigoplus_{i\in I} V_i$ whose image is $\{b_i \ : \ i \in I\}$. Hence $Im \ f|_{\bigoplus_{i\in I} V_i} = \bigoplus_{i\in I} Im \ f_i$.

Modules are abelian groups so all submodules are normal so their quotients are well-defined. They also come equiped with a natural projection map $\pi_i : S_i \to S_i/T_i$ and the rest goes by the our recent work.

$$\prod_{i\in I} S_i \qquad \prod_{i\in I} S_i/T_i$$

$$S_i \qquad S_i/T_i$$

where $f = \prod_{i\in I} \iota_i'\pi_i$ is now the induced map from above. [2] The map f is clearly surjective from our work above – each π_i is surjective; moreover its kernel is precisely $\prod_{i\in I} T_i$, so by the first isomorphism theorem:

$$\prod_{i\in I} S_i/\prod_{i\in I} T_i \cong \prod_{i\in I} S_i/T_i.$$

With direct sums the work is the same. [3] $\square$

IV.1.9 Idempotent and Splitting Maps.

If $f : A \to A$ is a module homomorphism such that $ff = f$ then $A = Ker\ f \oplus Im\ f$.

Proof: Consider the canonical exact sequence determined by f:

$$\mathbf{0} \qquad Ker\ f \qquad A \qquad Im\ f \qquad \mathbf{0}.$$

Taking any element $y \in Im\ f$ it follows $y = f(x)$ for some $x \in A$. Now $f(y) = f(f(x)) = f(x) = y$ since $ff = f$. Therefore $ff|_{Im\ f} = 1_{Im\ f}$ which satisfies the Split Exactness Theorem, so $A = Ker\ f \oplus Im\ f$. $\square$

IV.1.10 Split Decomposition.

If $f : A \to B$ and $g : B \to A$ are module homomorphisms such that $gf = 1_A$ then $B = Im\ f \oplus Ker\ g$.

Proof: Given $gf = 1_A$ certainly $x = g(f(x))$ for all $x \in A$ it follows there exists a $y \in B$, namely $f(x) = y$, such that $x = g(y)$ so g is surjective, or epimorphic. Taking the canonical exact sequence for epimorphisms:

$$\mathbf{0} \qquad Ker\ g \qquad B \qquad A \qquad \mathbf{0}$$

it follows the sequence is split exact so $B = Ker\ g \oplus A$.

Likewise taking $x, y \in A$ it follows $f(x) = f(y)$ implies $x = g(f(x)) = g(f(y)) = y$ thus f is injective and so it is a monomorphism. Therefore $A \cong A/\mathbf{0} \cong Im\ f$ so the following sequence is exact:

$$\mathbf{0} \qquad Ker\ g \qquad B \qquad A \qquad Im\ f \qquad \mathbf{0}$$

or simply

$$\mathbf{0} \qquad Ker\ g \qquad B \qquad Im\ f \qquad \mathbf{0}$$

Apllying the split extension theorem it follows $B = Ker\ g \oplus Im\ f$. $\square$

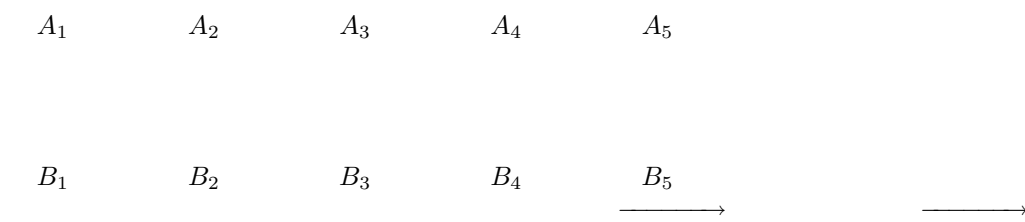
[2] Fomally, $\iota_i : s_i \mapsto \chi_{s_i}$ where $\chi_{s_i}(i) = s_i$ and $\chi_{s_i}(j) = 0$ when $j \neq i$. Likewise,

$$\iota_i' : s_i + T_i \mapsto \chi_{s_i} + \prod_{i\in I} T_i.$$

[3] It is also possible to note here the the direct sum is a coproduct in the category of modules (unlike the category of groups, refer to Exercise-I.8.) Thus f can be derived from the universal mapping property; certainly the uniqueness guarantees these two maps coincide.

IV.1.11 5-Lemma.

Suppose the following diagram commutes in an Algebraic Category.[4]



(i) Show if f_1 is monic and f_2, f_4 epic, then f_3 is epic.

(ii) Show if f_5 is epic and f_2, f_4 monic, then f_3 is monic.

(iii) Show if f_1 is monic, f_5 epic, and f_2, f_4 isomorphic then f_3 is isomorphic.

In particular notice if $A_1 \cong B_1 \cong A_5 \cong B_5 \cong \mathbf{0}$, then we obtain the short 5-lemma without the need of the functions f_1 and f_5.

(i) **Proof:** Let 1 be the identity of B_3 and choose $a_3 \in A_3$ so that $a_3 \in f_3^{-1}(1)$. If we map a_3 to a_4 via α_3, and then to a point $b_4 \in B_4$ through f_4, it follows

$$1 = \beta_3 f_3(a_3) = f_4 \alpha_3(a_3) = b_4$$

so $b_4 = 1$. Since f_4 is injective, this requies the kernel be trivial, so $1 = a_4 = \alpha_3(a_3)$. Now by the exactness of the row sequences, a_3 must be in the image of α_2 as it is in the kernel of α_3. So let $a_2 \in A_2$ with $\alpha_2(a_2) = a_3$. We may send a_2 to B_2 through f_2 to a point b_2. Since the diagram commutes it follows

$$1 = f_3 \alpha_2(a_2) = \beta_2 f_2(a_2) = \beta_2(b_2).$$

Therefore $b_2 \in Ker\ \beta_2$ and so by the exactness of the sequence $b_2 \in Im\ \beta_1$. Choose $b_1 \in B_1$ so that $\beta_1(b_1) = b_2$. With the assumption that f_1 is epic, we have know there exists a $a_1 \in A_1$ such that $f_1(a_1) = b_1$. Now we know the diagram commutes so it follows if take $a_2' = \alpha_1(a_1)$ that

$$f_2(a_2) = b_2 = \beta_1 f_1(a_1) = f_2 \alpha_1(a_1).$$

With this we now take the added assumption that f_2 is injective allows us to assert since $f_2(a_2) = b = f_2(a_2')$ certianly $a_2 = a_2'$. All this allows us to observe that a_1 maps to a_2, so by the exactness of the sequence $a_2 \in Ker\ \alpha_2$, and then we notice this means $1 = \alpha_2(a_2) = a_3$. Therefore f_3 has a trivial kernel so it is injective as well. □

(ii) **Proof:** Let $b_3 \in B_3$. We can send b_3 to $b_4 \in B_4$ by β_3. Here f_4 is epimorphic so we pull back a value $a_4 \in A_4$ such that $f_4(a_4) = b_4$. To be able to pull back along α_3 we must know that a_4 is in the kernel of α_5. But this follows from sending b_4 along β_4 to 1 (recall $b_4 \in Im\ \beta_3 = Ker\ \beta_4$). Since f_5 is a monomorphism its kernel is trivial so by the commutativity we have $1 = f_5 \alpha_4(a_4)$ so $\alpha_4(a_4) = 1$. This allows us to pull back to an element $a_3 \in A_3$ so that $\alpha_3(a_3) = a_4$ by the exactness of the sequence. This element projects to another $b_3' \in B_3$ via f_3.

[4] An Algebraic Category will be concrete, with a zero object, morphisms with the homomorphism property, and in which a bijective morphism is an isomorphism – this is all equivalent to having the Fundamental Homomorphism Theorem

Now we apply the trickery: consider $b'_3 b_3^{-1} \in B_3$. Certainly $\beta_3(b'_3 b_3^{-1}) = \beta(b'_3)(\beta(b_3))^{-1}$. Coupled with

$$\beta_3(b_3) = b_4 = f_4\alpha_3(a_3) = \beta_3 f_3(a_3) = \beta_3(b'_3) = b_4$$

so $\beta_3(b'_3 b_3^{-1}) = 1$. Now by the exactness we have an element $b_2 \in B_2$ where $\beta_2(b_2) = b'_3 b_3^{-1}$. Using the surjectivity of f_3 yields an $a_2 \in A_2$ where $f_2(a_2) = b_2$. Send a_2 to an element $a'_3 \in A_3$ via α_2. Now consider $a'^{-1}_3 a_3 \in A_3$. Certainly the commutativity insures:

$$f_3(a'^{-1}_3 a_3^{-1}) = (f_3\alpha_2(a_2))^{-1} f_3(a_3) = b_3 b'^{-1}_3 b'_3 = b_3.$$

Now we have an element that maps to b_3 via f_3 so f_3 is surjective. □

(iii) **Proof:** Follows from (i) and (ii) and the fact that in a Category of algebraic objects all bijective morphisms are isomorphisms. □

IV.1.12 Unitary Separation.

- If R has an identity and A is an R-module then there exists submodules B and C such that B is unitary, $RC = \mathbf{0}$, and $A = B \oplus C$.
- Let A_1 be another R-module with $A_1 = B_1 \oplus C_1$ with B_1 unitary and $RC_1 = \mathbf{0}$. If $f : A \to A_1$ then $f(B) \leq B_1$ and $f(C) \leq C_1$.
- If f is an epimorphism(or isomorphism) then so is $f|_B : B \to B_1$ and $f|_C : C \to C_1$.

See Exercise-?? for the extention of these properties to arbitrary modules.

Proof:

- Let $B = \{1a \mid a \in A\}$ and $C = \{a \in A \mid 1a = 0\}$. Thus C is clearly the kernel of the linear map $f : A \to B$ defined by $a \mapsto 1a$. Also f is seen as surjective since it matches the definition of B. Therefore the following sequence is exact:

$$\mathbf{0} \qquad C \qquad A \qquad B \qquad \mathbf{0}.$$

  Adding the inclusion map $g : B \to A$ it follows $f(g(b)) = 1b$. If B is unitary then clearly $fg = 1_B$ and so the sequence is split exact leaving $A = B \oplus C$.

  Take an element $a \in A$ and consider $a - 1a$. $f(a - 1a) = 1(a - 1a) = 1a - 1(1a) = 1a - (11)a = 1a - 1a = 0$ therefore $a - 1a \in C$ for all $a \in A$. Therefore $0 = f(a - 1a) = f(a) - 1f(a)$ so $f(a) = 1f(a)$. Since f is surjective this forces $b = 1b$ for all $b \in B$ so B is unitary.

  Finally note $ra = (r1)a = r(1a) = r0 = 0$ for all $a \in C$ and $r \in R$ so $RC = \mathbf{0}$.

- Now take $f : A \to A_1$ as described. Notice for any element (b_1, c_1) from $B_1 \oplus C_1$ it follows $1(b_1, c_1) = (1b_1, 1c_1) = (b_1, 0)$ so it is unitary if and only if $c_1 = 0$. Thus since B is unitary it follows for all $b \in B$, $f(b) = f(1b) = 1f(b)$ thus $f(B) \leq B_1$ since B_1 contains all unitary elements.

  In similar fashion $1(b_1, c_1) = (0, 0)$ if and only if $b_1 = 0$ so given $c \in C$, $0 = f(0) = f(1c) = 1f(c)$ so the image under C lands in C_1 as required.

- Using the same f suppose the map is an epimorphism, or even an isomorphism. This sets up the following commutative diagram:

$$\begin{array}{ccccccc} \mathbf{0} & & C & & B \oplus C & & B & & \mathbf{0} \\ \\ \mathbf{0} & & C_1 & & B_1 \oplus C_1 & & B_1 & & \mathbf{0} \end{array}$$

It was shown $f(B) \leq B_1$ and $f(C) \leq C_1$ so the restricted maps are well-defined. Start with an element $\overline{b} \in B_1$. Chasing $\overline{b}$ through $\overline{\iota}_B$ embeds it as $(\overline{b}, 0)$ in $B_1 \oplus C_1$. Since f is an epimorphism it is surjective thus there exists an element $(b, c) \in B \oplus C$ such that $(\overline{b}, 0) = f(b, c)$. Now project this element to B by π_B returning b such that to comply with the commutative right square $f|_B \pi_B(b, c) = \overline{\pi}_B f(b, c) = \overline{b}$. Therefore $f|_B$ is surjective so it is an epimorphism.

Following suit begin with an element $\overline{c} \in C_1$. Send c through $\overline{\iota}_C$ to the element $(0, \overline{c})$. Retract the element through the epimorphism f to an element (b, c) in $B \oplus C$ and project this element to C by way of π_C. Since the left square also commutes it follows once again $f|_C \pi_C(b, c) = \overline{\pi}_C f(b, c) = \overline{c}$ so $f|_C$ is also an epimorphism.

The analog for isomorphism is clear since in such a case (b, c) is equivalent to $f(b, c) = (\overline{b}, \overline{c})$.

□

IV.2 Free Modules and Vector Spaces

4 Quotient Modules 123
7 Non-trivial Automorphisms of Groups 123

IV.2.1 Quotient Modules.

Let R be a principal ideal domain and A a unitary R-module. Given any prime element of R – equivalently an irreducible – define $pA = \{pa \mid a \in A\}$ and $A[p] = \{a \in A \mid pa = 0\}$.

- $R/(p)$ is a field.
- pA and $A[p]$ are submodules of A.
- A/pA is a vector space over $R/(p)$ with $(r + (p))(a + pA) = ra + pA$.

Refer to Exercise-??3.

Proof:

- Since p is prime and equivalently irreducible given that R is a principal ideal domain, it follows (p) is a maximal ideal – follows from Theorem III.3.4. Thus $R/(p)$ is a field by Theorem III.2.20.
- Define the mapping $f : A \to A$ by $f(x) = px$. Since A is an R-module the map is a well-defined left translation and thus is R-linear – $f(x+y) = p(x + y) = px + py = f(x) + f(y)$, $f(rx) = p(rx) = (pr)x = (rp)x = r(p(x)) = rf(x)$. Clearly the image of f is pA and the kernel is $A[p]$ thus both are submodules of A.
- Notice $(p)A$ as defined in Exercise-??3 is simply $RpA = \{rpa = p(ra) = pa' \mid a \in A, r \in R\} = pA$. Thus A/pA is an $R/(p)$ module with the action as defined.
- Let $r \equiv r' \pmod p$. Then $(r + (p))a - (r' + (p))a = ra - r'a = (r - r')a = pa = 0$; thus $(r + (p))a = (r' + (p))a$ so scalar products are well-defined. $A[p]$ retains its abelian group structure so all that remains to be verified is that scalars behave correctly.

  Given $r, s \in R$ and $a, b \in A[p]$, $(r + (p))(a + b) = r(a + b) = ra + rb = (r+(p))a+(r+(p))b$ and $((r+(p))+(s+(p)))a = ((r+s)+(p))a = (r+s)a = ra + sa = (r + (p))a + (s + (p))a$ so both distribution laws hold. Finally $(r + (p))((s + (p))a) = r(sa) = (rs)a = (rs + (p))a = ((r + (p))(s + (p)))a$ so $A[p]$ is an $R/(p)$ module.

□

IV.2.2 Non-trivial Automorphisms of Groups.

Every group of order greater than 2 (or simply not isomorphic to **0** or $\mathbb{Z}/2$) has a non-trivial automoprhism. *Refer to Exercise-II.4.11.*

Proof: From Exercise-II.4.11 it is known any group with an element of order greater than 2 has a non-trivial automorphism. Now suppose G is a group in which every element is an involution – i.e.: an element of order 2. If $G =$ **0** only

one automorphism exists, the identity, and likewise with $G \cong \mathbb{Z}/2$, so let G have order greater than 2.

Given $a, b \in G$ it follows $(ab)^2 = e = a^2b^2$. Using cancellation $abab = aabb$ implies $ba = ab$ so G is abelian and in so being is a canonical $\mathbb{Z}$-module – now express G additively. Making use of Exercise-IV.2 note that $\mathbb{Z}$ is a prinicipal ideal domain and 2 is a prime in $\mathbb{Z}$. Thus $G/2G$ is a $\mathbb{Z}/2\mathbb{Z}$ module. But moreover $2G = \{2a \mid a \in G\} = \mathbf{0}$ since every element of G is of order 2. Therefore in fact G is a $\mathbb{Z}/2\mathbb{Z}$ module.

From here note $\mathbb{Z}/2\mathbb{Z}$ is a field and thus G is a vector space over $\mathbb{Z}/2\mathbb{Z}$ and applying Theorem-IV.2.4 it follows G is a free $\mathbb{Z}/2\mathbb{Z}$-module. Therefore there exists a basis for G. Since $|G| > 2$ – and G has no element of order 3 – G has at least 4 elements, and thus a subgroup H isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, which has a basis isomorphic to $\{(1,0),(0,1)\}$. By the basis extension theorem it follows we can pick a basis for G that contains the basis for H and thus this basis X contains at least two elements e_1 and e_2.

To create the non-trivial automorphism now we create a basis exchange by mapping $e_1 \mapsto e_2$ and $e_2 \mapsto e_1$. This map is linear, since it is simply a permutation, and it is non-trivial because $e_1 \neq e_2$. Therefore G has a non-trivial automorphism. $\square$

IV.3 Projective and Injective Modules

IV.4 Hom and Duality

IV.5 Tensor Products

IV.6 Modules over a Prinicpal Ideal Domain

IV.7 Algebras

Chapter V

Fields and Galois Theory

V.1 Field Extensions

1 Extension Degrees 131
2 Transcendental Dimension 131

V.1.1 Extension Degrees.

Hint$(1/5)$: Use Theorem-V.1.2 – the analog of Lagrange's Theorem.

(a) $[F : K] = 1$ if and only if $F = K$.

(b) If $[F : K]$ is prime, then there are no intermediate fields between F and K.

(c) If $u \in F$ has degree n over K, then n divides $[F : K]$.

(a) **Proof:** If $[F : K] = 1$ then F is a one dimensional vector space over K and thus the span of $1 \in F$ yields $K1 = F$. But as $1 \in K$ as well, it follows $K = F$.

Presuming $F = K$, there is no question that F is a one dimensional vector space over K – pick for instance the basis $\{1\}$; therefore, $[F : K] = 1$. □

(b) **Proof:** Let L be a field such that $F \geq L \geq K$. By Theorem-V.1.2 (for practical purposses, the Theorem of Lagrange) it follows

$$[F : K] = [F : L][L : K]$$

So by Euclid's Lemma $p|[F : L]$ or $p|[L : K]$, and thus either $[L : K] = 1$ or repsectively $[F : L] = 1$ in which case from part (a) it follows $L = K$ or $L = F$. □

(c) **Proof:** As u has degree n over K we mean $[K(u) : K] = n$. Since $\{u\}, K \subseteq F$, it follows $K(u) \leq F$, so now

$$[F : K] = [F : K(u)][K(u) : K] = [F : K(u)]n.$$

Hence, n divides $[F : K]$. □

V.1.2 Transcendental Dimension.

Give an example of a finitely generated field extension which is not finite dimensional. [*Hint:* think transcendental.]

Example: Consider $\mathbb{Q}(\pi)/\mathbb{Q}$. As π is transcendental over $\mathbb{Q}$ it is not a root of any polynomial over $\mathbb{Q}$. Thus the degree of the extension is infinite. In particular, as $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$ we may borrow a basis of $\mathbb{Q}(x)/\mathbb{Q}$:

$$\{1, x, x^2, \dots\}$$

which becomes

$$\{1, \pi, \pi^2, \dots, \}$$

in $\mathbb{Q}(\pi)/\mathbb{Q}$. □

Hint$(1/5)$: Transcendental extensions are equivalent to the quotient field of all polynomials – Theorem-V.1.5.

V.2 The Fundamental Theorem

V.3 Splitting Fields, Algebraic Closure and Normality

V.4 The Galois Group of a Polynomial

V.5 Finite Fields

V.6 Separability

V.7 Cyclic Extensions

V.8 Cyclotomic Extensions

V.9 Radical Extensions

Chapter VI

The Structure of Fields

Chapter VII

Linear Algebra

Chapter VIII

Commutative Rings and Modules

Chapter IX

The Structure of Rings

Chapter X

Categories

X.1 Functors and Natural Transformations

1 Example Functors 149
2 Functor Image 151

X.1.1 Example Functors.

Construct functors as follows:

Hint$(1/5)$: Make sure to define the functor on morphisms as well and to check that both parts are well-defined.

(a) A covariant functor $\mathcal{G} \to \mathcal{S}$ that assigns to each group the set of all its subgroups.

(b) A covariant functor $\mathscr{R} \to \mathscr{R}$ that assigns to each ring R the polynomial ring $R[x]$.

(c) A functor, covariant in both variables $\mathfrak{M} \times \mathfrak{M} \to \mathfrak{M}$ such that

$$(A, B) \mapsto A \oplus B.$$

(d) A covariant functor $\mathcal{G} \to \mathcal{G}$ that assigns to each group G its commutator subgroup G' (Definition-II.7.7).

Example:

(a) Define $Sub : \mathcal{G} \to \mathcal{S}$ as suggested:

$$Sub(G) = \{K \leq G\},$$

and together with this define the assignment of homomorphisms as restriction, so that:

$$Sub(f : G \to H) : Sub(G) \to Sub(H)$$

by $K \mapsto f(K)$ for every $K \leq G$. As the subgroups of a group are fixed the assignment of objects is well-defined. Moreover, the image of a group, under a group homomorphism, is again a group, so $f(K) \in Sub(H)$ and so the assignment of morphisms is also well-defined. Now we verify the functorial qualities of Sub.

Take any $K \leq G$ and notice $Sub(1_G : G \to G)(K) = 1_G(K) = K$ so $Sub(1_G) = 1_{Sub(G)}$ as required. Also consider any two morphisms $f : G \to H$ and $g : H \to K$. If we take any $L \leq G$ we see

$$Sub(g \circ f)(L) = g \circ f(L) = g(f(L)) = g(Sub(f)(L)) = (Sub(g) \circ Sub(f))(L)$$

as expected and required. Therefore Sub is a covariant functor.

(b) Declare $Poly : \mathscr{R} \to \mathscr{R}$ to be $Poly(R) = R[x]$ for each object and for morphisms define:

$$Poly(f : R \to S) : R[x] \to S[x] : \sum_i a_i x^i \mapsto \sum_i f(a_i) x^i.$$

As any ring can be used for coefficients of polynomials the object assignment is benign and likewise replacing coefficients in a polynomial results in further polynomials so morphisms are assigned adequitely.

Begin with any $p(x) = \sum_i a_i x^i \in R[x]$ for some ring R and apply $Poly(1_R : R \to R)(p(x))$ which equals

$$\sum_i 1_R(a_i) x^i = \sum_i a_i x^i = p(x)$$

proving that $Poly(1_R) = 1_{R[x]}$. Provided with maps $f : R \to S$ and $g : S \to T$ we quickly notice

$$\begin{aligned} Poly(g \circ f)(p(x)) &= \sum_i g(f(a_i)) x^i = Poly(g) \left(\sum_i f(a_i) x^i \right) \\ &= (Poly(g) \circ Poly(f))(p(x)). \end{aligned}$$

Hence $Poly$ is covariant functor.

(c) Take any family of (left) R-modules $\{A_i : i \in I\}$ for a fixed index set I, and define $\oplus(\{A_i : i \in I\}) = \bigoplus_{i \in I} A_i$. Also given the morphisms $f_i : A_i \to B_i$ we let

$$\bigoplus_{i \in I} f_i : \bigoplus_{i \in I} A_i \to \bigoplus_{i \in I} B_i$$

be given by the universal mapping property for coproducts ($f_i = (\bigoplus_{i \in I} f_i) \circ \iota_i$.) Since the universal mapping property returns a unique map we are assured this assignment is well-defined. Also clearly any product over I of modules is again a module. Now we need only verify the functor axioms.

Take any collection of maps $f_i : A_i \to B_i$ and $g_i : B_i \to C_i$ indexed of course by I. Take let $g = \bigoplus_{i \in I} g_i$ and $f = \bigoplus_{i \in I} f_i$. Now observe

$$(g \circ f) \circ \iota_i = g \circ \iota_i \circ f \circ \iota_i = g_i \circ f_i$$

but recall the universal mapping property asserts that this situation has a unique solution; thus, $g \circ f = \bigoplus_{i \in I} g_i \circ f_i$. Finally,

$$\left(\bigoplus_{i \in I} 1_{A_i} \right) \iota_i(a_i) = a_i = 1_{A_i}(a_i)$$

for any $a_i \in A_i$; so once again by the uniqueness of the universal mapping property together with the observation that the identity on $\bigoplus_{i \in I} A_i$ also solves this relation, we see identities are mapped to identities, so the direct sum is a functor.

(d) Finally, take $Com : \mathcal{G} \to \mathcal{G}$ to be defined on objects as $Com(G) = G'$ and on homomorphisms as restriction:

$$Com(f : G \to H) = f|_{G'} : G' \to H'.$$

The assignment for objects is clearly well-defined. Now take any generator $aba^{-1}b^{-1} \in G'$. It follows $f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} \in H'$ so restriction is indeed well-defined as it is so on generators.

Clearly restricting the identity map to any subgroup produces an identity map so consider now the composition of homomorphisms: Take $f : G \to H$ and $g : H \to K$. Recall the image of $f|_{G'}$ lies within H' so indeed:

$$Com(g \circ f) = (g \circ f)|_{G'} = g \circ f|_{G'} = g|_{H'} \circ f|_{G'} = Com(g) \circ Com(f).$$

Thus Com is a covariant functor.

□

X.1.2 Functor Image.

Hint$(4/5)$: Do part (b) first to discover which properties follow without the assumption of injectivity, and which may fail if the assumption is not given.

(a) If $T : \mathcal{C} \to \mathcal{D}$ is a covariant functor, let $Im\, T$ consist of the objects $\{T(C) : C \in \mathcal{C}\}$ and the morphisms $\{T(f) : T(C) \to T(C') | f : C \to C'$ a morphism in $\mathcal{C}\}$. Then show that $Im\, T$ need not be a category.

(b) If the object function of T is injective, then show that $Im\, T$ is category.

(a) **Example:** Consider the category of all groups $\mathcal{G}$ and the forgetful functor T to the category of sets $\mathcal{S}$. We may take $\mathbb{Z}/2 = \langle \{0, 1\}, + \rangle$ where 0 is the identity, and also $\mathbb{Z}'/2 = \langle \{0, 1\}, + \rangle$ but here we let 1 be the identity. Now we notice that $T(\mathbb{Z}/2) == \{0, 1\} = T(\mathbb{Z}'/2)$ so T is not injective on objects. Moreover we now may create a complication: take the homomorphism $f : \mathbb{Z}/2 \to \{0\}$ and $g : \mathbb{Z}'/2 \to \{1\}$ also the trivial map. Now

$$(T(f) \circ T(g))(0) =$$

PENDING: I just don't know!! □

(b) **Proof:** Given that the object function of T is injective it follows $T(A) = T(B)$ requires $A = B$. Thus if $T(f : A \to C) = T(g : B \to D)$ then we have $T(A) = T(B)$ and $T(C) = T(D)$ so $A = B$ and $C = D$. Thus as $Hom(-, -)$ classes are disjoint in $\mathcal{C}$ it follows $Hom(T(-), T(-))$ are disjoint in $\mathcal{C}'$. The remainder of the work follows without the assumption of injectivity.

Take two morphisms $T(f) : T(A) \to T(B)$, and $T(g) : T(B) \to T(C)$ in the image of T for which $f : A \to B$ and $g : B \to C$ lie in $\mathcal{C}$. Notice we have a composition defined in $\mathcal{C}'$ but we do not yet know if the image of T is closed to this composition. Thus consider $T(g) \circ T(f) = T(g \circ f)$ by the assumption that T is a covariant functor. Therefore as $g \circ f$ is closed in $\mathcal{C}$ it follows $T(g) \circ T(f)$ is closed in the image of T.

Next, given $f : A \to B$, $g : B \to C$ and $h : C \to D$ in $\mathcal{C}$ we see:

$$T(h) \circ (T(g) \circ T(f)) = T(h) \circ T(g \circ f) = T(h \circ (g \circ f)) = T((h \circ g) \circ f) = T(h \circ g) \circ T(f) = (T(h) \circ T(g)) \circ T(f)$$

so in fact the image of T maintains the associative property. Also given that $T(1_A) = 1_{T(A)}$ it follows each element in the image has an identity map. □

X.2 Adjoint Functors

X.3 Morphisms

Appendix A

Heuristics

A.1 Needle in the Haystack

[1]

When asked to prove existance, it is not uncommon to see a proof that majically proclaims some object into existance that some how verifies the properties required. On the rare occasion that the object is said to exist uniquely, the subsequent uniqueness proof can sometimes help explain the origins of the majical element previously declared. Such cases usually follow the pattern of the following proof.
Example: The category of groups contains a product.

Define $\prod_{i\in I} G_i$ as the cartesian product of the groups G_i. Furthermore define multiplication in $\prod_{i\in I} G_i$ pointwise; it can be shown $\prod_{i\in I} G_i$ is a group. Next we verify π_i is a homomorphism for each $i \in I$.

Now take T to be any group and $\{\varphi_i : T \to G_i \mid i \in I\}$ any family of homomorphisms. Define $\varphi : T \to \prod_{i\in I} G_i$ as $\varphi(g) = f_g$ where $f_g : I \to \cup_{i\in I} G_i$ and $f_g(i) = \varphi_i(g)$ for all $i \in I$. Certainly $\pi_i\varphi(g) = \pi_i(f_g) = \varphi_i(g)$ so $\pi_i\varphi = \varphi_i$ for all $i \in I$.

Suppose $\psi : T \to \prod_{i\in I} G_i$ is another map satisfying $\pi_i\psi = \varphi_i$ for all $i \in I$. Then $\pi_i\varphi = \pi_i\psi$ for all $i \in I$.

[PENDING: find a good example] □

A.2 Principle of Refinement

Consider Exercise-I.2. Two questions are asked in the exercise: first is the set $\{\sigma \in S_n \mid \sigma(n) = n\}$ a subgroup of S_n, and next is it isomorphic to S_{n-1}? Certain properties for subgroups will simplify the fisrt question and prove it is in fact a subgroup, however these properties do not resolve the question of wheter it is isomorphic to some other group. It is however to answer both questions simultaneously through the use of the *Principle of Refinement*. Consider the following theorem.

Theorem A.2.1 (Principle of Refinement) *Let A and B be groupoids (i.e.: sets with a binary operation). Given a mapping $f : A \to B$ such that $f(ab) = f(a)f(b)$ for all $a, b \in A$, define $f(A) = \{x \in B \mid x = f(a)$ for some $a \in A\}$, it follows if $a_1, \ldots, a_m$ and $b_1, \ldots b_n$ are elements in A with the property that*

$$a_1 \cdots a_m = b_1 \cdots b_n,$$

[1] Thanks to F.R. Beyl for the title and constant emphasis of this heuristic.

in the standard n-product, then the sequence of elements $f(a_1), \ldots, f(a_m)$ and $f(b_1), \ldots, f(b_n)$ are in $f(A)$ and have the property

$$f(a_1) \cdots f(a_m) = f(b_1) \cdots f(b_m),$$

again in the standard n-product.

Proof: Induction. □

While the definitions are seemingly trivial, and proved as such, the statement made by this theorem is fundamental: mappings with the homomorphism property preserve relations. The study of free groups makes it evident that each group is determined by its relations and thus homorphisms play a large role in understanding groups. Note we must be careful in how we percieve a relation to be preserved. It is completely possible for a homomorphism to preserve a relation by trivializing it; that is by making it equivalent to stating something obvious such as $x = x$. The relation remains true but may no longer be meaningful. The power of the principle lies in the following corollary.

Corollary A.2.2 *All the following are true:*

- *if G is a semigroup then $f(G)$ is also and furthermore f is a homomorphism;*
- *if G is a monoid then so is $f(G)$;*
- *if G is a group then $f(G)$ is a group.*
- *if G is an abelian group then $f(G)$ is abelian.*

Proof:

- If G is a semigroup then for all $a, b, c \in G$ we know $a(bc) = (ab)c$. By Theorem-A.2.1 it follows

  $$f(a)(f(b)f(c)) = f(a)f(bc) = f(a(bc)) = f((ab)c) = f(ab)f(c) = (f(a)f(b))f(c).$$

  So it is evident that the binary operation of A is associative with in the closed subset $f(G)$. Therefore $f(G)$ is a semigroup.

- Suppose G is a monoid, then there exists an element $e \in G$ which is the identity in G with the property $ae = a = ea$ for all $a \in G$. Applying Theorem-A.2.1 it must be that

  $$f(a)f(e) = f(a) = f(e)f(a).$$

  Therefore $f(e)$ is a two sided identity in $f(G)$ and so it is the identity for (the now termed) monoid $f(G)$.

- Consider G as a group. Every element $a \in G$ has an inverse a^{-1} and $a^{-1}a = e = aa^{-1}$ holds in G so by Theorem-A.2.1 the image has the relation:

  $$f(a^{-1})f(a) = f(e) = f(a)f(a^{-1}).$$

  Therefore $f(a^{-1})$ behaves as the inverse for $f(a)$ and so it is the inverse leaving $f(G)$ closed to inverses and so it is a group.

- Supposing G is abelian it follows given $a, b \in G$, $ab = ba$ and so once again by the Principle of Refinement $f(a)f(b) = f(b)f(a)$ in $f(G)$, so $f(G)$ is abelian.

□

Now returning the the exercise, consider constructing a map $f : S_{n-1} \to S_n$ that has the homomorphism property, and such that its image $f(S_{n-1})$ is simply the set $\{\sigma \in S_n \mid \sigma(n) = n\}$. Then by Corollary-A.2.2 it is automatic to state $f(S_{n-1})$ is a group, and thus a subgroup. And in addition we have a candidate for an isomorphism in hand. In this fashion we need not even know S_n is a group but only use that it has a well-defined binary operation.

It is important to emphasize that the properties apply to $f(G)$ and not to the entire codomain. Exercise-I.2 illustrates a situation where a careless generalization will fail.

The morphism principle is in fact a general heuristic for categories.

Definition A.2.3 *A category $\mathscr{D}$ is a refinement of a concrete category $\mathscr{C}$ if given any object A in $\mathscr{D}$ and any morphism $f \in Hom_{\mathscr{C}}(A, -)$, then $f(A)$ is an object in $\mathscr{D}$.*

A refinement therefore introduces a restriction on the objects in a category in such a way as to be complatible with all morphisms. Theorem-A.2.1 can be stated as follows:

Definition A.2.4 *A mapping R from a category $\mathscr{C}$ to the set $\{True, False\}$ is rule whenever $R(\mathscr{C})$, defined as the set of all objects in $\mathscr{C}$ that evaluate to true, is a subcategory of $\mathscr{C}$.*

A relational rule is a rule on the category of groupoids defined as true whenever some relation $\prod_{i=1}^{m} a_i = \prod_{j=1}^{n} b_j$ is true for all elements in an object A.

Theorem A.2.5 *Every relational rule determines a refinement.*

Refinement can of course take place in other categories.
Example: The category of connected spaces is a refinement of the category of all topologies. This is evident because continuous functions on connnected spaces have connected images. [PENDING: reference]

However the category of complete spaces is not a refinement of the category of topologies. This can be seen because completeness is not a topological invariant. For example consider the continuous function e^x defined on the complete domain $\mathbb{R}$ and mapping surjectively onto $\mathbb{R}^+$. $\mathbb{R}^+$ has the cauchy sequence $(1/n)_{n\in\mathbb{Z}^+}$ which converges outside $\mathbb{R}^+$ to 0; thus $\mathbb{R}^+$ is not complete and so $e^{\mathbb{R}}$ is not in the subcategory, so the category is not a refinement. □

Appendix B

Syntax and Usage

B.1 Lattices

A *lattice* is a partially ordered set, L, in which every pair of elements $a, b \in L$, there exists a *greatest lower bound* $a \Downarrow b$ and a *least upper bound* $a \Uparrow b$ in L. By definition $a \Downarrow b$ and $a \Uparrow b$ are unique and imply $a \Downarrow b = b \Downarrow a$ as well as $a \Uparrow b = b \Uparrow a$; likewise $a \Downarrow (b \Downarrow c) = (a \Downarrow b) \Downarrow c$ and $a \Uparrow (b \Uparrow c) = (a \Uparrow b) \Uparrow c$.

A *bottom element* of a lattice L is an element $0 \in L$ such that given any $x \in L$, $0 \Downarrow x = 0$. Analogously a *top element* is an element $1 \in L$ such that $1 \Uparrow x = 1$. Naturally these elements are unique since $0 = 0 \Downarrow 0' = 0'$ and $1 = 1 \Uparrow 1' = 1'$.

A partially ordered set P is *complete* if every nonempty subset, S, has both a greatest lower bound $\Downarrow S$ and a least upper bound $\Uparrow S$ in P; again both are unique given S. Every complete set is a lattice. If a lattice is complete then $\Downarrow S = \Downarrow_{a \in S} a$ and $\Uparrow S = \Uparrow_{a \in S} a$ by definition. If a lattice is finite then it is complete.

A lattice, L, is *distributive* if given $a, b, c \in L$, it follows:

$$\begin{aligned} a \Downarrow (b \Uparrow c) &= (a \Downarrow b) \Uparrow (a \Downarrow c), \\ a \Uparrow (b \Downarrow c) &= (a \Uparrow b) \Downarrow (a \Uparrow c). \end{aligned}$$

Suppose L is a lattice with top element 1 and bottom element 0. A lattice, L, is *complemented* if for every element $a \in L$, there exists an element $a^c \in L$ such that $a \Downarrow a^c = 0$ and $a \Uparrow a^c = 1$.

Example:

- The set of all subsets of a set is a complete, complemented, distributive lattice.
- The subgroups of a group form a complete lattice.
- The normal subgroups of a group form a complete distributive lattice.
- The subgroup lattices of $\mathbb{Z}_p$, $\mathbb{Z}_{pq}$, $\mathbb{Z}_p \oplus \mathbb{Z}_p$, and S_3, are examples of complemented subgroup lattices; the groups $\mathbb{Z}_m$ ($m \neq pq$), D_n and S_n with $n \geq 4$, are all noncomplemented lattices.
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, and S_3 are groups which have non-distributive subgroup lattices.

□

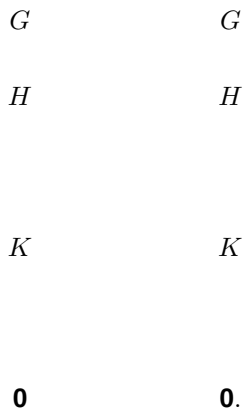
An important observation with greatest lower bounds and least upper bounds is that they are completely determined by the ordering of the elements in the lattice. This means, although a definition is given for a least upper bound in some

lattice, this definition is equivalent to any other definition that also matches the ordering. Therefore for instance the join of subgroups $\{H_i \mid i \in I\}$ can be defined equivalently as: the intersection of all subgroups which contains all H_i, the group generated by the union of each H_i, or the least subgroup which contains all H_i. Each definition should be verified as a compatible definition, but once known each from is interchangable.

A partially ordered set is traditionally depicted as a graph in which nodes represent elements in the set and edges connect elements virtically so that the lower element is less than the upper element in the ordering. Since partially orderings are transitive, generally edges connect elements that are proceed each other in the ordering and it is assumed any path from bottom to top relates to any additional orderings.

The subgroup lattice of a group always has a top and bottom element, namely **0** and G, where **0** is the set generated by the identity and G is the entire group. Despite having top and bottom elements, maximal and minimal subgroups of G are generally assumed to be proper subgroups.

Since normality is not transitive two distinct notations are adopted to illustrate normality in a subgroup lattice. In the case where $H \lhd K$, wher $H, K \leq G$, but H is not normal in G (the so called *local normal* case), the lattice is depicted as in the left diagram. However if H is also normal in all of G then the lattice is depicted as on the right.



Therefore the normal subgroup lattice can be picked out from the full subgroup lattice by deleting any edges that are not highlighted with $\lhd\lhd$. Although **0** is always normal in every subgroup, the notation is generally omited unless context requires an explicit use of this added information.[1]

When given a specific example group, the length of the edges can be proportioned to illustrate the relative orders of the subgroups. Generally this is done by making the unit length equal to the greatest common divisor of all indices in the subgroup lattice. [2] Subsequent edges scale by the ratio of their index to that of this unit index. This is contrary to the typical edge length ideal for sets which seeks to make edge lengths match the relative cardinalities of the elements. When proportions are considered, the edges may be labeled with the index and if any two subgroups are on the same vertical level then they can be assumed as having the same order.[3]

Subgroup lattices may also occasionally include horizontal dashed line segments. These lines connect subgroups that are conjugate, and thus isomorphic. Some presentations may label these edges with a conjugating element, although this rarely includes all possible conjugating elements.

[1] It is common to add this when identifing a normal sequence, such as a central sequence.

[2] From the first Sylow Theorem we see unless the group is a p-group, then the unit length will thus be one, even though no edge in the graph will have length one.

[3] By the Theorem of Lagrange the order can be calculated by taking the product of all the indicies from the subgroup **0** to the subgroup in question.

Example:

S_3 $\mathbb{Z}_6$

$\langle(123)\rangle$ $\langle 2\rangle$

$\langle(12)\rangle$ $\langle(13)\rangle$ $\langle(23)\rangle$ $\langle 3\rangle$

0 **0**

□

Bibliography

[Eyn] Charles Vanden Eynden, *Elementary number theory*, McGraw-Hill, Boston.

[Hun] Thomas W. Hungerford, *Algebra*, Springer-Verlag, New York.

Index

A_4 is not Simple, 71
A_4 is not solvable, 71
D_4 Table, 28
D_4 in $\mathbb{R}^{2\times 2}$, 37
D_n
    D_4 table, 28
    center, 73
    matrix form, 72
    matrix representation, 38
    normal subgroups, 73
D_n is Meta-cyclic, 72
D_n representation, 73
HK-subgroup, 56
Hom and Endomorphisms, 116
$Q_1 6$, 87
R/I-Modules, 114
S_n
    order, 29
S_n generators, 69
φ-function, 42
$\mathbb{Q}/\mathbb{Z}$ – Rationals Modulo One, 30
$\mathbb{Z}/n\mathbb{Z}$ Modules, 113
$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ lattice, 40
$\mathbb{Z}_p^\times$, 29
$\mathbb{Z}_{pq}$, 48
mA groups., 89
n-Product, 35
$n\mathbb{Z}$, 39
p-group Complex, 56
p-groups, 54
p-order Element Groups, 83
pq-groups, 58
5-Lemma, 119

Abelian
    automorphism, 37
    torsion, 52
abelian
    commutators, 91
Abelian Automorphism, 37
Abelian Relations, 32
Abelianization, 65
Automorphisms of $\mathbb{Z}_n$, 42
Axiom of Choice
    choice function, 14

Basis
    freeness, 80
basis
    linear independence, 90

Cancellation in Finite Semigroups, 34
Cantor's Diagonalization Method, 22
Cardinal Arithmetic, 19
Cardinal Arithmetic Properties, 20
Cardinal Exponents, 23
Cardinal Order, 22
Cardinality, 18
Cardinals
    countable, 19
    countable subsets, 22
    denumerable, 19
    exponents, 23
    finite products, 21
    finite sums, 21
    order, 22
    products, 19, 20
    sums, 19, 20
    unions, 26
Categories
    coproduct, 78
    coproducts, 77, 78
    epimorphisms, 114
    equivalence, 76
    free, 80
    free inclusion map, 79
    functors, 149
    left cancelable, 114
    monomorphisms, 114
    of modules, 114
    product projections, 15
    products, 77, 78, 117
    right cancelable, 114
    sums, 117
Center, 40
Center of D_n, 73
Center of S_n, 62
Choice Function, 14
Commutators, 91
Complete, 12
Congruence, 61
Conjugate Subgroups, 61
Cosets, 53
Countable, 18
Countable Subsets, 22
Counterexamples, 85
Cyclic Conjugates, 33

Cyclic Elements, 49
Cyclic Free Group, 86
Cyclic Groups of Order 4, 42
Cyclic Images, 41
Cyclic Products, 83

Direct Product, 28, 76
Division Rings have no Left Ideals, 103

Element Orders, 48
Elements of Free Groups, 86
Equivalence, 76
Euler
  φ, 54
  Euler's Theorem, 54
Example Functors, 149
Extension Degrees, 131

Fermat
  little theorem, 54
Fields
  of Integers, 30
Finite Cardinal Arithmetic, 21
Finite Groups, 51
Finite subgroups, 38
Finitely Generated, 63
Finitely Generated Modules, 116
Fixed Cardinal Unions, 25
Floops, 28
Free Basis, 80
Free Inclusion, 79
Free-Abelian Groups and Torsion, 91
Functions
  groups of, 28
Functor Image, 151
Functors
  commutator, 149
  direct sum, 149
  image, 151
  injective, 151
  polynomial, 149
  subgroup, 149

Generators, 41
Generators of PruferGroup, 44
Group Coproduct, 77
Groups
  HK-complex, 56
  n-Product, 35
  p-group complex, 56
  p-groups, 54
  abelianization, 65
  automorphisms, 37, 42
  cancellation laws, 34
  center, 41, 62
  center of S_n, 62
  commutator, 65
  complex, 57
  congruence, 61
  coproduct, 77
  cosets, 53
  cyclic, 41, 49
  direct product, 77
  element orders, 47, 48
  finite, 51
  finite subgroups, 39
  finitely generated, 63
  free, 92
  free-abelian groups, 92
  homomorphisms, 40
  index 2, 60
  infinite, 51
  infinite cyclic, 52
  intersect, 58
  join, 44, 55, 58
  lattice, 45
  normal extension, 65
  normal intersections, 60
  normal lattice, 64
  normality, 53, 61–63
  order $2n$, 58
  order pq, 58
  order 4, 55
  subgroup conjugation, 62
  subgroups, 38, 51, 53, 57, 66, 67
  torsion, 52
  torsion free, 92
  torsion-free, 92
Groups of Functions, 28
Groups of Involutions, 33
Groups of order $2n$, 57
Groups of Order 4, 55

Heuristics
  Pigeon-Hole Principle, 17
  Principle of Refinement, 155–157
Homomorphic Image of Ideals, 104
Homomorphic Pre-image, 66
Homomorphisms, 36
  element orders, 48
  pre-image, 66
  subgroups, 40

Idempotent and Splitting Maps, 119
Identifying Subgroups, 57
Index 2 Subgroups, 60
Index 2 subgroups of S_n, 70
Infinite Cyclic Groups, 52
Integer Quotients, 65
Integers
  subgroups, 39
Internal Product, 84
Involutions
  Even Groups, 33

Groups of, 33
Involutions in Even Groups, 33
Irreducible Non-Prime Elements, 107

Join, 55
Join and Intersect, 58
Join of Abelian Groups, 44
Join of Groups, 44

Klein Four Group, 29

Lattice, 11
Lattice of S_4, 69
Limitation of Chinese Remainder Theorem, 105
Linear Indepedence, 89
linear independence, 90
Little Theorem of Fermat, 54
Locating Finite Kernels, 66
Locating Finite Subgroups, 67

Matrices
Q_8-quaternions, 37
dihedral groups, 38
Matrix Form of D_n, 72
Maximal and Prime Principal Ideals, 107
Maximal Ideals in Non-Unital Rings, 105
Module Products and Sums, 117
Modules
$\mathbb{Z}/n\mathbb{Z}$-modules, 113
cyclic, 115
endomorphisms, 116
epimorphisms, 114
finitely generated, 116
fraction field module, 92
Hom, 116
monomorphisms, 114
products, 117
quotients, 115
R/I-Modules, 115
Schur's Lemma, 116
simple, 116
sums, 117
Torsion modules, 113
Monic/Epic Morphisms of Modules, 113
Monoids
n-Product, 35
examples, 27
Homomorphisms, 36
More S_n Generators, 70

Nilpotent Factor Ring, 104
Non-free, Torsion-free Groups, 92
Non-group Objects, 27
Non-normal Subgroups, 53
Non-Product Groups, 81
Non-trivial Automorphisms of Groups, 123
Normal and Congruence, 60
Normal Cyclic Subgroups, 63
Normal Extension, 65
Normal Intersections, 60
Normal Subgroup Lattice, 64
Normality in D_n, 72
Normality in Q_8, 62
Normality in S_n, 61
Normality is Not Transitive, 63

Order
completeness, 12
lattice, 11
lexicographic, 13
linear, 15
successors, 15
well-ordering, 13
Order of S_n, 29
Order of Elements, 47
Ordered Groups, 27
Orders in Abelian Groups, 47
Orders under Homomorphisms, 48

Permutation Conjugates, 69
Permutation Conjugation, 70
Permutations
A_n simple, 71
conjugates, 70
subgroups index 2, 70
permutations
A_4, 71
conjugates, 69
generators, 69, 70
subgroups, 69
Pigeon-Hole Principle, 17
Pointed Sets, 76
products, 78
Prüfer Group
generator, 44
Presentations
Q_8, 58
Prime Decomposition of Integer Rings, 105
Prime Ideal in Zero-Divisors, 104
Prime/Maximal Ideals in $\mathbb{Z}/m\mathbb{Z}$, 105
Product Decomposition, 81
Product Quotients, 84
Products
decomposition, 81
internal, 84
non-product groups, 81
of cyclics, 83
of quotients, 64
quotients, 84
split extension, 82
weak, 85
weak product, 82

Products of Pointed Sets, 78
Projections, 15
PruferGroup, 32
PruferGroup Structure, 49
PruferQuotients, 68

Quaternion Group Ring vs. Division Ring, 101
Quaternion Presentation, 58
Quaternions, 37
Quotient Modules, 123
Quotient Products, 64

Radical Ideal, 102
Rational Subgroups, 31
Rationals
  $\frac{a}{b}, p \nmid b$, 31
  $\frac{a}{p^i}$, 31
  Prüfer Group, 32
  roots of unity, 30
Relations
  abelian, 32
relations
  commutators, 91
Rings
  endomorphism ring, 116
  of Integers, 30

Schur's Lemma, 116
Semi-Lexicographic Order, 14
Semigroups
  n-Product, 35
  examples, 27
  Floops, 28
  with cancellation, 34
Set Coproduct, 77
Sets
  coproduct, 78
Simple
  modules, 116
Split Decomposition, 119
Split Extension, 81
Subgroup Lattices, 45
Subgroups, 38
Subgroups and Homomorphisms, 40
Subgroups and the Complex, 57
Subgroups of S_n, 39
Successors, 15

The "Idealizer", 103
The Annihilator Ideal, 103
The Little Radical Ideal, 102
Torsion Subgroup, 51
Transcendental Dimension, 131

Unions of Finite Sets, 25
Unique Subgroups Are Normal, 62
Unitary Cyclic Modules, 115
Unitary Separation, 121

Weak Product, 82, 84
Well-ordering, 13