

Contents

Comments for the Student	xi
Comments for the Instructor	xvii
Acknowledgments	xxi
1 Mathematical Constructions in ISETL	1
1.1 Using ISETL	1
1.1.1 Activities	1
1.1.2 Getting started	5
1.1.3 Simple objects and operations on them	6
1.1.4 Control statements	7
1.1.5 Exercises	8
1.2 Compound objects and operations on them	11
1.2.1 Activities	11
1.2.2 Tuples	14
1.2.3 Sets	15
1.2.4 Set and tuple formers	16
1.2.5 Set operations	17
1.2.6 Permutations	17
1.2.7 Quantification	18
1.2.8 Miscellaneous ISETL features	20
1.2.9 VISETL	20
1.2.10 Exercises	21

1.3	Functions in ISETL	25
1.3.1	Activities	25
1.3.2	Funcs	31
1.3.3	Alternative syntax for funcs	32
1.3.4	Using funcs to represent situations	33
1.3.5	Funcs for binary operations	33
1.3.6	Funcs to test properties	33
1.3.7	Smaps	34
1.3.8	Procs	35
1.3.9	Exercises	35
2	Groups	39
2.1	Getting acquainted with groups	39
2.1.1	Activities	39
2.1.2	Definition of a group	42
2.1.3	Examples of groups	43
	Number systems	43
	Integers mod n	45
	Symmetric groups	47
	Symmetries of the square	49
	Groups of matrices	52
2.1.4	Elementary properties of groups	52
2.1.5	Exercises	55
2.2	The modular groups and the symmetric groups	57
2.2.1	Activities	57
2.2.2	The modular groups $\mathcal{Z}_n$	60
2.2.3	The symmetric groups S_n	65
	Orbits and cycles	68
2.2.4	Exercises	69
2.3	Properties of groups	71
2.3.1	Activities	71
2.3.2	The specific and the general	72
2.3.3	The cancellation law—An illustration of the abstract method	74
2.3.4	How many groups are there?	75
	Classifying groups of order 4	77
2.3.5	Looking ahead—subgroups	79
2.3.6	Summary of examples and non-examples of groups	80
2.3.7	Exercises	81
3	Subgroups	83
3.1	Definitions and examples	83
3.1.1	Activities	83
3.1.2	Subsets of a group	86
	Definition of a subgroup	86

3.1.3	Examples of subgroups	88
	Embedding one group in another	88
	Conjugates	89
	Cycle decomposition and conjugates in S_n	91
3.1.4	Exercises	92
3.2	Cyclic groups and their subgroups	94
3.2.1	Activities	94
3.2.2	The subgroup generated by a single element	96
3.2.3	Cyclic groups	100
	The idea of the proof	101
3.2.4	Generators	103
	Generators of S_n	103
	Parity—even and odd permutations	104
	Determining the parity of a permutation.	105
3.2.5	Exercises	105
3.3	Lagrange's theorem	108
3.3.1	Activities	108
3.3.2	What Lagrange's theorem is all about	111
3.3.3	Cosets	112
3.3.4	The proof of Lagrange's theorem	113
3.3.5	Exercises	116
4	The Fundamental Homomorphism Theorem	119
4.1	Quotient groups	119
4.1.1	Activities	119
4.1.2	Normal subgroups	121
	Multiplying cosets by representatives	124
4.1.3	The quotient group	125
4.1.4	Exercises	126
4.2	Homomorphisms	129
4.2.1	Activities	129
4.2.2	Homomorphisms and kernels	133
4.2.3	Examples	133
4.2.4	Invariants	135
4.2.5	Homomorphisms and normal subgroups	136
	An interesting example	137
4.2.6	Isomorphisms	138
4.2.7	Identifications	139
4.2.8	Exercises	141
4.3	The homomorphism theorem	143
4.3.1	Activities	143
4.3.2	The canonical homomorphism	145
4.3.3	The fundamental homomorphism theorem	147
4.3.4	Exercises	150

5	Rings	153
5.1	Rings	153
5.1.1	Activities	153
5.1.2	Definition of a ring	156
5.1.3	Examples of rings	156
5.1.4	Rings with additional properties	157
	Integral domains	157
	Fields	158
5.1.5	Constructing new rings from old—matrices	159
5.1.6	Constructing new rings from old—polynomials	161
5.1.7	Constructing new rings from old—functions	164
5.1.8	Elementary properties—arithmetic	165
5.1.9	Exercises	165
5.2	Ideals	168
5.2.1	Activities	168
5.2.2	Analogies between groups and rings	170
5.2.3	Subrings	171
	Definition of subring	171
5.2.4	Examples of subrings	171
	Subrings of $\mathbb{Z}_n$ and $\mathbb{Z}$	171
	Subrings of $M(R)$	172
	Subrings of polynomial rings	172
	Subrings of rings of functions	173
5.2.5	Ideals and quotient rings	173
	Definition of ideal	173
	Examples of ideals	175
5.2.6	Elementary properties of ideals	175
5.2.7	Elementary properties of quotient rings	176
	Quotient rings that are integral domains— prime ideals	176
	Quotient rings that are fields—maximal ideals	177
5.2.8	Exercises	178
5.3	Homomorphisms and isomorphisms	181
5.3.1	Activities	181
5.3.2	Definition of homomorphism and isomorphism	182
	Group homomorphisms vs. ring homomorphisms	183
5.3.3	Examples of homomorphisms and isomorphisms	183
	Homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_k$	183
	Homomorphisms of $\mathbb{Z}$	184
	Homomorphisms of polynomial rings	184
	Embeddings— $\mathbb{Z}$, $\mathbb{Z}_n$ as universal subobjects	184
	The characteristic of an integral domain and a field	185
5.3.4	Properties of homomorphisms	186
	Preservation	186

	Ideals and kernels of ring homomorphisms . . .	186
5.3.5	The fundamental homomorphism theorem	187
	The canonical homomorphism	187
	The fundamental theorem	187
	Homomorphic images of $\mathcal{Z}$, $\mathcal{Z}_n$	188
	Identification of quotient rings	188
5.3.6	Exercises	190
6	Factorization in Integral Domains	193
6.1	Divisibility properties of integers and polynomials	193
6.1.1	Activities	193
6.1.2	The integral domains $\mathcal{Z}$, $\mathcal{Q}[x]$	198
	Arithmetic and factoring	198
	The meaning of unique factorization	199
6.1.3	Arithmetic of polynomials	200
	Long division of polynomials	200
6.1.4	Division with remainder	202
6.1.5	Greatest Common Divisors and the Euclidean algorithm	204
6.1.6	Exercises	208
6.2	Euclidean domains and unique factorization	209
6.2.1	Activities	209
6.2.2	Gaussian integers	212
6.2.3	Can unique factorization fail?	214
6.2.4	Elementary properties of integral domains	214
6.2.5	Euclidean domains	218
	Examples of Euclidean domains	219
6.2.6	Unique factorization in Euclidean domains	221
6.2.7	Exercises	225
6.3	The ring of polynomials over a field	226
6.3.1	Unique factorization in $F[x]$	227
6.3.2	Roots of polynomials	228
6.3.3	The evaluation homomorphism	230
6.3.4	Reducible and irreducible polynomials	231
	Examples	231
6.3.5	Extension fields	235
	Construction of the complex numbers	237
6.3.6	Splitting fields	237
6.3.7	Exercises	239
	Index	241