Modern Algebra Lecture Notes

Dr. Monks - University of Scranton - Fall 2019

1 Introduction

This is **not** a complete set of lecture notes for Math 448, Modern Algebra I. Additional material will be covered in class and discussed in the textbook. These notes are currently under development as a port from a previous version, so typos and formatting errors are inevitable. Check back frequently for updates.

2 Logic

In this section we give an informal overview of logic and proofs. For a more formal introduction see any logic textbook.

Proofs and Formal Axiom Systems

Definition. A *Formal Proof System* (or Formal Axiom System) consists of

1. A set of expressions $\mathcal{S}$, called the *statements*.
2. A set of rules $\mathcal{R}$, called the *rules of inference*.

Each rule of inference has zero or more inputs called *premises* and one or more outputs called *conclusions*. Most premises and all conclusions of a rule of inference are statements in the system.[1] There also may be *conditions* on when a particular rule of inference can be used.

Definition. An *axiom* is a conclusion of a rule of inference that has no premises.

Definition. A statement Q in a formal axiom system is *provable from* premises $P_1, \ldots, P_n$ if

1. Q is one of the premises $P_1, \ldots, P_n$, or
2. Q is a conclusion of a rule of inference whose premises are provable from $P_1, \ldots, P_n$.

In particular, if Q is an axiom, then Q is provable from no premises at all!

Definition. If Q follows from no premises in a formal axiom system, we say that Q is *provable* in the system. A provable statement is called a *theorem*.

And finally, the definition we've all been waiting for!

Definition. A *proof* of a statement in a formal axiom system is a finite sequence of applications of the rules of inference (i.e., *inferences*) that show that the statement is a theorem in that system.

[1] Other common premises are variable declarations, constant declarations, and subproofs.

Notation. If Q is provable from premises $P_1, \ldots, P_n$ in a formal system we can denote this symbolically as

$$P_1, \ldots, P_n \vdash Q$$

It is also commonplace to refer to such an expression as a theorem. To prove such a theorem is to give a proof of Q in the same formal system where additionally the premises are 'Given' as axioms.

Variables, Expressions, and Statements in Mathematics

Term	**Description**
set	A *set* is a collection of items.
element	The items in a set are called its *elements* (or members).
expression	An *expression* is an arrangement of symbols which represents an element of a set
type	The set of elements that an expression can represent is called the *type* of the expression.
value	The element of the domain that the expression represents is called a *value* of that expression.
variable	A *variable* is an expression consisting of a single symbol
constant	A *constant* is an expression whose domain contains a single element.
statement	A *statement* (or *Boolean expression*) is an expression whose domain is $\{\text{true}, \text{false}\}$.
truth value	The value of a statement is called its *truth value*.
solve	To *solve* a statement is to determine the set of all elements for which the statement is true.
solution set	The set of all solutions of a statement is called the *solution set*.
equation	An *equation* is a statement of the form $A = B$ where A and B are expressions.
inequality	An *inequality* is a statement of the form $A \star B$ where A and B are expressions and $\star$ is one of $\leq$, $\geq$, $>$, $<$, or $\neq$.

Remarks:

- An element is either in a set or it is not in a set, it cannot be in a set more than once.
- It is not necessary that we know specifically which element of the domain an expression represents, only that it represents some unspecified element in that set.
- We do not have to know if a statement is true or false, just that it is either true or false.
- If a statement contains n variables, $x_1, \ldots x_n$, then to solve the statement is to find the set of all n-tuples $(a_1, \ldots, a_n)$ such that each a_i is an element of the domain of x_i and the statement becomes true when $x_1, \ldots, x_n$ are replaced by $a_1, \ldots, a_n$ respectively. In this situation, each such n-tuple is called a *solution* of the statement.

- In formal mathematics, 'true' means 'provable'.

Substitution and Lambda Expressions

Definition. We can prefix an expression E to form the expression "$\lambda x, E$" (or "$x \mapsto E$") to indicate that all occurrences[2] of x in E are a variable that represents the same unspecified object of the same type as x. These prefixed expressions are called *lambda expressions* (or *anonymous functions*).

Definition. Lambda expressions can be *applied* to an expression a having the same type as x to form a new expression, $(\lambda x, E)(a)$ which has the same type as E. These can be further simplified to the expression obtained by replacing all occurrences[3] of x in E with a.

Remark. If we give a name to a lambda expression, e.g., define f to be $\lambda x, E$ then the expression $(\lambda x, E)(a)$ is just the usual notation for function application $f(a)$.[4]

Definition. Two lambda expressions are said to be *equivalent* if they simplify to the same or equivalent things when applied to any argument.

Remark. Renaming all occurrences of x in $\lambda x, E$ with a new identifier always produces a lambda expression that is equivalent to the original. Another common situation where we can simplify a lambda expression $\lambda x, E$ is when the expression E does not contain x. In this situation $(\lambda x, E)(a)$ simplifies to just E for every a, and thus we can say that $\lambda x, E$ simplifies to just E in that case.

Rules of Inference in Mathematics

Most rules of inference in mathematics are stated as assertions that something can be proven in the given system. Frequently these are given as lambda expressions. Such a lambda expression generate an entire family of specific rules of inference, one for each application of the expression. Because this is so common, we usually omit the lambda prefixes, and use the convention that any free variables that appear free in the premises or conclusion of a rule of inference can be replaced with an expression of the same type to form a particular instance of that rule of inference.

[2] These refer to free occurrences - see below.

[3] See footnote 2. Also no free identifier in a should become bound as a result of the substitution.

[4] Indeed, in precalculus they usually write $f(x) = x^3$ instead of writing $f = (\lambda x, x^3)$, but the latter is usually what they mean.

Template Notation for Rules of Inference

Notation. A rule of inference having premises $P_1, \ldots, P_k$ and conclusions $Q_1, \ldots, Q_n$ can be expressed in *template notation* as

P_1 (show)
$\vdots$
P_k (show)
Q_1 (conclude)
$\vdots$
Q_n (conclude)

In this notation, the rule looks like a template that we can fill in to create our proofs. In particular, the lines marked with a (show) need to be justified with a rule of inference that is supplied as a reason for that line, and those marked with (conclude) can be justified with the given rule of inference.

Some rules of inference have a premise of the form

$$(P_1, \ldots, P_k \vdash Q)$$

This is not a statement in the formal system itself, but rather the assertion that Q can be proven from $P_1, \ldots, P_k$ in the formal system. We call an expression of this form a *subproof* or *environment*. Such a premise is satisfied by including a subproof in a proof that shows that Q can be proved from the given premises (which do not need to be justified by a rule of inference). We denote this in recipe notation as an indented 'assume-block' as illustrated below.

Example 1. Suppose we have a rule of inference that justifies the following.

$$\varphi \text{ or } \psi, (\varphi \vdash \rho), (\psi \vdash \rho) \vdash \rho$$

where φ, ψ, and ρ are any mathematical statements. Then we would express this rule in recipe notation as

φ or ψ (show)
  Assume φ
  ρ (show)
  $\leftarrow$
  Assume ψ
  ρ (show)
  $\leftarrow$
ρ (conclude)

In this, everything between an Assume and the following $\leftarrow$ (the 'end assumption' symbol) is a *subproof* that demonstrates the corresponding premise in the rule of inference. We indent such

assumption blocks in our proofs. Subproofs can be nested, and the level of indentation corresponds to the level of nesting. Assumptions (lines that start with Assume) do not need to be justified by a rule of inference. We say that they are *given*. Lines marked with (show) must be justified. Lines marked with (conclude) are justified by the rule itself.

Note that we do include the word "Assume " in the proof itself, but not the words "show" or "conclude" which are just instructions to the proof author (as opposed to the reader) for how to justify the indicated lines.

Natural Deduction

We now turn our attention to a formal axiom system that is based on one first formulated by Gerhard Gentzen in 1934 as a formal system that closely imitates the way mathematicians actually reason when writing traditional expository proofs.

Propositional Logic

The Statements of Propositional Logic

Definition. Let φ, ψ be statements. Then the five expressions "$\neg\varphi$", "φ and ψ", "φ or ψ", "$\varphi \Rightarrow \psi$", and "$\varphi \Leftrightarrow \psi$" are also statements whose truth values are completely determined by the truth values of φ and ψ as shown in the following table:

φ	ψ	$\neg\varphi$	φ and ψ	φ or ψ	$\varphi \Rightarrow \psi$	$\varphi \Leftrightarrow \psi$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

We can also write 'not' for $\neg$, 'if and only if' for $\Leftrightarrow$, and 'implies' for $\Rightarrow$. A statement of the form '$\varphi \Rightarrow \psi$' is called a *conditional statement* or an *implication*, and can be written in English as 'φ implies ψ', 'if φ then ψ', 'ψ follows from φ', or 'ψ, if φ'.

Definition. The statements $\mathcal{S}$, of Propositional Logic consists of

1. Atomic Statements that do not contain any of the five logical operators, and
2. Compound Statements that are one of the five forms, $\neg\varphi$, φ and ψ, φ or ψ, $\varphi \Rightarrow \psi$, or $\varphi \Leftrightarrow \psi$ where φ and ψ are any elements of $\mathcal{S}$.

Note: In compound statements we usually put parentheses around the statements φ or ψ involved. For instance if φ is the statement 'P or Q' and ψ is the statement 'R and S' then $\varphi \Rightarrow \psi$ should be written

$$(P \text{ or } Q) \Rightarrow (R \text{ and } S)$$

in order to avoid the confusion that 'P or $Q \Rightarrow R$ and S' might actually mean something like P or $(Q \Rightarrow (R$ and $S))$. In order to cut down on parentheses, we assign a **precedence** order for our operators, meaning we apply the operators in the following order (from highest to lowest).

Precedence of Notation
parentheses, brackets, (), {}, [] etc.
arithmetic operations* $\wedge, \cdot, +, \ldots$ etc.
set operations $\times, -, \cap, \cup, \ldots$ etc.
arithmetic and set relations $=, \subseteq, \leq, \neq, \ldots$ etc.
not
and , or
$\Rightarrow$
$\Leftrightarrow$
$\forall, \exists, \exists!$

* with the usual precedence among them

The Rules of Propositional Logic

Natural deduction generially defines a pair of rules for each definition. A 'plus' rule is used to prove statements that contain the thing being defined from statements that do not, while 'minus' rules do the opposite.

Rules of Propositional Logic	
Name	Rule
and+	$\varphi, \psi \vdash (\varphi \text{ and } \psi)$
and−	$(\varphi \text{ and } \psi) \vdash \varphi$ $(\varphi \text{ and } \psi) \vdash \psi$
or+	$\varphi \vdash (\varphi \text{ or } \psi)$ $\psi \vdash (\varphi \text{ or } \psi)$
or− *(proof by cases)*	$(\varphi \text{ or } \psi), (\varphi \Rightarrow \rho), (\psi \Rightarrow \rho) \vdash \rho$
$\Rightarrow$+	$(\varphi \vdash \psi) \vdash (\varphi \Rightarrow \psi)$
$\Rightarrow$− *(modus ponens)*	$(\varphi \Rightarrow \psi), \varphi \vdash \psi$
$\Leftrightarrow$+	$(\varphi \Rightarrow \psi), (\psi \Rightarrow \varphi) \vdash (\varphi \Leftrightarrow \psi)$
$\Leftrightarrow$−	$(\varphi \Leftrightarrow \psi) \vdash (\varphi \Rightarrow \psi)$ $(\varphi \Leftrightarrow \psi) \vdash (\psi \Rightarrow \varphi)$
not+ *(proof by contradiction)*	$(\varphi \vdash \ \rightarrow\leftarrow) \vdash \text{not}\, \varphi$
not− *(proof by contradiction)*	$(\text{not}\, \varphi \vdash \ \rightarrow\leftarrow) \vdash \varphi$

Rules of Propositional Logic (cont.)

Name	Rule
$\rightarrow\leftarrow$ +	$\varphi, (\text{not}\,\varphi) \vdash \rightarrow\leftarrow$

We can also list these rules in template notation that mirrors how they are used in proofs.

Propositional Logic

and +	and +
φ (show) ψ (show) ..... φ and ψ (conclude)	φ and ψ (show) ..... φ (conclude) ψ (conclude)
$\Rightarrow$ +	$\Rightarrow$ – (modus ponens)
Assume φ ψ (show) $\leftarrow$ ..... $\varphi \Rightarrow \psi$ (conclude)	φ (show) $\varphi \Rightarrow \psi$ (show) ..... ψ (conclude)
$\Leftrightarrow$ +	$\Leftrightarrow$ –
$\varphi \Rightarrow \psi$ (show) $\psi \Rightarrow \varphi$ (show) ..... $\varphi \Leftrightarrow \psi$ (conclude)	$\varphi \Leftrightarrow \psi$ (show) ..... $\varphi \Rightarrow \psi$ (conclude) $\psi \Rightarrow \varphi$ (conclude)
or +	or – (proof by cases
φ (show) ..... φ or ψ (conclude) ψ or φ (conclude)	φ or ψ (show) $\varphi \Rightarrow \rho$ (show) $\psi \Rightarrow \rho$ (show) ..... ρ (conclude)
not + (proof by contradiction)	not – (proof by contradiction)
Assume φ $\rightarrow\leftarrow$ (show) $\leftarrow$ ..... $\neg\varphi$ (conclude)	Assume $\neg\varphi$ $\rightarrow\leftarrow$ (show) $\leftarrow$ ..... φ (conclude)

Propositional Logic (cont.)

$\rightarrow\leftarrow$ +	
φ	(show)
$\neg\varphi$	(show)
.....	
$\rightarrow\leftarrow$	(conclude)

copy	
φ	(show)
.....	
φ	(conclude)

Remarks:

- The symbol $\leftarrow$ is an abbreviation for "end assumption".
- The symbol $\rightarrow\leftarrow$ is called "contradiction" and represents the logical constant false.
- The word Assume is actually entered as part of the proof itself, it is not just an instruction in the recipe like '(show)' and '(conclude)'.
- The inputsAssume- and "$\leftarrow$" are not themselves statements that you prove or are given, but rather are inputs to rules of inference that may be inserted into a proof at any time. There is no useful reason however, to insert such statements unless you intend to use one of the rules of inference that requires them as an input.
- The statement following an Assume is the same as any other statement in the proof and can be used as an input to a rule of inference.
- Statements in an Assume-$\leftarrow$ block can be used as inputs to rules of inference whose conclusion is also inside the same block only. Once a Assume is closed with a matching $\leftarrow$, only the entire block can be used as an input to a rule of inference. The individual statements within a block are no longer valid outside the block. We usually indent and Assume-$\leftarrow$ block to keep track of what statements are valid under which assumptions.

Definition. A compound statement of propositional logic is called a *tautology* if it is true regardless of the truth values the atomic statements that comprise it. (Its "truth table" contains only T's.)

It can be shown that a statement can be proved with Propositional Logic if and only if the statement is a tautology.

Formal Proof Style

One way to write down the proof of a theorem is called a *formal proof*. This style of proof consists of a sequence of numbered lines containing statements, reasons, and references to premises. Every line contains exactly one statement (or declaration - see below), and the reason given on that line is the name of a rule of inference for which the statement on that line is the conclusion. If the rule of inference has premises, the reason is followed by the line numbers containing the statements (or variable declarations) which are the premises that the rule is being applied to. References to premises can only refer to lines which appear earlier in the same proof which are not contained in a subproof that has been closed. Subproofs used as a premise are cited by listing the range of line numbers comprising the subproof.

Example 2. Let P and Q be statements. Prove the following case of DeMorgan's Law, namely that

$$\neg P \text{ or } \neg Q \Rightarrow \neg(P \text{ and } Q)$$

Proof.

1.	Assume $\neg P$ or $\neg Q$	-
2.	Assume $\neg P$	-
3.	Assume P and Q	-
4.	P	by and $-$; 3
5.	$\rightarrow\leftarrow$	by $\rightarrow\leftarrow$ +; 2,4
6.	$\leftarrow$	-
7.	$\neg(P \text{ and } Q)$	by not+; 3,5,6
8.	$\leftarrow$	-
9.	$\neg P \Rightarrow \neg(P \text{ and } Q)$	by $\Rightarrow$+; 2,7,8
10.	Assume $\neg Q$	-
11.	Assume P and Q	-
12.	Q	by and $-$; 11
13.	$\rightarrow\leftarrow$	by $\rightarrow\leftarrow$ +; 10,12
14.	$\leftarrow$	-
15.	$\neg(P \text{ and } Q)$	by not+; 11, 13, 14
16.	$\leftarrow$	-
17.	$\neg Q \Rightarrow \neg(P \text{ and } Q)$	by $\Rightarrow$+; 10,15,16
18.	$\neg(P \text{ and } Q)$	by or $-$; 1,9,17
19.	$\leftarrow$	-
20.	$\neg P$ or $\neg Q \Rightarrow \neg(P \text{ and } Q)$	by $\Rightarrow$ +; 1,18

□

Notice that when a rule of inference has a subproof for a premise, we indicate this by citing the line numbers for the assumption, the conclusion, and the end of assumption block indicator ($\leftarrow$) e.g., as shown in line 7 above.

Exercise 3. Give a formal proof for the reverse case of DeMorgan's Law, namely that

$$\neg(P \text{ and } Q) \Rightarrow \neg P \text{ or } \neg Q$$

Exercise 4. Give a formal proof for yet another case of DeMorgan's Law, namely that

$$\neg(P \text{ or } Q) \Leftrightarrow \neg P \text{ and } \neg Q$$

Predicate Logic

We can extend Propositional Logic by adding more statements and rules of inference to those we already have in our formal system. This extended formal system is called *Predicate Logic*.

Quantifiers

The symbol λ in the lambda expression $(\lambda x, E)$ is an example of a *quantifier*. The thing that all quantifiers have in common is that they *bind variables*. If W is an expression that does not contain any quantifiers, then every occurrence of every identifier that appears in the expression is said to be a *free* occurrence of that identifier.

If a quantifier appears in an expression, there are one or more variables that it binds. All occurrences of the variables that are in the scope of the quantifier (usually everything to the right of it until a scope delimiter for that quantifier is encountered) are called *bound variables*.

Predicate logic extends propositional logic by defining two additional quantifiers.

Definition. The symbols $\forall$ and $\exists$ are *quantifiers*. The symbol $\forall$ is called "for all", "for every", or "for each". The symbol $\exists$ is called "for some" or "there exists".

We will encounter more quantifiers beyond just these two and λ.

Statements

Every statement of Propositional Logic is still a statement of Predicate Logic. In addition we define the following statements.

Definition. If x is any variable and W is a lambda expression[5] that simplifies to a statement when applied to any expression having the same type as x, then $(\forall x, W(x))$ and $(\exists x, W(x))$ are both statements.

We say that the *scope* of the quantifier in $(\forall x, W(x))$ and $(\exists x, W(x))$ is everything inside the outer parentheses. Sometimes these parentheses are omitted when the scope is clear from context. All occurrences if x throughout the scope are said to be bound by the quantifier.

Variable declaration

Before using a free identifier for the first time in any expression in our proofs we should tell the reader what that identifier represents. There are four ways to introduce a new free identifier.

1. It can be declared to be a variable (a variable declaration).
2. It can be declared to be a constant (a constant declaration).
3. It can be defined as temporary new notation, usually as an abbreviation for a larger expression (a notational definition).

[5] Not containing x.

4. It can occur free in an expression preceding the proof itself, such as in the statement of the theorem, in a premise that is given, or declared globally prior to the start of the proof (globally declared).

Bound variables do not have to be declared. They can be any identifier you like, as long as that identifier is not in the scope of more than one quantifier that binds it.

Rules of Inference

The rules of inference for these two quantifiers are as follows.

Rules of Inference for Predicate Logic

Name	Rule
$\forall+$	(Let s be arbitrary $\vdash \varphi(s)) \vdash (\forall x, \varphi(x))$
$\forall-$	$(\forall x, \varphi(x)) \vdash \varphi(t)$
$\exists+$	$\varphi(t) \vdash (\exists x, \varphi(x))$
$\exists-$	$(\exists x, \varphi(x)) \vdash$ For some constant $c, \varphi(c)$
$\exists!+$	$(\exists x, \varphi(x)$ and $\forall y, \varphi(y) \Rightarrow y = x) \vdash (\exists! x, \varphi(x))$
$\exists!-$	$(\exists! x, \varphi(x)) \vdash \exists x, \varphi(x)$ and $\forall y, \varphi(y) \Rightarrow y = x$

These can also be expressed in template notation.

Predicate Logic*

$\forall+$

Let s be arbitrary (variable declaration)
$\varphi(s)$ (show)
$\leftarrow$
.....
$\forall x, \varphi(x)$ (conclude)

$\forall-$

$\forall x, \varphi(x)$ (show)
.....
$\varphi(t)$ (conclude)

$\exists+$

$\varphi(t)$ (show)
.....
$\exists x, \varphi(x)$ (conclude)

$\exists-$

$\exists x, \varphi(x)$ (show)
.....
For some c, (constant declaration)
$\varphi(c)$ (conclude)

**Restrictions and Remarks*

- In $\forall+$, s must be a new variable in the proof, cannot appear as a free variable in any assumption or premise, and $W(s)$ cannot contain any constants which were produced by the $\exists-$ rule. The indentation and $\leftarrow$ symbol indicate the scope of the declaration of s. Variables s and x must have the same type.

- In $\forall-$ and $\exists+$, no free variable in t may become bound when t is substituted for x in $W(x)$. Variable x and expression t must have the same type.
- In $\exists+$, t can be an expression, and $W(x)$ can be the expression obtained by replacing one or more of the occurrences of t with x. The identifier x cannot occur free in $W(t)$. Variable x and expression t must have the same type.
- In $\exists-$, c must be a new identifier in the proof. Also $W(c)$ must immediately follow the constant declaration for c in the proof. The scope of the declaration continues indefinitely or until the end of the scope of any subproof block or variable declaration scope that contains the constant declaration. Variable x and constant c must have the same type.

  One consequence of this is that it enforces the restriction on $\forall+$ that prohibits any constant declared with $\exists-$ to appear in $W(s)$ because after the application of $\forall+$ any free occurrence of c is no longer in the scope of the original declaration (and therefore undeclared).

Equality

Finally, we can complete our definition of logic by adding the rules of inference for equality.

Definition. The equality symbol, $=$, is defined by the following two rules of inference.

Rules of Inference for Equality

Name	Rule
reflexivity	$\vdash (x = x)$
substitution	$(x = y), \varphi \vdash$ (φ with one or more free occurrences of x replaced by y)

Equality

Reflexivity	Substitution*
.....	$x = y$ (SHOW)
$x = x$	φ (SHOW)
	.....
	φ with any free occurrences of x replaced by y. (CONCLUDE)

**Restrictions and Remarks*

- Note that in the Reflexive rule there are no inputs, so you can insert a statement of the form $x = x$ into your proof at any time.
- No free variable in y can become bound when y is substituted for x.

Rather than make a formal definition for the symbol $\neq$ we will simply define $x \neq y$ to be convenient shorthand for $\neg(x = y)$

3 Appendix B: Sets, Functions, Numbers

The symbol $\in$ is formally undefined, but it means "is an element of". The expression $x \in A$ is a statement that is true if and only if A is a set and x is an element of A. Modern set theory is usually based on the Zermelo-Fraenkel axioms which are robust but sophisticated. Most mathematicians use the slightly more informal definitions listed below, which will be sufficient for our purposes.

As with $\neq$ we will consider $x \notin A$ to be an abbreviation for $\neg(x \in A)$ that can be used interchangeably rather than defining it separately.

Elementary Set Theory	
Name	Rule
Empty set	$\forall x, x \notin \{\,\}$
Finite set notation	$x \in \{x_1, \ldots, x_n\} \Leftrightarrow x = x_1$ or $\cdots$ or $x = x_n$
*Set builder notation**	$x \in \{\, y : \varphi(y) \,\} \Leftrightarrow \varphi(x)$
Subset	$A \subseteq B \Leftrightarrow \forall x, x \in A \Rightarrow x \in B$
Set equality	$A = B \Leftrightarrow A \subseteq B$ and $B \subseteq A$
Power set	$\mathcal{P}(A) = \{B : B \subseteq A\}$
Intersection	$x \in A \cap B \Leftrightarrow x \in A$ and $x \in B$
Union	$x \in A \cup B \Leftrightarrow x \in A$ or $x \in B$
Set Difference	$x \in B - A \Leftrightarrow x \in B$ and $x \notin A$
Complement	$x \in A' \Leftrightarrow x \notin A$
Indexed Intersection	$x \in \bigcap_{i \in I} A_i \Leftrightarrow \forall i, i \in I \Rightarrow x \in A_i$
Indexed Union	$x \in \bigcup_{i \in I} A_i \Leftrightarrow \exists i, i \in I$ and $x \in A_i$
Two convenient abbreviations	$(\forall x \in A, \varphi(x)) \Leftrightarrow \forall x, x \in A \Rightarrow \varphi(x)$ $(\exists x \in A, \varphi(x)) \Leftrightarrow \exists x, x \in A$ and $\varphi(x)$
Partition of a set	P is a partition of $A \Leftrightarrow (\forall S \in P, S \neq \varnothing$ and $S \subseteq A)$ and $A = \bigcup_{S \in P} S$ and $\forall S \in P, \forall T \in P, S = T$ or $S \cap T = \varnothing$
solution set of W	$\{s : W(s)\}$ where W is a lambda expression that returns a statement

*Set builder notation and indexed union and intersection are quantifiers that bind the variables y and i in their respective definitions. Thus, for example, y and i can be replaced by alpha substitution.

**To *solve* a statement is to find its solution set. The values of s in the solution set must have the same type as the input to W. For multivariable statements the solution set is the set of all ordered tuples that make it true.

Cartesian Products	
Name	Rule
Ordered Pairs	$(x, y) = (u, v) \Leftrightarrow x = u$ and $y = v$
Ordered n-tuple	$(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \Leftrightarrow x_1 = y_1$ and $\cdots$ and $x_n = y_n$
Cartesian Product	$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$
Cartesian Product	$A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) : x_1 \in A_1 \text{ and } \cdots \text{ and } x_n \in A_n\}$
Power of a Set	$A^n = A \times A \times \cdots \times A$ where there are n occurrences of A in the Cartesian product

Functions	
Name	Rule
Def of function	$f : A \to B \Leftrightarrow f \subseteq A \times B$ and $(\forall x, \exists! y, (x, y) \in f)$
Alt. function notation	$A \xrightarrow{f} B \Leftrightarrow f : A \to B$
Def of $f(x)$	$f : A \to B \Rightarrow f(x) = y \Leftrightarrow (x, y) \in f$
Domain	$f : A \to B \Rightarrow A$ is the *domain* of f
Codomain	$f : A \to B \Rightarrow B$ is the *codomain* of f
Function equality	$f = g \Leftrightarrow f : A \to B$ and $g : A \to B$ and $\forall a \in A, f(a) = g(a)$
Image (of a set)	$f : A \to B$ and $S \subseteq A \Rightarrow f(S) = \{f(x) : x \in S\}$
Range	$f : A \to B \Rightarrow f(A)$ is the *range* of f
Identity Map	$\mathrm{id}_A : A \to A$ and $\forall x, \mathrm{id}_A(x) = x$
Composition	$A \xrightarrow{f} B$ and $B \xrightarrow{g} C \Rightarrow A \xrightarrow{g \circ f} C$ and $\forall x, (g \circ f)(x) = g(f(x))$
Injective (one-to-one)[6]	f is *injective* $\Leftrightarrow \forall x \in A, \forall y \in A, f(x) = f(y) \Rightarrow x = y$
Surjective (onto)[1]	f is *surjective* $\Leftrightarrow \forall y \in B, \exists x \in A, y = f(x)$
Bijective	f is *bijective* $\Leftrightarrow f$ is injective and f is surjective
Inverse	g is an inverse of $f \Leftrightarrow$ $f : A \to B$ and $g : B \to A$ and $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$
Invertible	f is invertible $\Leftrightarrow \exists g, g$ is an inverse of f
Inverse Image	$f : A \to B$ and $S \subseteq B \Rightarrow f^{\mathrm{inv}}(S) = \{x \in A : f(x) \in S\}$
Binary Operation	Any function $* : G \times G \to G$ is called a *binary operation* on G

*Another way to define a function is to say that it is a triple, (f, A, B) where f is a lambda expression, A is a set of elements the type f can be applied to, and B is a set of elements of the type f outputs. Note that $f(a)$ represents the same element in both definitions.

[6] Where $f : A \to B$.

Famous Sets of Numbers	
Name	Rule
The Natural Numbers	$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$
The Integers	$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
The Rational Numbers	$\mathbb{Q} = \left\{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}, b > 0, \text{ and } \gcd(a, b) = 1\right\}$
The Real Numbers	$\mathbb{R} = \{x : x \text{ can be expressed as a decimal number}\}$
The Complex Numbers	$\mathbb{C} = \{x + yi : x, y \in \mathbb{R}\}$ where $i^2 = -1$
The positive real numbers	$\mathbb{R}^+ = \{x : x \in \mathbb{R} \text{ and } x > 0\}$
The negative real numbers	$\mathbb{R}^- = \{x : x \in \mathbb{R} \text{ and } x < 0\}$
The positive reals in a set A	$A^+ = A \cap \mathbb{R}^+$
The negative reals in a set A	$A^- = A \cap \mathbb{R}^-$
The first n positive integers	$\mathbb{I}_n = \{1, 2, \ldots, n\}$
The first n + 1 natural numbers	$\mathbb{O}_n = \{0, 1, 2, \ldots, n\}$

Sequences

Definition. A **finite sequence** is a function $t : \mathbb{I}_n \to A$ where n is a natural number and A is a set. An **infinite sequence** is a function $t : \mathbb{N}^+ \to A$ where A is a set. In either case, $t(k)$ is called the k^{th} term of the sequence.

Remark. It is often convenient to say that t is a finite (resp infinite) sequence if $t : \mathbb{O}_n \to A$ (resp. $t : \mathbb{N} \to A$). In this case we say that $t(k)$ is the $k + 1^{\text{st}}$ term of the sequence.

Notation 5. If $t : \mathbb{I}_n \to A$ is a finite sequence we write

$$t_1, t_2, t_3, \ldots, t_n$$

as another notation for t, where $t_k = t(k)$ for all $k \in \mathbb{I}_n$. Similarly if $t : \mathbb{N}^+ \to A$ we write

$$t_1, t_2, t_3, \ldots$$

for t where $t_k = t(k)$ for all $k \in \mathbb{N}^+$.

Remark. Sometimes for readability we might want to enclose a sequence in parenthesis. For example, we might write "Let $t = (1, 2, 3, 4)$" instead of "Let $t = 1, 2, 3, 4$". In this sense there is really no distinction between n-tuples and finite sequences.

Notation 6. We use an overbar to indicate an infinite repeating sequence, i.e.

$$t_0, t_1, \ldots, t_{k-1}, \overline{t_k, \ldots, t_{k+n-1}}$$

denotes the sequence infinite sequence t such that $t_i = t_{k+((i-k) \bmod n)}$ for all $i > n$.

4 Appendix D: Equivalence Relations

Definition. Let A be a set. We say that R is a *relation on* A if and only if $R \subseteq A \times A$.

Notation 7. Let R be a relation on A. For any $x, y \in A$, we write

$$x\,R\,y \Leftrightarrow (x, y) \in R \qquad \text{(infix notation)}$$

and

$$R\,(x, y) \Leftrightarrow (x, y) \in R \qquad \text{(prefix notation)}$$

Definition. Let R be a relation on A. Then

1. R is *reflexive* if and only $\forall x \in A, x\,R\,x$
2. R is *symmetric* if and only $\forall x \in A, \forall y \in A, x\,R\,y \Rightarrow y\,R\,x$
3. R is *transitive* if and only $\forall x \in A, \forall y \in A, \forall z \in A, x\,R\,y$ and $y\,R\,z \Rightarrow x\,R\,z$

Definition. Let R be a relation on A. Then R is an *equivalence relation* if and only if R is reflexive, symmetric, and transitive.

Definition. Let R be an equivalence relation on A and $a \in A$. Then the *equivalence class of* a, denoted, $[a]_R$, is the set

$$[a]_R = \{\, x : x\,R\,a \,\} \qquad \text{(equivalence class)}$$

Notation 8. We often abbreviate $[a]_R$ by $[a]$ when the relation R is clear from context.

Theorem (Burning!!)**.** *Let R be an equivalence relation on A and $a, b \in A$. Then*

$$[a] = [b] \Leftrightarrow a\,R\,b.$$

Corollary 9 (1)**.** *Let R be an equivalence relation on A. Then A is a disjoint union of equivalence classes, i.e.,*

$$A = \bigcup_{a \in A} [a]$$

and

$$\forall a, b \in X,\ [a] = [b] \ \text{ or } \ [a] \cap [b] = \emptyset$$

We summarize these definitions along with a few others regarding relations in the following table.

Relations	
Name	Rule
Def of relation	$\sim$ is a relation from A to $B \Leftrightarrow \sim \subseteq A \times B$
Relation on a set	$\sim$ is a relation on $A \Leftrightarrow \sim \subseteq A \times A$
Infix notation	$x \sim y \Leftrightarrow (x, y) \in \sim$
Prefix notation	$\sim (x, y) \Leftrightarrow (x, y) \in \sim$
Reflexive relation[7]	$\sim$ is reflexive $\Leftrightarrow \forall x \in A, x \sim x$
Symmetric relation[7]	$\sim$ is symmetric $\Leftrightarrow \forall x \in A, \forall y \in A, x \sim y \Rightarrow y \sim x$
Transitive relation[7]	$\sim$ is transitive $\Leftrightarrow \forall x \in A, \forall y \in A, \forall z \in A, x \sim y$ and $y \sim z \Rightarrow x \sim z$
Equivalence Relation	$\sim$ is an equivalence relation $\Leftrightarrow$ $\sim$ is reflexive, symmetric, and transitive.
*Equivalence Class**	$\sim$ is an equivalence relation and $a \in A \Rightarrow [a]_{\sim} = \{x \in A : x \sim a\}$

*We often abbreviate $[a]_{\sim}$ by $[a]$ when the relation $\sim$ is clear from context.

5 Appendix C: Math Induction

The Natural Numbers

It is possible to define the Natural Numbers and addition, multiplication, and $<$ for those numbers from scratch. One famous way of doing that was developed by Giuseppe Peano at the end of the 19^{th} century. It defines constants $0, +, \cdot, \sigma$ and $\mathbb{N}$.

Peano Postulates	
Name	Rule
(N0) existence of zero	$0 \in \mathbb{N}$
(N1) existence of successors	$\forall n, \sigma(n) \in \mathbb{N}$
(N2) uniqueness of predecessor	$\forall n, \forall m, \sigma(n) = \sigma(m) \Rightarrow m = n$
(N3) zero is first	$\forall n, 0 \neq \sigma(n)$
(N4) induction	$P(0)$ and $(\forall k, P(k) \Rightarrow P(\sigma(k))) \Rightarrow \forall n, P(n)$
(A0) additive identity	$\forall n, n + 0 = n$
(A1) successor addition	$\forall n, \forall m, m + \sigma(n) = \sigma(m + n)$
(M0) multiplication by zero	$\forall n, n \cdot 0 = 0$
(M1) successor multiplication	$\forall n, \forall m, m \cdot \sigma(n) = m + m \cdot n$
(I) order	$\forall n, \forall m, m \leq n \Leftrightarrow \exists k, m + k = n$

[7]Where $\sim$ is a relation on a set A

In all of the axioms the quantified variables have natural number type, so that in particular we can only apply the $\forall-$ rule for expressions which also are type natural number. In N4 above and in the following, $P(n)$ is a statement about a natural number variable n (i.e., P is a lambda expression that returns a statement when applied to a natural number variable n). Axiom N4 is called *mathematical induction*, or simply *induction*. While not strictly necessary, the following definitions are useful.

Definition (**base ten representation**)**.** We define the usual base ten representations of natural numbers such that $1 = \sigma(0)$, $2 = \sigma(1)$, $3 = \sigma(2)$, $4 = \sigma(3)$,... and so on.

Definition (**less than**)**.** $\forall m, \forall n, m < n \Leftrightarrow m \leq n$ and $m \neq n$.

Theorem. *For all* $n \in \mathbb{N}$,

$$\sigma(n) = n + 1$$

Strong Induction

Theorem (Strong Induction)**.** *Let* $P(n)$ *be any statement about a natural number variable* n*. Then*

$$(P(0) \text{ and } \forall k, (\forall j \leq k, P(j)) \Rightarrow P(\sigma(k))) \Rightarrow \forall n, P(n).$$

Note that for both standard induction and strong induction we can replace the $P(0)$ with $P(a)$ for some $a \in \mathbb{N}$ in which case the resulting conclusion is valid for all $n \geq a$. This gives us the following flavors of induction which can be stated in recipe notation.

Induction

induction	strong induction
$P(0)$ (show) Let $k \in \mathbb{N}$ (variable declaration) Assume $P(k)$ $P(k+1)$ (show) ← ← ..... $\forall n, P(n)$ (conclude)	$P(0)$ (show) Let $k \in \mathbb{N}$ (variable declaration) Assume $\forall j \leq k, P(j)$ $P(k+1)$ (show) ← ← ..... $\forall n, P(n)$ (conclude)
induction from a	**strong induction from** a
$P(a)$ (show) Let $k \geq a$ (variable declaration) Assume $P(k)$ $P(k+1)$ (show) ← ← ..... $\forall n \geq a, P(n)$ (conclude)	$P(a)$ (show) Let $k \geq a$ (variable declaration) Assume $\forall j \in \{a, a+1, \ldots, k\}, P(j)$ $P(k+1)$ (show) ← ← ..... $\forall n, P(n)$ (conclude)

6 Section 1.1: Integers

Theorem (Well Ordering Axiom)**.** *Every nonempty set of natural numbers contains a least element, i.e.*

$$\forall S \subseteq \mathbb{N},\ S \neq \emptyset \Rightarrow \exists m \in S, \forall n \in S, m \leq n.$$

Lemma. *The minimum of a set of natural numbers is unique.*

Notation 10. If S is a nonempty set of natural numbers, we denote its least element by $\min(S)$.

Remark. It can be shown that the following are equivalent: Math Induction, Strong Math Induction, and the Well Ordering Axiom.

Theorem (Division Algorithm for Integers)**.** *Let $a, b \in \mathbb{Z}$,and $b > 0$. Then there exist unique integers $q, r \in \mathbb{Z}$ such that*

$$a = qb + r \text{ and } 0 \leq r < b$$

Definition. In the Division Algorithm Theorem, we call q the **quotient** and r the **remainder** when a is divided by b. In this situation we also define

$$a \operatorname{quo} b = q$$
$$a \bmod b = r$$

Number Theory

Well ordering theorem		def of min	
$S \subseteq \mathbb{N}$	(show)	$S \subseteq \mathbb{N}$	(show)
$S \neq \emptyset$	(show)	$S \neq \emptyset$	
For some $m \in S$,	(constant declaration)	$\min(S) \in S$	(conclude)
$\forall s \in s, m \leq s$	(conclude)	$S \subseteq \mathbb{N}$	(show)
		$s \in S$	(show)
		$\min(S) \leq s$	(conclude)

Division Algorithm (existence)		Division Algorithm (uniqueness)	
$a, b \in \mathbb{Z}$	(show)	$a, b, q, r, s, t \in \mathbb{Z}$	(show)
$b > 0$	(show)	$b > 0$	(show)
For some $q, r \in \mathbb{Z}$,	(constant declaration)	$a = bq + r$ and $0 \leq r < b$	(show)
$a = bq + r$	(conclude)	$a = bs + t$ and $0 \leq t < b$	(show)
$0 \leq r < b$	(conclude)	$q = s$	(conclude)
		$r = t$	(conclude)

7 Section 1.2: Divisibility in $\mathbb{Z}$

Definition (divides)**.** Let $a, b \in \mathbb{Z}$ and $b \neq 0$. Then

$$b \mid a \Leftrightarrow \exists q \in \mathbb{Z}, a = qb$$

Definition (even and odd)**.** Let $a \in \mathbb{Z}$. We say that a is *even* if and only if $2|a$, and we say that a is *odd* if and only if a is not even.

Lemma. *Let $a, b \in \mathbb{Z}$. If $b \mid a$ and $a \neq 0$ then $b \leq |a|$.*

Definition (gcd)**.** Let $a, b, d \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$. Then we say $d = \gcd(a, b)$ if and only if

1. $d > 0$
2. $d \mid a$ and $d \mid b$
3. $\forall c \in \mathbb{Z}$, $c \mid a$ and $c \mid b \Rightarrow c \leq d$

Theorem (Bézout's Lemma)**.** *Let $a, b, d \in \mathbb{Z}$ and $d = \gcd(a, b)$. Then $\exists s, t \in \mathbb{Z}$, $sa + tb = d$ and d is the smallest positive integer of this form.*

Corollary 11 (alt def of gcd)**.** *Let $a, b, d \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$. Then $d = \gcd(a, b)$ if and only if*

1. $d > 0$
2. $d \mid a$ and $d \mid b$
3. $\forall c \in \mathbb{Z}$, $c \mid a$ *and* $c \mid b \Rightarrow c \mid d$

All identifiers in the following recipes have type integer.

Divisibility in $\mathbb{Z}$

divides	
$a, b, q \in \mathbb{Z}$	(show)
$a = qb$	(show)
.....	
$b \mid a$	

divides	
$a, b \in \mathbb{Z}$	(show)
$a \mid b$	(show)
.....	
For some $q \in \mathbb{Z}$,	(constant declaration)
$a = qb$	(conclude)

gcd	
$a, b, d \in \mathbb{Z}$	(show)
$a \neq 0$ or $b \neq 0$	(show)
$d > 0$	(show)
$d \mid a$ and $d \mid b$	(show)
Let $c \in \mathbb{Z}$	(variable declaration)
Assume $c \mid a$ and $c \mid b$	
$c \leq d$	(show)
←	
←	
.....	
$d = \gcd(a, b)$	(conclude)

gcd	
$d = \gcd(a, b)$	(show)
.....	
$a \neq 0$ or $b \neq 0$	(conclude)
$d > 0$	(conclude)
$d \mid a$	(conclude)
$d \mid b$	(conclude)
$d = \gcd(a, b)$	(show)
$c \mid a$	(show)
$c \mid b$	(show)
.....	
$c \leq d$	

Divisibility in $\mathbb{Z}$ (cont.)

alt. gcd	
$a, b, d \in \mathbb{Z}$	(show)
$a \neq 0$ or $b \neq 0$	(show)
$d > 0$	(show)
$d \mid a$ and $d \mid b$	(show)
Let $c \in \mathbb{Z}$	(variable declaration)
Assume $c \mid a$ and $c \mid b$	
$c \mid d$	(show)
←	
←	
.....	
$d = \gcd(a, b)$	(conclude)

alt. gcd	
$d = \gcd(a, b)$	(show)
.....	
$a \neq 0$ or $b \neq 0$	(conclude)
$d > 0$	(conclude)
$d \mid a$	(conclude)
$d \mid b$	(conclude)
$d = \gcd(a, b)$	(show)
$c \mid a$	(show)
$c \mid b$	(show)
.....	
$c \mid d$	(conclude)

8 Section 1.3: Primality in $\mathbb{Z}$

Definition. Let $p \in \mathbb{Z} - \{0, \pm 1\}$. We say that p is *prime* if and only if $\forall c \in \mathbb{Z}, c \mid p \Rightarrow c \in \{\pm 1, \pm p\}$

Definition. Let $p \in \mathbb{Z}$. We say p is *composite* if and only if $p \notin \{0, \pm 1\}$ and p is not prime.

Remark. Notice that the numbers $0, 1, {}^{-}1$ are neither prime nor composite. Hence "composite" does not mean "not prime".

Theorem. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.*

Lemma (mutual divisors)**.** *Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \mid a$ then $a = \pm b$.*

Theorem (alt def of prime)**.** *Let $p \in \mathbb{Z} - \{0, \pm 1\}$. Then*

$$p \text{ is prime } \Leftrightarrow \forall b, c \in \mathbb{Z}, p \mid bc \Rightarrow p \mid b \text{ or } p \mid c$$

Theorem (not prime)**.** *Let $p \in \mathbb{Z} - \{0, \pm 1\}$. Then*

$$p \text{ is not prime } \Leftrightarrow \exists a, b \in \mathbb{Z}, p = ab \text{ and } a, b \notin \{\pm 1, \pm p\}$$

Corollary 12. *Let $p \in \mathbb{N} - \{0, 1\}$.*

$$p \text{ is not prime} \Leftrightarrow \exists a, b \in \mathbb{Z},\ p = ab \text{ and } 1 < a, b < p$$

Theorem. *Every integer except $0, \pm 1$ is a product of primes.*

Note: Here a "product" can have only one factor.

Theorem (Fundamemtal Theorem of Arithmetic)**.** *Every integer n except $0, \pm 1$ can be expressed uniquely as a product of primes in the form*

$$n = \pm 2^{e_1} 3^{e_2} 5^{e_3} 7^{e_4} \cdots p_k^{e_k}$$

where p_i is the i^{th} positive prime and each $e_i \in \mathbb{N}$.

The free variables in the following proof recipes have type integer.

Primality in $\mathbb{Z}$

prime

$p \in \mathbb{Z} - \{0, \pm 1\}$ (show)
  Let $c \in \mathbb{Z}$ (variable declaration)
    Assume $c \mid p$
    $c \in \{\pm 1, \pm p\}$ (show)
    $\leftarrow$
  $\leftarrow$
……
p is prime (conclude)

prime

p is prime (show)
……
$p \notin \{0, \pm 1\}$ (conclude)

p is prime (show)
$c \mid p$ (show)
……
$c \in \{\pm 1, \pm p\}$ (conclude)

alt. def. of prime

$p \in \mathbb{Z} - \{0, \pm 1\}$ (show)
  Let $b, c \in \mathbb{Z}$ (variable declaration)
    Assume $p \mid bc$
    $p \mid b$ or $p \mid c$ (show)
    $\leftarrow$
  $\leftarrow$
……
p is prime (conclude)

alt. def. of prime

$p, b, c \in \mathbb{Z}$ (show)
p is prime (show)
$p \mid bc$
……
$p \mid b$ or $p \mid c$ (conclude)

composite

c is not prime (show)
$c \notin \{0, \pm 1\}$ (show)
……
p is composite (conclude)

composite

p is composite (show)
……
p is not prime (conclude)
$p \notin \{0, \pm 1\}$ (conclude)
For some c with $1 < c < |p|$, (constant declaration)
$c \mid p$ (conclude)

Fund. Thm. of Arithmetic (existence)

$n \in \mathbb{Z} - \{0\}$ (show)
……
For some $e_1, \ldots, e_n \in \mathbb{N}$, (constant declaration)
$n = \pm 2^{e_1} 3^{e_2} 5^{e_3} 7^{e_4} \cdots p_k^{e_k}$ (conclude)
(*where p_i is the i^{th} positive prime*)

Fund. Thm. of Arithmetic (uniqueness)

$n \in \mathbb{Z} - \{0\}$ (show)
$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ (show)
(*where $p_1, \ldots, p_k$ are distinct primes in increasing order)*
$n = \pm q_1^{d_1} q_2^{d_2} \cdots q_m^{d_m}$ (show)
(*where $q_1, \ldots, q_k$ are distinct primes in increasing order*))
……
$k = m$ (conclude)
$p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$ (conclude)
(*and the signs match*)

9 Section 2.1: Congruence in $\mathbb{Z}$

Definition. Let $a, b, n \in \mathbb{Z}$ and $n > 0$.

$$a \underset{n}{\equiv} b \Leftrightarrow n \mid a - b$$

Remark. The textbook writes $a = b \pmod{n}$ for $a \underset{n}{\equiv} b$.

Theorem (1). $\underset{n}{\equiv}$ *is an equivalence relation on* $\mathbb{Z}$.

Definition. Let $n \in \mathbb{N}$ and $n > 1$. Then

$$\mathbb{Z}_n = \{[x] : x \in \mathbb{Z}\}$$

Remark. Note that in the definition of $\mathbb{Z}_n$, $[x]$ is the equivalence class of x with respect to $\underset{n}{\equiv}$.

Corollary 13 (2). *Let* $n \in \mathbb{N}, n > 1$.
a. Let $a \in \mathbb{Z}$. *If* r *is the remainder when* a *is divided by* n *then* $[a] = [r]$ *(and* $a \underset{n}{\equiv} r$*).*
b. $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$ *and the* n *elements are distinct.*

10 Section 2.2: Arithmetic in $\mathbb{Z}_n$

Theorem (1). *Let* $a, b, c, d, n \in \mathbb{Z}$, $n > 1$. *If* $a \underset{n}{\equiv} b$ *and* $c \underset{n}{\equiv} d$ *then*

$$a + c \underset{n}{\equiv} b + d$$

and

$$ac \underset{n}{\equiv} bd$$

Definition. Let X be a set. A **binary operator** on X is a function $f : X \times X \to X$.

Definition. Let $n \in \mathbb{N}^+, n > 0$.

$$\begin{aligned} \oplus &= \{((A, B), C) : \exists a, b \in \mathbb{Z},\ A = [a], B = [b], \text{ and } C = [a + b]\} \\ \otimes &= \{((A, B), C) : \exists a, b \in \mathbb{Z},\ A = [a], B = [b], \text{ and } C = [ab]\} \end{aligned}$$

(where the equivalence classes are with respect to $\underset{n}{\equiv}$.)

Theorem (2). $\oplus, \otimes$ *are binary operators on* $\mathbb{Z}_n$, *i.e.* $\oplus : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ *and* $\otimes : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$.

Remark. This theorem allows us to use infix notation to write the definitions more conveniently in this form:

$$\begin{aligned} [a] \oplus [b] &= [a + b] \\ [a] \otimes [b] &= [ab] \end{aligned}$$

Theorem (3). *For all $A, B, C \in \mathbb{Z}_n$,*
2. $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ *(associativity of $\oplus$)*
3. $A \oplus B = B \oplus A$ *(commutativity of $\oplus$)*
4. $[0] \oplus A = A \oplus [0] = A$ *(identity of $\oplus$)*
5. $\exists X \in \mathbb{Z}_n, A \oplus X = [0]$ *(inverse of $\oplus$)*
7. $A \otimes (B \otimes C) = (A \otimes B) \otimes C$ *(associative of $\otimes$)*
8. $A \otimes (B \oplus C) = (A \otimes B) \oplus (A \otimes C)$ *(distributivity of $\otimes, \oplus$)*
9. $A \otimes B = B \otimes A$ *(commutativity of $\otimes$)*
10. $A \otimes [1] = [1] \otimes A = A$ *(identity of $\otimes$)*

Lemma (mult by 0 in $\mathbb{Z}_n$). *Let $n \in \mathbb{Z}$, $n > 0$. $\forall A \in \mathbb{Z}_n$, $[0] \otimes A = [0]$*

Notation 14. We will often abbreviate $[a]$ as a. We will also often abbreviate $\oplus$ as $+$ and $\otimes$ as $\times, \cdot$, or concatentation.

11 Section 2.3: Algebra in $\mathbb{Z}_n$

Theorem (1). *Let $p \in \mathbb{Z}$ and $p > 1$.T.F.A.E.*
1. p is prime
2. $\forall a \in \mathbb{Z}_p - \{[0]\}, \exists x \in \mathbb{Z}_p, ax = [1]$
3. $\forall a, b \in \mathbb{Z}_p, ab = [0] \Rightarrow a = [0]$ *or* $b = [0]$

Theorem (linear eqns in $\mathbb{Z}_n$). *1. Let p be a positive prime,$a, b \in \mathbb{Z}_p$, and $a \neq [0]$. Then $ax = b$ has a unique solution in $\mathbb{Z}_p$.*
2. Let $a, b, n, d \in \mathbb{Z}$, $n > 1$, and $d = \gcd(a, b)$. Then

$$[a]\, x = [b]$$

i. has d solutions in $\mathbb{Z}_n$ if $d \mid b$ and
ii. has no solutions if $d \nmid b$.

12 Section 3.1: Rings

Definition. A **ring** is a triple $(R, +, \cdot)$ where R is a set and $+, \cdot$ are binary operations on R such that for all $x, y, z \in R$,
1. $x + (y + z) = (x + y) + z$ (associativity of $+$)
2. $x + y = y + x$ (commutativity of $+$)
3. $\exists t \in R, \forall x \in R, t + x = x = x + t$ (identity of $+$)
4. $\exists u \in R, x + u = t$ (inverse of $+$)
5. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (associative of $\cdot$)
6. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ and $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$ (distributivity of $\cdot, +$)

Remark. The t in #4 refers to the t given in #3, so that technically #4 should say:

$$\forall t \in R, (\forall x \in R, t + x = x = x + t) \Rightarrow \forall x \in R, \exists u \in R, x + u = t$$

Lemma (uniq of add ident)**.** *Let* $(R,+,\cdot)$ *be a ring and* $t,u \in R$*. If* $\forall x \in R, t+x = x = x+t$ *and* $u+x = x = x+u$ *then* $t = u$ *(i.e. the additive identity for a ring is unique)*

Notation 15. We write 0_R for the unique additive identity of a ring $(R,+,\cdot)$.

Notation 16. We also usually abbreviate $a \cdot b$ as ab.

Notation 17. We often refer to the ring $(R,+,\cdot)$ as the ring R.

Lemma (uniq of add inv)**.** *Let* $(R,+,\cdot)$ *be a ring and* $u,v,x \in R$*. If* $u+x = 0_R = x+u$ *and* $v+x = 0_R = x+v$ *then* $u = v$ *(i.e. the additive inverse of* x *in a ring is unique)*

Notation 18. We write ^-x for the additive inverse of x in a ring R.

Definition (of subtraction)**.** Let $(R,+,\cdot)$ be a ring and $a,b \in R$. Then $a-b$ is defined to be $a+(^-b)$.

Types of Rings

Definition. A ring $(R,+,\cdot)$ is a **commutative ring** $\Leftrightarrow \forall a,b \in R, ab = ba$.

Definition. A ring $(R,+,\cdot)$ is a **ring with identity** $\Leftrightarrow \exists s \in R, \forall x \in R, sx = x = xs$.

Lemma (uniq of mult ident)**.** *Let* $(R,+,\cdot)$ *be a ring and* $s,u \in R$*. If* $\forall x \in R, sx = x = xs$ *and* $ux = x = xu$ *then* $s = u$ *(i.e. the multiplicative identity for a ring is unique)*

Notation 19. If R is a ring with identity we write 1_R for the unique multiplicative identity of R.

Definition. A ring $(R,+,\cdot)$ is an **integral domain** $\Leftrightarrow$ $(R,+,\cdot)$ is a commutative ring with identity $1_R \neq 0_R$ and $\forall a,b \in R, ab = 0_R \Rightarrow a = 0_R$ or $b = 0_R$.

Definition. A ring $(R,+,\cdot)$ is a **field** $\Leftrightarrow$ $(R,+,\cdot)$ is a commutative ring with identity $1_R \neq 0_R$ and $\forall a \in R - \{0_R\}, \exists x \in R, ax = 1_R$.

Subrings

Definition. Let $(R,+,\cdot)$ be a ring and $S \subseteq R$. S is a **subring** of R if $(S,+,\cdot)$ is a ring (where $+$ and $\cdot$ denote the restrictions of the original $+,\cdot$ to S).

Theorem (subring thm)**.** *Let* $(R,+,\cdot)$ *be a ring and* $S \subseteq R$ *and* $S \neq \emptyset$*. If*
1. $\forall a,b \in S, a-b \in S$
2. $\forall a,b \in S, ab \in S$
then $(S,+.\cdot)$ *is a subring of* $(R,+,\cdot)$*.*

Cartesian Product of Rings

Theorem (Cart Prod of Rings)**.** *Let* R,S *be rings and define*

$$\begin{aligned}(r,s)\oplus(u,v) &= (r+u,s+v)\\ (r,s)\otimes(u,v) &= (ru,sv)\end{aligned}$$

for any $(r,s),(u,v) \in R \times S$*. Then* $(R \times S, \oplus, \otimes)$ *is a ring.*

Remark. In the previous theorem we are using $+, \cdot$ for the addition and subtraction in both rings R, S, but in general they will be different operations.

13 Section 3.2: Algebra in Rings

Theorem (the Algebra Thm I)**.** *Let $(R, +, \cdot)$ be a ring and $a, b, c \in R$. Then*

1. $a + b = a + c \Leftrightarrow b = c$
2. $a + b = c \Leftrightarrow a = c - b$
3. $a + c = c \Leftrightarrow a = 0_R$
4. $a = b \Leftrightarrow a - b = 0_R$

Theorem (the Sign Thm)**.** *Let $(R, +, \cdot)$ be a ring and $a, b \in R$. Then*

1. $a \cdot 0_R = 0_R = 0_R \cdot a$
2. $a\,(^-b) = {}^-(ab) = (^-a)\,b$
3. $^-(^-a) = a$
4. $^-(a + b) = (^-a) + (^-b)$
5. $^-(a - b) = {}^-a + b$
6. $(^-a)\,(^-b) = ab$
7. *If R has identity then* $(^-1_R)\,a = {}^-a$

Corollary 20 (to sign thm)**.** *Let $(R, +, \cdot)$ be a ring and $a, b, c \in R$. If $a \neq 0_R$ and $a = bc$ then $b \neq 0_R$ and $c \neq 0_R$.*

Definition. Let $n \in \mathbb{N}^+$, $(R, +, \cdot)$ a ring, and $a \in R$.

$$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ factors}}$$

and

$$na = \underbrace{a + a + \cdots + a}_{n \text{ summands}}$$

Lemma (1)**.** *Let $(R, +, \cdot)$ be a ring with identity and $a, x, y \in R$.*

$$ax = 1_R \text{ and } ya = 1_R \Rightarrow x = y$$

Corollary 21 (uniq of mult inverse)**.** *Let $(R, +, \cdot)$ be a ring with identity and $a, x, y \in R$.*

$$ax = xa = 1_R \text{ and } ya = ay = 1_R \Rightarrow x = y,$$

i.e. multiplicative inverses are unique.

Definition. Let $(R, +, \cdot)$ be a ring with identity and $a, x \in R$. If $ax = xa = 1_R$ we say x is the **multiplicative inverse of** a and define a^{-1} to be this unique element x.

Definition. Let $(R,+,\cdot)$ be a ring with identity and $a \in R$. If a has a multiplicative inverse then we say a is a **unit** in R.

Definition. Let $(R,+,\cdot)$ be a ring with identity. The set of all units of R is denoted $\mathcal{U}(R)$.

Theorem (the Algebra Thm II)**.** *Let $(R,+,\cdot)$ be a ring with identity and $a,b,x,y \in R$, and $a \in \mathcal{U}(R)$. Then*

1. $ax = b \Leftrightarrow x = a^{-1}b$
2. $ya = b \Leftrightarrow y = ba^{-1}$
3. $a^{-1} \in \mathcal{U}(R)$ *and* $\left(a^{-1}\right)^{-1} = a$

Remark. Remember the BAN ON FRACTIONS! You may not write $\frac{b}{a}$ instead of $a^{-1}b$ or ba^{-1} because in a non-commutative ring these last two expressions might not be equal! So the symbol $\frac{b}{a}$ is **undefined** for elements in an arbitrary ring.

Theorem (the Algebra Thm III)**.** *Let $(R,+,\cdot)$ be an integral domain, $a,b,c \in R$, and $a \neq 0_R$.*

$$ab = ac \Rightarrow b = c.$$

Definition. Let $(R,+,\cdot)$ be a ring and $a \in R$. Then a is called a **zero divisor** of R if and only if

$$a \neq 0 \text{ and } \exists b \in R, b \neq 0_R \text{ and } (ab = 0_R \text{ or } ba = 0_R).$$

Theorem (fields are int doms)**.** *Every field is an integral domain.*

Remark. As usual in mathematics, we will often omit parenthesis for associative operations such as the addition and multiplication in a ring. We also use the precendence of operators with the ring multiplication having a higher precedence than the addition so that e.g. $a + bc$ means $a + (bc)$ and not $(a + b)c$.

14 Section 3.3: Ring Homomorphisms

Definition. Let $(R,+,\cdot),(S,\oplus,\otimes)$ be rings. R is **isomorphic** to $S \Leftrightarrow \exists f : R \to S$ such that

1. $\forall a,b \in R, f(a+b) = f(a) \oplus f(b)$
2. $\forall a,b \in R, f(a \cdot b) = f(a) \otimes f(b)$
3. f is bijective

In such a situation the map f is called an **isomorphism**.

Notation 22. For rings R,S,we write $R \cong S \Leftrightarrow R$ is isomorphic to S.

Lemma (0)**.** *An identity map is a bijection.*

Lemma (1)**.** *The identity map is a ring isomorphism.*

Theorem (2)**.** $\cong$ *is an equivalence relation on any set of rings.*

Definition. Let $(R,+,\cdot),(S,\oplus,\otimes)$ be rings and $f: R \to S$. The map f is a **homomorphism** (or **ring homomorphism**) $\Leftrightarrow$

1. $\forall a,b \in R, f(a+b) = f(a) \oplus f(b)$
2. $\forall a,b \in R, f(a \cdot b) = f(a) \otimes f(b)$

Remark. An isomorphism is a bijective homomorphism.

Remark. Note that in most situations we use $+,\cdot$ for the addition and multiplication (and concatentation for $\cdot$) in both R and S so that requirements #1,#2 in the defintions of isomorphism and homomorphism above would be written:

1. $\forall a,b \in R, f(a+b) = f(a) + f(b)$
2. $\forall a,b \in R, f(ab) = f(a) f(b)$

in this notation.

Lemma (2)**.** *The composition of ring homomorphisms is a ring homomorphism.*

Lemma (3)**.** *The composition of ring isomorphisms is a ring isomorphism.*

Lemma (4)**.** *If f is a ring isomorphism then $f^{-1}$is a ring isomorphism.*

Theorem (Homomorphism Properties)**.** *Let $f: R \to S$ be a ring homomorphism. Let $a,b \in R$.*

1. $f(0_R) = 0_S$
2. $f(^-a) = {}^-f(a)$
3. $f(a-b) = f(a) - f(b)$

   and if R has identity and f is surjective then
4. *S has identity*
5. $f(1_R) = 1_S$
6. *If u is a unit in R then $f(u)$ is a unit in S and $f\left(u^{-1}\right) = f(u)^{-1}$.*

Corollary 23. *Let $f: R \to S$ be a ring homomorphism. Then $f(R)$ is a subring of S.*

15 Section 4.1: Polynomials

Definition. Let $(R,+,\cdot)$ be a ring. A **polynomial with indeterminate x and coefficients in R** is an expression of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $a_0,\ldots,a_n \in R, n \in \mathbb{N}$, and x is a symbol (not a variable). If $a_n \neq 0_R$ then n is called the **degree** of the polynomial and a_n is called the **leading coefficient**. In this situation we write $\deg(P) = n$ (where P is the polynomial) and $\mathrm{LC}(f) = a_n$.

Remark. $\deg(0_R)$ is undefined.

Remark. We can also write our polynomials using summation notation:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i.$$

Remark. Two polynomials are considered equal if they only differ in the order of terms and terms whose coefficient is 0_R. See Appendix G for a formal defintion.

Definition. Let $(R, +, \cdot)$ be a ring. Then

$$R[x] = \{P : P \text{ is a polynomial with indeterminate } x \text{ and coefficients in } R\}.$$

Remark. Notice that we can consider R to be a subset of $R[x]$ by identifying $a \in R$ with the constant polynomial a in $R[x]$.

Definition. Let $(R, +, \cdot)$ be a ring and $P, Q \in R[x]$. Then $P = a_0 + a_1 x + \cdots + a_n x^n$ and $Q = b_0 + b_1 x + \cdots + b_m x^m$ for some $a_0, \ldots, a_n, b_0, \ldots, b_m \in R$. Define $a_k = 0_R$ for $k > n$, $b_k = 0_R$ for $k > m$, and $s = \max(m, n)$. Then

$$\begin{aligned} P \oplus Q &= (a_0 + b_0) + (a_1 + b_1) x + \cdots + (a_s + b_s) x^s \\ P \otimes Q &= (a_0 b_0) + (a_1 b_0 + a_0 b_1) x + \cdots + \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i + \cdots + (a_n b_m) x^{n+m} \end{aligned}$$

Remark. This is just the ordinary addition and multiplication of polynomials, except with the coefficients in an arbitrary ring. We usually write $+, \cdot$ (or concatentation) for $\oplus, \otimes$.

Theorem ($R[x]$ is a ring)**.** *$(R[x], \oplus, \otimes)$ is a ring.*

Lemma (1)**.** *Let $(R, +, \cdot)$ be a ring. Then*

1. $0_{R[x]} = 0_R$
2. $^-(a_0 + a_1 x + \cdots + a_n x^n) = {}^-a_0 + ({}^-a_1) x + \cdots + ({}^-a_n) x^n$
3. *If R has identity then so does $R[x]$ and $1_{R[x]} = 1_R$*
4. *If R is commutative then so is $R[x]$*

Remark. We also write $a_0 - a_1 x - \cdots - a_n x^n$ as another expression for the polynomial $a_0 + ({}^-a_1) x + \cdots + ({}^-a_n) x^n$ (and allow any combination of these two notations).

Remark. The book uses $f(x)$ to denote an arbitrary element of $R[x]$, but this notation can easily be confused with the value of a function f at x, so we will simply write f for an arbitrary polynomial in $R[x]$.

Theorem (additivity of deg)**.** *Let R be a ring and $f, g \in R[x] - \{0_R\}$. If R is an integral domain, then*

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

Corollary 24 (2)**.** *If R is an integral domain then so is $R[x]$.*

Corollary 25 ($F[x]$ is int dom)**.** *If F is a field then $F[x]$ is an integral domain.*

Division Algorithm in $R[x]$

Theorem (Div Alg in $F[x]$)**.** *Let F be a field, $f, g \in F[x]$,and $g \neq 0_{F[x]}$. Then there exist unique polynomials $q, r \in F[x]$ such that*

$$f = qg + r \text{ and } \left(r = 0_{F[x]} \text{ or } \deg(r) < \deg(g)\right).$$

Remark. In the Division Algorithm Theorem for polynomials, we call q the quotient and r the remainder when f is divided by g just as we did in the integer case.

16 Section 4.2: Divisibility in $F[x]$

Definition. Let F be a field and $f, g \in F[x]$ with $f \neq 0_{F[x]}$. Then

$$f \mid g \Leftrightarrow fk = g \text{ for some } k \in F[x].$$

If $f \mid g$ we say f **divides** g.

Lemma (1)**.** *Let F be a field, $f, g \in F[x]$, $f \neq 0_{F[x]}$, and $c \in F - \{0_F\}$. Then*

$$(f \mid g) \Rightarrow (cf \mid g).$$

Lemma (2)**.** *Let F be a field, $f, g \in F[x] - \left\{0_{F[x]}\right\}$. If $f \mid g$ then $\deg(f) \leq \deg(g)$.*

Definition. Let F be a field, $f \in F[x]$. We say f is **monic** if and only if $\mathrm{LC}(f) = 1_F$.

Lemma (3)**.** *Let F be a field, $f \in F[x] - \{0_F\}$, and $c = \mathrm{LC}(f)$. Then $c^{-1} \in F$ and $c^{-1}f$ is monic.*

Definition. Let F be a field, $f, g, d \in F[x]$,and ($f \neq 0_{F[x]}$ or $g \neq 0_{F[x]}$). Then

$$\begin{aligned} d = \gcd(f, g) \Leftrightarrow \quad & (0)\ d \text{ is monic} \\ & (1)\ d \mid f \text{ and } d \mid g \\ & (2)\ \forall c \in F[x], c \mid f \text{ and } c \mid g \Rightarrow \deg(c) \leq \deg(d) \end{aligned}$$

Remark. Technically the symbol $\gcd(a, b)$ is not well defined until we show that there is only one such polynomial in the following theorem. Until then we can say that d is a $\gcd(a, b)$ if it satisfies the three properties listed above.

Theorem (u, v gcd)**.** *Let F be a field, $f, g, d \in F[x]$,($f \neq 0_{F[x]}$ or $g \neq 0_{F[x]}$), and $d = \gcd(f, g)$. Then $\exists u, v \in F[x]$, $au + bv = d$ and d is the unique monic polynomial of smallest degree that is of this form.*

Corollary 26 (alt def of gcd)**.** *Let F be a field, $f, g, d \in F[x]$,and ($f \neq 0_{F[x]}$ or $g \neq 0_{F[x]}$). Then*

$$\begin{aligned} d = \gcd(f, g) \Leftrightarrow \quad & (0)\ d \text{ is monic} \\ & (1)\ d \mid f \text{ and } d \mid g \\ & (2)\ \forall c \in F[x], c \mid f \text{ and } c \mid g \Rightarrow c \mid d \end{aligned}$$

Theorem (4)**.** *Let F be a field, $f, g, h \in F[x]$. If $f \mid gh$ and $\gcd(f, g) = 1_F$ then $f \mid h$.*

Theorem (Euclidean Algorithm II)**.** *Let F be a field, $f, g, q, r \in F[x]$ and $g \neq 0_{F[x]}$. If $f = gq + r$ and ($r = 0_{F[x]}$ or $\deg(r) \leq \deg(g)$) then*

$$\gcd(f, g) = \gcd(g, r)$$

17 Section 4.3: Primality (Irreducible) in $F[x]$

Theorem (units in $R[x]$)**.** *Let $(R,+,\cdot)$ be an integral domain and $f \in R[x]$. Then*

$$\mathcal{U}(R[x]) = \mathcal{U}(R)$$

i.e. the units in $R[x]$ are the constant polynomials u where u is a unit of R.

Corollary 27 (units in $F[x]$)**.** *Let F be a field. The units of $F[x]$ are the nonzero constant polynomials.*

Definition. Let R be a commutative ring with identity and $a, b \in R$. We say a is an **associate** of b in $R \Leftrightarrow a = bu$ for some $u \in \mathcal{U}(R)$. If a is an associate of b we write $a \diamond b$.

Lemma (alt def of $\diamond$)**.** *Let F be a field, $f, g \in F[x] - \left\{0_{F[x]}\right\}$. Then*

$$f \mid g \text{ and } g \mid f \Leftrightarrow f \diamond g$$

Theorem ($\diamond$ is equiv reln)**.** *$\diamond$ is an equivalence relation on R.*

Lemma (1)**.** *Let F be a field and $a, b \in F[x] - \{0_F\}$. If $a \diamond b$ then $\deg(a) = \deg(b)$.*

Definition. Let F be a field and $p \in F[x]$.

$$\begin{aligned} p \text{ is } \textbf{irreducible} \Leftrightarrow \quad & (1)\ p \text{ is non-constant (i.e. } \deg(p) > 0) \\ & (2)\ \forall c \in F[x], c \mid p \Rightarrow c \in \mathcal{U}(F[x]) \text{ or } c \diamond p \end{aligned}$$

Definition. Let F be a field and $p \in F[x]$. We say p is **reducible** if and only if p is non-constant and p is not irreducible.

Remark. The definitions of irreducible and reducible in $F[x]$ correspond to the definitions of prime and composite in $\mathbb{Z}$.

Theorem (alt def of reducible)**.** *Let F be a field and $p \in F[x]$.*

$$\begin{aligned} p \text{ is reducible} \Leftrightarrow \quad & \exists g, h \in F[x], \\ & (1)\ p = gh \\ & (2)\ 0 < \deg(g) < \deg(p) \\ & (3)\ 0 < \deg(h) < \deg(p) \end{aligned}$$

Corollary 28 (linear is irred)**.** *Let F be a field and $p \in F[x]$. If $\deg(p) = 1$ then p is irreducible.*

Theorem (alt def of irreducible)**.** *Let F be a field and $p \in F[x]$. T.F.A.E.*

1. *p is irreducible*
2. *$\forall b, c \in F[x], p \mid bc \Rightarrow p \mid b$ or $p \mid c$*
3. *$\forall r, s \in F[x], p = rs \Rightarrow r \in F - \{0_F\}$ or $s \in F - \{0_F\}$*

Remark. In #3 we are identifying $F - \{0_F\}$ with the nonzero constant polynomials in $F[x]$.

Corollary 29 (2)**.** *Let F be a field, $p, a_1, \ldots, a_n \in F[x]$,and p irreducible.*

$$p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid a_i \text{ for some } i \in \{1, 2, \ldots, n\}.$$

Theorem (Fund Thm of Arith in $F[x]$)**.** *Let F be a field. Every nonconstant polynomial $f \in F[x]$ can be expressed as a product of irreducible polynomials in the form*

$$n = cp_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$$

where $c \in F$, each p_i is a distinct monic irreducible polynomial in $F[x]$, and each $e_i \in \mathbb{N}$. This expression is unique up to reordering of the factors.

18 Section 4.4: Polynomial Functions

Definition. Let R be a commutative ring and $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. Define $\overline{f} : R \to R$ by $\forall r \in R, \overline{f}(r) = a_0 + a_1 r + \cdots + a_n r^n$. The function $\overline{f}$ is called the **polynomial function induced** by f (or the **function associated** with f).

Definition. Let R be a commutative ring, $f \in R[x]$, and $a \in R$.

$$a \text{ is a } \textbf{root} \text{ of } f \Leftrightarrow \overline{f}(a) = 0_R.$$

Theorem (Remainder Thm)**.** *Let F be a field, $f \in F[x]$, and $a \in F$. Then there exists $q \in F[x]$ such that*

$$f = q \cdot (x - a) + \overline{f}(a)$$

i.e. the remainder when f is divided by $x - a$ is $\overline{f}(a)$.

Corollary 30 (to Rem Thm I)**.** *Let F be a field, $f \in F[x]$, and $a \in F$. Then a is a root of f if and only if $(x - a)$ is a factor of f.*

Corollary 31 (to Rem Thm II)**.** *Let F be a field, $f \in F[x]$. If $\deg(f) \geq 2$ and f is irreducible then f has no roots in F.*

Corollary 32 (to Rem Thm III)**.** *Let F be a field, $f \in F[x]$. If $\deg(f) = 2$ or $\deg(f) = 3$ then*

$$f \text{ is irreducible} \Leftrightarrow f \text{ has no roots in } F.$$

Corollary 33 (to Rem Thm IV)**.** *Let F be an infinite field and $f, g \in F[x]$. Then*

$$\overline{f} = \overline{g} \Leftrightarrow f = g.$$

19 Section 5.1: Congruence in $F[x]$

Definition. Let F be a field, $f, g, p \in F[x]$, and $p \neq 0_F$.

$$f \underset{p}{\equiv} g \Leftrightarrow p \mid f - g$$

Remark. The textbook writes $f = g \pmod{p}$ for $f \underset{p}{\equiv} g$.

Theorem (1)**.** $\underset{p}{\equiv}$ *is an equivalence relation on $F[x]$.*

Definition. Let $p \in F[x] - \{0_F\}$. Then

$$F[x]/(p) = \{[f] : f \in F[x]\ \}$$

Remark. Note that in the definition of $F[x]/(p)$, $[f]$ is the equivalence class of x with respect to $\underset{p}{\equiv}$.

Corollary 34 (2). *Let $p \in F[x] - \{0_F\}$, $f \in F[x]$.*
a. If r is the remainder when f is divided by p then $[f] = [r]$ (and $f \underset{p}{\equiv} r$).
b. $F[x]/(p) = \{[0_F]\} \cup \{[f] : f \in F[x]$ and $\deg(f) < \deg(p)\}$ and these elements are distinct.

20 Section 5.2: Arithmetic in $F[x]/(p)$

Theorem (1). *Let F be a field, $f, g, h, i, p \in F[x]$, and $\deg(p) > 0$. If $f \underset{p}{\equiv} h$ and $g \underset{p}{\equiv} i$ then*

$$f + g \underset{p}{\equiv} h + i$$

and

$$fg \underset{p}{\equiv} hi$$

Definition. Let F be a field, $f, q, r, p \in F[x]$, and $\deg(p) > 0$. If $f = pq + r$, and ($r = 0_F$ or $\deg(r) < \deg(p)$) then we define

$$(f \text{ Mod } p) = r.$$

Definition. Let F be a field, $p \in F[x]$, and $\deg(p) > 0$.

$$\begin{aligned} \oplus &= \{((A,B),C) : \exists f, g \in F[x],\ A = [f], B = [g], \text{ and } C = [f+g]\} \\ \otimes &= \{((A,B),C) : \exists f, g \in F[x],\ A = [f], B = [g], \text{ and } C = [fg]\} \end{aligned}$$

(where the equivalence classes are with respect to $\underset{p}{\equiv}$).

Theorem (2). *$\oplus, \otimes$ are binary operators on $F[x]/(p)$.*

Remark. This theorem allows us to use infix notation to write the definitions more conveniently in this form:

$$\begin{aligned} [f] \oplus [g] &= [f+g] \\ [f] \otimes [g] &= [fg] \end{aligned}$$

Theorem (3). *Let F be a field, $p \in F[x]$, and $\deg(p) > 0$. Then $(F[x]/(p), \oplus, \otimes)$ is a commutative ring with identity and $1_{F[x]/(p)} = [1_F]$.*

Notation 35. As in $\mathbb{Z}_n$, we will often abbreviate $[f]$ as f. We will also often abbreviate $\oplus$ as $+$ and $\otimes$ as $\times, \cdot$, or concatentation.

Theorem (4). *Let F be a field, $p \in F[x]$, $\deg(p) > 0$, and define*

$$F^* = \{[c] : c \in F\}.$$

Then F^* is a subring of $F[x]/(p)$ which is isomorphic to F.

Remark. We often identify $c \in F$ with $[c] \in F[x]/(p)$ and simply say that F is a subring of $F[x]/(p)$.

Theorem (units in $F[x]/(p)$)**.** *Let F be a field, $p, f \in F[x]$, $\deg(p) > 0$. Then*

$$f \in \mathcal{U}\left(F[x]/(p)\right) \Leftrightarrow \gcd(f,p) = 1_F$$

21 Section 5.3: Finite fields

Theorem (1)**.** *Let F be a field, $p \in F[x]$, $\deg(p) > 0$. T.F.A.E.*
1. p is irreducible
2. $F[x]/(p)$ is a field
3. $F[x]/(p)$ is an integral domain

Definition. Let F be a field, $p, f \in F[x]$, $\deg(p) > 0$, $a_0, \ldots, a_n \in F$, and $f = a_0 + a_1 x + \cdots + a_n x^n$. Define $\overline{f} : F[x]/(p) \to F[x]/(p)$ by

$$\forall r \in F[x]/(p), \overline{f}(r) = [a_0] + [a_1] r + \cdots + [a_n] r^n$$

Remark. If we identify F with $F^* \subseteq F[x]/(p)$, then this function $\overline{f}$ is just an extension of our original function $\overline{f}$ from F to $F[x]/(p)$.

Theorem (2)**.** *Let F be a field, $p \in F[x]$, and p irreducible. Then $F[x]/(p)$ is an extension field of F which contains a root of p.*

Corollary 36 (3)**.** *Let F be a field, $f \in F[x]$, and $\deg(p) > 0$. There exists an extension field K of F containing a root of f.*

22 Section 6.1: Congruence in Rings

Definition. Let R be a ring and $I \subseteq R$.

$$I \text{ is an } \textbf{ideal} \Leftrightarrow \begin{array}{l} (1)\ I \text{ is a subring of } R \\ (2)\ \forall r \in R, \forall a \in I, ra \in I \text{ and } ar \in I \end{array}$$

Theorem (1)**.** *Let R be a commutative ring with identity and $c_1, \ldots, c_n \in R$. The set*

$$I = \{c_1 r_1 + c_2 r_2 + \cdots + c_n r_n : r_1, \ldots, r_n \in R\}$$

is an ideal of R.

Definition. The ideal I in the previous theorem is called the **ideal generated by** $\{c_1, \ldots, c_n\}$. If $n = 1$then I is called a **principal ideal**. Since $\{c_1, \ldots, c_n\}$ is a finite set, we say that I is **finitely generated**.

Definition. Let R be a ring, $a, b \in R$, and I an ideal of R.

$$a \underset{I}{\equiv} b \Leftrightarrow a - b \in I$$

Remark. The textbook writes $a = b \pmod{I}$ for $a \underset{I}{\equiv} b$.

Theorem (2). *$\underset{I}{\equiv}$ is an equivalence relation on R.*

Definition. Let R be a ring and I and ideal of R. Then

$$R/I = \{[r] : r \in R\}$$

Remark. Note that in the definition of R/I, $[r]$ is the equivalence class of x with respect to $\underset{I}{\equiv}$.

Theorem (3). *Let R be a ring, $a \in R$, and I an ideal of R. Then*

$$[a] = \{a + i : i \in I\}$$

Definition. Let R be a ring, $a \in R$, and I an ideal of R. The set

$$a + I = \{a + i : i \in I\} = [a]$$

is called the **left coset of** $a \bmod I$. The notation $a + I$ is called **coset notation** for the equivalence class $[a]$.

Remark. I hate coset notation.

23 Section 6.2: Arithmetic in R/I

Theorem (1). *Let R be a ring, $a, b, c, d \in R$, and I an ideal of R. If $a \underset{I}{\equiv} b$ and $c \underset{I}{\equiv} d$ then*

$$a + c \underset{I}{\equiv} b + d$$

and

$$ac \underset{I}{\equiv} bd$$

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

$$\begin{aligned} \oplus &= \{((A, B), C) : \exists a, b \in R,\ A = [a], B = [b], \text{ and } C = [a + b]\} \\ \otimes &= \{((A, B), C) : \exists a, b \in R,\ A = [a], B = [b], \text{ and } C = [ab]\} \end{aligned}$$

(where the equivalence classes are with respect to $\underset{I}{\equiv}$).

Theorem (2). *$\oplus, \otimes$ are binary operators on R/I.*

Remark. This theorem allows us to use infix notation to write the definitions more conveniently in this form:

$$\begin{aligned} [a] \oplus [b] &= [a + b] \\ [a] \otimes [b] &= [ab] \end{aligned}$$

or equivalently in left coset notation:

$$\begin{aligned} (a + I) \oplus (b + I) &= (a + b) + I \\ (a + I) \otimes (b + I) &= ab + I \end{aligned}$$

Theorem (3)**.** *Let R be a ring and I an ideal of R. Then $(R/I, \oplus, \otimes)$ is a ring.*

Definition. Let R be a ring and I an ideal of R. Then $(R/I, \oplus, \otimes)$ is calles a **quotient ring**.

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

1. *If R is commutative then so is R/I.*
2. *If R has identity then so does R/I and $1_{R/I} = [1_R]$.*

Notation 37. As in $\mathbb{Z}_n$, and $F[x]/(p)$ we will often abbreviate $[a]$ as a. We will also often abbreviate $\oplus$ as $+$ and $\otimes$ as $\times, \cdot$, or concatentation.

Homomorphisms and Quotient Rings

Definition. Let $f: R \to S$ be a ring homomorphism. The **kernel** of f is the set

$$\text{Ker}(f) = \{x \in R : f(x) = 0_S\}$$

Theorem (Ker is an ideal)**.** *Let $f: R \to S$ be a ring homomorphism.* $\text{Ker}(f)$ *is an ideal of R.*

Theorem (inj vs Ker)**.** *Let $f: R \to S$ be a ring homomorphism.*

$$f \text{ is injective} \Leftrightarrow \text{Ker}(f) = \{0_R\}$$

Definition. Let R be a ring, I an ideal of R, and define $f: R \to R/I$ by $\forall r \in R, f(r) = [r]$. The map f is called the **quotient map** (or **natural homomorphism**)

Theorem (quo maps are surj homo)**.** *A quotient map is a surjective ring homomorphism.*

Theorem (First Isomorphism Thm)**.** *Let $f: R \to S$ be a surjective ring homomorphism. Then*

$$S \cong R/Ker(f)$$

24 Section 7.1: Groups

Definition. Let G be a set and $* : G \times G \to G$ a binary operator.

$$(G, *) \text{ is a } \textbf{group} \Leftrightarrow \begin{array}{ll} 1.\ \forall a, b, c \in G, a * (b * c) = (a * b) * c & \text{(associative)} \\ 2.\ \exists e \in G, \forall a \in G, a * e = a = e * a & \text{(identity)} \\ 3.\ \forall a \in G, \exists d \in G, a * d = e = d * a & \text{(inverses)} \end{array}$$

Remark. We will often abbreviate abbreviate $a * b$ by ab. We will also often refer to the group $(G, *)$ as simply G.

Types of Groups

Definition. A group $(G, *)$ is **abelian** $\Leftrightarrow \forall a, b \in G, a * b = b * a$

Definition. A group $(G, *)$ is **finite** $\Leftrightarrow G$ is a finite set.

Definition. If S is a finite set, the $\#(S)$ denotes the number of elements in the finite set S.

Remark. The book writes $|S|$ for the number of elements in S, but I will use $\#(S)$.

Definition. If $(G, *)$ is a finite group then $\#(G)$ is called the **order** of the group.

Examples of Groups

Theorem (1). *Let $(R, +, \cdot)$ be a ring. Then $(R, +)$ is a group.*

Theorem (2). *Let $(R, +, \cdot)$ be a ring with identity. Then $(\mathcal{U}(R), \cdot)$ is a group.*

Theorem (3). *Let $(F, +, \cdot)$ be a field. Then $(F - \{0_F\}, \cdot)$ is a group.*

Definition. Let T be a set. A **permutation** of T is a bijection $f: T \to T$.

Definition. Let $n \in \mathbb{N}$.Define $\mathbb{I}_n = \{1, 2, \ldots, n\}$.

Definition. Let $n \in \mathbb{N}^+$. Then

$$S_n = \{\alpha : \alpha \text{ is a permutation of } \mathbb{I}_n\}$$

i.e. S_n is the set of all permutations of $\mathbb{I}_n$.

Theorem (4). $(S_n, \circ)$ *is a group.*

Notation 38. $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \Leftrightarrow \forall i \in \mathbb{I}_n,\ f(i) = a_i.$

Theorem (5). $\#(S_n) = n!$

Definition. Let $X \subseteq \mathbb{R}^n$. A **symmetry operation** of X is a bijection $f: X \to X$ which preserves the distances between points, i.e. $\forall a, b \in X, d(a, b) = d(f(a), f(b))$.

Definition. Let $X \subseteq \mathbb{R}^n$. Then

$$\text{Sym}(X) = \{\alpha : \alpha \text{ is a symmetry operation of } X\}$$

i.e. $\text{Sym}(X)$ is the set of all symmetry operations of X.

Theorem (6). $(\text{Sym}(X), \circ)$ *is a group.*

Definition. Let P_n be a regular n-gon in $\mathbb{R}^2$. Then

$$D_n = \text{Sym}(P_n)$$

D_n is called a **dihedral group**.

Theorem (Direct Product)**.** *Let* $(G,*)$ *and* $(H,\cdot)$ *be groups and define* $\otimes : (G\times H)\times(G\times H) \to G\times H$ *by*

$$(a,b)\otimes(c,d) = (a*c, b\cdot d)$$

for all $(a,b),(c,d) \in G\times H$*. Then* $(G\times H,\otimes)$ *is a group.*

Definition. $(G\times H,\otimes)$ is called the **direct product** of the groups G and H.

25 Section 7.2: Properties of Groups

Theorem (1)**.** *Let* $(G,*)$ *be a group.*

1. *G has a unique identity element*
2. *Every element of G has a unique inverse*
3. $\forall a,b,c \in G, ab = ac \Rightarrow b = c$
4. $\forall a,b,c \in G, ba = ca \Rightarrow b = c$

Definition. Let $(G,*)$ be a group. Then e_G denotes the unique identity element of G.

Definition. Let $(G,*)$ be a group and $a \in G$.Then a^{-1}denotes the unique inverse of a.

Theorem (Inverse Thm)**.** *Let* $(G,*)$ *be a group and* $a,b \in G$*.*

1. $\left(a^{-1}\right)^{-1} = a$
2. $(ab)^{-1} = b^{-1}a^{-1}$
3. $e_G^{-1} = e_G$

Definition. Let $(G,*)$ be a group, $a \in G$, and $n \in \mathbb{N}^+$. Then

$$a^n = \underbrace{a\cdot a\cdot\cdots\cdot a}_{n \text{ factors}}$$

and

$$a^{-n} = \underbrace{a^{-1}\cdot a^{-1}\cdot\cdots\cdot a^{-1}}_{n \text{ factors}}$$

and

$$a^0 = e_G$$

Theorem (power thm)**.** *Let* $(G,*)$ *be a group,* $a \in G$*, and* $n,m \in \mathbb{Z}$*. Then*

$$a^n a^m = a^{n+m}$$

and

$$(a^n)^m = a^{nm}$$

Remark. Note that $(ab)^n$ is not always equal to $a^n b^n$ in a group.

Notation 39 (Addititive notation). For abelian groups we sometimes write $*$ as $+$ and a^n as na and a^{-1} as ^-a.

Definition. Let $(G,*)$ be a group, $k \in \mathbb{N}^+$, and $a \in G$.

$$a \text{ has } \textbf{order } k \Leftrightarrow a^k = e_G \text{ and } \left(\forall j \in \mathbb{N}^+, a^j = e_G \Rightarrow j \geq k\right)$$

If a has order k for some $k \in \mathbb{N}^+$ we say a has **finite order**, otherwise we say a has **infinite order**. If a has finite order we define $|a|$ to be the order of a.

Theorem (order thm)**.** *Let $(G,*)$ be a group, $a \in G$, and $k, j, n \in \mathbb{N}^+$.*

1. *If a has infinite order then $a^k = a^j \Rightarrow k = j$*
2. *If $|a| = n$ and $a^k = e_G \Rightarrow n \mid k$*
3. *If $|a| = n$ and $a^k = a^j \Leftrightarrow k \underset{n}{\equiv} j$*
4. *If $|a| = n$ and $n = td$ for some $t \in \mathbb{Z}, d \in \mathbb{N}^+$ then $\left|a^t\right| = d$*

Corollary 40 (to order thm)**.** *Every element of a finite group has finite order.*

26 Section 7.3: SubGroups

Definition. Let $(G,*)$ be a group and $H \subseteq G$. Then $(H,*)$ is a **subgroup** of $(G,*)$ if and only if $(H,*)$ is a group (where $*$ denotes the restriction of the original $*$ to H).

Definition. Let $(H,*)$ be a subgroup of $(G,*)$. Then $(H,*)$ is a **proper subgroup** of $(G,*)$ if and only if $H \neq G$ and $H \neq \{e_G\}$.

Notation 41. We sometimes write "$H \sqsubseteq G$" as a shorthand for "H is a subgroup of G".

Theorem (subgroup thm)**.** *Let $(G,*)$ be a group, $H \subseteq G$, and $H \neq \emptyset$.*

$$(H,*) \text{ is a subgroup} \Leftrightarrow \begin{array}{ll} 1. & \forall a, b \in H, ab \in H \\ 2. & \forall a \in H, a^{-1} \in H \end{array}$$

Theorem (subgroup thm II)**.** *Let $(G,*)$ be a group and $H \subseteq G$ a finite nonempty set.*

$$(H,*) \text{ is a subgroup } \Leftrightarrow \forall a, b \in H, ab \in H$$

Lemma (subgroup identity)**.** *Let $H \sqsubseteq G$. Then $e_G \in H$ and $e_H = e_G$.*

Definition. Let $(G,*)$ be a group. The **center** of G is the set

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

Theorem (center is subg)**.** *The center of a group is a subgroup of the group.*

Cyclic groups

Definition. Let $(G,*)$ be a group, $a \in G$. Define

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

The set $\langle a \rangle$ is called the **cyclic subgroup generated by** a.

Theorem ($\langle a \rangle$ is abel group)**.** *Let $(G,*)$ be a group, $a \in G$. Then $(\langle a \rangle, *)$ is an abelian subgroup of G.*

Theorem (elts of $\langle a \rangle$)**.** *Let $(G,*)$ be a group, $a \in G$.*

1. *If $|a| = n$ for some $n \in \mathbb{N}$ then $\langle a \rangle = \left\{e_G, a, a^2, a^3, \ldots, a^{n-1}\right\}$*
2. *If $|a| = \infty$ then $\langle a \rangle = \left\{\ldots, a^{-3}, a^{-2}, a^{-1}, e_G, a, a^2, a^3 \ldots\right\}$*

and in both cases the elements listed are distinct.

Theorem (1)**.** *Any subgroup of the group of units of a finite field is cyclic.*

Theorem (2)**.** *Every subgroup of a cyclic group is cyclic.*

Definition. Let $S \subseteq G$ and $(G,*)$ a group. The **subgroup generated by** S is the smallest subgroup of G which contains S and is denoted by $\langle S \rangle$.

Theorem (3)**.** *Let $S \subseteq G$ and $(G,*)$ a group. Then $\langle S \rangle$ is the set of all products of elements of S and their inverses.*

27 Section 7.4: Group Homomorphisms

Definition. Let $(G,*), (H,\cdot)$ be groups and $f: G \to H$. The map f is a **homomorphism** (or **group homomorphism**) $\Leftrightarrow \forall a, b \in G, f(a*b) = f(a) \cdot f(b)$. If a group homomorphism is bijective it is called an **isomorphism** (or **group isomorphism**). If there exists an isomorphism mapping G to H we say the groups G and H are **isomorphic groups** and write $G \cong H$.

Theorem (1)**.** *Every infinite cyclic group is isomorphic to $(\mathbb{Z},+)$. Every finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n,+)$.*

Theorem (props of group homo)**.** *Let $(G,*), (H,\cdot)$ be groups, $f: G \to H$ a group homomorphism, and $a \in G$. Then*

1. $f(e_G) = e_H$
2. $f\left(a^{-1}\right) = f(a)^{-1}$
3. *$f(G)$ is a subgroup of H*
4. *If f is injective then $G \cong f(G)$*

Theorem (Caley's Thm)**.** *Every group is isomorphic to a group of permutations.*

Corollary 42 (2)**.** *Every group of order n is isomorphic to a subgroup of S_n.*

28 Section 7.5: Symmetric and Alternating Groups

Definition. Let $k, n \in \mathbb{N}^+$, $a_1, \ldots, a_k \in \mathbb{I}_n$. Define

$$p = (a_1 a_2 \ldots a_k) \Leftrightarrow p \in S_n \text{ and } \forall x \in \mathbb{I}_n, p(x) = \begin{cases} a_{i+1} & \text{if } x = a_i \text{ and } i < k \\ a_1 & \text{if } x = a_k \\ x & \text{otherwise} \end{cases}$$

The permutation $(a_1 a_2 \ldots a_k)$ is called a **k-cycle**.

Definition. Two cycles $(a_1 a_2 \ldots a_k), (b_1 b_2 \ldots b_m) \in S_n$ are **disjoint** if and only if $\{a_1, \ldots, a_n\} \cap \{b_1, \ldots, b_n\} = \emptyset$.

Theorem (disj cycles commute)**.** *If $\sigma, \tau \in S_n$ are disjoint cycles then $\sigma\tau = \tau\sigma$.*

Theorem (disj factorization)**.** *Every element of S_n is a product of disjoint cycles.*

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

Corollary 43 (1)**.** *Every element of S_n is a product of transpositions.*

Theorem (even and odd in S_n)**.** *No element of $S_n$is both a product of an even number of transpositions and also a product of an odd number of transpositions.*

Definition. Let $\sigma \in S_n$. σ is **even** if it can be written as a product of an even number of transpositions. σ is odd if it is not **even**.

Definition. Let $n \in \mathbb{N}^+$. Define $A_n = \{\sigma \in S_n : \sigma \text{ is even}\}$. A_n is called the **alternating groups** on n-letters.

Theorem (1)**.** *$A_n \lhd S_n$ and if $n \geq 2$ then $\#(A_n) = \frac{n!}{2}$.*

29 Appendix I: Some Useful Proof Recipes

Using the shortcuts that are allowed for semi-formal proofs, we can usually produce several different derived rules of inference from a given definition. Here are some of the more useful ones we will need frequently in our course.

Proof Recipes - Set Theory

empty set	empty set
.....	$A \neq \{\}$ (SHOW)
$x \notin \{\}$ (CONCLUDE)	.....
	For some c, (constant declaration)
	$c \in A$ (CONCLUDE)
finite set notation	finite set notation
.....	$x \in \{x_1, \ldots, x_n\}$ (SHOW)
$x_1 \in \{x_1, \ldots, x_n\}$ (CONCLUDE)	.....
$x_2 \in \{x_1, \ldots, x_n\}$ (CONCLUDE)	$x = x_1$ or $\cdots$ or $x = x_n$ (CONCLUDE)
$\vdots$	
$x_n \in \{x_1, \ldots, x_n\}$ (CONCLUDE)	
set builder notation	set builder notation
$\varphi(x)$ (SHOW)	$x \in \{y : \varphi(y)\}$ (SHOW)
.....	.....
$x \in \{y : \varphi(y)\}$ (CONCLUDE)	$\varphi(x)$ (CONCLUDE)
subset	subset
Let $x \in A$ (variable declaration)	$A \subseteq B$ (SHOW)
$x \in B$ (SHOW)	$x \in A$ (SHOW)
$\leftarrow$	.....
.....	$x \in B$ (CONCLUDE)
$A \subseteq B$ (CONCLUDE)	
set equality	set equality
Let $x \in A$ (variable declaration)	$A = B$ (SHOW)
$x \in B$ (SHOW)	.....
$\leftarrow$	$A \subseteq B$ (CONCLUDE)
Let $y \in B$ (variable declaration)	$B \subseteq A$ (CONCLUDE)
$y \in A$ (SHOW)	
$\leftarrow$	
.....	
$A = B$ (CONCLUDE)	
power set	power set
$B \subseteq A$ (SHOW)	$B \in \mathcal{P}(A)$ (SHOW)
.....	.....
$B \in \mathcal{P}(A)$ (CONCLUDE)	$B \subseteq A$ (CONCLUDE)

Proof Recipes - Set Theory (cont.)

intersection	intersection
$x \in A$ (SHOW) $x \in B$ (SHOW) ..... $x \in A \cap B$ (CONCLUDE)	$x \in A \cap B$ (SHOW) ..... $x \in A$ (CONCLUDE) $x \in B$ (CONCLUDE)
union	**union**
$x \in A$ or $x \in B$ (SHOW) ..... $x \in A \cup B$ (CONCLUDE)	$x \in A \cup B$ (SHOW) ..... $x \in A$ or $x \in B$ (CONCLUDE)
set difference	**set difference**
$x \in A$ (SHOW) $x \notin B$ (SHOW) ..... $x \in A - B$ (CONCLUDE)	$x \in A - B$ (SHOW) ..... $x \in A$ (CONCLUDE) $x \notin B$ (CONCLUDE)
complement	**complement**
$x \notin A$ (SHOW) ..... $x \in A'$ (CONCLUDE)	$x \in A'$ (SHOW) ..... $x \notin A$ (CONCLUDE)
indexed intersection	**indexed intersection**
Let $i \in I$ (variable declaration) $x \in A_i$ (SHOW) $\leftarrow$ ..... $x \in \bigcap_{i \in I} A_i$ (CONCLUDE)	$x \in \bigcap_{i \in I} A_i$ (SHOW) $i \in I$ (SHOW) ..... $x \in A_i$ (CONCLUDE)
indexed union	**indexed union**
$\exists i \in I, x \in A_i$ (SHOW) ..... $x \in \bigcup_{i \in I} A_i$ (CONCLUDE)	$x \in \bigcup_{i \in I} A_i$ (SHOW) ..... For some $j \in I$, (constant declaration) $x \in A_j$ (CONCLUDE)
typed forall	**typed forall**
Let $x \in A$ (variable declaration) $\varphi(x)$ (SHOW) $\leftarrow$ ..... $\forall x \in A, \varphi(x)$ (CONCLUDE)	$\forall x \in A, \varphi(x)$ (SHOW) $a \in A$ (SHOW) ..... $\varphi(a)$ (CONCLUDE)

Proof Recipes - Set Theory (cont.)

typed exists

$a \in A$ (show)
$\varphi(a)$ (show)

$\exists x \in A, \varphi(x)$ (conclude)

typed exists

$\exists x \in A, \varphi(x)$ (show)

For some $c \in A$, (constant declaration)
$\varphi(c)$ (conclude)

partition

Let $S \in P$
$S \subseteq A$ (show)
←
Let $S, T \in P$
Assume $S \neq T$
$S \cap T = \{\}$ (show)
←
←
Let $x \in A$
For some $S \in P$,
$x \in S$ (show)
←

P is a partition of A (conclude)

partition

P is a partition of A (show)
$S \in P$ (show)

$S \subseteq A$ (conclude)

P is a partition of A (show)
$S, T \in P$ (show)
$S \neq T$ (show)

$S \cap T = \{\}$ (conclude)

P is a partition of A (show)
$x \in A$ (show)

For some $S \in P$, (constant declaration)
$x \in S$ (conclude)

Proof Recipes - Cartesian Product

ordered pair

$x = u$ (show)
$y = v$ (show)

$(x, y) = (u, v)$ (conclude)

ordered pair

$(x, y) = (u, v)$ (show)

$x = u$ (conclude)
$y = v$ (conclude)

ordered n-tuple

$x_1 = y_1$ (show)
⋮
$x_n = y_n$ (show)

$(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ (conclude)

ordered n-tuple

$(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ (show)

$x_1 = y_1$ (conclude)
⋮
$x_n = y_n$ (conclude)

Cartesian product

$x \in A$ (show)
$y \in B$ (show)

$(x, y) \in A \times B$ (conclude)

Cartesian product

$z \in A \times B$ (show)

For some $x \in A, y \in B$, (constant declaration)
$z = (x, y)$ (conclude)

Proof Recipes - Cartesian Product (cont.)

Cartesian product

$x_1 \in A_1$ (show)
$\vdots$
$x_n \in A_n$ (show)

$(x_1, \ldots, x_n) \in A_1 \times \cdots \times A_n$ (conclude)

Cartesian product

$z \in A_1 \times \cdots \times A_n$ (show)

For some $x_1 \in A_1, \ldots, x_n \in A_n$, (constant decl.)
$z = (x_1, \ldots, x_n)$ (conclude)

Power of a set

$A^n = \underbrace{A \times \cdots \times A}_{n \text{ copies}}$ (conclude)

Proof Recipes - Functions

formal def of function

$f \subseteq A \times B$ (show)
  Let $x \in A$
  $\exists! y \in B, (x, y) \in f$ (show)
  $\leftarrow$

$f : A \to B$ (conclude)

formal def of function

$f : A \to B$ (show)
$x \in A$ (show)

$f \subseteq A \times B$ (conclude)
$\exists! y \in B, (x, y) \in f$ (conclude)

function application

$f : A \to B$ (show)
$x \in A$ (show)

$f(x) \in B$ (conclude)

function application

$f : A \to B$ (show)
$(x, y) \in f$ (show)

$y = f(x)$ (conclude)

function equality

$f : A \to B$ (show)
$g : A \to B$ (show)
  Let $x \in A$ (variable declaration)
  $f(x) = g(x)$ (show)
  $\leftarrow$

$f = g$ (conclude)

identity map

$x \in A$ (show)

$\mathrm{id}_A(x) = x$

Proof Recipes - Functions (cont.)

image	image
$f: A \to B$ (show) $S \subseteq A$ (show) $x \in S$ (show) ..... $f(x) \in f(S)$	$f: A \to B$ (show) $S \subseteq A$ (show) $y \in f(S)$ (show) ..... For some $x \in S$, (constant declaration) $y = f(x)$ (conclude)

composition	composition
$f: A \to B$ (show) $g: B \to C$ (show) ..... $(g \circ f) : A \to C$ (conclude)	$f: A \to B$ (show) $g: B \to C$ (show) $x \in A$ (show) ..... $(g \circ f)(x) = g(f(x))$ (conclude)

injective	injective
$f: A \to B$ (show) Let $x, y \in A$ (variable declaration) Assume $f(x) = f(y)$ $x = y$ (show) $\leftarrow$ $\leftarrow$ ..... f is injective (conclude)	$f: A \to B$ (show) f is injective (show) $f(x) = f(y)$ (show) ..... $x = y$ (conclude)

surjective	surjective
$f: A \to B$ (show) Let $b \in B$ (variable declaration) $\exists a \in A, f(a) = b$ (show) $\leftarrow$ ..... f is surjective (conclude)	$f: A \to B$ (show) f is surjective (show) $b \in B$ (show) ..... For some $a \in A$, (constant declaration) $b = f(a)$ (conclude)

bijective	bijective
f is surjective (show) f is injective (show) ..... f is bijective (conclude)	f is bijective (show) ..... f is surjective (conclude) f is injective (conclude)

Proof Recipes - Functions (cont.)

inverse function	
$f: A \to B$	(show)
f is bijective	(show)
.....	
$f^{-1}: B \to A$	(conclude)
$f^{-1} \circ f = \mathrm{id}_A$	(conclude)
$f \circ f^{-1} = \mathrm{id}_B$	(conclude)

inverse function	
$f^{-1}: B \to A$	(show)
.....	
$f: A \to B$	(conclude)
f is bijective	(conclude)
$f^{-1} \circ f = \mathrm{id}_A$	(conclude)
$f \circ f^{-1} = \mathrm{id}_B$	(conclude)

inverse function	
$f^{-1}: B \to A$	(show)
$y = f(x)$	(show)
.....	
$x = f^{-1}(y)$	(conclude)

inverse function	
$f^{-1}: B \to A$	(show)
$x = f^{-1}(y)$	(show)
.....	
$y = f(x)$	(conclude)

inverse image	
$f: A \to B$	(show)
$T \subseteq B$	(show)
$f(x) \in T$	(show)
.....	
$x \in f^{\mathrm{inv}}(T)$	

inverse image	
$f: A \to B$	(show)
$T \subseteq B$	(show)
$x \in f^{\mathrm{inv}}(T)$	(show)
.....	
$f(x) \in T$	(conclude)

In the following recipes, let A be a set and $\sim$ a relation on A.

Proof Recipes - Equivalence Relations

reflexive	
Let $x \in A$	(variable declaration)
$x \sim x$	(show)
$\leftarrow$	
.....	
$\sim$ is reflexive	(conclude)

reflexive	
$\sim$ is reflexive	(show)
$x \in A$	(show)
.....	
$x \sim x$	(conclude)

symmetric	
Let $x, y \in A$	(variable declaration)
Assume $x \sim y$	
$y \sim x$	(show)
$\leftarrow$	
$\leftarrow$	
.....	
$\sim$ is symmetric	(conclude)

symmetric	
$\sim$ is symmetric	(show)
$x \sim y$	(show)
.....	
$y \sim x$	(conclude)

Proof Recipes - Equivalence Relations (cont.)

transitive	transitive

Let $x, y, z \in A$ (variable declaration)
  Assume $x \sim y$ and $y \sim z$
  $x \sim z$ (show)
  $\leftarrow$
$\leftarrow$
$\sim$ is symmetric (conclude)
	$\sim$ is transitive (show)
	$x \sim y$ (show)
	$y \sim z$ (show)
	$x \sim z$ (conclude)

equivalence relation	equivalence relation

Let $x, y, z \in A$ (variable declaration)
$x \sim x$ (show)
  Assume $x \sim y$
  $y \sim x$ (show)
  $\leftarrow$
  Assume $x \sim y$ and $y \sim z$
  $x \sim z$ (show)
  $\leftarrow$
$\leftarrow$
$\sim$ is an equivalence relation (conclude)
	$\sim$ is an equivalence relation (show)
	$\sim$ is reflexive (conclude)
	$\sim$ is transitive (conclude)
	$\sim$ is symmetric (conclude)

equivalence class	equivalence class
$x \sim y$ (show) $x \in [y]$ (conclude)	$x \in [y]$ (show) $x \sim y$ (conclude)

Burning theorem	Burning theorem
$x \sim y$ (show) $[x] = [y]$ (conclude)	$[x] = [y]$ (show) $x \sim y$ (conclude)