Modern Algebra Lecture Notes

Dr. Monks - University of Scranton - Fall 2021

Contents

0 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.

0.1 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* or *recipe notation* as

Rule Name Here	
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

Proof by Cases	
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 ← (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 ¬, 'if and only if' for ⇔, and 'implies' for ⇒. 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)*	$(\text{not}\, \varphi \vdash \ \rightarrow\leftarrow) \vdash \varphi$
$\rightarrow\leftarrow +$	$\varphi, (\text{not}\, \varphi) \vdash \ \rightarrow\leftarrow$

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)
⇒ +	**⇒ − (modus ponens)**
Assume φ ψ (show) ← ..... $\varphi \Rightarrow \psi$ (conclude)	φ (show) $\varphi \Rightarrow \psi$ (show) ..... ψ (conclude)
⇔ +	**⇔ −**
$\varphi \Rightarrow \psi$ (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 →← (show) ← ..... $\neg\varphi$ (conclude)	Assume $\neg\varphi$ →← (show) ← ..... φ (conclude)
→← +	**copy**
φ (show) $\neg\varphi$ (show) ..... →← (conclude)	φ (show) ..... φ (conclude)

Remarks:

- The symbol ← is an abbreviation for "end assumption".
- The symbol →← 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 "←" 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-← 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 ←, 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-← 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).
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
$\forall+$	$(\text{Let } s \text{ be arbitrary} \vdash \varphi(s)) \vdash (\forall x, \varphi(x))$
$\forall-$	$(\forall x, \varphi(x)) \vdash \varphi(t)$

[5] Not containing x.

Rules of Inference for Predicate Logic (cont.)

Name	Rule
$\exists+$	$\varphi(t) \vdash (\exists x, \varphi(x))$
$\exists-$	$(\exists x, \varphi(x)) \vdash$ 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*
$x = x$	$x = y$ (SHOW) 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 $\neg(x = y)$

0.2 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	Definition
Empty set	$\forall x, x \notin \{\,\}$
Finite set notation	$x \in \{x_1, \ldots, x_n\} \Leftrightarrow x = x_1$ or $\cdots$ or $x = x_n$

Elementary Set Theory (cont.)

Name	Definition
*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	Definition
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	$A \times B = \{(x, y) : x \in A$ and $y \in B\}$
Cartesian Product	$A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) : x_1 \in A_1$ and $\cdots$ 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	Definition
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.

Famous Sets of Numbers	
Name	Definition
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	$\mathbb{R} = \{x : x$ 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	$A^+ = A \cap \mathbb{R}^+$

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

Famous Sets of Numbers (cont.)

Name	Definition
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. 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. 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 $i > n$.

0.3 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. 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. 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. *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

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

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

Relations

Name	Definition
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.

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

Relations (cont.)

Name	Definition
*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.

0.4 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	Axiom
(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	$\forall n, \forall m, m \leq n \Leftrightarrow \exists k, m + k = n$

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

1 Arithmetic in $\mathbb{Z}$ Revisited

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. 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

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

def of min

$S \subseteq \mathbb{N}$	(show)
$S \neq \emptyset$	
$\min(S) \in S$	(conclude)

$S \subseteq \mathbb{N}$	(show)
$S \neq \emptyset$	(show)
$s \in S$	(show)
$\min(S) \leq s$	(conclude)

Division Algorithm (existence)

$a, b \in \mathbb{Z}$	(show)
$b > 0$	(show)
For some $q, r \in \mathbb{Z}$,	(constant declaration)
$a = bq + r$	(conclude)
$0 \leq r < b$	(conclude)

Division Algorithm (uniqueness)

$a, b, q, r \in \mathbb{Z}$	(show)
$b > 0$	(show)
$a = bq + r$ and $0 \leq r < b$	(show)
$q = a \operatorname{quo} b$	(conclude)
$r = a \bmod b$	(conclude)

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 $2 \mid a$, 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 $a, b \in \mathbb{Z}$ not both zero, 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 (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		divides	
$a, b, q \in \mathbb{Z}$	(SHOW)	$a, b \in \mathbb{Z}$	(SHOW)
$a = qb$	(SHOW)	$b \mid a$	(SHOW)
$b \mid a$	(CONCLUDE)	For some $q \in \mathbb{Z}$,	(constant declaration)
		$a = qb$	(CONCLUDE)

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

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)
.....	
$c \leq d$	

Bézout's Lemma	
$a, b \in \mathbb{Z}$	(SHOW)
$a \neq 0$ or $b \neq 0$	(SHOW)
.....	
For some $s, t \in \mathbb{Z}$,	(constant declaration)
$\gcd(a, b) = s \cdot a + t \cdot b$	(CONCLUDE)

Bézout's Lemma	
$a, b, u, v \in \mathbb{Z}$	(SHOW)
$a \neq 0$ or $b \neq 0$	(SHOW)
.....	
$\gcd(a, b) \mid u \cdot a + v \cdot b$	(CONCLUDE)

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 (composite)**.** *Let* $p \in \mathbb{Z} - \{0, \pm 1\}$*.*

$$p \text{ is composite} \Leftrightarrow \exists a, b \in \mathbb{Z}, p = \pm ab \text{ and } 1 < a, b < |p|$$

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

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

Theorem (Fundamental 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,* k *and* e_k *are positive integers, and each* $e_i \in \mathbb{N}$*.*

Notation. It is commonplace to write the prime factorization of an integer by omitting any prime factor whose exponent is zero in the expression given by the Fundamental Theorem. Thus we can say that the prime factorization of n is

$$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1 < p_2 < \cdots < p_k$ are positive primes and $e_1, ..., e_k \in \mathbb{Z}^+$

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

Primality in $\mathbb{Z}$

prime		prime	
$p \in \mathbb{Z} - \{0, \pm 1\}$	(SHOW)	p IS PRIME	(SHOW)
Let $c \in \mathbb{Z}$	(variable declaration)	.....	
Assume $c \mid p$		$p \notin \{0, \pm 1\}$	(CONCLUDE)
$c \in \{\pm 1, \pm p\}$	(SHOW)	p IS PRIME	(SHOW)
←		$c \mid p$	(SHOW)
←		.....	
.....		$c \in \{\pm 1, \pm p\}$	(CONCLUDE)
p IS PRIME	(CONCLUDE)		

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

alt. def. of prime	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)	$p, b, c \in \mathbb{Z}$ (SHOW) p IS PRIME (SHOW) $p \mid bc$ …… $p \mid b$ or $p \mid c$ (CONCLUDE)
composite	**composite**
c IS NOT PRIME (SHOW) $c \notin \{0, \pm 1\}$ (SHOW) …… p IS COMPOSITE (CONCLUDE)	p IS COMPOSITE (SHOW) …… p IS NOT PRIME (CONCLUDE) $p \notin \{0, \pm 1\}$ (CONCLUDE) For some a, b, (constant declaration) $1 < a, b < \lvert p \rvert$ and $p = \pm ab$ (CONCLUDE)
Fund. Thm. of Arithmetic (existence)	**Fund. Thm. of Arithmetic (uniqueness)**
$n \in \mathbb{Z} - \{0\}$ (SHOW) …… For some $k \in \mathbb{N}, p_1, \ldots, p_k, e_1, \ldots, e_k \in \mathbb{N}^+$, (constant declaration) $p_1, \ldots, p_k$ ARE PRIMES (CONCLUDE) $1 < p_1 < p_2 < \cdots < p_k$ (CONCLUDE) $n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ (CONCLUDE)	$n \in \mathbb{Z} - \{0\}$ (SHOW) $k, m \in \mathbb{N}$ (SHOW) $p_1, \ldots, p_k, q_1, \ldots, q_m$ ARE PRIMES (SHOW) $e_1, \ldots, e_k, d_1, \ldots, d_m \in \mathbb{Z}^+$ (SHOW) $1 < p_1 < p_2 < \cdots < p_k$ (SHOW) $1 < q_1 < q_2 < \cdots < q_m$ (SHOW) $n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ (SHOW) $n = \pm q_1^{d_1} q_2^{d_2} \cdots q_m^{d_m}$ (SHOW) …… $k = m$ (CONCLUDE) $p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$ (CONCLUDE) $e_1 = d_1, e_2 = d_2, \ldots, e_k = d_k$ (CONCLUDE) (*and the signs match*)

2 Congruence in $\mathbb{Z}$ and Modular Arithmetic

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

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

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

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

Corollary. *Let* $n \in \mathbb{N}$ *with* $n > 1$.

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

In the following table all variables have type integer, n is a positive integer, and the equivalence classes are for the relation $\underset{n}{\equiv}$.

Congruence in $\mathbb{Z}$

$\underset{n}{\equiv}$	$\underset{n}{\equiv}$
$n \mid a - b$ (SHOW)	$a \underset{n}{\equiv} b$ (SHOW)
$a \underset{n}{\equiv} b$ (CONCLUDE)	$n \mid a - b$ (CONCLUDE)

$\mathbb{Z}_n$	$\mathbb{Z}_n$
$x \in \mathbb{Z}_n$ (SHOW)	$k, j \in \{0, 1, 2, \cdots, n-1\}$ (SHOW)
	$k \neq j$ (SHOW)
For some $a \in \mathbb{Z}$, (constant declaration)	
$x = [a]$ (CONCLUDE)	$[k] \neq [j]$ (CONCLUDE)

class representative (existence)	class representative (uniqueness)
$x \in \mathbb{Z}_n$ (SHOW)	$0 \leq i, j \leq n-1$ (SHOW)
	$[i] = [j]$ (SHOW)
For some k, (constant declaration)	
$0 \leq k \leq n-1$ (CONCLUDE)	$i = j$ (CONCLUDE)
$x = [k]$ (CONCLUDE)	

2.2 Arithmetic in $\mathbb{Z}_n$

Theorem. *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

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

Corollary. *Let $a, b, c, d, n \in \mathbb{Z}, n > 1$. If $[a] = [b]$ and $[c] = [n]$ then*

$$[a + c] = [b + d]$$

and

$$[a \cdot c] = [b \cdot d]$$

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

Remark. We usually use infix notation when applying binary operators to their arguments, i.e., we write $(a \ f \ b)$ instead of $f(a, b)$.

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

$$\oplus = \left\{ ((A, B), C) : \exists a, b \in \mathbb{Z},\ A = [a],\ B = [b], \text{ and } C = [a + b] \right\}$$
$$\odot = \left\{ ((A, B), C) : \exists a, b \in \mathbb{Z},\ A = [a],\ B = [b], \text{ and } C = [a \cdot b] \right\}$$

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

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

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

$$[a] \oplus [b] = [a + b]$$
$$[a] \odot [b] = [a \cdot b]$$

Theorem (Ring Properties of $\mathbb{Z}_n$)**.** *For all $A, B, C \in \mathbb{Z}_n$,*

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

Lemma (mult by 0 in $\mathbb{Z}_n$)**.** *Let $n \in \mathbb{Z}^+$ and $A \in \mathbb{Z}_n$. Then $[0] \odot A = [0]$*

Again in this table, n is a positive integer and all equivalence classes are with respect to $\underset{n}{\equiv}$.

Arithmetic in $\mathbb{Z}_n$

modular arithmetic		modular arithmetic	
$a, b, c, d \in \mathbb{Z}$	(SHOW)	$a, b \in \mathbb{Z}$	(SHOW)
$a \underset{n}{\equiv} b$	(SHOW)		
$c \underset{n}{\equiv} d$	(SHOW)		
$a + c \underset{n}{\equiv} b + d$	(CONCLUDE)	$[a] \oplus [b] = [a + b]$	(CONCLUDE)
$a \cdot c \underset{n}{\equiv} b \cdot d$	(CONCLUDE)	$[a] \odot [b] = [a \cdot b]$	(CONCLUDE)

2.3 Algebra in $\mathbb{Z}_n$

As is frequently the convention, write will sometimes write st as an abbreviation for $s \odot t$ as long as it is clear what the missing multiplication is from context.

Any number that has a multiplicative inverse is called a *unit*. Two nonzero numbers whose product is zero are called *zero divisors*. In these terms the following theorem says that p is prime precisely when $\mathbb{Z}_p$ has no zero divisors, and equivalently, every nonzero element of $\mathbb{Z}_p$ has a multiplicative inverse.

Theorem. *Let $p \in \mathbb{Z}$ and $p > 1$. The following are equivalent.*

1. *p is prime*
2. $\forall a \in \mathbb{Z}_p - \left\{[0]\right\}, \exists x \in \mathbb{Z}_p, ax = [1]$
3. $\forall a, b \in \mathbb{Z}_p, ab = [0] \Rightarrow a = [0]$ *or* $b = [0]$

Theorem (solving linear equations $\mathbb{Z}_n$)**.** *Let $n \in \mathbb{N}^+$, $a, b \in \mathbb{Z}_n$, $r, s \in \mathbb{Z}$, $a = [r]$, $b = [s]$, $a \neq [0]$, $d = \gcd(r, n)$, and x a variable of type $\mathbb{Z}_n$.*

1. *If n is prime then $ax = b$ has a unique solution in $\mathbb{Z}_n$.*
2. *If n is not prime and $d \mid b$ then $ax = b$ has d solutions in $\mathbb{Z}_n$.*
3. *If n is not prime and $d \nmid b$ then $ax = b$ has no solutions in $\mathbb{Z}_n$.*

Solving Linear Equations in $\mathbb{Z}_n$

$\mathbb{Z}_p$ for prime p	
p is prime	(SHOW)
$a \in \mathbb{Z}_p - [0]$	(SHOW)
.....	
For some $c \in \mathbb{Z}_p$,	(constant declaration)
$a \odot c = [1]$	(CONCLUDE)

$\mathbb{Z}_p$ for prime p	
p is prime	(SHOW)
$a, b \in \mathbb{Z}_p$	(SHOW)
$a \odot b = [0]$	(SHOW)
.....	
$a = [0]$ or $b = [0]$	(CONCLUDE)

$\mathbb{Z}_p$ for prime p	
Let $a \in \mathbb{Z}_p - [0]$	(variable declaration)
$\exists x \in \mathbb{Z}_p, a \odot x = [1]$	(SHOW)
$\leftarrow$	
.....	
p is prime	(CONCLUDE)

$\mathbb{Z}_p$ for prime p	
Let $a, b \in \mathbb{Z}_p$	(variable declaration)
Assume $a \odot b = [0]$	
$a = [0]$ or $b = [0]$	(SHOW)
$\leftarrow$	
$\leftarrow$	
.....	
p is prime	(CONCLUDE)

3 Rings

3.1 Definition and Examples of Rings

Definition (ring)**.** 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 any t described 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 of a ring is unique).*

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

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

Notation. 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. 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 $a + \left(^-b\right)$.

Types of Rings

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

Definition (ring with identity)**.** A ring $(R, +, \cdot)$ is a **ring with identity** if and only if $\exists i \in R, \forall x \in R, ix = x = xi$.

Lemma (uniq of mult ident)**.** *Let $(R, +, \cdot)$ be a ring and $u, v \in R$. If*

$$\forall x \in R, ux = x = xu \text{ and } vx = x = xv$$

then $u = v$ (i.e. the multiplicative identity for a ring is unique).

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

Lemma (uniq of mult inverse)**.** *Let $(R, +, \cdot)$ be a ring with identity 1_R and $x, u, v \in R$. If*

$$ux = 1_R = xu \text{ and } vx = 1_R = xv$$

then $u = v$ (i.e. a multiplicative inverse of an element of a ring is unique).

Notation. If R is a ring with identity we write x^{-1} for the unique multiplicative inverse of x in R.

Definition (integral domain)**.** A ring $(R, +, \cdot)$ is an **integral domain** if and only if it 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 (field)**.** A ring $(R, +, \cdot)$ is a **field** if and only if is a commutative ring with identity $1_R \neq 0_R$ and $\forall a \in R - \{0_R\}, \exists x \in R, ax = 1_R$ (i.e., every nonzero element has a multiplicative inverse).

Rings

ring

$+ : R \times R \to R$ (SHOW)
$\cdot : R \times R \to R$ (SHOW)
Let $x, y, z \in R$ (variable declaration)
$x + (y + z) = (x + y) + z$ (SHOW)
$x + y = y + x$ (SHOW)
$\exists 0_R \in R, \forall x, 0_R + x = x = x + 0_R$ (SHOW)
$\exists\, ^-x \in R, {}^-x + x = x + ({}^-x) = 0_R$ (SHOW)
$x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (SHOW)
$x \cdot (y + z) = x \cdot y + x \cdot z$ (SHOW)
$(y + z) \cdot x = y \cdot x + z \cdot x$ (SHOW)
←

$(R, +, \cdot)$ is a ring

ring

$(R, +, \cdot)$ is a ring (SHOW)
$x, y, z \in R$ (SHOW)

$x + (y + z) = (x + y) + z$ (CONCLUDE)
$x + y = y + x$ (CONCLUDE)
$0_R \in R$ (CONCLUDE)
$0_R + x = x = x + 0_R$ (CONCLUDE)
$^-x \in R$ (CONCLUDE)
$^-x + x = x + (^-x) = 0_R$ (CONCLUDE)
$x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (CONCLUDE)
$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (CONCLUDE)

commutative ring

$(R, +, \cdot)$ is a ring (SHOW)
Let $x, y \in R$ (variable declaration)
$x \cdot y = y \cdot x$ (SHOW)
←

$(R, +\cdot)$ is a commutative ring (CONCLUDE)

commutative ring

$(R, +, \cdot)$ is a commutative ring (SHOW)
$x, y \in R$ (SHOW)

$x \cdot y = y \cdot x$ (CONCLUDE)

ring with identity

$(R, +, \cdot)$ is a ring (SHOW)
$i \in R$ (SHOW)
Let $x \in R$ (variable declaration)
$i \cdot x = x = x \cdot i$ (SHOW)
←

$(R, +\cdot)$ is a ring with identity (CONCLUDE)
$1_R = i$ (CONCLUDE)

ring with identity

$(R, +, \cdot)$ is a ring with identity (SHOW)
$x \in R$ (SHOW)

$1_R \in R$ (CONCLUDE)
$1_R \cdot x = x = x \cdot 1_R$ (CONCLUDE)

Rings (cont.)

integral domain

$(R,+,\cdot)$ is a commutative ring (SHOW)
$(R,+,\cdot)$ is a ring with identity (SHOW)
$1_R \neq 0_R$ (SHOW)
  Let $x, y \in R$ (variable declaration)
    Assume $x \cdot y = 0_R$
    $x = 0_R$ or $y = 0_R$ (SHOW)
    ←
  ←
$(R,+\cdot)$ is an integral domain (CONCLUDE)

integral domain

$(R,+,\cdot)$ is an integral domain (SHOW)
$(R,+,\cdot)$ is a commutative ring (CONCLUDE)
$(R,+,\cdot)$ is a ring with identity (CONCLUDE)
$1_R \neq 0_R$ (CONCLUDE)

$(R,+,\cdot)$ is an integral domain (SHOW)
$x, y \in R$ (SHOW)
$x \cdot y = 0_R$ (SHOW)
$x = 0_R$ or $y = 0_R$ (CONCLUDE)

field

$(R,+,\cdot)$ is a commutative ring (SHOW)
$(R,+,\cdot)$ is a ring with identity (SHOW)
$1_R \neq 0_R$ (SHOW)
  Let $x \in R - \{0_R\}$ (variable declaration)
  $\exists y \in R, x \cdot y = 1_R$
  ←
$(R,+,\cdot)$ is a field (CONCLUDE)

field

$(R,+,\cdot)$ is a field (SHOW)
$(R,+,\cdot)$ is a commutative ring (CONCLUDE)
$(R,+,\cdot)$ is a ring with identity (CONCLUDE)
$1_R \neq 0_R$ (CONCLUDE)

$(R,+,\cdot)$ is a field (SHOW)
$x \in R$ (SHOW)
$x^{-1} \in R$ (CONCLUDE)
$x \cdot x^{-1} = x^{-1} \cdot x = 1_R$ (CONCLUDE)

subtraction

$(R,+,\cdot)$ is a ring (SHOW)
$x, y \in R$ (SHOW)
$x - y = x + (^-y)$ (CONCLUDE)

Subrings

Definition (subring)**.** Let $(R,+,\cdot)$ be a ring and $S \subseteq R$. $(S,+,\cdot)$ is a **subring** of $(R,+,\cdot)$ if and only 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 (Cartesian Product of Rings). *Let* $(R,+,\cdot),(S,\dot{+},\bullet)$ *be rings and define*

$$(r,s)\oplus(u,v)=(r+u,s\dot{+}v)$$
$$(r,s)\odot(u,v)=(r\cdot u,s\bullet v)$$

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

Remark. In the previous theorem if we use + for the addition in both rings R,S and abbreviate products by concatentation, then the previous definitions become simply

$$(r,s)\oplus(u,v)=(r+u,s+v)$$
$$(r,s)\odot(u,v)=(ru,sv)$$

Subrings and Cartesian Product Rings

subring	
$(R,+,\cdot)$ is a ring	(SHOW)
$S\subseteq R$	(SHOW)
Let $x,y\in S$	(variable declaration)
$x+y\in S$	(SHOW)
$x\cdot y\in S$	(SHOW)
←	
$(S,+,\cdot)$ is a ring	(SHOW)
$(S,+,\cdot)$ is a subring of $(R,+,\cdot)$	(CONCLUDE)

subring	
$(S,+,\cdot)$ is a subring of $(R,+,\cdot)$	(SHOW)
$S\subseteq R$	(CONCLUDE)
$(S,+,\cdot)$ is a ring	(CONCLUDE)

Cartesian product ring	
$(R,+,\cdot)$ is a ring	(SHOW)
$(S,\dot{+},\bullet)$ is a ring	(SHOW)
Let $r,s\in R$ and $u,v\in S$	(variable declaration)
$(r,s)\oplus(u,v)=(r+s,u\dot{+}v)$	(SHOW)
$(r,s)\odot(u,v)=(r\cdot s,u\bullet v)$	(SHOW)
←	
$(R\times S,\oplus,\odot)$ is a ring	(CONCLUDE)

Cartesian product ring	
$(R,+,\cdot)$ is a ring	(SHOW)
$(S,\dot{+},\bullet)$ is a ring	(SHOW)
$(R\times S,\oplus,\odot)$ is the Cartesian product ring of R and S	(SHOW)
$r,s\in R$ and $u,v\in S$	(SHOW)
$(r,s)\oplus(u,v)=(r+s,u\dot{+}v)$	(CONCLUDE)
$(r,s)\odot(u,v)=(r\cdot s,u\bullet v)$	(CONCLUDE)

Subrings and Cartesian Product Rings (cont.)

subring theorem	
$(R,+,\cdot)$ is a ring	(show)
$S \subseteq R$	(show)
$S \neq \emptyset$	(show)
Let $x, y \in S$	(variable declaration)
$x - y \in S$	(show)
$x \cdot y \in S$	(show)
$\leftarrow$	
.....	
$(S,+,\cdot)$ is a subring of $(R,+,\cdot)$	(conclude)

3.2 Algebra in Rings

Theorem (the Algebra Theorem 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 Theorem). *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 (to the Sign Theorem). *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 (exponentiation and multiples). 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. *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 (uniqness of multiplicative 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 (multiplicative inverse)**.** 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 (unit)**.** 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 ($\mathcal{U}(R)$)**.** Let $(R, +, \cdot)$ be a ring with identity. The set of all units of R is denoted $\mathcal{U}(R)$.

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

Theorem (the Algebra Theorem 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. $xa = b \Leftrightarrow x = ba^{-1}$
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 $a \neq 0_R$. Then*

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

Definition (zero divisor)**.** 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 integral domains)**.** *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 ring addition so that e.g. $a + bc$ means $a + (bc)$ and not $(a + b)c$.

Algebra in Rings

unit & inverse		unit & inverse	
$(R, +, \cdot)$ is a ring with identity	(SHOW)	$(R, +, \cdot)$ is a ring with identity	(SHOW)
$a, x \in R$	(SHOW)	a is a unit of $(R, +, \cdot)$	(SHOW)
$ax = xa = 1_R$	(SHOW)	.....	
.....		$a^{-1} \in R$	(CONCLUDE)
a is a unit of $(R, +, \cdot)$	(CONCLUDE)	$a \cdot a^{-1} = a^{-1} \cdot a = 1_R$	(CONCLUDE)
$x = a^{-1}$	(CONCLUDE)		

associate		associate	
$(R, +, \cdot)$ is a comm. ring with identity	(SHOW)	$(R, +, \cdot)$ is a comm. ring with identity	(SHOW)
$a, b \in R$	(SHOW)	$a, b \in R$	(SHOW)
$u \in \mathcal{U}(R)$	(SHOW)	$a \diamond b$	(SHOW)
$a = ub$	(SHOW)	.....	
.....		For some $u \in \mathcal{U}(R)$,	(constant declaration)
$a \diamond b$	(CONCLUDE)	$a = ub$	(CONCLUDE)

zero divisor		zero divisor	
$(R, +, \cdot)$ is a ring	(SHOW)	$(R, +, \cdot)$ is a ring	(SHOW)
$a, b \in R$	(SHOW)	$a \in R$	(SHOW)
$a \neq 0_R$ and $b \neq 0_R$	(SHOW)	a is a zero divisor of $(R, +, \cdot)$	(SHOW)
$a \cdot b = 0_R$ or $b \cdot a = 0_R$	(SHOW)	.....	
.....		For some $b \in R - \{0_R\}$,	(constant declaration)
a is a zero divisor	(CONCLUDE)	$a \cdot b = 0_R$ or $b \cdot a = 0_R$	(CONCLUDE)

3.3 Ring Homomorphisms

Recall that we will frequently refer to a ring $(R, +, \cdot)$ by its set, i.e., we will call it the ring R when $+, \cdot$ are understood.

Definition. Let $(R, +, \cdot), (S, \oplus, \odot)$ be rings. Then ring R is **isomorphic** to ring S if and only if there exists a function $f : R \to S$ such that

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

Such a map f is called an **isomorphism**.

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

Lemma. *The identity map is a ring isomorphism.*

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

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

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

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. $\forall a, b \in R, f(a \cdot b) = f(a) \cdot f(b)$

in this notation.

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

Corollary. *The composition of ring isomorphisms is a ring isomorphism.*

Theorem (inverse of an isomorphism)**.** *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. $f(a-b) = f(a) - f(b)$

Additionally, 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 (homomorphic image)**.** *Let $f: R \to S$ be a ring homomorphism. Then $f(R)$ is a subring of S.*

Ring Homomorphisms

ring homomorphism		ring homomorphism	
$(R, +, \cdot)$ is a ring	(show)	$(R, +, \cdot)$ is a ring	(show)
$(S, \oplus, \odot)$ is a ring	(show)	$(S, \oplus, \odot)$ is a ring	(show)
$f: R \to S$	(show)	$f: R \to S$ is a ring homomorphism	(show)
Let $x, y \in R$	(variable declaration)	$x, y \in R$	(show)
$f(x+y) = f(x) \oplus f(y)$	(show)	$f(x+y) = f(x) \oplus f(y)$	(conclude)
$f(x \cdot y) = f(x) \odot f(y)$	(show)	$f(x \cdot y) = f(x) \odot f(y)$	(conclude)
←			
f is a ring homomorphism	(conclude)		

ring isomorphism		ring isomorphism	
f is a ring homomorphism	(show)	f is a ring isomorphism	(show)
f is bijective	(show)	f is a ring homomorphism	(conclude)
f is a ring isomorphism	(conclude)	f is bijective	(conclude)

4 Arithmetic in $F[x]$

4.1 Polynomials

Definition (eventually zero)**.** Let $(R, \oplus, \odot)$ be a ring. An infinite sequence of elements of R,

$$a_0, a_1, a_2, \ldots, a_n, \ldots$$

is said to be *eventually zero* if and only if there exists $N \in \mathbb{N}$ such that for all $i \geq N$, $a_i = 0_R$.

Definition (polynomial)**.** Let $(R, \oplus, \odot)$ 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 $n \in \mathbb{N}, a_0, \ldots, a_n \in R$, and x is a symbol that is neither a variable nor a constant. 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 $\mathrm{LC}(P) = a_n$. The eventually zero sequence

$$a_0, a_1, \ldots, a_n, 0_R, 0_R, \ldots$$

is called the **sequence of coefficients** of the polynomial. We define $\mathrm{coeff}(P, i)$ to be a_i in this case.

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

Remark. Note that given a polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ we define $a_i = 0_R$ for $i > n$.

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

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

If some coefficient $a_i = 0_R$ we can omit the summand $a_i x^i$ when writing the polynomial. Similarly, if R has identity, we can abbreviate $1_R x^i$ as simply x^i. Finally, we can also permute the order of the summands in a polynomial to obtain another equivalent expression.

Definition. Two polynomials are equal if and only if their corresponding sequence of coefficients are equal.

Definition ($R[x]$)**.** Let $(R, \oplus, \odot)$ be a ring. Then $R[x]$ is the set of all polynomial with indeterminate x 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 $(R, \oplus, \odot)$ be a ring and $P, Q \in R[x]$. Then there exist $a_0, \ldots, a_n, b_0, \ldots, b_m \in R$ such that $P = a_0 + a_1 x + \cdots + a_n x^n$ and $Q = b_0 + b_1 x + \cdots + b_m x^m$. Define $a_k = 0_R$ for $k > n$, $b_k = 0_R$ for $k > m$, and $s = \max(m, n)$. Then

$$P + Q = (a_0 \oplus b_0) + (a_1 \oplus b_1)\, x + \cdots + (a_s \oplus b_s)\, x^s$$

$$P \cdot Q = (a_0 \odot b_0) + (a_1 \odot b_0 \oplus a_0 \odot b_1)\, x + \cdots + \left(\bigoplus_{j=0}^{i} a_j \odot b_{i-j} \right) x^i + \cdots + (a_n \odot b_m)\, x^{n+m}$$

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 $\oplus, \odot$ when it is clear from context.

Theorem ($R[x]$ is a ring)**.** *$(R[x], +, \cdot)$ is a ring.*

Lemma (properties of $R[x]$)**.** *Let $(R, \oplus, \odot)$ be a ring $n \in \mathbb{N}$ and $a_0, \ldots, a_n \in R$. 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 degree (Tepid!!))**.** *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. *If R is an integral domain then so is $R[x]$.*

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

Division Algorithm in $F[x]$

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*

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

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.

In the following recipies, $(R, \oplus, \odot)$ is a ring.

Polynomials

polynomial	
$f \in R[x] - \{0_R\}$	(show)
For some $n \in \mathbb{N}, a_0, \ldots, a_n \in R$,	(constant declaration)
$f = a_0 + \cdots + a_n x^n$ and $a_n \neq 0_R$	(conclude)

polynomial equality	
$f, g \in R[x]$	(show)
Let $i \in \mathbb{N}$	(variable declaration)
$\text{coeff}(f, i) = \text{coeff}(g, i)$	(show)
$\leftarrow$	
$f = g$	(conclude)

degree	
$f = a_0 + a_1 x + \cdots a_n x^n \in R[x]$	(show)
$a_n \neq 0_R$	(show)
$\deg(f) = n$	(conclude)

degree	
$f \in R[x]$	(show)
$\deg(f) = n$	(show)
$\text{coeff}(f, n) \neq 0_R$	(conclude)
$\forall i > n, \text{coeff}(f, i) = 0_R$	(conclude)

4.2 Divisibility in $F[x]$

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

$$f \mid g \Leftrightarrow \exists q \in F[x], g = qf$$

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

Lemma. *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. *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 $\text{LC}(f) = 1_F$.

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

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

1. d is monic
2. $d \mid f$ and $d \mid g$
3. $\forall c \in F[x], c \mid f$ and $c \mid g \Rightarrow \deg(c) \leq \deg(d)$

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 (Bézout for polynomials)**.** *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 $\exists s, t \in F[x]$, $sf + tg = d$ and d is the unique monic polynomial of smallest degree that is of this form.*

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

1. *d is monic*
2. *$d \mid f$ and $d \mid g$*
3. *$\forall c \in F[x], c \mid f$ and $c \mid g \Rightarrow c \mid d$*

Theorem. *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 $f = qg + r$ and ($r = 0_{F[x]}$ or $\deg(r) \leq \deg(g)$) then*

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

In the following recipes, F is a field.

Divisibility in $F[x]$

divides		divides	
$a, b, q \in F[x]$	(SHOW)	$a, b \in F[x]$	(SHOW)
$a = qb$	(SHOW)	$b \mid a$	(SHOW)
.....		.....	
$b \mid a$	(CONCLUDE)	For some $q \in F[x]$,	(constant declaration)
		$a = qb$	(CONCLUDE)

Divisibility in $F[x]$ (cont.)

gcd	gcd
$a, b, d \in F[x]$ (show) $a \neq 0_F$ or $b \neq 0_F$ (show) d is monic (show) $d \mid a$ and $d \mid b$ (show) Let $c \in F[x]$ (variable declaration) Assume $c \mid a$ and $c \mid b$ $\deg(c) \leq \deg(d)$ (show) $\leftarrow$ $\leftarrow$ $d = \gcd(a, b)$ (conclude)	$d = \gcd(a, b)$ (show) $a \neq 0_F$ or $b \neq 0_F$ (conclude) d is monic (conclude) $d \mid a$ (conclude) $d \mid b$ (conclude) $d = \gcd(a, b)$ (show) $c \mid a$ (show) $c \mid b$ (show) $\deg(c) \leq \deg(d)$
Bézout's Lemma	**Bézout's Lemma**
$a, b \in F[x]$ (show) $a \neq 0_F$ or $b \neq 0_F$ (show) For some $s, t \in F[x]$, (constant declaration) $\gcd(a, b) = s \cdot a + t \cdot b$ (conclude)	$a, b, u, v \in F[x]$ (show) $a \neq 0_F$ or $b \neq 0_F$ (show) $\gcd(a, b) \mid u \cdot a + v \cdot b$ (conclude)

4.3 Primality (Irreducibilty) in $F[x]$

Theorem (units in $R[x]$)**.** *Let $(R, +, \cdot)$ be an integral domain. 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 (units in $F[x]$)**.** *Let F be a field. The units of $F[x]$ are the nonzero constant polynomials, i.e., $\mathcal{U}(F[x]) = F - \{0_F\}$.*

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

Definition (irreducible)**.** Let F be a field and $p \in F[x] - F$. We say p is **irreducible** if and only if $\forall c \in F[x], c \mid p \Rightarrow c \in \mathcal{U}(F[x])$ or $c \diamond p$.

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 (alternate def of reducible)**.** *Let F be a field and $p \in F[x]$. We say p is reducible if and only if there exist $g, h \in F[x]$ such that*

1. $p = gh$
2. $0 < \deg(g) < \deg(p)$

Remark. Note that in the previous theorem, since $0 < \deg(g) < \deg(p)$ it follows that $0 < \deg(h) < \deg(p)$ also.

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

Theorem (alternate def of irreducible)**.** *Let F be a field and $p \in F[x]$. The following are equivalent (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. $\forall r, s \in F[x], p = rs \Rightarrow r \in \mathcal{U}(F[x])$ or $s \in \mathcal{U}(F[x])$.

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

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

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

Theorem (Fundamental Theorem of Arithmetic for $F[x]$)**.** *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.

Note that in the following we identify F with the constant polynomials in $F[x]$. For example, $F[x] - F$ is the set of polynomials with positive degree.

Irreducibility in $F[x]$

irreducible

$p \in F[x] - F$ (SHOW)
  Let $c \in F[x]$ (variable declaration)
    Assume $c \mid p$
    $c \in \mathcal{U}(F[x])$ or $c \diamond p$ (SHOW)
    ←
  ←
……
p IS IRREDUCIBLE (CONCLUDE)

irreducible

p IS IRREDUCIBLE (SHOW)
……
$\deg p > 0$ (CONCLUDE)

p IS IRREDUCIBLE (SHOW)
$c \mid p$ (SHOW)
……
$c \in \mathcal{U}(F[x])$ or $c \diamond p$ (CONCLUDE)

alt. def. of irreducible

$p \in F[x] - F$ (SHOW)
  Let $b, c \in F[x]$ (variable declaration)
    Assume $p \mid bc$
    $p \mid b$ or $p \mid c$ (SHOW)
    ←
  ←
……
p IS IRREDUCIBLE (CONCLUDE)

alt. def. of irreducible

$p, b, c \in F[x]$ (SHOW)
p IS IRREDUCIBLE (SHOW)
$p \mid bc$
……
$p \mid b$ or $p \mid c$ (CONCLUDE)

alt. def. of irreducible

$p \in F[x] - F$ (SHOW)
  Let $b, c \in F[x]$ (variable declaration)
    Assume $p = bc$
    $b \in \mathcal{U}(F[x])$ or $c \in \mathcal{U}(F[x])$ (SHOW)
    ←
  ←
……
p IS IRREDUCIBLE (CONCLUDE)

alt. def. of irreducible

$p, b, c \in F[x]$ (SHOW)
p IS IRREDUCIBLE (SHOW)
$p = bc$
……
$b \in \mathcal{U}(F[x])$ or $c \in \mathcal{U}(F[x])$ (CONCLUDE)

Irreducibility in $F[x]$ (cont.)

reducible	
c is not irreducible	(show)
$c \notin F$	(show)
c is reducible	(conclude)

reducible	
c is reducible	(show)
c is not irreducible	(conclude)
$c \notin F$	(conclude)

Fundamental Theorem of Arithmetic for Polynomials (existence)	
$f \in F[x] - F$	(show)
For some $k \in \mathbb{N}, c \in F - 0_F$,	
$p_1, \ldots, p_k \in F[x]$,	
$e_1, \ldots, e_k \in \mathbb{N}^+$,	(constant declaration)
$p_1, \ldots, p_k$ are irreducible	(conclude)
$p_1, \ldots, p_k$ are monic	(conclude)
$f = c \cdot p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$	(conclude)

Fundamental Theorem of Arithmetic for Polynomials (uniqueness)	
$f \in F[x] - F$	(show)
$k, m \in \mathbb{N}$	(show)
$c, d \in F - \{0_F\}$	(show)
$p_1, \ldots, p_k, q_1, \ldots, q_m$ are monic irreducibles	(show)
$e_1, \ldots, e_k, d_1, \ldots, d_m \in \mathbb{N}^+$	(show)
$f = c \cdot p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$	(show)
$f = d \cdot q_1^{d_1} q_2^{d_2} \cdots q_m^{d_m}$	(show)
$k = m$	(conclude)
$c = d$	(conclude)
$p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$	(conclude)
$e_1 = d_1, e_2 = d_2, \ldots, e_k = d_k$ (*for some order of the factors*)	(conclude)

4.4 Polynomial Functions

Definition (polynomial function)**.** 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 (root)**.** Let R be a commutative ring, $f \in R[x]$, and $a \in R$. We say a is a **root** of f if and only if $\overline{f}(a) = 0_R$.

Theorem (Remainder Theorem)**.** *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 (Factor Theorem)**.** *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 (to the Remainder Theorem 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 (to the Remainder Theorem 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 (to the Remainder Theorem IV). *Let F be a field, $f \in F[x] - \{0_F\}$, and $n = \deg(f)$. Then f has at most n roots in F.*

Corollary (to the Remainder Theorem V). *Let F be an infinite field and $f, g \in F[x]$. Then*

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

Polynomial Functions

Remainder Theorem		Remainder Theorem	
$f \in F[x]$	(show)	$f \in F[x]$	(show)
$a \in F$	(show)	F is infinite	(show)
For some $q \in F[x]$		$\overline{f} = \overline{g} \Leftrightarrow f = g$	(conclude)
$f = q \cdot (x - a) + \overline{f}(a)$	(conclude)		
Factor Theorem		**Factor Theorem**	
$f \in F[x]$	(show)	$f \in F[x]$	(show)
$\overline{f}(a) = 0_F$	(show)	$(x - a) \mid f$	(show)
$(x - a) \mid f$	(conclude)	$\overline{f}(a) = 0_F$	(conclude)

5 Congruence in $F[x]$ and Congruence Class Arithmetic

5.1 Congruence in $F[x]$

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

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

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

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

Corollary (the set $F[x]_p$)**.** *Let* $p \in F[x] - \{0_F\}$ *and* $f \in F[x]$.

a. *If* r *is the remainder when* f *is divided by* p *then* $[f] = [r]$ *(and* $f \underset{p}{\equiv} r$*).*

b. $F[x]_p = \left\{ [0_F] \right\} \cup \left\{ [f] : f \in F[x] \text{ and } \deg(f) < \deg(p) \right\}$ *and these elements are distinct.*

In the following table, all free variables have type $F[x]$ and equivalence classes are with respect to $\underset{p}{\equiv}$.

Congruence in $F[x]$

$\underset{p}{\equiv}$	$\underset{p}{\equiv}$
$p \mid f - g$ (SHOW)	$f \underset{p}{\equiv} g$ (SHOW)
$f \underset{p}{\equiv} g$ (CONCLUDE)	$p \mid f - g$ (CONCLUDE)

$F[x]_p$	$F[x]_p$
$z \in F[x]_p$ (SHOW)	$k, j \in \{ f \in F[x] : f = 0_F \text{ or } \deg(f) < \deg(p) \}$ (SHOW)
For some $f \in F[x]$, (constant declaration)	$k \neq j$ (SHOW)
$z = [f]$ (CONCLUDE)	$[k] \neq [j]$ (CONCLUDE)

class representative (existence)	class representative (uniqueness)
$z \in F[x]_p$ (SHOW)	$i, j \in \{0_F\} \cup \{ f \in F[x] : \deg(f) < \deg(p) \}$ (SHOW)
For some k, (constant declaration)	$[i] = [j]$ (SHOW)
$k = 0_F$ or $\deg(k) \leq \deg(p)$ (CONCLUDE)	$i = j$ (CONCLUDE)
$z = [k]$ (CONCLUDE)	

5.2 Arithmetic in $F[x]_p$

Theorem (polynomial modular arithmetic)**.** *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

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

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

$$f \text{ Mod } p = r$$

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

$$\oplus = \left\{ ((A, B), C) : \exists f, g \in F[x], A = [f], B = [g] \text{ and } C = [f + g] \right\}$$
$$\odot = \left\{ ((A, B), C) : \exists f, g \in F[x], A = [f], B = [g] \text{ and } C = [f \cdot g] \right\}$$

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

Theorem. *$\oplus, \odot$ 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:

$$[f] \oplus [g] = [f + g]$$
$$[f] \odot [g] = [f \cdot g]$$

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

Notation. As in $\mathbb{Z}_n$, we will often abbreviate $[f] \in F[x]_p$ as f. We will also often abbreviate $\oplus$ as $+$ and $\odot$ as $\times, \cdot$, or concatenation.

Theorem (F is a subring of $F[x]_p$)**.** *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*

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

Arithmetic in $F[x]_p$

modular arithmetic		modular arithmetic	
$a, b, c, d, p \in F[x]$	(SHOW)	$a, b \in F[x]$	(SHOW)
$a \underset{p}{\equiv} b$	(SHOW)		
$c \underset{p}{\equiv} d$	(SHOW)	$[a] \oplus [b] = [a + b]$	(CONCLUDE)
$a + c \underset{p}{\equiv} b + d$	(CONCLUDE)	$[a] \odot [b] = [a \cdot b]$	(CONCLUDE)
$a \cdot c \underset{p}{\equiv} b \cdot d$	(CONCLUDE)		

5.3 Finite fields

Theorem ($F[x]_p$ for irreducible p)**.** *Let F be a field, $p \in F[x]$, $\deg(p) > 0$. The following are equivalent (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, $p, f \in F[x]$, $\deg(p) > 0$, $n \in \mathbb{N}^+$, $a_0, \ldots, a_n \in F$, 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 (extension field)**.** *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 (existence of extension fields)**.** *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.*

6 Ideals and Quotient Rings

6.1 Congruence in Rings

Definition (ideal)**.** Let R be a ring and $I \subseteq R$. Then I is an **ideal** of R if and only if

1. I is a subring of R
2. $\forall r \in R, \forall a \in I, ra \in I$ and $ar \in I$

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

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

is an ideal of R.

Definition (principle and finitely generated ideals)**.** 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 (congruence modulo ideals)**.** 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. $\underset{I}{\equiv}$ *is an equivalence relation on R.*

Definition (R/I)**.** Let R be a ring and I and ideal of R. Then

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

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

Theorem (equivalence class mod I)**.** *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 mod I. The notation $a + I$ is called **coset notation** for the equivalence class $[a]$.

Remark. I hate coset notation.

Ideals and Quotient Rings

ideal	
$I \sqsubseteq R$	(show)
Let $r \in R$ and $a \in I$	(variable declaration)
$ra \in I$	(show)
$ar \in I$	(show)
$\leftarrow$	
I is an ideal of ring R	(conclude)

ideal	
I is an ideal of ring R	(show)
$I \sqsubseteq R$	(conclude)
I is an ideal of ring R	(show)
$a \in I$	(show)
$r \in R$	(show)
$ar \in I$	(conclude)
$ra \in I$	(conclude)

congruence mod an ideal	
I an ideal of ring R	(show)
$a, b \in R$	(show)
$a - b \in I$	(show)
$a \underset{I}{\equiv} b$	(conclude)

congruence mod an ideal	
I an ideal of ring R	(show)
$a, b \in R$	(show)
$a \underset{I}{\equiv} b$	(show)
$a - b \in I$	(conclude)

6.2 Arithmetic in R/I

Theorem (modular arithmetic in R/I)**.** *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

$$\oplus = \left\{ ((A, B), C) : \exists a, b \in R,\ A = [a],\ B = [b], \text{ and } C = [a + b] \right\}$$
$$\odot = \left\{ ((A, B), C) : \exists a, b \in R,\ A = [a],\ B = [b], \text{ and } C = [a \cdot b] \right\}$$

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

Theorem. *$\oplus, \odot$ are binary operators on R/I.*

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

$$[a] \oplus [b] = [a + b]$$
$$[a] \odot [b] = [a \cdot b]$$

or equivalently in left coset notation:

$$(a + I) \oplus (b + I) = (a + b) + I$$
$$(a + I) \odot (b + I) = ab + I$$

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

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

Theorem (properties of quotient rings)**.** *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. As in $\mathbb{Z}_n$, and $F[x]_p$ we will often abbreviate $[a]$ as a. We will also often abbreviate $\oplus$ as $+$ and $\odot$ as $\times, \cdot$, or concatentation.

Homomorphisms and Quotient Rings

Definition (kernel)**.** 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 (injectivity vs Kernel)**.** *Let $f : R \to S$ be a ring homomorphism.*

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

Definition (quotient map)**.** 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. *A quotient map is a surjective ring homomorphism.*

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

$$S \cong R/\operatorname{Ker}(f)$$

Arithmetic in Quotient Rings

Kernel	
$f : R \to S$ a ring homomorphism	(show)
$a \in \operatorname{Ker} f$	(show)
$f(a) = 0_R$	(conclude)

Kernel	
$f : R \to S$ a ring homomorphism	(show)
$f(a) = 0_R$	(show)
$a \in \operatorname{Ker} f$	(conclude)

Quotient Ring	
$f : R \to S$ a ring homomorphism	(show)
f is surjective	(show)
$S \cong R/\operatorname{Ker} f$	(conclude)

7 Groups

7.1 Groups

Definition (group)**.** Let G be a set and $* : G \times G \to G$ a binary operator. The pair $(G, *)$ is a **group** if and only if

1. $\forall a, b, c \in G, a * (b * c) = (a * b) * c$ (associative)
2. $\exists e \in G, \forall a \in G, a * e = a = e * a$ (identity)
3. $\forall a \in G, \exists d \in G, a * d = e = d * a$ (inverses)

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

Remark. The e in condition #3 refers to any e satisfying condition #2, so technically it should be written

$$\forall e \in G, (\forall a \in G, a * e = a = e * a) \Rightarrow (\forall a \in G, \exists d \in G, a * d = e = d * a)$$

Types of Groups

Definition (abelian group)**.** A group $(G, *)$ is **abelian** if an only if $\forall a, b \in G, a * b = b * a$ (i.e., $*$ is commutative).

Definition (finite group)**.** A group $(G, *)$ is **finite** if and only if G is a finite set.

Definition (cardinality)**.** If S is a finite set, the $\#(S)$ denotes the number of elements in the finite set S. Two sets (finite or infinite) have the same *cardinality* if an only if there is a bijection between them.

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

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

Examples of Groups

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

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

Corollary (group of units in a field)**.** *Let $(F, +, \cdot)$ be a field. Then $(F - \{0_F\}, \cdot)$ is a group.*

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

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

Definition (symmetric group)**.** 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 (symmetric group)**.** *The pair $(S_n, \circ)$ is a group.*

Notation (table notation). Let $f \in S_n$. We can describe f in **table notation** by defining

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

Theorem (cardinality of S_n)**.** $\#(S_n) = n!$

Definition (symmetry operation)**.** 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., $\forall a, b \in X, d(a,b) = d(f(a), f(b))$.

Remark. Note: in geometry a symmetry operation is called an *isometry*.

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

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

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

Theorem (group of symmetries)**.** *The pair* $(\mathrm{Sym}(X), \circ)$ *is a group.*

Definition (dihedral group)**.** Let P_n be a regular n-gon in $\mathbb{R}^2$. Define

$$D_n = \mathrm{Sym}\,(P_n)$$

$(D_n, \circ)$ is called a **dihedral group**.

Theorem (direct product)**.** *Let* $(G, *)$ *and* $(H, \cdot)$ *be groups and define* $\odot : (G \times H) \times (G \times H) \to G \times H$ *by*

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

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

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

Groups

Group		Group	
$* : G \times G \to G$	(show)	$(G*)$ is a group	(show)
$e \in G$	(show)	$a, b, c \in G$	
Let $a, b, c \in G$	(variable declaration)	.....	
$a * (b * c) = (a * b) * c$	(show)	$* : G \times G \to G$	(conclude)
$a * e = e * a = a$	(show)	$a * (b * c) = (a * b) * c$	(conclude)
$u \in G$	(show)	$e_G \in G$	(conclude)
$a * u = u * a = e$	(show)	$e_G * a = a * e_G = a$	(conclude)
$\leftarrow$		$a^{-1} \in G$	(conclude)
.....		$a * a^{-1} = e_G = a^{-1} * a = a$	(conclude)
$(G, *)$ is a group	(conclude)		

7.2 Properties of Groups

Theorem (basic group properties)**.** *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. *$\forall a, b, c \in G, ba = ca \Rightarrow b = c$*

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

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

Theorem (Inverse Theorem)**.** *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 (powers)**.** 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 laws). *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 (Additive notation). For abelian groups we sometimes write $*$ as $+$ and a^n as na and a^{-1} as ^-a.

Definition (order of an element). Let $(G,*)$ be a group, $k \in \mathbb{N}^+$, and $a \in G$. We say a has **order** k if and only if k is the smallest positive integer such that $a^k = e_G$. In other words, a has order k if

$$a^k = e_G \text{ and } \forall j \in \mathbb{N}^+, a^j = e_G \Rightarrow j \geq k$$

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

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

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

Properties of Groups

order of an element	
$n \in \mathbb{N}^+$	(show)
$a \in G$	(show)
$a^n = e_G$	(show)
Let $m \in \mathbb{N}^+$	(variable declaration)
Assume $a^m = e_G$	
$n \leq m$	(show)
$\leftarrow$	
$\leftarrow$	
a has order n	(conclude)

order of an element	
a has order n in group G	(show)
$a^n = e_G$	(conclude)
a has order n in group G	(show)
$a^m = e_G$	(show)
$n \mid m$	(conclude)

7.3 SubGroups

Definition (subgroup)**.** 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 (proper subgroup)**.** 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 ($\sqsubseteq$). We sometimes write "$H \sqsubseteq G$" as a shorthand for "H is a subgroup of G".

Theorem (subgroup theorem)**.** *Let $(G, *)$ be a group, $H \subseteq G$, and $H \neq \emptyset$. Then $(H, *)$ is a subgroup of $(G, *)$ if and only if*

1. $\forall a, b \in H, ab \in H$
2. $\forall a \in H, a^{-1} \in H$

Theorem (subgroup theorem II)**.** *Let $(G, *)$ be a group and $H \subseteq G$ a finite nonempty set. Then $(H, *)$ is a subgroup of $(G, *)$ if and only if*

$$\forall a, b \in H, ab \in H$$

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

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

Cyclic groups

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

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

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

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

Theorem. *Every subgroup of a cyclic group is cyclic.*

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

Theorem (subgroup generated by S)**.** *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.*

Notation 5. If $S \subseteq G$ we write S^{-1} for the set of all inverses of elements of S, i.e.,

$$S^{-1} = \left\{ s^{-1} : s \in S \right\}$$

Subgroups and Cyclic Groups

subgroup	
$H \subseteq G$	(SHOW)
Let $a, b \in H$	(variable declaration)
$a * b \in H$	(SHOW)
$a^{-1} \in H$	(SHOW)
$\leftarrow$	
$(H, *)$ is a subgroup of $(G, *)$	(CONCLUDE)

subgroup	
$H \subseteq G$	(SHOW)
H is finite	(SHOW)
Let $a, b \in H$	(variable declaration)
$a * b \in H$	(SHOW)
$\leftarrow$	
$(H, *)$ is a subgroup of $(G, *)$	(CONCLUDE)

subgroup generated by S	
$S \subseteq G$	(SHOW)
Let $a \in G$	(variable declaration)
$b_1, \ldots, b_n \in S \cup S^{-1}$	(SHOW)
$a = b_1 * b_2 * \cdots * b_n$	(SHOW)
$\leftarrow$	
$G = \langle S \rangle$	(CONCLUDE)

finitely generated subgroup	
$k, n \in \mathbb{N}^+$	(SHOW)
$s_1, \ldots, s_n \in G$	(SHOW)
Let $g \in G$	(variable declaration)
$g \in \langle \{ s_1, \ldots, s_n \} \rangle$	
$\leftarrow$	
$(G, *)$ is finitely generated	(CONCLUDE)

abelian	
Let $a, b \in G$	(variable declaration)
$a * b = b * a$	(SHOW)
$\leftarrow$	
$(G, *)$ is abelian	(CONCLUDE)

abelian	
$(G, *)$ is abelian	(SHOW)
$a, b \in G$	
$a * b = b * a$	(CONCLUDE)

7.4 Group Homomorphisms

Definition (group morphisms)**.** Let $(G, *), (H, \cdot)$ be groups and $f : G \to H$. The map f is a **homomorphism** (or **group homomorphism**) if and only if

$$\forall a, b \in G, f(a * b) = f(a) \cdot f(b)$$

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

Theorem (properties of group homomorphisms). *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. $(f(G),\cdot)$ *is a subgroup of* $(H,\cdot)$
4. *If f is injective then $G \cong f(G)$*

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

Corollary (Cayley's theorem for finite groups). *Every group of order n is isomorphic to a subgroup of S_n.*

Group Homomorphisms

group homomorphism	
$(G,*)$ is a group	(SHOW)
$(H,\cdot)$ is a group	(SHOW)
$f: G \to H$	(SHOW)
Let $x, y \in G$	(variable declaration)
$f(x*y) = f(x)\cdot f(y)$	(SHOW)
$\leftarrow$	
.....	
f is a group homomorphism	(CONCLUDE)

group homomorphism	
$(G,*)$ is a group	(SHOW)
$(H,\cdot)$ is a group	(SHOW)
$f: G \to H$ is a group homomorphism	(SHOW)
$x, y \in G$	(SHOW)
.....	
$f(x*y) = f(x)\cdot f(y)$	(CONCLUDE) $f(e_G) = e_H$ (CONCLUDE)
$f(x^{-1}) = f(x)^{-1}$	(CONCLUDE)

group isomorphism	
f is a group homomorphism	(SHOW)
f is bijective	(SHOW)
.....	
f is a group isomorphism	(CONCLUDE)

group isomorphism	
f is a group isomorphism	(SHOW)
.....	
f is a group homomorphism	(CONCLUDE)
f is bijective	(CONCLUDE)

7.5 (Section 8.1) Congruence and Lagrange's Theorem

Definition (congruence modulo subgroups). Let $(K,*)$ be a subgroup of $(G,*)$ and $a, b \in G$.

$$a \underset{K}{\equiv} b \Leftrightarrow a * b^{-1} \in K$$

Theorem. $\underset{K}{\equiv}$ *is an equivalence relation.*

Theorem (group cosets)**.** *Let* $(K, *)$ *be a subgroup of* $(G, *)$ *and* $a \in G$*. Then*

$$[a] = \{ ka : k \in K \}$$

Definition. Let $(K, *)$ be a subgroup of $(G, *)$ and $a \in G$. Then the set

$$Ka = \{ ka : k \in K \} = [a]$$

is called the **right coset** of a mod K (or a right coset of K). The notation Ka is called **coset notation** for the equivalence class $[a]$.

Theorem (cosets are the same size)**.** *Let* $(K, *)$ *be a subgroup of* $(G, *)$ *and* $a \in G$*. Then there exists a bijection* $f : K \to Ka$*. Thus, if* K *is finite, then every coset of* K *has the same number of elements.*

Definition. Let $(K, *)$ be a subgroup of $(G, *)$. Define $[G : K]$ to be the number of distinct right cosets of K. The number $[G : K]$ is called the **index of** K **in** G.

Theorem (Lagrange)**.** *Let* $(K, *)$ *be a subgroup of a finite group* $(G, *)$*. Then*

$$\#(G) = \#(K)[G : K]$$

Corollary (order)**.** *Let* $(G, *)$ *be a finite group of order* n*,* $a \in G$*, and* K *a subgroup of* G*.*

1. $\#(K) \mid n$
2. $|a| \mid n$
3. $a^n = e_G$

Classification of Groups I

Theorem (Classification I)**.** *If* $(G, *)$ *is a group,* $p \in \mathbb{N}$ *is prime, and* $\#(G) = p$ *then* $G \cong \mathbb{Z}_p$*.*

Theorem (Classification II)**.** *If* $(G, *)$ *is a group and* $\#(G) = 4$ *then* $G \cong \mathbb{Z}_4$ *or* $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$*.*

Theorem (Classification III). *If $(G,*)$ is a group and $\#(G) = 6$ then $G \cong \mathbb{Z}_6$ or $G \cong S_3$.*

Congruence and Lagrange's Theorem

$\underset{K}{\equiv}$		$\underset{K}{\equiv}$	
$(G,*)$ is a group	(SHOW)	$(G,*)$ is a group	(SHOW)
$(K,*)$ is a subgroup of G	(SHOW)	$(K,*)$ is a subgroup of G	(SHOW)
$a, b \in G$	(SHOW)	$a, b \in G$	(SHOW)
$a * b^{-1} \in K$	(SHOW)	$a \underset{K}{\equiv} b$	(SHOW)
$a \underset{K}{\equiv} b$	(CONCLUDE)	$a * b^{-1} \in K$	(CONCLUDE)

Lagrange		Lagrange	
$(G,*)$ is a group	(SHOW)	$(G,*)$ is a group	(SHOW)
$(K,*)$ is a subgroup of G	(SHOW)	$a \in G$	(SHOW)
$\#(G) = \#(K)[G:K]$	(CONCLUDE)	$\lvert a \rvert \mid \#(G)$	(CONCLUDE)
$\#(K) \mid \#(G)$	(CONCLUDE)	$a^{\#(G)} = e_G$	(CONCLUDE)

7.6 (Section 7.5) Symmetric and Alternating Groups

Definition (cycle notation). Let $k, n \in \mathbb{N}^+$, $a_1, \ldots, a_k \in \mathbb{I}_n$ be distinct, and $p \in S_n$. Define **cycle notation** for p by writing $p = (a_1 a_2 \cdots a_k)$ if and only if

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

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

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

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

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

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

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

Theorem (even and odd permutations). *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 can be written as a product of an odd number of transpositions.

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

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

8 Appendix: 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 - Logic Extras

proof by cases (alternate or-)	
P or Q	(SHOW)
not Q	(SHOW)
.....	
P	(CONCLUDE)

proof by cases (alternate or-)	
P or Q	(SHOW)
Assume Q	
$\rightarrow\leftarrow$	(SHOW)
$\leftarrow$	
.....	
P	(CONCLUDE)

Proof Recipes - Set Theory

empty set	
.....	
$x \notin \{\}$	(CONCLUDE)

empty set	
$A \neq \{\}$	(SHOW)
.....	
For some c,	(constant declaration)
$c \in A$	(CONCLUDE)

Proof Recipes - Set Theory (cont.)

finite set notation

$x_1 \in \{x_1, \ldots, x_n\}$ (conclude)
$x_2 \in \{x_1, \ldots, x_n\}$ (conclude)
$\vdots$
$x_n \in \{x_1, \ldots, x_n\}$ (conclude)

finite set notation

$x \in \{x_1, \ldots, x_n\}$ (show)

$x = x_1$ or $\cdots$ or $x = x_n$ (conclude)

set builder notation

$\varphi(x)$ (show)

$x \in \{ y : \varphi(y) \}$ (conclude)

set builder notation

$x \in \{ y : \varphi(y) \}$ (show)

$\varphi(x)$ (conclude)

subset

Let $x \in A$ (variable declaration)
$x \in B$ (show)
$\leftarrow$

$A \subseteq B$ (conclude)

subset

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

$x \in B$ (conclude)

set equality

Let $x \in A$ (variable declaration)
$x \in B$ (show)
$\leftarrow$
Let $y \in B$ (variable declaration)
$y \in A$ (show)
$\leftarrow$

$A = B$ (conclude)

set equality

$A = B$ (show)

$A \subseteq B$ (conclude)
$B \subseteq A$ (conclude)

power set

$B \subseteq A$ (show)

$B \in \mathcal{P}(A)$ (conclude)

power set

$B \in \mathcal{P}(A)$ (show)

$B \subseteq A$ (conclude)

intersection

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

$x \in A \cap B$ (conclude)

intersection

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

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

union

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

$x \in A \cup B$ (conclude)

union

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

$x \in A$ or $x \in B$ (conclude)

Proof Recipes - Set Theory (cont.)

set difference	
$x \in A$	(SHOW)
$x \notin B$	(SHOW)
.....	
$x \in A - B$	(CONCLUDE)

set difference	
$x \in A - B$	(SHOW)
.....	
$x \in A$	(CONCLUDE)
$x \notin B$	(CONCLUDE)

complement	
$x \notin A$	(SHOW)
.....	
$x \in A'$	(CONCLUDE)

complement	
$x \in A'$	(SHOW)
.....	
$x \notin A$	(CONCLUDE)

indexed intersection	
Let $i \in I$	(variable declaration)
$x \in A_i$	(SHOW)
$\leftarrow$	
.....	
$x \in \bigcap_{i \in I} A_i$	(CONCLUDE)

indexed intersection	
$x \in \bigcap_{i \in I} A_i$	(SHOW)
$i \in I$	(SHOW)
.....	
$x \in A_i$	(CONCLUDE)

indexed union	
$\exists i \in I, x \in A_i$	(SHOW)
.....	
$x \in \bigcup_{i \in I} A_i$	(CONCLUDE)

indexed union	
$x \in \bigcup_{i \in I} A_i$	(SHOW)
.....	
For some $j \in I$,	(constant declaration)
$x \in A_j$	(CONCLUDE)

typed forall	
Let $x \in A$	(variable declaration)
$\varphi(x)$	(SHOW)
$\leftarrow$	
.....	
$\forall x \in A, \varphi(x)$	(CONCLUDE)

typed forall	
$\forall x \in A, \varphi(x)$	(SHOW)
$a \in A$	(SHOW)
.....	
$\varphi(a)$	(CONCLUDE)

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)

Proof Recipes - Set Theory (cont.)

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)
……
$S \cap T = \{\}$ or $S = T$ (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) ← ← …… 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) ← …… 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)
  ←
←
……
$\sim$ is transitive (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)
  ←
  Assume $x \sim y$ and $y \sim z$
  $x \sim z$ (SHOW)
  ←
←
……
$\sim$ 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)