AM 106/206: Applied Algebra	**Madhu Sudan**[1]

Lecture Notes 1

August 31, 2016

1 Course Overview

- Algebra is the study of *sets* with *binary operations,* such as:

Set	Operation
integers	addition & multiplication
reals	"
$n \times n$ matrices	"
polynomials	"
vectors	addition
n-bit strings	bitwise XOR
permutations over $\{1, \ldots, n\}$	composition
symmetries of a crystal	"

- In addition to studying these specific sets & operations individually, we identify general *properties* shared by many of them, such as:
  - commutativity: $a \cdot b = b \cdot a$
  - inverses (e.g. $-a$ for addition, a^{-1} for multiplication)
  - unique factorization
- By *abstracting* such properties, algebra unifies our understanding of many disparate mathematical structures.
- Abstract algebra is useful in many science and engineering applications. Three that we will cover in this course:
  - Crystallography: the symmetry group of a crystal gives information about its physical properties.
  - Cryptography: encrypting data so that only the intended recipient can decrypt.
  - Error-correcting codes: encoding data so that it can be recovered from errors.

[1] These notes are copied mostly verbatim from the lecture notes from the Fall 2010 offering, authored by Prof. Salil Vadhan. I will attempt to update them, but apologies if some references to "my daughters Malia and Sasha" remain.

2 The Integers

- Reading: Gallian Chapter 0.
- The *integers* are $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The *natural numbers* are $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- Three (equivalent) forms of induction:
  - Well-ordering Principle: every nonempty subset of $\mathbb{N}$ has a least element.
  - Standard Induction (Thm 0.4): if $0 \in S$ and for all $n \in \mathbb{N}$ we have $n \in S \Rightarrow n+1 \in S$, then S contains all of $\mathbb{N}$. (Induction can also be started at an arbitrary integer $a \in \mathbb{Z}$ instead of 0; see text.)
  - Strong Induction (Thm 0.5): if $0 \in S$ and for all $n \in \mathbb{N}$ we have $\{0, \ldots, n\} \subseteq S \Rightarrow n+1 \in S$, then S contains all of $\mathbb{N}$.
- Induction usually formulated in terms of sequences of mathematical statements $P(0), P(1), \ldots$, e.g. $P(n) =$ "$1 + \cdots + n = n \cdot (n+1)/2$". Correspondence to versions in terms of sets (Thms 0.4,0.5) is $S = \{n : P(n) \text{ true}\}$.
- **Proposition:** For all $n \in \mathbb{N}$, $1 + 2 + \cdots + n = \frac{n \cdot (n+1)}{2}$.

  Proof by Induction:

- **Thm 0.4**: The Well-ordering Principle implies Standard Induction.

  Proof:

- Other directions are left as an exercise.