AM 106/206: Applied Algebra	**Madhu Sudan**[1]
Lecture Notes 14	
	October 25, 2017

- Reading: Gallian Chs. 12 & 13

1 General Properties of Rings, Integral Domains, and Fields

- **Def:** A *zero-divisor* in a ring R is a *nonzero* element $a \in R$ such that $ab = 0$ for some *nonzero* element $b \in R$.

- **Def:** An *integral domain* is a commutative ring with unity that has no zero-divisors.

- **Prop:** Let R be a commutative ring with unity. Then the following are equivalent:

  1. R is an integral domain, and
  2. R satisfies cancellation: if $a, b, c \in R$ satisfy $ab = ac$ and $a \neq 0$, then $b = c$.

  Proof (1⇒2):

- **Def:** A *unit* in a ring R is an element with a multiplicative inverse.

  - Not to be confused with *unity*, which is the multiplicative identity, 1.

- **Def:** A *field* is a commutative ring with unity in which all nonzero elements are units.

- **Prop:** Every field is an integral domain.
  Proof:

- **Thm:** Every finite integral domain is a field.
  Proof:

[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 old dates and contents remain.

- **General Properties of Rings (Thm 12.1):** In a ring R,

  1. For every $r \in R$, $0 \cdot r = 0$.
  2. For every $a, b \in R$, $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$.
  3. If R is a ring with unity and $0 = 1$, then $R = \{0\}$.

  Proof:

- **Def:** For a commutative ring R with unity, the *characteristic* of R is defined as follows. If 1 has finite additive order n, then the characteristic of R is defined to be n. If 1 has infinite order, then the characteristic of R is defined to be zero.

- **Thm 13.4:** The characteristic of any integral domain is either 0 or prime.
  Proof: