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

Lecture Notes 15

October 31, 2016

1 Ideals

- Reading: Gallian Ch. 14
- **Goal:** ring-theoretic analogue of normal subgroup, a set of elements we can "mod out" (set to zero) to get a factor ring.
  - Normal subgroups: since $a\varepsilon a^{-1} = \varepsilon$ in every group, we need $aNa^{-1} \subseteq N$ for N to work as an identity element in a factor group G/N.
  - Ideals: since $a \cdot 0 = 0$ in every ring, we need $aI \subseteq I$ for I to work as an identity element in a factor ring R/I.
- **Def:** Let R be a commutative ring with unity. A set $I \subseteq R$ is an *ideal* iff (a) I is a subgroup of R under addition, and (b) for every $a \in I$ and $r \in R$, we have $ar \in I$.
  - Contrast with a *subring* I, where we would only require condition (b) to hold when $r \in I$.
- **Thm 14.2 (Factor Rings):** If R is a commutative ring with unity and $I \subseteq R$ is an ideal, then the additive cosets of I form a ring, denoted R/I, under the operations $(a+I)+(b+I) = (a+b)+I$ and $(a+I)(b+I) = ab+I$
- **Examples and Non-examples:**
  - $\{0\}$.
  - R.
  - Ideals in $\mathbb{Z}$.

[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.

- $R = \mathbb{R}[x]$, $I = \{p(x) : p(11) = 0\}$.

- $R = \mathbb{R}[x]$, $I = \{p(x) : p(11) = 5\}$.

- $R = \mathbb{C}[x]$, $I = \mathbb{Q}[x]$.

- Ideals in a field.

- *Principal ideal* generated by $a \in R$: $\langle a \rangle = \{ra : r \in R\}$. (Which of above ideals are principal?)

- Ideal generated by $a_1, \ldots, a_k$: $\langle a_1, \ldots, a_k \rangle = \{r_1 a_1 + \cdots + r_k a_k : r_1, \ldots, r_k \in R\}$.

- $R = \mathbb{Z}$, $I = \langle m, n \rangle$.

- $R = \mathbb{Q}[x]$, $I = \langle x^2 - 7, x \rangle$.

- $R = \mathbb{Z}[x]$, $I = \langle 17, x \rangle$.

- **Theorem 14.4**: Let R be a commutative ring with unity and I an ideal in R. Then R/I is a field if and only if I is a *maximal ideal*. That is, $I \neq R$ but I is not contained in any ideal of R other than I and R.
  Proof:

- **Examples:**
  - Maximal Ideals in $\mathbb{Z}$:
  - $\langle 17, x\rangle$ vs. $\langle 17\rangle$ and $\langle x\rangle$ in $\mathbb{Z}[x]$.
- There is also a characterization of when R/I is an integral domain (namely, when I is a "prime ideal") but we won't cover it.

2 Homomorphisms

- Reading: Gallian Ch. 15.
- **Def:** A mapping $\varphi : R \to S$ between two rings is a *ring homomorphism* iff $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$. If φ is a bijection (one-to-one and onto), we call φ a *ring isomorphism* and write $R \cong S$.
- **Ring Analogues of Familiar Facts about Homomorphisms:**
  - The *image* $\mathrm{Im}(\varphi) \stackrel{\text{def}}{=} \varphi(R) = \{\varphi(r) : r \in R\}$ is a subring of S.
  - The *kernal* $\mathrm{Ker}(\varphi) \stackrel{\text{def}}{=} = \{r \in R : \varphi(r) = 0\}$ is an ideal of R.
  - $R/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.
  - φ is one-to-one (and thus establishes an isomorphism between R and $\mathrm{Im}(\varphi)$) iff $\mathrm{Ker}(\varphi) = \{0\}$.
- **Examples and non-examples:**
  - $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(x) = x \bmod n$.
  - $\varphi : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $\varphi(x) = (x \bmod m, x \bmod n)$.
  - $\varphi : R \to R/I$, $\varphi(a) = a + I$.
  - $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}[i]$, $\varphi(a, b) = a + bi$.

- $\varphi : M_n(\mathbb{R}) \to \mathbb{R}$, $\varphi(M) = \det M$.

- $\varphi : \mathbb{R}[x] \to \mathbb{Q}$, $\varphi(p) = p(11)$.

- $\varphi : \mathbb{R}[x] \to \mathbb{C}$, $\varphi(p) = p(i)$.

- $\varphi : \mathbb{C} \to \mathbb{C}$, $\varphi(a + bi) = a - bi$.

- $\varphi_1 \circ \varphi_2$, where φ_1, φ_2 ring homomorphisms.

- $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_{17}$, where $\varphi(p) = p(0) \bmod 17$.

- $\varphi : \mathbb{Z} \to R$, $\varphi(n) = 1 + 1 + \cdots + 1$ (n times).

- **Corollary of Last Example:** A ring of characteristic 0 contains a subring isomorphic to $\mathbb{Z}$. A ring of finite characteristic n contains a subring isomorphic to $\mathbb{Z}_n$.