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

Lecture Notes 15

October 30, 2017

# 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 $\varphi$ is a bijection (one-to-one and onto), we call $\varphi$ a *ring isomorphism* and write $R \cong S$.
- **Ring Analogues of Familiar Facts about Homomorphisms:**
  - The *image* $\mathrm{Im}(\varphi) \overset{\text{def}}{=} \varphi(R) = \{\varphi(r) : r \in R\}$ is a subring of $S$.
  - The *kernal* $\mathrm{Ker}(\varphi) \overset{\text{def}}{=} = \{r \in R : \varphi(r) = 0\}$ is an ideal of $R$.
  - $R/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.
  - $\varphi$ 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 $\varphi_1$, $\varphi_2$ 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 $\mathbb{Z}_n$.

## Addendum/Correction (added 10/31/2017)

In class on Monday, I claimed **incorrectly** that multiplication in a factor ring is defined as $(a + I)(b + I) = \{a'b' | a' \in a + I, b' \in b + I\}$. This is **not** correct. The correct definition is what was always in these (Prof. Vadhan's!) notes: $(a + I)(b + I) \stackrel{\text{def}}{=} (ab) + I$. In particular, it is **not** always the case that $(ab) + I = \{a'b' | a' \in a + I, b' \in b + I\}$. The following example might be worth going over carefully to both illustrate the example of a factor ring, and to stress the difference above.

**Example:** Let $R = \mathbb{Z}_8$ and $I = \{0, 4\}$. (The reader should verify that $I$ is an ideal in $R$).

The "cosets" of this ideal are:

- $S_0 = 0 + I = 4 + I = \{0, 4\}$,
- $S_1 = 1 + I = 5 + I = \{1, 5\}$,

- $S_2 = 2 + I = 6 + I = \{2, 6\}$,
- and $S_3 = 3 + I = 7 + I = \{3, 7\}$.

Using the definitions one can build addition and multiplication tables for the ring $R/I$, whose elements are $\{S_0, S_1, S_2, S_3\}$. For instance $S_3 + S_2 = (3+I)+(2+I) = (5+I) = S_1$. It is important that this definition be consistent. For instance, we could have used $S_3 = 7 + I$. In this case we would get $S_3 + S_2 = (7 + I) + (2 + I) = 1 + I = S_1$. (The second equality holds since we are working in $\mathbb{Z}_8$ where $7 + 2 = 1$.) The important fact is that no matter which definition of $S_3$ we use (black or red), the equation remains $S_3 + S_2 = S_1$. This is not too surprising for addition since here we could have defined $(a + I) + (b + I)$ to be $\{a' + b' | a' \in a + I, b' \in b + I\}$ — this set turns out to be $(a + b) + I$ (and we relied on this when factoring groups by normal subgroups. But with multiplication the product of sets definition is no longer correct.

| $+$ | $S_0$ | $S_1$ | $S_2$ | $S_3$ |
|---|---|---|---|---|
| $S_0$ | $S_0$ | $S_1$ | $S_2$ | $S_3$ |
| $S_1$ | $S_1$ | $S_2$ | $S_3$ | $S_0$ |
| $S_2$ | $S_2$ | $S_3$ | $S_0$ | $S_1$ |
| $S_3$ | $S_3$ | $S_0$ | $S_1$ | $S_2$ |

| $*$ | $S_0$ | $S_1$ | $S_2$ | $S_3$ |
|---|---|---|---|---|
| $S_0$ | $S_0$ | $S_0$ | $S_0$ | $S_0$ |
| $S_1$ | $S_0$ | $S_1$ | $S_2$ | $S_3$ |
| $S_2$ | $S_0$ | $S_2$ | $S_0$ | $S_2$ |
| $S_3$ | $S_0$ | $S_3$ | $S_2$ | $S_1$ |

For instance the product of elements in $S_2 \times S_2 = \{4, 12 \pmod 8, 36 \pmod 8\} = \{4\}$ which is not equal to $S_i$ for any $i \in \{0, 1, 2, 3\}$. So with mutliplication we need a lemma to prove that it is well-defined.

**Lemma 1** *Let $R$ be a commutative ring with unity and $I \subseteq R$ be an ideal of $R$. Let $a + I = a' + I$. Then for every $b \in R$, $(ab) + I = (a'b) + I$.*

**Proof:** Note that sets of the $c + I$ are cosets of $I$ in the additive group $(R, +)$ and cosets are either disjoint or identical. So to prove $(ab) + I = (a'b) + I$ it suffices to prove that they have a non-empty intersection, which in turn would be implied by the fact that $ab \in (a'b) + I$. To see this note that since $a \in a + I = a' + I$ there exists $j \in I$ such that $a = a' + j$. Thus $ab = (a' + j)b = (a'b) + j' \in (a'b) + I$ where $j' = jb \in I$ (since $I$ is closed under ring multiplication). We conclude that $ab$ is contained in both $ab + I$ and $a'b + I$ and thus the two are identical. ■