Introduction to Rings

All rings in this note are commutative.

New rings from old
Polynomial rings $R[x]$ or $R[x_1, x_2, \cdots, x_n]$
Matrix rings $\mathrm{Mat}_{n\times n}(R)$
Ring of fractions $\{(a, b) : a \in R, b \in D\}$
Group rings $RG = \{r_1g_1 + \cdots r_ng_n : r_i \in R, g_i \in G\}$
Quotient rings R/I, R ideal of R

Definition: Let R be a ring.

(1) A nonzero a of R is called a *zero divisor* if there is a nonzero element $s \in R$ such that $as = 0$ or $sa = 0$.

(2) Assume R has an identity $1 \neq 0$. An element r of R is called a *unit* in R if there is some $s \in R$ such that $rs = sr = 1$.

(3) An element $x \in R$ is called *nilpotent* if there is some $m \in \mathbb{Z}^+$ such that $x^m = 0$.

(4) An element $e \in R$ is called an *idempotent* if $e^2 = e$.

Example:

- The ring $\mathbb{Z}$ of integers has only ± 1 as its units.
- The ring $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$, if $n = r \cdot s$ then r and s are zero divisors.
  If $\gcd(a, n) = 1$ then a is a unit of $\mathbb{Z}_n$.
- $\mathbb{Z}_2[x]/(x^2 + x + 1)$ is a field with four elements.

1. Ring Homomorphisms and Quotient Rings

Theorem: There is a canonical projection, $\pi : R \to R/J$, where J is an ideal of R. The map is a surjective ring homomorphism with kernel J. Thus every ideal is the kernel of a ring homomorphism and vice versa.

There are analogues of the isomorphism theorems.

$$R \xrightarrow{\pi} R/J \qquad\qquad S \subseteq R/J$$

$$\{J \subseteq K \subseteq R\} \underset{ideal}{\longleftrightarrow} \{\overline{K} \subseteq R/J\} \qquad\qquad \pi^*(S) = \bigcup_{a+J\in S}(a + J)$$

$$\{J \subseteq S \subseteq R\} \underset{subring}{\longleftrightarrow} \{\overline{S} \subseteq R/J\}$$

Proposition: Let R and S be rings and let $\phi : R \to S$ be a homomorphism.

(1) $\ker(\phi)$ is a subring of R. Furthermore, if $\alpha \in \ker(\phi)$ then $r\alpha$ and $\alpha r \in \ker(\phi)$ for every $r \in R$, i.e., $\ker(\phi)$ is closed under multiplication by elements from R.

(2) $\mathrm{im}(\phi)$ is a subring of S, and $\mathrm{im}(\phi) \cong R/\ker(\phi)$.

Theorem: Let R be a ring.

(1) (*The Second Isomorphism Theorem for Rings*) Let $A \subseteq R$ be a subring and let B be an ideal of R. Then$A + B = \{a + b | a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.

(2) (*The Third Isomorphism Theorem for Rings*) If I and J are ideals of R with $I \subseteq J$, then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

(3) (*The Fourth or Lattice Isomorphism Theorem for Rings*) Let J be an ideal of R. The corresponding $S \longleftrightarrow S/J$ is an inclusion preserving bijection between the set of subrings S of R that contain J and the set of subrings of R/J. Furthermore, A (a subring containing J) is an ideal of R if and only if S/J is an idea of R/J.

2. Properties of Ideals

Proposition: Let R be a ring with identity 1.

(a) $I = R$ if and only if I contains a unit.

(b) If R is commutative. Then R is a field if and only if its only ideals are 0 and R.

Sketch of a proof: $u \in R \Longrightarrow \quad (u) = R \Longrightarrow uv = 1$

Ideal is similar to notion of a normal subgroup of a group in that quotient structure comes from cosets of ideals.

Definition: Let J be any subset of the ring R. $J \subseteq R$ is an ideal if

(1) J is a subgroup of $(R, +)$

(2) $\{ra : r \in R, a \in J\} \subseteq J$ (left ideal)
$\{ar : r \in R, a \in J\} \subseteq J$ (right ideal)
$\{rar' : r, r' \in R, a \in J\} \subseteq J$(*two-sided* if both left and right OR just ideal).

If J is an ideal of R, then $R/J = \{a + J : a \in R\}$ is a ring ($a + J = \{a + r : r \in J\}$).

$(R/J, +_{R/J})$ is an abelian group $\qquad (a + J) +_{R/J} (b + J) = (a + b) + J$
$(R/J, \cdot_{R/J})$ is well defined $\qquad (a +_R J) \cdot_{R/J} (b + J) = ab +_R Jb +_R aJ +_R JJ = ab + J$

Lemma: A division ring has no non-trivial ideals. If $a \neq 0 \in J$ then $a^{-1} \in R \Rightarrow raa^{-1} \in J \Rightarrow r \in J \; \forall \; r \in R$.

Wedderburn's little theorem: A finite division ring D is a field (i.e., is commutative).

Proofs generally require facts about cyclotomic polynomials.
Idea: Show that if D is a finite division ring with center Z then Z is a field and D is a v.s. over Z. Use the class equation to show $dim D$ over $Z = 1$ so $D = Z$.

Remark: Quaternions $a + bi + cj + dk \cong \left\{ \left[\begin{smallmatrix} y & z \\ \bar{z} & \bar{y} \end{smallmatrix} \right] : y, z \in \mathbb{C} \right\}$ are not $\cong \mathbb{R}Q_8$.

The notion of ideals generated by subsets of a ring is analogous to that of subgroups generated by subsets of a group. Since the intersection of any nonempty collection of ideals of R is also an ideal and $A = \{a_1, a_2, \cdots\}$ is always contained in atleast one ideal (namely R), we have

$$(A) = \bigcap_{\substack{I \text{ ideal} \\ A \subseteq I}} I,$$

i.e., (A) is the intersection of all ideals of R that contain the set A.

Definition: Let A be any subset of the ring R. Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$ i.e.,

$$RA = \{r_1a_1 + r_2a_2 + \cdots + r_na_n | r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$$

the left ideal generated by R, similarly

$$AR = \{a_1r_1 + a_2r_2 + \cdots + a_nr_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$$

right ideal generated by R and

$$RAR = \{r_1a_1r'_1 + r_2a_2r'_2 + \cdots + r_na_nr'_n | r_i, r'_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$$

(*two-sided*) ideal generated by R. If R commutative $RA = AR = RAR = (A)$.

Definition: Let I be an ideal of R with an identity $1 \neq 0$.

(1) I is *principal ideal* if it is generated by a single element.

(2) I is *finitely generated* if it is generated by a finite set of elements.

(3) $I \neq R$ is *maximal ideal* if the only ideals containing I are I and R.

(4) If R is commutative I is called *prime ideal* if $I \neq R$ and if $\forall a, b \in R$ and $ab \in I$ implies that either $a \in I$ or $b \in I$.

Proposition: If R has an identity, every ideal is contained (at least one) in a maximal ideal.

Sketch of a proof: Show if $\mathcal{S}$ is the set of ideals containing an ideal I and $\mathcal{C}$ a chain (ordered) by inclusion

$$J = \bigcup_{A \in \mathcal{C}} A$$

is a maximal ideal.

Proposition: If R is commutative, M is maximal ideal of R if and only if R/M is a field.

Sketch of a proof: By the fourth (lattice) isomorphism theorem and fact that only ideals of a field are 0 and R.

Proposition: Assume R is commutative. P is a prime ideal if and only if R/P is an integral domain.

Sketch of a proof: translate definition of prime ideal into language of quotients.

Proposition: Assume R is commutative. Every maximal ideal of R is a prime ideal.

Sketch of a proof: M maximal $\implies R/M$ is a field and integral domain.