MTHSC 851/852: Ring Theory

1: Rings, ideals, homomorphisms, & fraction fields

Def: A ring is an additive group R with an additional associative binary operation (multiplication), satisfying the distributive law:

$$x(y+z) = xy + xz \quad \text{and} \quad (y+z)x = yx + zx \quad \forall x, y, z \in R$$

Note: R is a semigp wrt multiplication.

Def: If $xy = yx$ $\forall x, y \in R$, then R is commutative.
If R has a mult. identity $1 = 1_R \neq 0$, we say that "R has identity" or "R is a ring with 1."

Def: A subring of a ring R is a subset $S \subseteq R$ that is also a ring (with the binary operation restricted to S).

Examples:

(1) $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ are commutative rings with 1.

(2) If $R = \mathbb{Z}_n$, and $\bar{a} \cdot \bar{b} := \overline{ab}$, then R is comm. with 1.

(3) Let R be any ring with 1, and $n \in \mathbb{Z}$. The set $M_n(R)$ of $n \times n$ matrices over R is a ring with $1 = I_n$.
If $n > 1$ or R is not commutative, then $M_n(R)$ is not comm.

(4) Let X be any non-empty set, A any ring. The set R of functions $f : X \to A$ is a ring by defining operations:

$$(f+g)(x) = f(x) + g(x) \qquad (fg)(x) = f(x)\,g(x).$$

(5) Let A be an abelian group, $R = \mathrm{End}(A)$, the set of endomorphisms of A. Define operations by

$$(f+g)(x) = f(x) + g(x), \qquad (fg)(x) = f(g(x)).$$

Then R is a ring with 1 (identity function), and in general, R is not commutative.

Prop: If R is a ring and $\emptyset \neq S \subseteq R$, then S is a subring of R iff $x-y \in S$ and $xy \in S$ $\forall x, y \in S$.

Pf: ($\Rightarrow$) ✓

($\Leftarrow$) If $x-y \in S$ $\forall x, y \in S$ then S is an additive subgp. ✓

Since $xy \in S$ $\forall x, y \in S$, S is closed under mult. ✓

Associative & distributive laws are inherited. ✓

$\square$

Examples (cont.)

(6) $S = 2\mathbb{Z}$ is a subring of $R = \mathbb{Z}$, but does not have 1

(7) Let $R = M_2(\mathbb{R})$, and let S be the subring $\left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, a \in \mathbb{R} \right\}$

Note: $1_R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \neq 1_S = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

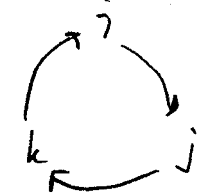
(8) Let
$$\mathbb{H} = \left\{ \begin{bmatrix} a & -b & -c & -d \\ -b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix} \right\} \subseteq M_4(\mathbb{R}).$$

Check: $\mathbb{H}$ is a subring of $M_4(\mathbb{R})$.

Let
$$i = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad j = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad k = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Then, each $x \in \mathbb{H}$ can be written uniquely as $x = a\mathbb{1} + bi + cj + dk$, $a, b, c, d \in \mathbb{R}$.

<u>Note:</u> $i^2 = j^2 = k^2 = -1$ and multiplication is "cyclic":



e.g, $ij = k$, $jk = i$, $ki = j$
$ji = -k$ $kj = -i$, $ik = -j$.

$\mathbb{H}$ is the <u>Hamiltonians</u>, or quaternions.

<u>Def:</u> If R is a ring with 1, then $x \in R$ is a <u>unit</u> if it has a multiplicative inverse. The set (group) of all units in R is denoted $\mathcal{U}(R)$.

<u>Def:</u> A nonzero elt $x \in R$ is a <u>left zero divisor</u> if $xy = 0$ for some $y \neq 0$ (and y is a right zero divisor).

<u>Note:</u> If R is commutative, then left & right zero divisors are the same.

<u>Ex:</u> (1) $\mathbb{Z}_n$ has no zero divisors iff n is prime.

(2) Let $x = \begin{bmatrix} 1 & -2 \\ -2 & 4 \end{bmatrix}$ and $y = \begin{bmatrix} 6 & 2 \\ 3 & 1 \end{bmatrix}$ in $R = M_2(\mathbb{Z})$.

Then $xy = 0$, so x is a left & y a right zero divisor.

<u>Def:</u> A comm. ring $R \neq 0$ is an <u>integral domain</u> if it has no zero divisors (equivalently, if $R \setminus \{0\}$ is a mult. semigp). If all non-zero elts have a mult. inverse, then R is a <u>division ring</u> (or <u>skew field</u>). If R is also commutative, then it is a <u>field</u>.

Note: $\mathbb{H}$ is a division ring, since if $x = a1 + bi + cj + dk \in \mathbb{H}$ and if $\bar{x} = a1 - bi - cj - dk$, then $x\bar{x} = N(x)1$, where $N(x) = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$.

Def: A ring homomorphism $f: R \longrightarrow S$ is a function satisfying $f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ $\forall x, y \in R$. As before, it is a monomorphism if f is 1-1, an epimorphism if f is onto, and an isomorphism if it is both.

Def: The kernel of a homom $f: R \longrightarrow S$ is $\ker f = \{x \in R : f(x) = 0\}$.

Check: A subring I of R is a left ideal if for any $x \in I$, and $r \in R$, $rx \in I$. Similarly, R is a right ideal if $xr \in I$.

Prop 1.2: A non-empty set $I \subseteq R$ is a (left) ideal iff $x - y \in I$, $rx \in I$ $\forall x, y \in I$ and $r \in R$.

Pf: Exercise.

Examples:

(1) $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

(2) If $R = M_2(\mathbb{Z})$, then $I = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} : a, c \in \mathbb{Z} \right\}$ is a left ideal of R, but not a right ideal of R.

Note: If an ideal I of R contains 1, then $I = R$. Thus, if I contains any unit of R, then $I = R$.

Cor 1.3: If $\{I_\alpha\}_{\alpha \in A}$ is any family of ideals of R, then $I = \bigcap \{I_\alpha : \alpha \in A\}$ is an ideal of R.

For $X \subseteq R$, the ideal generated by X is defined to be

$$(X) := \bigcap \{ I : I \supseteq X \text{ is a ideal} \}$$

<u>Def</u>: An ideal I of R is <u>principal</u> if $I = (a)$ for some $a \in R$.

If R is comm. with 1, then $(a) = \{ ra : r \in R \}$, so $(a) = Ra$.

e.g., in $R = \mathbb{Z}$, $(5) = 5\mathbb{Z}$ is principal.

Since an ideal I of R is an additive subgp, so is

$$R/I = \{ x + I : x \in R \}.$$

<u>Claim</u>: It is well-founded to define multiplication on R/I by $(x+I)(y+I) = xy + I \in R/I$.

Check this is well-defined: Suppose $x + I = r + I$ and $y + I = s + I$, i.e, $x - r,\ y - s \in I$.

Now, $xy - rs = xy - ry + ry - rs = (x-r)y + r(y-s) \in I$.

Thus $xy + I = rs + I$. ✓

Call R/I the <u>quotient ring</u>.

<u>Thm 1.4</u>: (Fundamental Homomorphism Theorem for Rings)

If R and S are rings and $f : R \to S$ a homom., with $\ker f = I$, then there is an isomorphism $g : R/I \to \mathrm{Im}(f)$ s.t. $g\eta = f$.

$$\begin{tikzcd}
R \arrow[rr, "f"] \arrow[dr, "\eta"'] & & \mathrm{Im}(f) \subseteq S \\
& R/I \arrow[ur, dashed, "g"'] &
\end{tikzcd}$$

Pf: The statement holds for the underlying additive group R, and $g(x+I) = f(x)$. Thus, it remains to show that g is a ring homomorphism:

$$g((x+I)(y+I)) = g(xy+I) = f(xy) = f(x)f(y) = g(x+I)\,g(y+I). \qquad \square$$

The other isomorphism theorems hold for rings as well. We state them here without proof. Once again, all that's needed to show is that the multiplicative structure carries through.

Prop 1.5: Suppose R & S are rings and $f: R \to S$ is an epimorphism with $\ker f = I$. Then there is a 1-1 correspondence between the set of all ideals J in S, and the set of all ideals K in R with $I \subseteq K$, given by $J \longleftrightarrow f^{-1}(J)$. In particular, each ideal in R/I is of the form K/I for some ideal $K \supseteq I$.

e.g.
$$\begin{array}{ccccc} I & \subseteq & K & \subseteq & R \\ 0 = I/I & \subseteq & K/I & \subseteq & R/I \end{array}$$

Thm 1.6: (Freshman Theorem for Rings): Suppose R is a ring, I & J ideals, and $J \subseteq I$. Then I/J is an ideal of R/J and $(R/J)/(I/J) \cong R/I$.

Thm 1.7: (Isomorphism Theorem for Rings): Suppose I and J are ideals of R. Then $I+J$ and $I \cap J$ are ideals, and $(I+J)/I \cong J/(I\cap J)$.

$$\begin{tikzcd}[column sep=small] & I+J \arrow[dl, dash] \arrow[dr, dash] & \\ I \arrow[dr, dash] & & J \arrow[dl, dash] \\ & I \cap J & \end{tikzcd}$$

Def:
- A ring R is called <u>simple</u> if its only (two-sided) ideals are 0 and R.
- An ideal I of R is <u>maximal</u> if $I \neq R$ and if $I \subseteq J \subseteq R$ for some ideal J, then $J = I$ or R.

Note: By Prop 1.5, I is maximal iff R/I is simple.

Example: If $I = (n) \subseteq \mathbb{Z}$, then I is max'l iff n is prime.

Def: A partial ordering on a set P is a relation $\leq$ that is:

(i) Reflexive: $a \leq a$
(ii) Antisymmetric: $a \leq b$ and $b \leq a \Rightarrow a = b$
(iii) Transitive: $a \leq b \leq c \Rightarrow a \leq c$.

If P has a partial ordering then it is a <u>poset</u>.

Examples:
(1) Let $P = \mathbb{Z}^+$, with $\leqslant$ (less-than-or-equal-to)
(2) Let $P = \mathbb{Z}^+$, where $d \leq n$ iff $d \mid n$.
Note: This is not a poset if $P = \mathbb{Z}$! (why?)
(3) Let P be a collection of subsets of a set S, where the relation is $\subseteq$.
(4) Any directed graph D is a poset on the vertex set, where $v_1 \leq v_2$ iff $\exists$ directed path $v_1 \longrightarrow v_2$.

Def: A <u>linear ordering</u> on a set C is a partial ordering $\leq$ in which any two elements a & b are comparable, i.e., $a \leq b$ or $b \leq a$.

Picture: $\ldots \leq a \leq b \leq c \leq d \leq \ldots$

Def: • A <u>chain</u> in a poset $\mathcal{P}$ is a nonempty subset $\mathcal{C} \subseteq \mathcal{P}$ that is linearly ordered (under $\leq$, inherited from $\mathcal{P}$).

• An <u>upper bound</u> for a chain $\mathcal{C}$ is an elt $b \in \mathcal{P}$ such that $a \leq b \ \forall a \in \mathcal{C}$ (<u>note</u>: b need not be in $\mathcal{C}$!)

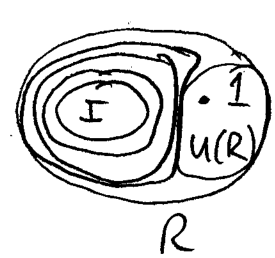
• A <u>maximal element</u> in $\mathcal{C}$ is an elt $m \in \mathcal{C}$ such that if $a \in \mathcal{C}$ and $m \leq a$, then $a = m$.

<u>Zorn's lemma</u>: If $\mathcal{P}$ is a nonempty poset in which every chain has an upper bound, then $\mathcal{P}$ has a maximal element.

This is equivalent to the <u>axiom of choice</u>.

<u>Prop 1.8</u>: If R is a ring with 1 and $I \neq R$ is an ideal, then R has a max'l ideal M with $I \subseteq M \subsetneq R$.

<u>Pf</u>: Let $\mathcal{P} = \{ J : J \text{ an ideal}, I \subseteq J \subsetneq R \}$, ordered by inclusion. If $\mathcal{C}$ is any chain in $\mathcal{P}$, then $L_{\mathcal{C}} = \bigcup \{ J : J \in \mathcal{C} \}$ is an ideal containing I, and $L_{\mathcal{C}} \neq R$, since $1 \notin L_{\mathcal{C}}$ (and $L_{\mathcal{C}} \cap U(R) = \emptyset$).



Thus, $L \in \mathcal{C}$ is an upper bound for $\mathcal{C}$.

By Zorn's lemma, $\exists$ max'l elt M in $\mathcal{P}$, which by definition is a max'l ideal. $\square$

<u>Prop 1.9</u>: Suppose R is a comm. ring with 1. Then R is simple iff R is a field.

Pf: ($\Rightarrow$) If $0 \neq a \in R$, then $(a) = R$. Thus $1 \in (a)$, so $1 = ba$ for some $b \in R$, thus $a \in U(R)$ and R is a field.

($\Leftarrow$) Suppose R is a field, and $I \subseteq R$ is a non-zero ideal. Take $a \in I$. Then $a^{-1}a \in I \Rightarrow 1 \in I \Rightarrow I = R$. $\square$

Cor: Suppose R is a comm. ring with 1. Then an ideal $I \subseteq R$ is maximal iff R/I is a field.

Pf: I max'l $\Longleftrightarrow$ R/I simple (By Correspondence thm)

$\Longleftrightarrow$ R/I a field (Prop 1.9). $\square$

Def: Let R be commutative. Then an ideal $P \subsetneq R$ is prime if $\forall a, b \in R$ with $ab \in P$, either $a \in P$ or $b \in P$.

Example: In $R = \mathbb{Z}$, the prime ideals are (p) (prime p) and (0).

Note: R is an integral domain iff 0 is a prime ideal.

The ring $\mathbb{Z}$ is an integral domain. The field $\mathbb{Q}$ is the "smallest" ring containing $\mathbb{Z}$ where every element has an inverse.

Question: Is there always such a minimal field that has this property?

Def: A field of fractions for an integral domain R is a field F_R with a monom. $\phi : R \hookrightarrow F_R$ s.t. if K is any field and $\theta : R \hookrightarrow K$ a monom, then there is a unique homom $f : F_R \longrightarrow K$ s.t. $\theta = f\phi$.

$$
\begin{tikzcd}
R \arrow[r, hook, "\phi"] \arrow[dr, "\theta"'] & F_R \arrow[d, dashed, "f"] \\
& K
\end{tikzcd}
$$

<u>Prop 1.10</u>: If an integral domain $R \neq 0$ has a field of fractions F_R, then it is unique up to isom.

<u>Thm 1.11</u>: If $R \neq 0$ is an integral domain, then R has a field of fractions.

<u>Pf</u>: Let $X = R \times (R \setminus \{0\})$.

Define an equiv. relation $(a,b) \sim (c,d)$ if $ad = bc$.

Motivation: $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$

<u>Check</u>: This is an equiv. relation (reflexive, transitive, symm).

Let $F_R = X/\sim$ (set of equiv. classes).

Denote the equiv. class containing (a,b) as a/b.

Define operations on $X/\sim$ as follows:

$$a/b + c/d = (ad+bc)/bd, \qquad (a/b)(c/d) = ac/bd.$$

<u>Check</u>: Well-defined, associative.

F_R is a comm. ring with 1, with $0 = 0/b$ for any $b \in R \setminus \{0\}$, and $-(a/b) = -a/b$, and $1 = a/a$ for any $a \in R \setminus \{0\}$.

If $a/b \neq 0$, then $a \neq 0$ so $b/a \neq 0$.

Then, $(a/b)(b/a) = 1 \in F_R$, so F_R is a field.

<u>Check universal property</u>: Define $\phi: R \longrightarrow F_R$, $\phi(r) = ra/a$.

<u>Check</u>: ϕ is a well-defined ring homom & 1-1.

Define: $f: F_R \longrightarrow K$ by $f(a/b) = \theta(a)\,\theta(b)^{-1}$ (check well-defined).

Then f is a monom since θ is, and $f\phi = \theta$ ✓

Check uniqueness. Suppose $g: F_R \longrightarrow K$ is another monomorphism s.t. $g\phi = f\phi = \Theta$. Then if $r/s \in F$, we have:

$$g(r/s) = g((ra/a)\cdot(sa/a)^{-1}) = g(ra/a)\, g(sa/a)^{-1}$$
$$= g(\phi(r))\, g(\phi(s))^{-1} = \Theta(r)\,\Theta(s)^{-1} = f(r/s)$$

Thus, $g = f$ and F_R is a field of fractions for R. $\square$

Usually, we identify r with ra/a, and view R as a subring of F_R.

Note: Up to isomorphism, F_R is a minimal field containing R.

This can be generalized a lot.

Let R be a comm. ring and $S \subseteq R$ a semigroup containing no zero divisors.

Let $X = R \times S$ and define $\sim$ on X by $(a,b) \sim (c,d)$ if $ad = bc$.

The ring $R_S := X/\sim$ is the "smallest" ring containing R such that all elements in S have an inverse in R_S. This is called the localization of of R at S.

As before, these claims must be verified (see HW #9).

Example: If $R = \mathbb{Z}$, $S = \{5^{-k} : k = 0,1,2,\ldots\}$.

Then $R_S = \{n\, 5^{-k} : n \in \mathbb{Z},\ k = 0,1,2,\ldots\}$.