MATH 494: HONORS ALGEBRA II

CONTENTS

1. JANUARY 4, 2017

Rings

Definition 1.1.

a) A **ring** is a tuple $(R, +, \cdot, 0)$ where:
  - R is a set
  - $0 \in R$
  - $+, \cdot : R \times R \to R, \quad (a, b) \mapsto a + b, a \cdot b$

  subject to:
  - $(R, +, 0)$ is an abelian group
  - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - $(a + b) \cdot c = a \cdot c + b \cdot c$
  - $a \cdot (b + c) = a \cdot b + a \cdot c$

b) A **ring with unity** is a tuple $(R, +, \cdot, 0, 1)$, where $(R, +, \cdot, 0)$ is a ring, and $1 \in R$ is subject to $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

c) A ring $(R, +, \cdot, 0)$ is called **commutative** if $ab = ba$ for all $a, b \in R$.

d) A **field** is a commutative ring with unity $(R, +, \cdot, 0, 1)$ such that $(R \backslash \{0\}, \cdot, 1)$ is a group.

Remark.

  - We don't really need to include 0,1 in notation: they are unique if they exist
  - There is a notion of a **skew field**: ring with unity $(R, +, \cdot, 0, 1)$ such that $(R \backslash \{0\}, \cdot, 1)$ is a group. (This drops the commutative condition from the definition of a field).
  - In French: *corps* is a skew field, and *corps commutatif* is a field.

Fact 1.2. *Let R be a ring. For all $a \in R$, $0 \cdot a = 0$.*

Proof. $(0 \cdot a) = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \Rightarrow 0 = 0 \cdot a$ $\square$

Example.

  - $\mathbb{Z}$ is a ring, commutative, with unity
  - $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields
  - $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ where $i^2 = j^2 = k^2 = ijk = -1$ are called the **Hamiltonian Quaternions** and are a skew-field
  - $\mathcal{C}_C(\mathbb{R}) = $ functions on $\mathbb{R}$ with compact support $(\text{supp}(f) = \overline{\{x \in \mathbb{R} \mid f(x) \neq 0\}})$ is a commutative ring without unity

- $R = \{\star\}, 0 = 1 = \star$ is the **zero ring**.

Fact 1.3. *If $(R, +, \cdot, 0, 1)$ is a ring with unity and $0 = 1$, then R is the zero ring.*

Proof. Take $a \in R$. Then $a = a \cdot 1 = a \cdot 0 = 0$ by Fact 1.2. $\square$

Convention: Unless otherwise noted, ring will refer to a commutative ring with 1.

Definition 1.4. Let R be a ring. Its **group of units** is

$$R^\times = \{a \in R \mid \exists b \in R : ab = 1\}$$

Fact 1.5.
- *For $a \in R^\times$, there is a unique $b \in R$ such that $ab = 1$. Write $b = a^{-1}$.*
- *For $a, b \in R^\times$, $a \cdot b \in R^\times$.*

Proof.
- Given b, b', we have $b = b \cdot 1 = b(ab') = (ba)b' = 1 \cdot b' = b'$.
- $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = 1$

$\square$

Example. $\mathbb{R}^\times = \mathbb{R} \backslash \{0\}$, $\mathbb{Z}^\times = \{1, -1\}$

Definition 1.6. Let R, S be rings. A **morphism** $\phi : R \to S$ is a map of sets $\varphi : R \to S$ satisfying
- $\varphi(a + b) = \varphi(a) + \varphi(b)$
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
- $\varphi(1) = 1$

Example. $\varphi : \mathbb{Z} \to \mathbb{Z}$ $u \mapsto 0$ is not a morphism of rings with 1. (it is a morphism of general rings).

Fact 1.7. *For any ring R there is a unique morphism $\varphi : \mathbb{Z} \to R$. Given $z \in \mathbb{Z}$, we write z_R, or simply z for its image under φ.*

Example. $5 \in \mathbb{Z}$, $5_\mathbb{Q} \in \mathbb{Q}$ usual number 5. $5_{\mathbb{Z}/2\mathbb{Z}} = 1_{\mathbb{Z}/2\mathbb{Z}}$

Definition 1.8. Let R be a ring. A subset $I \subset R$ is called an **ideal** if
- I is a subgroup of $(R, +, 0)$
- $a \cdot f \in I$ for all $a \in R, f \in I$.

Definition 1.9. Let R be a ring. A subset $S \subset R$ is called a subring if
- S is a subgroup of $(R, +, 0)$
- $a \cdot b \in S$ for all $a, b \in S$.
- $1 \in S$.

Remark.
- The only subset that is both a subring and an ideal is R itself. (reason: if $1 \in I$, then $a \cdot 1 \in I$ for all $a \in R$, meaning $I = R$)
- $I = \{0\}, I = R$ are always ideals.
- In rings without unity, the 2 notions align closer: ideal becomes a special case of subring as $1 \in S$ condition is dropped.

Example.
- Every subgroup of $(\mathbb{Z}, +, 0)$ is an ideal of $\mathbb{Z}$.
- If F is a field, then $\{0\}, R$ are the only ideals

- Let $R = \mathcal{C}_C(\mathbb{R}), S \in R$ subset.

$$I = \{f \in \mathcal{C}_C(\mathbb{R}) \mid f \mid_S = 0\}$$

  is an ideal

Definition 1.10. An ideal $I \in R$ is called **principal** if $I = \{a \cdot r \mid r \in R\}$ for some $a \in R$. Then a is called a **generator**.

Definition 1.11. Let $a_1, a_2, \ldots a_n \in R$. An **ideal generated by** $a_1, \ldots a_n$ is

$$(a_1, \ldots a_n) = \{a_1 r_1 + \cdots + a_n r_n \mid r_i \in R\}$$

Fact 1.12. *Given ideals $I, J \subset R$ we have*

- *$I \cap J$ is an ideal*
- *$I + J = \{a + b \mid a \in I, b \in J\}$ is an ideal*
- *$I \cdot J = \left\{ \sum\limits_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J \right\}$ is an ideal*

2. JANUARY 6, 2017

Fact 2.1. *Let $\varphi : R \to S$ be a morphism. Then*

$$\ker(\varphi) = \{x \in R \mid \varphi(x) = 0\}$$

is an ideal.

Proof. (A Pranav Exclusive) We first show that the kernel is a subgroup of $(R, +, 0)$. Well, we first show that $0 \in \ker(\varphi)$. Well,

$$\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0)$$

so, we have that $\varphi(0) = 0$ and thus $0 \in \ker(\phi)$. Next, we show that inverses are in the kernel as well. If we have that $\varphi(a) = 0$, then we have

$$0 = \varphi(0) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a) = \varphi(-a)$$

Now, we complete this step by proving closure. Assume $a, b \in \ker(\varphi)$. Then,

$$\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$$

Thus, we have that the kernel is a subgroup. Now, we verify the second condition. Fix $a \in R$ and $f \in \ker(\varphi)$. We have that

$$\phi(a \cdot f) = \phi(a) \cdot \phi(f) = \phi(a) \cdot 0 = 0$$

Thus, we have that $a \cdot f \in \ker(\varphi)$, meaning that $\ker(\varphi)$ is an ideal. $\square$

Question: Is every ideal the kernel of morphism?

Propostion 2.2. *Let R be a ring, $I \subset R$ an ideal. Let R/I be the quotient of abelian groups and $p : R \to R/I$ the canonical projection. Then there is a unique product map*

$$\cdot : R/I \times R/I \to R/I$$

making R/I into a ring such that p is a morphism.

Proof. For p to be a morphism of rings, we need

- $p(1_R) = 1_{R/I}$

- The following diagram to commute

$$
\begin{array}{ccc}
R \times R & \xrightarrow{\ \cdot_R\ } & R \\
{\scriptstyle p \times p} \downarrow & & \downarrow {\scriptstyle p} \\
R/I \times R/I & \xrightarrow{\ \cdot_{R/I}\ } & R/I
\end{array}
$$

Uniqueness of $\cdot_{R/I}$ follows from surjectivity of $p \times p$ (each element in $R/I \times R/I$ must go precisely to the result of the composition of p and $\cdot_R$)

For existence, define $1_{R/I} = p(1_R)$ and $(a + I) \cdot (b + I) \stackrel{\text{def}}{=} (a \cdot b) + I$. We have to show this is well-defined (i.e it is independent of choice of a, b).

Well, choose a', b' such that $a' + I = a + I, b' + I = b + I$. Thus, $a' = a + i$, $b' = b + j$ for some $i, j \in I$. Then
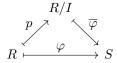
$$
(a' + I)(b' + I) = (a' \cdot b') + I = ((a + i) \cdot (b + j)) + I = (a \cdot b + a \cdot j + b \cdot i + i \cdot j) + I = a \cdot b + I
$$

as we note that $a \cdot j, b \cdot i$, and $i \cdot j$ are all in I as I is an ideal.

We have that all of the ring axioms for R/I are inherited from the ring structure on R. $\qquad\square$

Remark. $\ker(p) = I$

Theorem 2.3. *(**Homomorphism Theorem**): Let $\phi : R \to S$ be a morphism of rings, $I \subset \ker(\varphi)$ be an ideal of R. There is a unique morphism $\overline{\varphi} : R/I \to S$ such that $\overline{\varphi} \circ p = \varphi$ i.e.*

$$
\begin{array}{ccc}
 & R/I & \\
{\scriptstyle p} \nearrow & & \nwarrow {\scriptstyle \overline{\varphi}} \\
R & \xrightarrow{\ \varphi\ } & S
\end{array}
$$

commutes. Moreover, $\overline{\varphi}$ is injective $\iff$ $\ker(\varphi) = I$

Proof. All statements follow from looking at the abelian group $(R, +, 0)$ and its subgroup I, except multiplicativity of $\overline{\varphi}$.

(A Pranav Exclusive) Some justification: the uniqueness of this morphism follows because the projection map is surjective, meaning that in order for the composition to be commutative, we must have that each element in R/I maps exactly to where its associated element maps under φ. Now, the existence. We simply need to check that the map $\overline{\varphi}$ that sends $a + I$ to $\varphi(a)$ is well defined and is a morphism. We note that the additive morphism properties are inherited from the fact that φ is a morphism itself. So, we check the well-definedness of $\overline{\varphi}$. Pick 2 representatives of $a + I$, call them $a + I$ and $a' + I$. We have that $a' = a + i$ for $i \in I$. Then, we have that

$$
\overline{\varphi}(a' + I) = \overline{\varphi}(a + i + I) = \overline{\varphi}(a + I) + \overline{\varphi}(i + I) = \overline{\varphi}(a + I) + \overline{\varphi}(I) = \overline{\varphi}(a + I) + 0
$$

as we have that $\varphi(i) = 0$ for all $i \in I$ (since $I \subset \ker(\varphi)$). We finally verify the injective biconditional. Assume $\overline{\varphi}$ is injective. We already have that $I \subset \ker(\varphi)$. Now, since $\overline{\varphi}$ is injective, its kernel is trivial, and is thus the identity of R/I, namely I itself. For any $g \in \ker(\varphi)$ we note that $g + I$ must belong to the kernel of $\overline{\varphi}$, meaning that $g + I = I$ and thus $g \in I$. This gives us double containment and thus equality.

Now, assume that $\ker(\varphi) = I$. We consider $\ker(\overline{\varphi})$. This is exactly the collection $\{a + I \mid a \in \ker(\varphi)\}$. Thus, this is $\{a + I \mid a \in I\}$ and thus we have that $\ker(\overline{\varphi}) = I$. Since the kernel of $\overline{\varphi}$ is trivial, we have that $\overline{\varphi}$ is

injective.

Checking Multiplicativity: Let $A, B \in R/I$. Choose $a, b \in R$ such that $p(a) = A, p(b) = B$. Then

$$\overline{\varphi}(A \cdot B) = \overline{\varphi}(p(a) \cdot p(b)) = \overline{\varphi}(p(ab)) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(p(a))\overline{\varphi}(p(b)) = \overline{\varphi}(A)\overline{\varphi}(B)$$

$\square$

Definition 2.4. Let R be a ring.
- Let $a, b \in R$. We say that a **divides** b (denoted $a \mid b$) if there is $c \in R$ such that $ac = b$.
- We say $0 \neq a \in R$ is a **zero divisor** if there is $0 \neq b \in R$ such that $ab = 0$.
- We call R a **domain** (or **integral domain**) if it has no zero divisors.

Fact 2.5. $a \mid b \iff (b) \subset (a) \iff b \in (a)$

Proof. (A Pranav Exclusive) We first show the first forward implication. Assume that $a \mid b$. Then, there is $c \in R$ such that $ac = b$. Now, fix $g \in (b)$. It is of the form br for some $r \in R$. Thus, we have that $g = (ac)r = a(cr)$. Since $cr \in R$, we have that $g \in (a)$.

Next, we show the second forward implication. Assume that $(b) \subset (a)$. Well, $b \in (b) \subset (a)$.

Finally, we show that $b \in (a)$ implies the original condition. Well, if $b \in (a)$, then $b = ar$ for $r \in R$. This is exactly what it means for $a \mid b$!. Thus, we have shown equality of the above statements. $\square$

Fact 2.6. *(Cancellation Law) If $a \neq 0 \in R$ is not a zero divisor, then for $x, y \in R$*

$$ax = ay \Rightarrow x = y$$

Proof. $ax = ay \iff a(x - y) = 0$. $a \neq 0$ implies that $x - y = 0$ as a is not a zero divisor. $\square$

Definition 2.7. An ideal $I \subsetneq R$ is called
- **prime** if $a \cdot b \in I$ implies $a \in I$ or $b \in I$ for all $a, b \in R$.
- **maximal** if I and R are the only ideals containing I.

Example. In $R = \mathbb{Z}$, the ideals are of the form $n\mathbb{Z}$. $n\mathbb{Z}$ is prime $\iff n$ is prime or $n = 0$.

Proof. (A Pranav Exlusive). We start with the forward direction. We proceed by contrapositive. Assume tablehat $n \neq 0$ and that n is not prime. Then, n is composite (we exclude $n = 1$ as we must have a properly contained ideal by definition). Thus, we have that $n = ab$ for some $1 < a, b < n$. Note that we have $ab = n \in n\mathbb{Z}$, but we have that both a and b are less than n, and thus there is no $z \in \mathbb{Z}$ such that $nz = a$ or $nz = b$. This means that $n\mathbb{Z}$ is not prime, as we have found a, b such that $ab \in n\mathbb{Z}$ but neither a nor b are in $n\mathbb{Z}$.

Now, the reverse direction. First, we show the condition for n prime. Assume that we have $a, b \in \mathbb{Z}$ such that $ab \in n\mathbb{Z}$. This means that we have $ab = nq$ for some $q \in \mathbb{Z}$. In particular, this means that n divides the product ab. However, we note that as n is prime, we have that n must divide a or b by Euclid's lemma. Thus, we have that either $a = nr$ or $b = nr$ (or both), which implies that $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$. Next, for $n = 0$. Well, if $ab \in 0\mathbb{Z}$, then $ab = 0$. This in $\mathbb{Z}$ implies that either a or b is 0 and is also in $n\mathbb{Z}$. This completes the reverse direction. $\square$

Theorem 2.8. *Let R be a ring.*
  i) *R is a domain $\iff \{0\}$ is prime.*
 ii) *R/I is a domain $\iff I \subset R$ is a prime ideal.*
iii) *Let $\varphi : R \to S$ be a morphism, S a domain. Then $\ker(\varphi)$ is prime. The converse is true if φ is surjective.*
 iv) *R is a field $\iff \{0\}$ is maximal.*
  v) *R/I is a field $\iff I \subset R$ is a maximal ideal.*
 vi) *Every field is a domain.*

vii) Every maximal ideal is prime.

Proof. We first claim that iii) implies ii) which in turn implies i). First, for iii) implies ii), we note that letting S be R/I (which means φ is the projection map p (which is definitely surjective)) gives us ii). (We have that $\ker(p) = I$).

ii) implies i) simply by letting I be the zero ideal.

Now, we prove statement iii).

Let $a, b \in R$ such that $a \cdot b \in \ker(\varphi)$. Then $0 = \varphi(a \cdot b) = \varphi(a)\varphi(b)$. Since we have that S is a domain, then we have no zero divisors, meaning that either $\varphi(a) = 0$ or $\varphi(b) = 0$. This in turn implies that either $a \in \ker(\varphi)$ or $b \in \ker(\varphi)$, so we have show that $\ker(\varphi)$ is a prime ideal. Now, the converse assuming surjectivity. We want to show that S has no zero divisors. Well, fix $A, B \in S$ such that $A \cdot B = 0$. Since φ is surjective, we have $a, b \in R$ such that $\varphi(a) = A$ and $\varphi(b) = B$. Then, we have $0 = \varphi(a)\varphi(b) = \varphi(ab)$, meaning that ab is in $\ker(\varphi)$. Because we assume that $\ker(\varphi)$ is prime, this in turn implies that either a or b is in $\ker(\varphi)$ meaning that either $\varphi(a) = 0$ or $\varphi(b) = 0$. This means that either A or B is 0, and thus S is a domain, as desired.

Next, note that v) implies iv). This comes from letting I be the zero ideal.

The proof of v) comes from the bijection

$$\{\text{ideals in } R \text{ containing } I\} \leftrightarrow \{\text{ideals in } R/I\}$$

This is a homework problem.

Now, we show vi). Assume that F is a field. Pick $a, b \in F$ such that $a \cdot b = 0$ with $a \neq 0$. We will show that b must be 0, thereby showing that F is a domain. Well, since $a \neq 0$, and $F \backslash \{0\}$ is a group, we have that a^{-1} exists. Thus, we have that $ab = 0$ implies that $a^{-1}ab = 0$ and thus $b = 0$, as desired.

vii) follows from the facts vi), v) and ii). We have that

$$I \text{ is a maximal ideal} \overset{\text{v}}{\iff} R/I \text{ is a field} \overset{\text{vi}}{\Rightarrow} R/I \text{ is a domain} \overset{\text{ii}}{\iff} I \text{ is prime.}$$

$\square$