MATH 494: HONORS ALGEBRA II

Contents

1. January 4, 2017 — 1
2. January 6, 2017 — 3
3. January 9, 2017 — 6
4. January 11, 2017 — 8
5. January 13, 2017 — 10

1. January 4, 2017

Rings

Definition 1.1.

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

   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. $(0 \cdot a) = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \Rightarrow 0 = 0 \cdot a$ □

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 $(\operatorname{supp}(f) = \overline{\{x \in \mathbb{R} \mid f(x) \neq 0\}})$ 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. □

<u>Convention</u>: 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 $b = b \cdot 1 = b(ab') = (ba)b' = 1 \cdot b' = b'$.
- $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = 1$

□

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 <u>not</u> 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 $a_1, a_2, \dots a_n \in R$. An **ideal generated by** $a_1, \dots a_n$ is
$$(a_1, \dots a_n) = \{a_1 r_1 + \cdots + a_n r_n \mid r_i \in R\}$$

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*
- *$I \cdot J = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J \right\}$ 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. □

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

$$\begin{tikzcd} R \times R \arrow[r, mapsto, "\cdot_R"] \arrow[d, mapsto, "p \times p"'] & R \arrow[d, mapsto, "p"] \\ R/I \times R/I \arrow[r, mapsto, "\cdot_{R/I}"] & R/I \end{tikzcd}$$

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 $(a + I) \cdot (b + I) \overset{\text{def}}{=} (a \cdot b) + I$. 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. $\square$

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.*

$$\begin{tikzcd} & R/I \arrow[dr, mapsto, "\overline{\varphi}"] & \\ R \arrow[ur, mapsto, "p"] \arrow[rr, mapsto, "\varphi"] & & S \end{tikzcd}$$

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 that $n \neq 0$ 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

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

□

3. January 9, 2017

Definition 3.1. Let R b a domain. The canonical morphism $\mathbb{Z} \to R$ of Fact 1.7 has a prime ideal as its kernel. By Thm 2.8, this is of the form $p\mathbb{Z}$ with p prime of $p = 0$. We call p the **characteristic** of R.

Example.

$$\begin{array}{ll} \text{char}(\mathbb{Z}) = 0 & \text{char}(\mathbb{Z}/3\mathbb{Z}) = 3 \\ \text{char}(\mathbb{Q}) = 0 & \text{char}(\mathbb{Z}/6\mathbb{Z}) \text{ doesn't exist! } \mathbb{Z}/6\mathbb{Z} \text{ is not a domain.} \end{array}$$

Lemma. ***(Zorn's Lemma)*** *(from Artin). An* ***inductive*** *(every totally ordered subset has an upper bound) partially ordered set S has at least one maximal element.*

Theorem 3.2. *Let R be a ring. Every proper ideal is contained in a max ideal.*

Proof. Let $I \subset R$ be a proper ideal. Let $\mathcal{M}$ be the set of all proper ideals of R that contain I, with partial order given by inclusion.
Let $\mathcal{C} \subset \mathcal{M}$ be a totally ordered subset.

Claim. $J_0 = \left(\bigcup_{J \in \mathcal{C}} J \right) \in \mathcal{M}$

Proof. (of claim). We want to show that J_0 is a proper ideal containing I. First, we show it is an ideal by showing closure of the subgroup and the ideal multiplicative closure. Let $f_1, f_2 \in J_0$ and $a \in R$. Now, this means there is $J_1, J_2 \in \mathcal{C}$ such that $f_1 \in J_1$ and $f_2 \in J_2$. However, since $\mathcal{C}$ is totally ordered, we have that the larger of J_1 and J_2 contains both f_1 and f_2, meaning that we have the existence of $J \in \mathcal{C}$ such that $f_1, f_2 \in J$. Since J is an ideal, we have that $f_1 + f_2 \in J$ and that $a \cdot f_1 \in J$. This thus implies that since $J \in \mathcal{C}$, we have that $a \cdot f_1$ and $f_1 + f_2$ are both in J_0. Thus J_0 is an ideal. Since $I \in \mathcal{C}$, we also have that $I \subset J_0$. Finally, J_0 is not R, because otherwise $1 \in J_0$, which would mean that $1 \in J$ for some $J \in \mathcal{C}$. This would then imply that that $J = R$, which is not possible as J itself is a proper ideal. Thus, we have that $J_0 \in \mathcal{M}$. □

Thus, for every totally ordered subset of $\mathcal{M}$, we have the existence of an upper bound (namely J_0). This gives us, by Zorn's Lemma, that $\mathcal{M}$ has a maximal element. This maximal element is exactly what we wished to show existed. □

Definition 3.3. Let R, S be rings. Their product is the set $R \times S$ with component-wise operations

- $(r, s) + (r', s') = (r + r', s + s')$
- $(r, s) \cdot (r', s') = (r \cdot r', s \cdot s')$
- $1_{R\times S} = (1_R, 1_S), 0_{R\times S} = (0_R, 0_S)$

Remark. Given morphisms $\varphi_1 : R \to S_1, \varphi_2 : R \to S_2$, we get a unique morphism $\varphi_1 \times \varphi_2 : R \to S_1 \times S_2$.

Remark. Given $I, J \subset R$ ideals we have

$$I \cdot J \subset I \cap J \subset I, J \subset I + J$$

Definition 3.4. Two ideals $I, J \subset R$ are **coprime** if $I + J = R$.

Theorem 3.5. ***(Chinese Remainder Theorem)*** *Let R be a ring, $I_1, \dots I_n \subset R$ be pairwise coprime ideals. Then the natural morphism*

$$p : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

factors through the quotient $R/(I_1 \cap I_2 \cap \cdots \cap I_n)$ and induces an isomorphism of rings

$$\overline{p} : R/(I_1 \cap I_2 \cap \cdots \cap I_n) \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$$

Moreover, $I_1 \cdot I_2 \cdots I_n = I_1 \cap I_2 \cap \dots I_n$

Proof. As p is the natural morphism to a product of rings, we let $p = p_1 \times p_2 \cdots \times p_n$, where each p_i is the projection morphism from R to R/I_i. Now, we can say that $\ker(p) = \{r \in R \mid 0 = p_1(r), 0 = p_2(r), \dots 0 = p_n(r)\}$. Well, since each p_i by definition has kernel exactly I_i, this is the same as saying that $\ker(p) = \{r \in R \mid r \in I_1 \cap I_2 \cap \cdots \cap I_n\}$.
By the homomorphism theorem (2.3), we have that p factors through $R/I_1 \cap I_2 \cap \dots I_n$ and also induces an injective ring morphism $\overline{p} : R/I_1 \cap \cdots \cap I_n \to R/I_1 \times \dots R/I_n$.

Claim. *$\overline{p}$ is also surjective, and hence a isomorphism.*

Proof. (of claim) We note that since each of the ideals are coprime, we have that $I_1 + I_k = R$. Now, we also note that $R \cdot R = R$. Thus, we can express

$$R = (I_1 + I_2) \cdot (I_1 + I_3) \cdots (I_1 + I_n)$$

expanding the product, we note that by the earlier remark that any term containing an I_1 (which is almost all of them) will be contained in I_1. The only term that is outside arises from selecting the second term in every single term of the product, so we can write that the above expression is

$$\subset I_1 + (I_2 \cdot I_3 \cdots I_n)$$

Now, since $R \subset I_1 + (I_2 \cdot I_3 \cdots I_n)$, we can take $v_1 \in I_1$ and $u_1 \in I_2 \cdots I_n$ such that $u_1 + v_1 = 1$. Now, since $u_1 \in I_2 \cdots I_n$, $u_1 \in I_j$ for $j \neq 1$. Thus, we can say that u_1 maps to $0_{R/I_j}$ under the projection map, as it is

in the kernel.
Similarly, since $u_1 = 1 - v_1$, with $v_1 \in I_1$, we have that $u_1 \in 1 + I$, meaning that u_1 maps to $1_{R/I_1}$ under the projection map.
So, we have (abusing notation) that $u_1 = 1$ in R/I_1 and $u_1 = 0$ in R/I_j for $j \neq 1$ (really, as we showed above, it belongs to the associated cosets).
Now, we can repeat this construction with any I_i instead of I_1. Thus, we get for each such construction a $v_i \in I_i$ and $u_i \in I_1 \cdot I_2 \cdots \widehat{I_i} \cdots I_n$ With this construction, we now have the existence of the u_i that belong to the 1 coset in exactly R/I_i and the 0 coset in all remaining R/I_j. With this, we can prove surjectivity. Fix any $(x_1, \ldots x_n) \in R/I_1 \times \ldots R/I_n$. We have that there exists an associated $r_1, \ldots r_n \in R$ such that $p_1(r_1) = x_1, \ldots p_n(r_n) = x_n$. Now, if we consider the element $r \in R$ that equals $u_1r_1 + u_2r_2 \ldots u_nr_n$, note that $p(r) = (p_1(r), p_2(r) \ldots p_n(r))$. However, since the u_i map to 1 under p_i and to 0 otherwise, this maps precisely to $(x_1, \ldots x_n)$. Thus, we have that $p(r)$ maps to the desired element in the product, meaning that the associated coset will map to the desired element under $\overline{p}$. This proves surjectivity. $\square$

Thus, we have that $\overline{p}$ is an isomorphism. Now, we show the second part of part of the statement.
Well, we know by definition that $I_1 \cdot I_2 \cdots I_n \subset I_1 \cap \cdots \cap I_n$. So, we simply need to show the other containment, which we do by induction on n.
$n = 1$: $I_1 \subset I_1$.
$n = 2$: Take $u_1 \in I_1$ and $u_2 \in I_2$ such that $1 = u_1 + u_2$ (this exists as $I_1 + I_2 = R$.) Now, for any $u \in I_1 \cap I_2$, we have

$$u = u \cdot 1 = u \cdot (u_1 + u_2) = u \cdot u_1 + u \cdot u_2$$

Since $u \in I_1$ and $u \in I_2$, we have $u \cdot u_1 \in I_2 \cdot I_1$ and $u \cdot u_2 \in I_1 \cdot I_2$. Thus, we have the sum in $I_1 \cdot I_2$. This gives us $I_1 \cap I_2 \in I_1 \cdot I_2$.
Now, for general n. By the inductive hypothesis, we have that $I_1 \cap I_2 \ldots I_n \subset (I_1 \cdots I_{n-1}) \cap I_n$. From the claim above, we know that $R = (I_1 \cdot I_{n-1}) + I_n$. This implies thus that the ideals $(I_1 \cdots I_{n-1})$ and I_n are coprime. Thus, applying the $n = 2$ case on these 2 ideals, we have that $(I_1 \cdots I_{n-1}) \cap I_n \subset (I_1 \cdots I_{n-1}) \cdot I_n$, thereby proving the desired result. $\square$

4. January 11, 2017

Remark. .

- Any field is a domain.
- Any subring of a domain is a domain.
- Any subring of a field is a domain.

Is the opposite true?

Theorem 4.1. Let R be a domain.

1) There exists a pair (i, K) with K a field, $i : R \to K$ an injective morphism such that if (j, L) is another such pair, there exists a morphism $l : K \to L$ such that $j = l \circ i$, which is to say that the following diagram commutes.

$$\begin{tikzcd} & R \arrow[dl, maps to, "i"'] \arrow[dr, "j"] & \\ K \arrow[rr, maps to, "l"] & & L \end{tikzcd}$$

2) If (i', K') is another pair as in 1) there exists a unique isomorphism $\phi : K \to K'$ such that

$$\begin{tikzcd} & R \arrow[dl, mapsto, "i"'] \arrow[dr, mapsto, "i'"] & \\ K \arrow[rr, mapsto, "\phi"] & & K' \end{tikzcd}$$ *commutes.*

Remark. .

- (i, K) is an example of a "universal object"
- (j, L) is called a test object
- K is produced from R, just like the rationals are produced from the integers.

Proof. 2) Given two universal objects $(i, K), (i', K')$, apply 1) with (i, K) as the universal object, and (i', K') as a test object to get $l : K \to K'$. Do it the other way to get $l' : K' \longrightarrow K$.

Claim. $l \circ l' = id_{K'}, l' \circ l = id_K$

Proof. Note that both $l' \circ l$ and id_k make the diagrams

$$\begin{tikzcd} & R \arrow[dl, mapsto, "i"'] \arrow[dr, mapsto, "i"] & \\ K \arrow[rr, mapsto, "l' \circ l"] & & L \end{tikzcd}$$

$$\begin{tikzcd} & R \arrow[dl, mapsto, "i"'] \arrow[dr, mapsto, "i"] & \\ K \arrow[rr, mapsto, "\text{id}_K"] & & L \end{tikzcd}$$ commute.

When (i, k) is both a universal object and a test object, we get $l \circ l = \text{id}_K$. □

1) Consider the set $P = R \times R \setminus \{0\}$. Introduce the relation $(n, d) \sim (n', d') \iff nd' = n'd$.

Claim. $\sim$ *is an equivalence relation.*

Proof. Reflexive: $(n, d) \sim (n, d) \iff nd = nd$.

Symmetric $(n, d) \sim (n', d') \iff nd' = n'd \iff n'd = nd' \iff (n', d') \sim (n, d)$.

Transitive: Assume $(n_1, d_1) \sim (n_2, d_2) \sim (n_3, d_3)$. We want $(n_1, d_1) \sim (n_3, d_3)$. We have $n_1d_2 = n_2d_1, n_2d_3 = n_3d_2$ and want $n_1d_3 = n_3d_1$. We see that $n_1d_3n_2d_2 = n_1d_3n_2d_3 = n_2d_1n_3d_2 = n_3d_1n_2d_2$. Since R is a domain, n_2d_2 is not a zero-divisor. If $n_2d_2 \neq 0$, then by Fact 6, Jan 6, we get $n_1d_3 = n_3d_1$. If $n_2d_2 = 0$, then ($d_2 \neq 0$ and not a 0-divisor) $n_2 = 0$. For the same reason, $n_1 = n_3 = 0$. Again, $n_1d_3 = n_3d_1$. Either way, we are done. □

Put $K = P/\sim$. Write $[n, d]$ for the image of $(n, d) \in P$ in K. Define

$$[n, d] \cdot [n', d'] = [nn', dd']$$

$$[n, d] + [n', d'] = [nd' + n'd, dd']$$

$$0 = [0, 1], 1 = [1, 1]$$

$$i : R \to K, i(r) = [r, 1].$$

We leave as homework the verifications that $+, \cdot$ are well defined, that K is a field, and that i is a morphism. Injectivity is obvious. Given (j, L), define $l : K \longrightarrow L$ by

$$l([n,d]) = l(i(n)) \cdot l(i(d)^{-1}) = j(n)j(d)^{-1}.$$

Homework: l is well defined and a ring morphism.

□

Definition 4.2. A pair (i, K) is called a (the) field of fractions (fraction field) of R.

Definition 4.3. 1) Let R be a ring. A polynomial in T over R is a formal expression $a_nT^n + a_{n-1}T^{n-1} + \ldots + a_0, a_i \in R$.

2) Given $P(T) = a_nT^n + \ldots + a_0, Q(T) = b_nT^n + \ldots + b_0$ define

$$(P+Q)(T) = (a_n + b_n)T^n + \ldots + (a_0 + b_0)$$

$$(P \cdot Q)(T) = (c_mT^m + c_{m-1}T^{m-1} + \ldots + c_0$$

where

$$c_k = \sum_{i+j=k} a_i \cdot b_j.$$

3) Given $r \in R$ we have the constant polynomial $r : (a_nT^n + \ldots + a_0, a_0 = r, a_i = 0 \text{ for } i > 0)$. In particular, we have $0, 1$ as constant polynomials.

4) Let $R[T]$ be the set of al polynomial in T over R.

Fact 4.4. *$(R[T], +, \cdot, 0, 1)$ is a ring. Moreover $R \to R[T]$, $r \to$ constant polynomial r is an injective morphism. The proof is left as an exercise to the reader.*

Definition 4.5. Given $0 \neq P \in R[T]$, define $\deg(P) = \min\{n | a_m = 0 \forall m > n\}$, $\deg(0) = -\infty$.

Fact 4.6. *1) $deg(P+Q) \leq \max(deg(P), deg(Q))$ with equality if $deg(P) \neq deg(Q)$. 2) $deg(P \cdot Q) \leq deg(P) + deg(Q)$ with equality if the leading coefficient of P (or Q) is not a 0 divisor. 3) In particular, if R is a domain, so is $R[T]$. The proof is left as an exercise to the reader.*

5. January 13, 2017

Remark. Any $P \in R[T]$ gives a function $R \to R$ by $r \mapsto P(r) = a_nr^n + ... + a_0$. However, P is not necessarily determined by this function. For example, let $R = \mathbb{Z}/p\mathbb{Z}$ where p is a prime and $P(T) = T^p - T$. Since $x^p = x$ for all $x \in R$, P and 0 give the same function. However, $P \neq 0$.

Example.
$P = T^2 + 3T - 2$, $Q = -T^2 + 3T - 7$ gives $P + Q = 6T - 9$ $(\deg(P+Q) < \max(\deg(P), \deg(Q)))$
$R = \mathbb{Z}/4\mathbb{Z}$, $P = 2T^2 + 1$, $Q = 2T^3 + 3T$ gives $PQ = 3T$ $(\deg(PQ) < \deg(P) + \deg(Q))$

Fact 5.1. *Let $\phi : R \to S$ be a morphism and let $s \in S$. There exists a unique morphism $\phi_s : R[T] \to S$ such that $\phi_s(r) = \phi(r)$ for all $r \in R$ and $\phi_s(T) = s$.*

Proof. If ϕ_s is any such morphism then $\phi_s(a_nT^n + ... + a_0)$ must equal $\phi(a_n)s^n + ... + \phi(a_0)$. This proves uniqueness and existence (upon checking that this is a morphism). □

Example.

- If $\phi = id : R \to R$ then we get evaluation morphism $R[T] \to R$ given by $P \mapsto P(s)$.
- Let $I \subseteq R$ be an ideal and let $\phi : R \to R/I \hookrightarrow R/I[T]$ and let $s = T$. We get "reduction mod I" morphism $R[T] \to R/I[T]$.

Remark. (def. 1.5) $a \in R$ is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{N}$

Propostion 5.2. *Let $P = a_nT^n + ... + a_0 \in R[T]$. We have $P \in R[T]^\times$ iff $a_0 \in R^\times$ and $a_1, ..., a_n$ are nilpotent.*

Proof.

Assume that R is a domain. We have that P is a unit iff there exists $Q \in R[T]$ such that $PQ = 1$. By 1-11 Fact 6, $0 = deg(1) = deg(PQ) = deg(P) + deg(Q)$ (R is a domain so the leading coefficient of P (alternatively Q) is not a zero divisor). Thus $deg(P), deg(Q) = 0$. Thus $a_1, ..., a_n = 0$ are nilpotent and $a_0 \in R^\times$.

Let R be a general ring. Let $\mathcal{P} \subseteq R$ be a prime ideal. Since P is a unit in $R[T]$, the image of P in $R/\mathcal{P}[T]$ is a unit. Since $R/\mathcal{P}$ is a domain by 1-6 thm. 8, by the above argument $a_1, ..., a_n = 0_{R/\mathcal{P}}$ and thus $a_1, ..., a_n \in \mathcal{P}$. Since this holds for all $\mathcal{P}$, by HW we have that $a_1, ..., a_n$ are nilpotent.

□

Lemma 5.3. *Let $P \in R[T]$ and $r \in R$. We have $P(r) = 0$ iff $(T - r) \mid P$.*

Proof. The backward direction is clear. Apply fact 1 with $S = R[T]$, $\phi : R \hookrightarrow R[T]$, $s = T + r$ to get a morphism $R[T] \to R[T]$. This is an isomorphism with inverse given by the same construction with $s = T - r$. Under this isomorphism, $P \mapsto Q$ with $Q(0) = 0$. Thus $Q(T) = b_nT^n + ... + b_1T$ so $T \mid Q$. Taking the preimage under the above isomorphism, we have $(T - r) \mid P$.

Gitlin's thoughts: The constructed isomorphism can be thought of as the map $R[T] \to R[T]$ which "replaces every T with $T + r$." Thus $Q(x) = P(x + r)$ for all $x \in R$. In particular, $Q(0) = P(r)$ which is 0. The inverse map is the map $R[T] \to R[T]$ which "replaces every T with $T - r$." In particular, the preimage of $Q(T) = b_nT^n + ... + b_1T$ is $b_n(T - r)^n + ... + b_1(T - r)$.

□

Propostion 5.4. *Let $P, D \in R[T]$. Assume that $D \neq 0$ and that the leading coefficient of D is a unit. There exist unique $Q, Z \in R[T]$ with $deg(Z) < deg(D)$ such that $P = QD + Z$.*

Proof.

Choose Q so that $deg(Z)$ is minimal where $Z = P - QD$. We claim $deg(Z) < deg(D)$. Suppose not. Let $D = d_nT^n + ... + d_0$ and $Z = z_mT^m + ... + z_0$ with $m \geq n$. Note that $P - (Q + z_md_n^{-1}T^{m-n})D = Z - (z_md_n^{-1}T^{m-n})D$ has degree less than $deg(Z)$, contradicting the minimality of Z. This shows existence.

Gitlin's thoughts: The set of "candidates" is the set of elements of $R[T]$ that have the form $P - *D$ where $*$ varies over $R[T]$. Clearly $P - (Q + z_md_n^{-1}T^{m-n})D$ is a candidate. Furthermore, the leading term z_mT^m of Z cancels with the leading term $z_md_n^{-1}T^{m-n} \cdot d_nT^n = z_mT^m$ of $(z_md_n^{-1}T^{m-n})D$ in the subtraction $Z - (z_md_n^{-1}T^{m-n})D$ so the degree of Z is at least one more than the degree of $Z - (z_md_n^{-1}T^{m-n})D$.

Let Q', Z' be another such pair. We have $QD + Z = P = Q'D + Z'$ so $(Q - Q')D = Z' - Z$. Thus (1-11 fact 6) $deg(D) > \max(deg(Z'), deg(Z)) \geq deg(Z' - Z) = deg((Q - Q')D) = deg(Q - Q') + deg(D)$ (the leading coefficient of D is a unit and thus not a divisor of zero). This means $deg(Q - Q') = -\infty$ so $Q - Q' = 0$ so $Q = Q'$. Thus $Z = P - QD = P - Q'D = Z'$. This shows uniqueness.

Gitlin's thoughts: My uniqueness proof likely differs from the one given in class. Sorry Tasho. I couldn't follow your inequalities.

□