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
   - $0 \in R$
   - $+, \cdot : R \times R \to R, \qquad (a, b) \mapsto a + b, a \cdot b$

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

<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 $b = b \cdot 1 = b(ab') = (ba)b' = 1 \cdot b' = b'$.
- $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = 1$

$\square$

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

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

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. □

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.*

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

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

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

□

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. □

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. □

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. □

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 **??** has a prime ideal as its kernel. By Thm **??**, 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 (**??**), 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 $(x_1, \dots x_n) \in R/I_1 \times \dots R/I_n$. We have that there exists an associated $r_1, \dots r_n \in R$ such that $p_1(r_1) = x_1, \dots p_n(r_n) = x_n$. Now, if we consider the element $r \in R$ that equals $u_1 r_1 + u_2 r_2 \dots u_n r_n$, note that $p(r) = (p_1(r), p_2(r) \dots p_n(r))$. However, since the u_i map to 1 under p_i and to 0 otherwise, this maps

precisely to $(x_1, \dots x_n)$. 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 $I_1 \cap I_2 \dots I_n \subset (I_1 \cdots I_{n-1}) \cap I_n$. 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.

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

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

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

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

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

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 $Q(T) = b_n T^n + ... + b_1 T$ 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 $Q(T) = b_n T^n + ... + b_1 T$ 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 $D = d_n T^n + ... + d_0$ and $Z = z_m T^m + ... + z_0$ with $m \geq n$. Note that $P - (Q + z_m d_n^{-1} T^{m-n})D = Z - (z_m d_n^{-1} T^{m-n})D$ 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 $P - (Q + z_m d_n^{-1} T^{m-n})D$ is a candidate. Furthermore, the leading term $z_m T^m$ of Z cancels with the leading term $z_m d_n^{-1} T^{m-n} \cdot d_n T^n = z_m T^m$ of $(z_m d_n^{-1} T^{m-n})D$ in the subtraction $Z - (z_m d_n^{-1} T^{m-n})D$ so the degree of Z is at least one more than the degree of $Z - (z_m d_n^{-1} T^{m-n})D$.

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.

□

6. January 18, 2017

Lemma 6.1. *(This is Lemma 3 from Jan. 13) Given $P \in R[T], r \in R$, then $P(r) = 0 \Leftrightarrow (T - r) \mid P$.*

Propostion 6.2. *(This is Proposition 4 from Jan. 13) Given $P, D \in R[T]$ such that D has a unit as a leading coefficient, there exists unique $Q, Z \in R[T]$ with $deg(Z) < deg(D)$ such that $P = DQ + Z$.*

Proof. This proof rehashes the one given in class by Tasho to rectify any mistakes or lack of clarity in the one given on Jan. 13 (no offense Gitlin). Following the proof given on Jan. 13 (before the proof of uniqueness), we have the following string of inequalities:

$$deg(D) > deg(Z) \geq deg(Z - Z') = deg(D) + deg(Q - Q').$$

This implies that $deg(Q - Q') = -\infty = deg(Z - Z')$, so $Q - Q' = Z - Z' = 0$, i.e. $Q = Q'$ and $Z = Z'$, completing the proof. □

The following is a proof Tasho gave of Lemma 3 from Jan. 13 which utilizes Proposition 4 from Jan. 13.

Proof. As per Proposition 4, write $P(T) = (T - r) \cdot Q(T) + Z(T)$ with $deg(Z) < deg(T - r) = 1 \Rightarrow Z \in R$. We have then $P(r) = (r - r) \cdot Q(r) + Z(r) = Z$, but since $P(r) = 0$ we have now $Z = 0 \Leftrightarrow (T - r) \mid P$. □

Definition 6.3. Let $P \in R[T], r \in R$. Define **the multiplicity of r in P** by $\max\{n \in \mathbb{N} \colon (T - r)^n \mid P\}$.

Corollary 1. *Let R be a domain. Then $0 \neq P \in R[T]$ has at most $deg(P)$-many zeroes, counted with multiplicity.*

Proof. We induct on $deg(P)$. As a base case take $deg(P) = 0$: $P \in R$ has no zeroes, as required. For an inductive step assume that the statement holds for all polynomials of degree less than $deg(P)$. If P has no zeroes, we are done. Otherwise let $r \in R$ be a zero of P. By Lemma 3 from Jan. 13, $P = (T - r) \cdot Q(T)$ for some $Q \in R[T]$ with $deg(Q) < deg(P)$. By inductive hypothesis Q has at most $deg(Q) = deg(P) - 1$ zeroes. Since R is a domain, a zero of P is either r or a zero of Q, so P has at most $deg(Q) + 1 = deg(P)$ zeroes, as required. This completes the inductive step, and thus the proof. $\square$

The following example answers the question "does this fail when R is not a domain?":

Example. If $R = \mathbb{Z}/6\mathbb{Z}$ and we define $P(T) = 3T$, then $\#\{\text{zeroes of } P\} = \#\{0, 2\} > 1 = deg(P)$.

Definition 6.4. A field k is called **algebraically closed** provided that every nonconstant $P \in k[T]$ has a zero.

Propostion 6.5. *Let k be an algebraically closed field, $P \in k[T]$. Then*

$$P(T) = c \cdot (T - r_1)^{m_1} \cdots (T - r_n)^{m_n}$$

for $c, r_1, ..., r_n \in k, m_1, ..., m_n \in \mathbb{N}$.

Proof. This is proved on Homework 2. (Future readers: feel free to input the proof here when completed.) $\square$

Definition 6.6. Define $\mathbf{R}[\mathbf{T_1}, ..., \mathbf{T_n}]$ recursively as $(R[T_1, ..., T_{n-1}])[T_n]$. More concretely: a **monomial** in $T_1, ..., T_n$ is an expression $T_1^{m_1} \cdots T_n^{m_n}$, for $m_i \in \mathbb{N}$. A polynomial in $T_1, ..., T_n$ with coefficients in R is an R-linear combination of monomials; the set of all polynomials in $T_1, ..., T_n$ is $R[T_1, ..., T_n]$.

Recall: $P \in R[T] \leftrightarrow$ an eventually-zero sequence $(a_0, a_1, ...) \leftrightarrow$ a map $\mathbb{N} \to R$ with finite support. So $P \in R[T_1, ..., T_n] \leftrightarrow$ a map $\mathbb{N}^n \to R$ with finite support, so we may think of a polynomial $P \in R[T_1, ..., T_n]$ as

$$P(T) = \sum_{c_i \in \mathbb{N}} a_{c_1, ..., c_n} \cdot T_1^{c_1} \cdots T_n^{c_n}.$$

Fact 6.7. *Given a ring morphism $\phi \colon R \to S, s_1, ..., s_n \in S$, there exists a unique ring morphism*

$$\phi_{s_1, ..., s_n} \colon R[T_1, ..., T_n] \to S$$

such that $\phi_{s_1, ..., s_n}(r) = \phi(r)$ for $r \in R$, and $\phi_{s_1, ..., s_n}(T_i) = s_i$.

Proof. We induct on n. As a base case let $s \in S$. Fact 5.1, Jan. 13 above guarantees the existence of a unique morphism $\phi_s \colon R[T] \to S$ with the given properties. For an inductive case assume the statement holds for $n - 1$. By inductive hypothesis we have a unique morphism $\phi_{s_1, ..., s_{n-1}} \colon R[T] \to S$ satisfying the given properties. Applying the base case to $\phi_{s_1, ..., s_{n-1}}$ with $s = s_n$ gives the desired (unique) morphism, completing the inductive step and thus the proof. $\square$

Definition 6.8.

- The image of $\phi_{s_1, ..., s_n}$ is called the R**-subalgebra of** S **generated by** $s_1, ..., s_n$
- $s_1, ..., s_n$ are called **algebraically independent** provided that $\phi_{s_1, ..., s_n}$ is injective.

To gain some intuition about algebraic independence, consider the algebraic relation

$$r_1 s_1^{m_{1,1}} \cdots s_n^{m_{1,n}} + \cdots + r_n s_1^{m_{n,1}} \cdots s_n^{m_{n,n}} = 0.$$

Taking preimages under $\phi_{s_1,\dots,s_n}$ we have

$$\begin{aligned}\phi^{-1}_{s_1,\dots,s_n}(r_1 s_1^{m_{1,1}} \cdots + s_n^{m_{1,n}} + \cdots + r_n s_1^{m_{n,1}} \cdots s_n^{m_{n,n}}) &\in \phi^{-1}_{s_1,\dots,s_n}(0) = \ker(\phi_{s_1,\dots,s_n}) \\ \Rightarrow \phi^{-1}(r_1)T_1^{m_{1,1}} \cdots T_n^{m_{1,n}} + \cdots + \phi^{-1}(r_n)T_1^{m_{n,1}} \cdots T_n^{m_{n,n}} &\in \ker(\phi_{s_1,\dots,s_n})\end{aligned}$$

thus if there exists such a relation that is nontrivial, there is a nonzero element in $\ker(\phi_{s_1,\dots,s_n})$, so it is not injective. (Note from Ben: this seems to assume that the coefficients r_i are in the image of ϕ, which is not generally true. Will bring up with Tasho and edit as necessary.)

Definition 6.9. Let R be a ring, $0 \neq a \in R$ not a unit.

- a is called **irreducible** provided that $a = bc \Rightarrow b \in R^\times$ or $c \in R^\times$.
- a is called **prime** provided that $a = bc \Rightarrow a \mid b$ or $a \mid c$.

Fact 6.10. *R a domain $\Rightarrow$ every prime element of R is irreducible.*

Proof. Let $p \in R$ be prime and write $p = ab$. Then without loss of generality we have $p \mid a \Rightarrow a = pc$ for some $c \in R$, so we may rewrite $p = pcb$, so $p(1 - bc) = 0$. Since R is a domain and $p \neq 0$, we have $1 = bc$, so $c = b^{-1} \Leftrightarrow b \in R^\times$. □

Remark.

- If R is not a domain, prime elements need not be irreducible (see Homework 2).
- Even if R is a domain, irreducible elements need not be prime (see Homework 2).

Definition 6.11. Let R be a domain.

(1) R **has factorization** provided that every $0 \neq r \in R$ can be written $\epsilon \cdot u_1 \cdots u_k$ with $\epsilon \in R^\times$ and $u_i \in R$ irreducible.
(2) Write $a \sim b \Leftrightarrow a = \epsilon \cdot b, \epsilon \in R^\times$.
(3) R has **unique factorization** provided that R has factorization and if $\epsilon \cdot u_1 \cdots u_k = \mu \cdot v_1 \cdots v_m$ then $k = m$ and there exists a permutation $\sigma \in S_m$ such that $u_i \sim v_{\sigma(i)}$.
(4) Such an R is called a **unique factorization domain**, or UFD.

7. January 20, 2017

Propostion 7.1. *Let R be a domain with factorization. Then R has unique factorization if and only if every irreducible element is prime.*

Proof. Say R has unique factorization. Let p be irreducible. We will show that p is prime. Let $a, b \in R$ be such that $p \mid ab$. Using factorization, we write that $a = \zeta u_1 u_2 \cdots u_k$, $b = \mu v_1 \cdots v_l$, and that $\frac{ab}{p} = \alpha w_1 w_2 \cdots w_m$. From the fact that $\frac{ab}{p} \cdot p = ab$, we have that $\alpha p w_1 w_2 \cdots w_m = \zeta \mu u_1 \cdots u_k v_1 \cdots v_l$. By uniqueness of factorization, we have that these expressions are permutations upto multiplication by units, so we have that $p \sim u_i$ or $p \sim v_j$. In the first case, we have that $p \mid a$ and in the second, we have that $p \mid b$.
Assume now that every irreducible is prime. We will show uniqueness by induction on the length of the factorization.
Length = 0: Then, a is a unit, so a is not divisible by any irreducible.
Assume now that the statement holds for a length k factorization. Assume now that we have

$$a = \zeta u_1 \cdots u_{k+1} = \mu v_1 \cdots v_l$$

Now u_{k+1} divides $v_1 \cdots v_l$. But since u_{k+1} is prime, $u_{k+1} \mid v_j$ for some $1 \leq j \leq l$. Reordering the factors, we have that $u_{k+1} \mid v_l$. Since v_l is irreducible, this thus implies that if $u_{k+1} x = v_l$, x must be a unit, and thus $v_l \sim u_{k+1}$. Furthermore, we can write that $\zeta u_1 \cdots u_k = \mu \left(\frac{v_l}{u_{k+1}}\right) v_1 \cdots v_{l-1}$. Applying the inductive hypothesis, we have $l-1=k$ and the the first k terms are simply a permutation of each other, while the last is simply a unit scaling away from the other. Thus, these are the same factorization. $\square$

Definition 7.2. A ring is called **principal**, if every ideal is principal. If, in addition, the ring is a domain, it is a **Prinicipal Ideal Domain**, or **PID**.

Example. $\mathbb{Z}$ is a PID. $\mathbb{Z}/n\mathbb{Z}$ are principal, any field is a PID. Quotients and products of principal rings are principals.

Theorem 7.3. *Every PID is a UFD*

Proof. Let R be a PID. We first show the existence of factorization. Say that $a \in R$, $a \neq 0$, $a \in R^\times$, and has no factorization. Then, a is not irreducible, (as otherwise, it itself is a factorization). So, we can right that $a = a_0 = a_1 b_1$. However, note that one of these must not have a factorization, as otherwise the product of their factorizations is a factorization of R. So, WoLOG assume that a_1 does not have a factorization. Again, a_1 is not irreducible, and we write $a_1 = a_2 b_2$. Recursively applying this argument, we have that $a_0 = a_1 a_2 a_3 \ldots$ an infinite sequence with $a_i \neq 0$, $a_i \notin R^\times$ and $a_i \not\sim a_{i+1}$, and $a_{i+1} \mid a_i$ In terms of the ideals, we have that

$$(a_0) \subsetneq (a_1) \subsetneq \ldots$$

Now, we consider $I = \bigcup_{i=0}^{\infty} (a_i)$. Since we have a nested sequence of ideals, we have that I itself is an ideal. We have that R is a principal ideal, which means that $I = (c)$ for some $c \in R$. This means though that $c \in I$, which means that $c \in (a_k)$ for some $k \in \mathbb{N}$. However, this means that for any $n \geq k$, we have that $(c) \subset (a_k) \subset I = (c)$, meaning that each $(a_n) = (c)$. However, we assumed proper inclusion above, and this is thus a contradiction. Thus, we have factorization.

Next, we verify uniqueness. We can show this by showing that every irreducible is prime. Let u be an irreducible. We want to show it is prime, so assume that $u \mid ab$. Assume that $u \nmid a$. We will show that $u \mid b$. Since we have that $u \nmid a$, we have that $u \notin (a)$, so we have that $(a) \subsetneq (a,u)$. Since R is principal, we have that $(u,a) = (d)$. Since $u \in (d)$ we have that $d \mid u$. However, since u is irreducible, d must be a unit, or $d \sim u$. We know because $(u) \subsetneq (u,a)$, we have that $d \sim u$ is impossible. Thus, assume that d is a unit. This means though that $(u,a) = R$. This means that we have $1 \in R$, so $1 = \alpha u + \beta a$ (this is what it means to be in (u,a)). Scaling this equality by b, we have that $b = b\alpha u + \beta(ab)$. Now, since $u \mid ab$ and $u \mid u$, $u \mid b$, as desired. $\square$

Definition 7.4. A **Euclidean Domain** is a pair (R,H), where R is a domain, and $H : R \setminus \{0\} \to \mathbb{N}$ is a function such that

1. $H(ab) \geq H(a)$
2. Given $X, d \in R$ with $d \neq 0$, there are $q, r \in R$ such that
   (a) $X = qd + r$
   (b) either $r = 0$ or $H(r) < H(d)$

Example. If F is a field, then $(F[T], deg)$ is a Euclidean domain.

Propostion 7.5. *Every Euclidean domain is a PID.*

Proof. Let $I \subset R$ be an ideal. WoLOG, $I \neq \{0\}$. Choose $d \in I$ such that $H(d)$ is minimal. To show that $I = (d)$, let $a \in I$ and take $q, r \in R$ such that $a = qd + r$. Then, $r = a - qd \in I$. If $r \neq 0$, we have that $H(r) < H(d)$, contradicting the minimality of d. Thus $r = 0$, and $a = qd$. Thus, every ideal is of the form (d), showing it is principal. $\square$

Corollary 2. *If F is a field, $F[T]$ is a PID, and hence a UFD.*

Definition 7.6. Let R be a UFD. We call $0 \neq P \in R[T]$ **primitive** if $a \in R$ with $a \mid P$ means that $a \in R^{\times}$.

Remark. This is equivalent to no irreducible $p \in R$ divides all the coefficients of P. Intuitively, we can say the "gcd" of the coefficients of P is 1.

Lemma 7.7. ***(Gauss)*** *If P, Q are primitive, so is PQ.*

Proof. Let $P \neq 0$, $Q \neq 0$ such that PQ is not primitive. Let $p \in R$ prime such that $p \mid PQ$. Thus, PQ becomes 0 under the $R[T] \to (R/(p))[T]$.
But $R/(p)$ is a domain by **??**, and thus, by **??**, we have that $(R/(p))[T]$ is also a domain. Thus, we have that either P or Q is 0 in $(R/(p))[T]$, meaning it is also divisible p, as desired. □

8. January 23, 2017

Recall: $P \in R[T]$ is primitive if $a|P \implies a \in R^{\times}$. Lemma 8 (Gauss): P, Q primitive $\implies P \cdot Q$ primitive. R is a UFD, F is it's fraction field

Lemma 8.1. *Let $P, Q \in R[T], P$ primitive. If $Q = a \cdot P, a \in F$, then $a \in R$.*

Proof. Write $a = \frac{n}{d}$ with $n, d \in R$. Decompose $n = \epsilon n_1, \ldots, n_k, d = \mu v_1, \ldots, v_k$ into irreducibles. We may assume $n_i \sim v_j$ for i, j. Then $\mu v_1, \ldots, v_k Q = \epsilon n_1 \ldots n_k P$. So $v_1 | n_1 \ldots n_k a_i$ for all i, where $P(T) = a_n T^n + \ldots + a_0$. Since v_1 is prime, and n_i are irreducible, and $v_1 \nsim u_1, \ldots, u_k$, so $v_1 | a_i$ for all i. This contradicts primitivity of P. □

Theorem 8.2. *The ring $R[T]$ is a UFD and its irreducible elements are (1) $p \in R$ irreducible (2) $P \in R[T]$ primitive, and irreducible in $F[T]$.*

Proof. Step 1: The above elements are irreducible. Given $p \in R$ irreducible, write $p = PQ$, with $P, Q \in R[T]$. Since R is a domain, we have $0 = \deg(P) = \deg(P) + \deg(Q)$, so $P, Q \in R$. But then either $P \in R^{\times}$ or $Q \in R^{\times}$. Let $P \in R[T]$ be primitive, irreducible in $F[T]$. Write $P = QS$ with $Q, S \in R[T]$. Since P is irreducible in $F[T]$, either Q or S lies in $F[T]^{\times} = F^{\times}$ by proposition 2, Jan 13th. Say WOLOG $S = R[T] \cap F^{\times} = R \setminus [0]$. Then $S^{-1} P = Q$. By lemma 1, $S^{-1} \in R$. So $S \in R^{\times}$. Step 2: Every element of $R[T]$ has a decompose with factors as in 1), 2). Take $P \in R[T]$. Decompose P as an element of $F[T]$. $P = c \cdot \tilde{Q}_1, \ldots, \tilde{Q}_n, c \in F^{\times}, \tilde{Q}_i \in F[T]$ irreducible. By lemma 3, write $\tilde{Q}_I = c_i \cdot Q_i$ with $c_i \in F^{\times}, Q_i \in R[T]$ primitive. Thus $P = c \cdot c_1, \ldots c_n \cdot Q_1, \ldots Q_n$. By Gauss lemma, $Q_1, \ldots Q_n$ is primitive, so by lemma 1, $a \in R$. Factor $a = \epsilon n_1, \ldots n_k$ in R.

Remark: This shows in particular, that (1)+(2) are all the irreducible elements in $R[T]$. Uniqueness of factorization Let $\epsilon n_1, \ldots, n_k P_1, \ldots, P_n = \mu v_1 \ldots v_l Q_1 - Q_m$ with u_i, v_j as in (1) and P_i, Q_j as in (2). Uniqueness in $F[T]$ tells us $n > m$, and after reordering, $P_i = c_i Q_i$ with $c_i \in F^{\times}$. Applying lemma 1 to $P_i = c P_i Q_i$ and $c_i^{-1} P_i = Q_i$ to see $c_i \in R^{\times}$. Thus $P_i \sim Q_i$ is $R[T]$. Then $\epsilon n_1, \ldots, n_k = \mu \frac{Q_1 \ldots Q_n}{P_1 \ldots P_n} \cdot v_1 \ldots_l$ and uniqueness in R gives us $k = l$ and $n_i \sim v_i$ after reordering. □

Lemma 8.3. *Let $0 \neq P \in F[T]$. There exists $c \in F^{\times}$ such that $cP \in R[T]$ primitive.*

Proof. There is $a \in R$ such that $aP \in R[T]$. Let d be a gcd of all coefficients of aP. Then $d|ap$ and $ad^{-1}P \in R[T]$ primitive. □

Lemma 8.4. *Let $P, Q \in R[T], P$ primitive. Then P/Q in $R[T] \iff P/Q \in F[T]$.*

Proof. $\implies$: trivial. $\impliedby$: Let $Q = P\tilde{S}$ with $\tilde{S} \in F[T]$. By lemma 3, $\tilde{S} = aS, a \in F^{\times}$. $S \in R[T]$ primitive. So $Q = aPS$. By Gauss lemma, PS is primitive. By lemma 1, $a \in R$, then $\tilde{S} = aS \in R[T]$. □

9. January 25, 2017

Propostion 9.1. *(Eisenstein Criterion) Let R be a UFD, F its fraction field (as before). Let $P(T) = a_nT^n + \ldots + a_0 \in R[T]$. If $p \in R$ prime such that p does not divide a_n, then $p|a_{n-1}, \ldots, a_0$ and p^2 does not divide p_0 then P is irreducible in $F[T]$.*

Proof. Suppose not. By Thm 2 last time we have that P is not irreducible in $R[T] \Longrightarrow P = Q \cdot S$ where $Q, S \in R[T]$. Let $\bar{P}, \bar{Q}, \bar{S}$ be images in $(R/(P))[T]$. Write $Q(T) = b_mT^m + \ldots + b_0, S(T) = c_jT^j + \ldots + c_0$. Then $\bar{P}(T)(= \bar{a_n}T^n) = Q(T)(= \bar{b_k}T^k) \cdot \bar{S}(T)(= \bar{c_j}T^j)$ with $k + j = n$ since $R/(P)$ is a domain since P is prime). Then $p|b_0, p|c_0 \Longrightarrow p^2|a_0 = b_0c_0$ which is a contradiction. ☐

Cyclotomic Polynomials:

Definition 9.2. For $n \in \mathbf{N}$, the nth cyclotomic polynomial is $\Phi_n(T) = \Pi^n_{gcd(k,n)=1,k=1}(T - e^{2\pi ik/n})$.

Propostion 9.3. *Φ is monic and has integer coefficients.*

Proof. Induction on $n \in \mathbf{N}$.

$n = 1 : T - 1, n = 2 : T + 1$

$k < n \Longrightarrow k = n : T^n - 1 = \Pi^n_{k=1}(T - e^{2\pi ik/n}) = \Pi_{d|n}\Phi_d(T)$. By induction, $\Phi_d \in \mathbf{Z}[T]$ and monic for $d|n, d \neq n$. In particular, these Φ_d are primitive, so Gauss' lemma implies that $\Pi_{d|n,d\neq n}\Phi_d =: P$ is primitive. $T^n - 1 = \Phi_n(T) \cdot P(T)$ in $\mathbf{C}[T]$. So $P|T^n - 1$ in $\mathbf{C}[T] \Longrightarrow P|T^n - 1$ in $\mathbf{Q}[T]$. By lemma 4 of January 23, $P|T^n - 1$ in $\mathbf{Z}[T]$. ☐

Propostion 9.4. *If $p \in \mathbf{N}$ prime, then Φ_p is irreducible.*

Proof. $T^p - 1 = \Phi_1 \cdot \Phi_p = (T - 1) \cdot \Phi_p$ and $T^p - 1 = (T - 1)(T^{p-1} + T^{p-2} + \ldots + 1) \Longrightarrow \Phi_p = T^{p-1} + \ldots + 1$. Reduce mod p: $(T - 1)\bar{\Phi_p}(T) = T^p - 1 = (T - 1)^p$ implies that $\bar{\Phi_p}(T) = (T - 1)^{p-1}$. Consider the isomorphism $\mathbf{Z}[T] \longrightarrow \mathbf{Z}[T]$ defined by $T \longrightarrow T + 1$. Let Q be image of Φ_p. Then Φ_p irreducible if and only if Q is irreducible. But $\bar{Q}(T) = \bar{\Phi}_p(T + 1) = T^{p-1}$. Thus if $Q(T) = a_{p-1}T^{p-1} + \ldots + a_0$, p does not divide $a_{p-1}, p|a_{p-2}, \ldots, a_0$. But $a_0 = Q(0) = \Phi_p(1) = p$. Apply Prop 1. ☐

Adjoining Elements:

Let R be a ring. We want to add a new element s, subject to some relation $a_ns^n + \ldots + a_n = 0$ for $a_i \in R$. More precisely, we want a ring S, a morphism $R \longrightarrow S$, an element $s \in S$ satisfying the relation, such that (T, t) another such pair then there exists a unique morphism $S \longrightarrow T, s \longrightarrow t$.

Set $P \in R[T], P(T) = a_nT^n + \ldots + a_0, S = R[T]/(P)$, s = image of T in S. Note that $P(S) \in S$, if we think of $P \in (R[T])[T]$ (with "constant" coefficients), $P(T) = P$.

Definition 9.5. Let R be ring.

(i) An R-algebra is a pair $(S, \phi), S$ ring, $\phi : R \longrightarrow S$ morphism (rmk: ϕ usually suppressed, $\phi(r)s =$ "rs").

(ii) A morphism of R-alg $(S, \phi) \longrightarrow (T, \psi)$ is a ring morphism $f : S \longrightarrow T$ such that $f(\phi(r)s) = f(rs) = rf(s) = \psi(r)f(s)$.

Remark. ψ need not be injective.

Example. $R[T]$ is an R-algebra, R/I is an R-algebra, any ring is a $\mathbf{Z}$-algebra in a canonical way.

10. January 27, 2017

Definition 10.1.

(i) A *morphism of fields* is a morphism of rings whose source and target are fields
(ii) A *subfield* is a subring of a field that is a field

(iii) An *extension* of a field k is a field L containing k, denoted L/k.

Remark. If L/k is an extension, then L is a k-algebra, and in particular a k-vector space. An extension L/k is called *finite* if $\dim_k(L) < \infty$. In this case define the *degree* of L/k, denoted $[L : k] \stackrel{\text{def}}{=} \dim_k(L)$.[§]

Fact 10.2. *If k_1, k_2 are subgields of L, $k_1 \cap k_2$ is a subfield.*

Definition 10.3.

(i) Every field has a smallest field, called the *prime subfield*, equal to $\bigcap_{k \subset L} k^{\text{field}}$, the intersection of all subfields of L.
Example: The prime subfield of $\mathbb{R}$ is $\mathbb{Q}$. To see this, observe: any subfield of $\mathbb{R}$ must contain 1 and 0, thus sums of the form $1 + \cdots + 1$, so it must contain $\mathbb{N}$. Throwing in additive and then multiplicative inverses gives $\mathbb{Q}$.

(ii) Given an extension L/k and any subset $S \subset L$, let $k(S)$ be the smallest subfield of L containing k and S.

Propostion 10.4. *Let L be a ring and $k \subset L$ a subfield. If L is a domain and* $\dim_k(L) < \infty$ *then L is a field.*

Proof. Let $0 \neq a \in L$. The map $a\cdot \colon L \to L$ that sends x to ax is k-linear, and since L is a domain, injective: if $ax = 0$ then since $a \neq 0$, $x = 0$. By rank-nullity, the dimension of the image of $a\cdot$ must be equal to that of the target, i.e. $a\cdot$ is surjective. Thus there exists $G \in L$ so that $aG = 1$, implying that, as desired, L is a field. □

Definition 10.5. Let L/k be an extension, $L \supset E, F \supset k$ intermediate fields, each finite over k. The *composite of E and F* is

$$E \cdot F = \left\{ \sum_{i=1}^{n} e_i \cdot f_i \colon n \in \mathbb{N}, e_i \in E, f_i \in F \right\}.$$

Propostion 10.6. *EF is a field extension of k. It is finite and* $[EF : k] \leq [E : k] \cdot [F : k]$.

Proof. It is clear that EF is a subring of L containing k. Let $\{e_1, ..., e_n\}$ and $\{f_1, ..., f_m\}$ be, respectively, bases for E/k and F/k. Then the set $\{e_i \cdot f_j \colon i \in \{1, ..., n\}, j \in \{1, ..., m\}\}$ spans the k-vector space EF. Thus by elementary results, $\dim_k(EF) \leq \#\{e_i \cdot f_j\} = [E : k] \cdot [F : k]$. In particular, $[EF : k] < \infty$. Applying **Proposition 1.4** above, we have that EF is a field. □

Propostion 10.7. *Let L/k be a finite extension, V a finite dimensional L-vector space. Then V is finite dimensional as a k-vector space, with* $\dim_k(V) = \dim_L(V) \cdot [L : k]$.

Proof. Let $\{v_1, ..., v_n\}$ be a basis for V over L, $\{\ell_1, ..., \ell_m\}$ be a basis for L over k. We will show $\{\ell_i \cdot v_j \colon i \in \{1, ..., n\}, j \in \{1, ..., j\}\}$ is a basis for V over k:

(i) Spanning: given $x \in V$ we may write $x \in \lambda_1 v_1 + \cdots + \lambda_n v_n$ for $\lambda_i \in L$, with each $\lambda_i = \mu_{i,1}\ell_1 + \cdots + \mu_{i,m}\ell_m$. Then $x = \sum_i \sum_j \mu_{i,j}\ell_j v_i$ with the $\mu_{i,j} \in k$.

(ii) Linear independence: Write $\sum \mu_{i,j}\ell_j v_i = 0$. Then $0 = \sum_i \left(\sum_j \mu_{i,j}\ell_j\right) v_i$. By linear independence of the v_i we have $\sum_j \mu_{i,j}\ell_j = 0$, by linear independence of the ℓ_j we have $\mu_{i,j} = 0$ for all i, j.

□

Corollary 3. *If $M/L/k$ is a tower of finite ixtensions, then* $[M : k] = [M : L] \cdot [L : k]$.

[§]Debacker noted that the use of this notation, identical to the index of a subgroup, is because field extensions are in fact group-theoretic. When Galois groups are added to the notes, this will be discussed below.

Definition 10.8. Let L/k be an extension, and $a \in L$. If there is $0 \neq p \in k[T]$ such that $p(a) = 0$, then a is *algebraic over* k. Otherwise, a is *transcendental over* k.

As per the above definitions, we would like to study the following construction: let $\mathrm{ev}\colon k[T] \to L$, $p \mapsto p(a)$ be the evaluation morphism. If a is transcendental, ev is injective. Further, since L is a field, we have that ev factors uniquely through the fraction field $k(T)$[¶] and induces an isomorphism $k(T) \xrightarrow{\sim} k(a)$. If a is algebraic, let $0 \neq I \subset k[T]$ be the kernel of ev. Since $k[T]$ is a Euclidean domain, hence a PID (see a proposition from Jan. 20), so there exists a unique monic polynomial $p \in k[T]$ such that $(p) = I$.

Definition 10.9. p is called the *minimal polynomial* of a over k, a/k, written $M_{a/k}$. $deg(a/k) := \deg(M_{a/k})$ is its *degree*.

Remark. $M_{a/k}$ is also the minimal polynomial of the endomorphism (linear operator that is not necessarily an isomorphism) $a\cdot\colon L \to L$.

11. February 3, 2017

Definition 11.1. Let K be a field. An algebraic closure of K is an algebraic extension $\bar{K}/K$ such that $\bar{K}$ is alg. closed.

Lemma 11.2. *Let L/K be an extension of K that is algebraically closed and $\bar{K} \subset L$ be the subfield of all elements algebraic over K. Then $\bar{K}$ is algebraically closed.*

Proof. $P \in \bar{K}[T] - \bar{K}$. Let $a \in L$ such that $P(a) = 0$. Then a is algebraic over $\bar{K}, \bar{K}(a)$ is algebraic over $\bar{K}$. By Prop 1, Feb 1, $\bar{K}(a)$ is algebraic over k, hence a is algebraic over k. Thus $a \in \bar{K}$. ☐

Corollary 4. *Every field has an algebraic closure.*

Proof. Thm 4, Feb 1 and Lemma 2. ☐

Propostion 11.3. *Let K be a field, $G \subset K^\star$ is a finite subgroup. Then G is cyclic.*

Proof. Commutative G is a direct product of its Sylow subgroups. We will show that all these Sylow subgroups are isomorphic to $(\mathbb{Z}/p^n\mathbb{Z}, t)$ for some n and p. Then by the CRT we conclude that G is cyclic. WOLOG assume G has p-power order. That is, $|G| = p^n$. If G is not isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$, then there exists $m < n$ such that every element is killed by p^m. Then every element of G is a root of $T^{p^m} - 1$. But corollary 1, Jan 28, $T^{p^m} - 1$ has at most p^m distinct roots. Oops! This contradicts $|G| = p^n$. ☐

Finite Fields

Fact 11.4. *If F is a finite field, then its characteristic is $p > 0$, and $|F| = p^n$ for some integer n.*

Proof. Since F is finite, the canonical morphisms $\mathbb{Z} \longrightarrow F$ (Fact 0, Jan 4) cannot be injective. Hence the character of $F = p > 0$. The image of this morphism is $\mathbb{F}_p$. F is a vector space over $\mathbb{F}_p$, thus $|F| = p^n$ where n is the dimension of this vector space. ☐

Propostion 11.5. *If P is a prime, $n \in \mathbb{N}$, then there exists a finite field with p^n elements.*

Proof. Let $\bar{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$ (corollary 3). Consider the map $\sigma : \mathbb{F}_p \longrightarrow \bar{\mathbb{F}}_p$ defined by $x \longrightarrow x^{p^n}$. By hwk this is a ring homomorphism. Let $F \subset \bar{\mathbb{F}}_p$ be the subfield of elements fixed by σ. The elements of F are precisely the roots of $T^{p^n} - T$. In $\bar{\mathbb{F}}_p$, this polynomial has p^n many roots, counted with multiplicity. In order to have multiplicity 1, we need to check that the derivation of $P(T) = T^{p^n} - 1$ is nonzero on these roots. $P'(T) = p^n T^{p^n - 1} - 1 = -1 \neq 0$ in $\bar{\mathbb{F}}_p$ which implies that all zeros have multiplicity 1, hence $|F| = p^n$. ☐

[¶] This notation was established on homework: $k(T)$ is the set of rational functions with coefficients in k.

Propostion 11.6. *Let F_1, F_2 be finite fields of the same size. Then there exists an isomorphism from F_1 to F_2.*

Proof. Any $a \in F_n$ is algebraic over $\mathbb{F}_p$ and if $M_a \in \mathbb{F}_p(T)$, then $\mathbb{F}_p(a)$ is isomorphic to $\mathbb{F}_p[T]/(M_a)$.We have $[\mathbb{F}_p(a) : \mathbb{F}_p] = \deg(M_a)$ by prop 1, Jan 27. On the other hand, $|F_1^{\times}| = p^n - 1 \longrightarrow a^{p^n} = a$ for all $a \in F_1$ which implies that F_1 consists of roots of $P(T) = T^{p^n} - T$ and $P(T)$ has precisely p^n roots, F_1 consists precisely of the zero's of $P(T)$. In particular $P(T)$ factors into linear factors over F_1. Thus the M_a $(a \in F_i)$ are precisely the irreducible factors of $T^{p^n} - T = P(T)$. Now $F_1 = \mathbb{F}_p(a) \iff |F_1| = p^n = |\mathbb{F}_p(a)| \iff n = \deg M_a$ in which case f_1 is isomorphic to $\mathbb{F}_p[T]/(M_a)$. By prop 4 we know that such an a exists. Thus F_1 is isomorphic to $\mathbb{F}_p[T]/(Q)$ where Q is any irreducible factor of $P(T)$ of deg n. Since the right hand side is independent of F_1 (just depends on $|F_1|$) we have F_1 is isomorphic to F_2. $\square$

Corollary 5. *Let F_1, F_2 be finite fields. Then we can imbed F_1 into F_2 if and only if $|F_1| = p^k$ and $|F_2| = p^n$ with $k|n$. By proposition 6 and 7, F_1 is isomorphic to $\bar{\mathbb{F}_p}^{\sigma_1}$ and F_2 is isomorphic to $\bar{\mathbb{F}_p}^{\sigma_2}$, and $\sigma_1(x) = x^{p^k}$ and $\sigma_2(x) = x^{p^n}$ if $k|n$ then $F_1 \subset F_2$. If F_1 imbeds into F_2 then F_2 is a vector space over $F!$ and hence $|F_2|$ is a power of $|F_1|$ and so $k|n$.*